Information Security

DECAP194

Edited by
Ajay Kumar Bansal

LOVELY
PROFESSIONAL
UNIVERSITY

LOVELY
PROFESSIONAL
UNIVERSITY

Information Security

Edited By:
Ajay Kumar Bansal

CONTENT

Unit 01: Introduction to Information Systems

CONTENTS

Objectives

- Understand meaning and importance of information systems
- Acquire the knowledge about OSI Security Architecture.
- Explain the concept of information system security & threats
- Learn about Security Design Principles

Introduction

Information System is a particular discipline or branch of learning that is concerned with the application of information to organizational needs. The scope of information system includes manual, computer-based and other forms of automated procedures and applications of information technology generally.

In order for organizations to use information technologies effectively, information systems must be designed, developed, implemented and managed in ways that fit with the specific work processes and organizational contexts. A thorough understanding of information systems development and management concepts together with skills in desktop computing enables the manager to develop end user systems and provide the business perspective to participate in the creation and management of major information systems. Management Information System (MIS) concepts also provide a foundation on which to base expertise in information systems for specialized work processes such as marketing, accounting and international business.

1.1 Basic of Information Systems

Information system (IS) refers to a collection of multiple pieces of equipment involved in the collection, processing, storage, and dissemination of information.

Hardware, software, computer system connections and information, information system users, and the system's housing are all part of an IS. Personal computers, smartphones, databases, and networks are just some examples of information systems.

Enterprises and corporations use information systems to interact with their suppliers and customer base, perform their operations, manage their organization, and carry out their marketing campaigns.

They can be used for a broad variety of purposes, from managing supply chains to interacting with digital marketplaces. Individuals also rely on ISs to interact with peers and friends through social networks, carrying out everyday activities such as banking and shopping, or simply looking for knowledge and information. Some basic terms used for Information Systems are mentioned below:

- **Data:** Raw facts such as an employee's name and number of hours worked in a week, inventory part numbers or sales orders.
- **Information**: It is the set of data that has been organized for direct utilization of mankind, as information helps human beings in their decision-making process.

Examples are Timetable, Merit List, Report card, Headed tables, printed documents, pay slips, receipts, reports etc.

Information system (IS) is a set of interrelated elements that :

- Collect (input)
- Manipulate (process)
- Store
- Distribute (output) data and information
- Provide a corrective reaction (feedback mechanism) to meet an objective

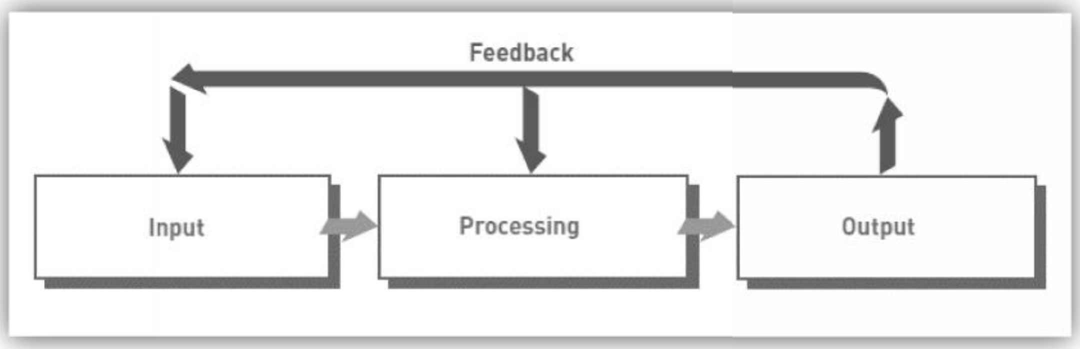


Figure 1 Structure of Information System

Meaning of Information System

An **information system** is defined as the software that helps organize and analyze data. So, the purpose of an **information system** is to turn raw data into useful **information** that can be used for decision making in an organization. IS accepts the data from the environment and manipulate the data to produce the information that is used to solve problems.In early days, majority of the systems were manual. These days information systems are mostly the computerized.

Computer-based Information System

An Information System is an organized combination of people, hardware, software, communication networks and the data resources that collects, transforms, and disseminates information in an organization.

Components of Information System are:

An Information system is a combination of hardware and software and telecommunication networks that people build to collect, create and distribute useful data, typically in an organization. It defines the flow of information within the system. The objective of an information system is to provide appropriate information to the user, to gather the data, process the data and communicate information to the user of the system.

- Hardware
- Software
- Database
- Network
- Human Resources

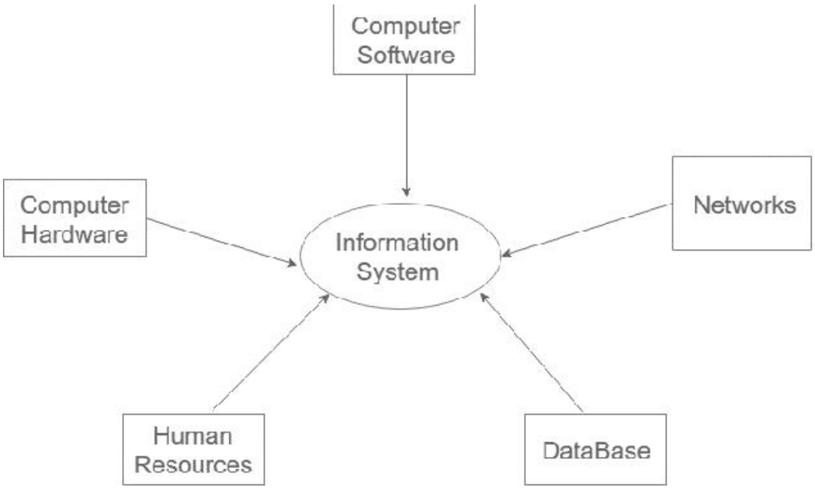


Figure 2 Components of Information Systems

1. Computer Hardware:

Physical equipment used for input, output and processing. The hardware structure depends upon the type and size of the organization. It consists of an input and an output device, operating system, processor, and media devices. This also includes computer peripheral devices.

2. Computer Software:

The programs/ application program used to control and coordinate the hardware components. It is used for analyzing and processing of the data. These programs include a set of instruction used for processing information.

Software is further classified into 3 types:

System Software

Application Software

Procedures

3. Databases:

Data are the raw facts and figures that are unorganized that are and later processed to generate information. Software's are used for organizing and serving data to the user, managing physical storage of media and virtual resources. As the hardware can't work without software the same as software needs data for processing. Data are managed using Database management system.

Database software is used for efficient access for required data, and to manage knowledge bases.

4. Network:

Networks resources refer to the telecommunication networks like the intranet, extranet and the internet.

These resources facilitate the flow of information in the organization.

Networks consists of both the physicals devises such as networks cards, routers, hubs and cables and software such as operating systems, web servers, data servers and application servers.

Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by software.

Networks include communication media, and Network Support.

5. Human Resources:

It is associated with the manpower required to run and manage the system. People are the end user of the information system, end-user use information produced for their own purpose, the main purpose of the information system is to benefit the end user. The end user can be accountants, engineers, salespersons, customers, clerks, or managers etc. People are also responsible to develop and operate information systems. They include systems analysts, computer operators, programmers, and other clerical IS personnel, and managerial techniques.

1.2 Importance of Information System

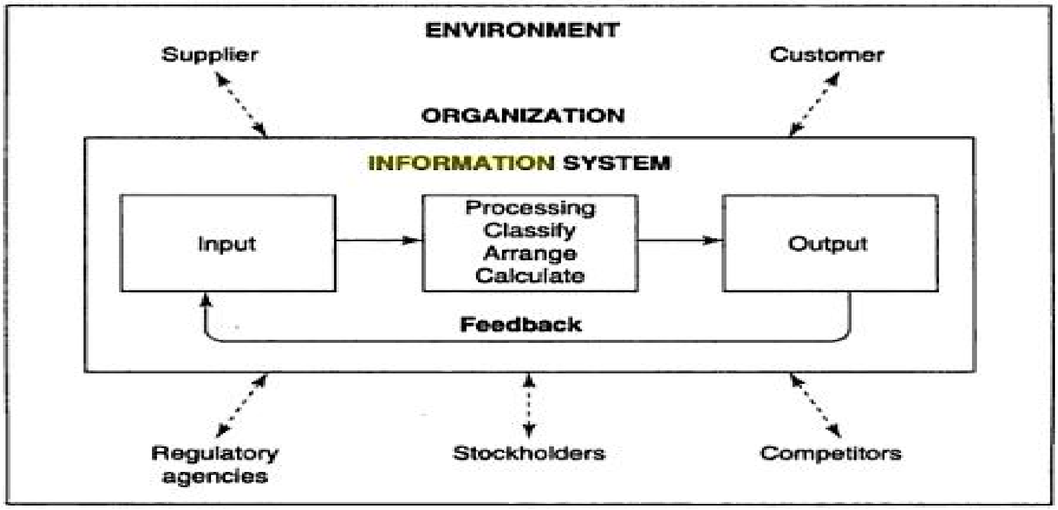
Information system is the study of information production, flows and use within organizations.Information system makes extensive use of information technology means. But it is very important to appreciate that its scope encompasses systems in their entirety, including manualactivities, the interface between manual and automated components of systems, design aspectsof IT means, and economic, legal, organizational, behavioral, and social aspects of systems.Information systems overlap with both the computer science and business managementdisciplines.

The information system of an organization may be defined as a system that serves to provide information within the organization when and where it is needed at any managerial level. An information system is a set of people, procedures and resources that interact to satisfy the information processing needs of an organization. During the processing, the data is collected, stored, transformed and distributed in an organization. Such a system must take the information received and store, retrieve, transform, process, and communicate it using the computer system or some other means. It is not necessary that an information system cannot function in the absence of computers. An information system is a logically interrelated set of business processes that accomplish organizational goals. Management Information System is mainly dependent upon information, which is a vital ingredient of any Management Information System. Information is the most critical resource of Management Information System. We all know that information is a vital factor for our existence. Just as our body needs air, water and clothes, we are as much dependent upon information. To make life more interesting and to achieve the feeling of being a part of the social system, we want to know our surroundings and for that we need information. Information is an important input for achieving our goals such as learning to help each other and to become integral part of society.

Information system is not a new concept; it is as old as the hills. From biblical times, humans have been making the use of information generated through information systems in all times. There have been systems that generated and communicated information. Kings and rulers had their own ways of designing information systems to retrieve information. The main objective of these information systems was to ascertain the wellbeing of their people in the kingdom and to manage the kingdom effectively and efficiently. The church had its own information system. In India, Tainali Rama, Akbar and many others had impressive management information systems in operation. Similarly, the merchants of Venice had their own fully functional appropriate management information system in place.

Most of us think only of hardware and software when we think of an Information System. There is another component of the triangle that should be considered, and that's the people side, or "liveware."

We talk about the input, processing, output, and feedback processes. Most important is the feedback process; unfortunately, it's the one most often overlooked. Just as we discussed above, the hardware (input and output) and the software (processing) receive the most attention. With those two alone, you have computer literacy. But if you don't use the "liveware" side of the triangle to complete the feedback loop, you don't accomplish much. Add the "liveware" angle with good feedback and then you have the beginnings of information literacy. An information system differs from other kinds of systems in that its objective is to monitor/ document the operations of some other system, which we can call a target system. An information system cannot exist without such a target system.



1.3 Types of Information System

Information Systems
Support Systems (ESS)
Systems (MIS)
Support Systems (DSS)
Transaction Processing Systems (TPS)
Office Automation Systems (OAS)
Knowledge Work Systems (KWS)

1. Transaction Processing Systems: Transaction processing systems today generally work in on-line mode by immediately processing a firm's business transactions. A Transaction is an elementary activity conducted during business operations.TPS may work either in batch mode, processing accumulated transactions at a single time later, or in on-line mode, processing incoming transactions immediately. Today, most TPS work in the on-line mode.

A transaction encompasses all of the purchases and sales of products and services, along with any daily business transactions or activities required to operate a company.

It handles all the customer and employee transaction data so an organization can streamline workflows and easily retrieve the required information.

2. Office Automation Systems: The main objective of OIS is to facilitate communication between the members of an organization and between the organization and its environment. OIS are used to:

- Help manage documents represented in an electronic format
- Handle messages, such as electronic mail, facsimile, and voice mail
- Facilitate teleconferencing and electronic meetings
- Facilitate the use of the Internet for communication and access to information
- Facilitate the use of task-oriented teams using groupware

3. Knowledge Management Systems: A knowledge management system can be defined in many ways. For some, it’s a teaching and learning platform. For many others, it’s a platform for solving problems efficiently. Simply put, a knowledge management system is the platform or the tool you use for sharing knowledge

For example, with a knowledge management system, you can create articles, documents, and guides. You can then make them available to your customers or employees to let them find solutions to common issues related to your product.

Whether it’s to educate your customers on how to use a product. Or teach your employees how to handle different situations. We can all agree that a knowledge base can be beneficial for all types of businesses in many ways.

4. Management Information Systems: Management Information Systems (MIS) is the study of people, technology, organizations, and the relationships among them. MIS professionals help firms realize maximum benefit from investment in personnel, equipment, and business processes. MIS is a people-oriented field with an emphasis on service through technology. If you have an interest in technology and have the desire to use technology to improve people’s lives, a degree in MIS may be for you.

5. Decision Support Systems: Decision support systems directly support a decision-making session. These systems facilitate a dialog between the user, who is considering alternative problem solutions, and the system that provides built-in models and access to databases. The DSS databases are often extracts from the general databases of the enterprise or from external databases.It stores and gathers the information required for management to take the proper actions at the correct time. For example, a bank manager can use a DSS to assess the evolving loan trends to determine which yearly loan targets to meet

6. Executive Support System: It manages all the required information needed for enterprise leaders to monitor the competition, track internal performance, and pinpoint growth opportunities.

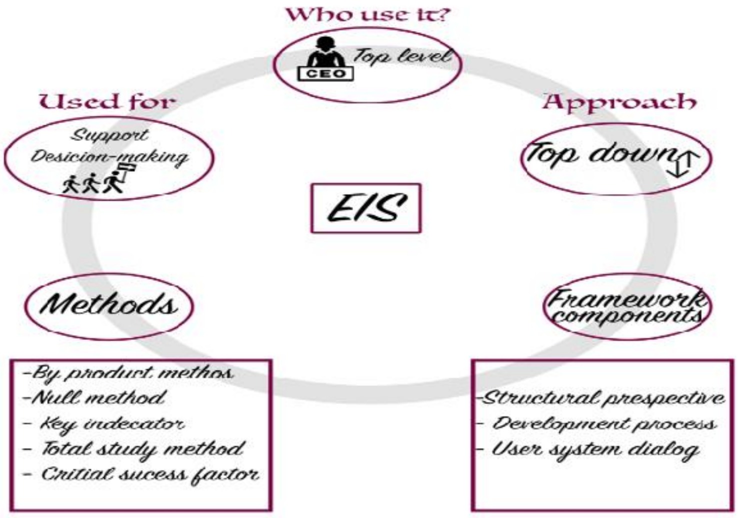


Figure 3 Executive Support System

1.4 Security

We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs.

Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements)

Computer Security

Computer security, also called cybersecurity, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment—namely, serial numbers, doors and locks, and alarms. The protection of information and system access, on the other hand, is achieved through other tactics, some of them quite complex.

The security precautions related to computer information and access address four major threats: (1) theft of data, such as that of military secrets from government computers; (2) vandalism, including the destruction of data by a computer virus; (3) fraud, such as employees at a bank channeling funds into their own accounts; and (4) invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database. The most basic means of protecting a computer system against theft, vandalism, invasion of privacy, and other irresponsible behaviors is to electronically track and record the access to, and activities of, the various users of a computer system. This is commonly done by assigning an individual password to each person who has access to a system. The computer system itself can then automatically track the use of these passwords, recording such data as which files were accessed under particular passwords and so on. Another security measure is to store a system's data on a separate device or medium that is normally inaccessible through the computer system. Finally, data is often encrypted so that it can be deciphered only by holders of a singular encryption key. (See data encryption.)

Computer security has become increasingly important since the late 1960s, when modems (devices that allow computers to communicate over telephone lines) were introduced. The proliferation of personal computers in the 1980s compounded the problem because they enabled hackers (irresponsible computerphiles) to illegally access major computer systems from the privacy of their homes. With the tremendous growth of the Internet in the late 20th and early 21st centuries, computer security became a widespread concern. The development of advanced security techniques aims to diminish such threats, though concurrent refinements in the methods of computer crime pose ongoing hazards.

It processes of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether someone attempted to break into your system, if they were successful, and what they may have done

Three key objectives of security

Security of computer networks and systems is almost always discussed within information security that has three fundamental objectives, namely confidentiality, integrity, and availability.

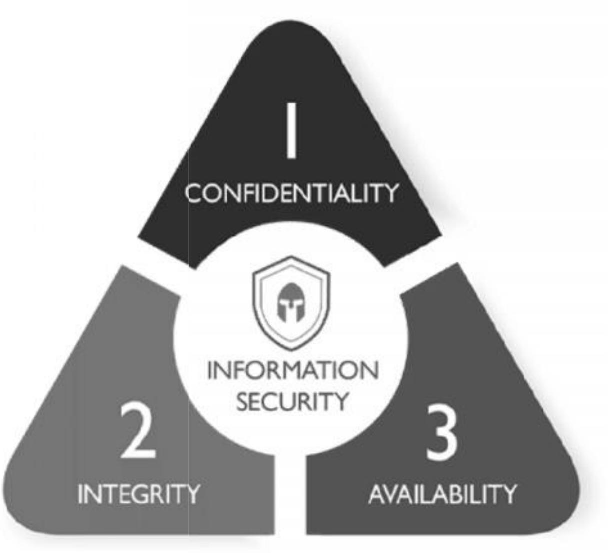


Figure 4 CIA triads

Confidentiality:

The first objective of security is confidentiality: keeping information away from people who should not have it. Accomplishing this objective requires that we know what data we are protecting and who should have access to it. It requires that we provide protection mechanisms for the data while it is stored in the computer and while it is being transferred over networks between computers. We will need to know the application programs that we use (or could use) to manipulate the data and control the use of those applications. Luckily, the Chief Security Officer (CSO) and the IT team will handle the mechanics of doing all this—just as soon as we tell them how to figure out who should have access to which data,

In the internet world confidentiality has taken on an expanded meaning in the form of privacy controls. For some industries, such as health care and finance, privacy is now a regulatory issue. The U.S., European, Canadian, and Australian governments (with others following) have legislated privacy controls to varying degrees. Even U.S. companies in other industries are now governed by privacy legislation of other countries if they have employees or customers in any of those other geographies. We will cover the legal requirements for security in much more detail in a later chapter. In addition, public demand for privacy has forced many companies to formulate clear privacy policies to prevent their customers from going to competitors.

There are numerous technologies available to provide confidentiality for computer applications, systems, and networks. They will be described with their strengths, costs, and weaknesses in later chapters of this book. plications and how far to go in providing confidentiality.

Notes: Confidentiality mechanisms keep information from being read by unauthorized people.

Integrity

The second objective of security is integrity: assuring that the information stored in the computer is never contaminated or changed in a way that is not appropriate. Both confidentiality and availability contribute to integrity. Keeping data away from those who should not have it and making sure that those who should have it can get it are basic ways to maintain the integrity of the data.

But many security failures happen despite reasonably strong controls on who has access. Sometimes, the people we trust are not trustworthy. Sometimes, we need to extend levels of trust to people about whom we know little or nothing, such as temporary workers, third-party business partners, or consultants. Integrity constraints must go beyond the simple "who" definitions and handle the "what" conditions. Once someone has been granted access, what operations can they perform on our computers? This leads to requirements for detailed constraints on different types of access within the computer system and, thus, to much of the complexity of a modern business computer system. If a typical end user can change the behavior of the operating system or network, anyone inside our company can stop business from being processed—intentionally or not.

The need for data integrity connects computer security to a closely related discipline: business continuity planning and data recovery. Data will eventually be damaged by hardware failure, software failure, human errors, or security failures. Recovery processes are a necessary part of any business IT plan and frequently are under the control of a security department.

Availability

The third objective of security is availability: ensuring that data stored in the computer can be accessed by the people who should access it. Availability is a broad subject addressing things such as fault tolerance to protect against denial of service and access control to ensure that data is available to those authorized to access it. Most computers can at least differentiate between two classes of users: system administrators and general end users. The major exceptions to this rule are the desktop operating systems that have become common on personal computers.

If you read, you'll find references in most IT publications describing Microsoft Windows 95/98, in all its versions, as being insecure. One of the reasons for this is that the operating system has no ability to discriminate between system administrators and general end users. Many other desktop operating systems have this same shortcoming. Anyone who uses one of these computers can change its security environment and can, in fact, turn security off. A few users in an enterprise deciding to turn off security can open the network to attack in some cases. Of course, these operating systems also have many other security weaknesses, even when security is turned on.

1.5 OSI Security Architecture

To effectively assess the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture was developed in the context of the OSI protocol architecture, which is described in Appendix H. However, for our purposes in this chapter, an understanding of the OSI protocol architecture is not required.

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

1.6 Security Attacks

Security attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data. Security Attacks can be categorized in to 2 types:

- Active Attack
- Passive Attack

Active Attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

Masquerade:Masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks.

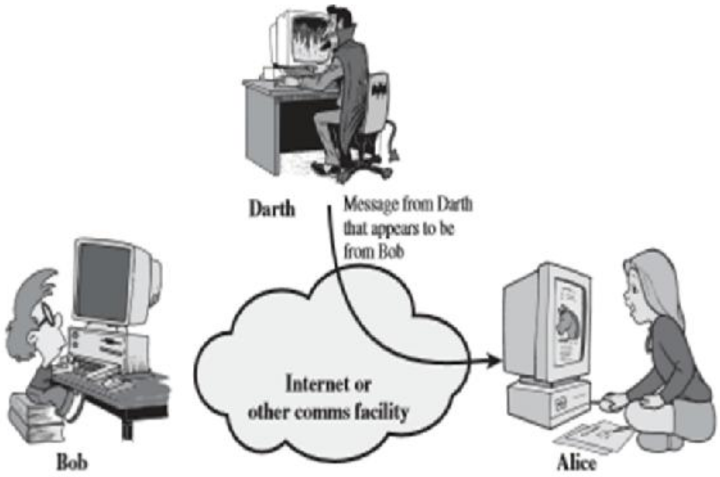
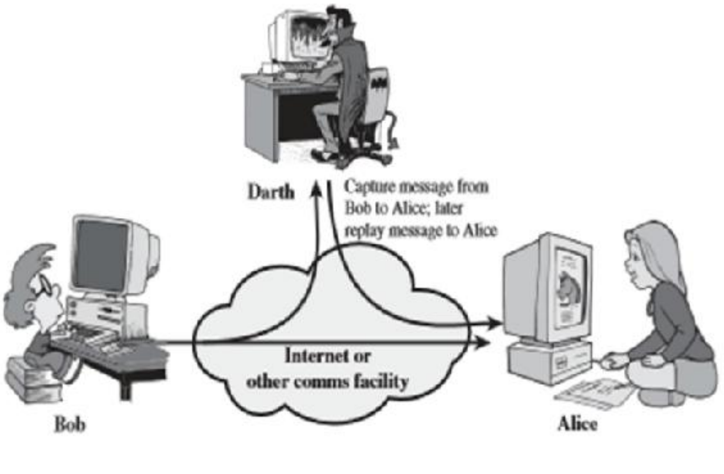

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Figure 5 Masquerade Attack

Replay: involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Modification of messages:Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect**.**

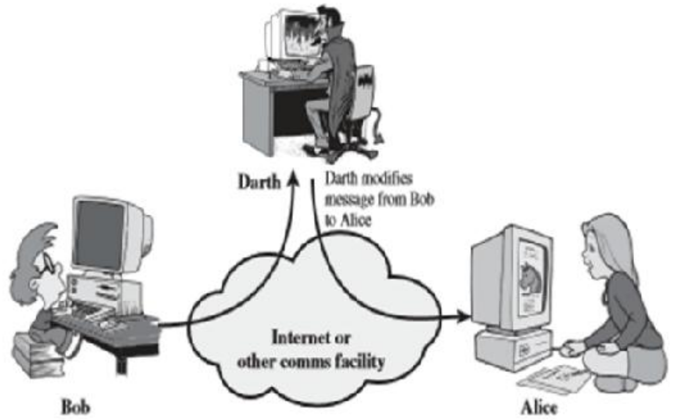

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Figure 6 Modification of messages

Denial Of Service:

It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.

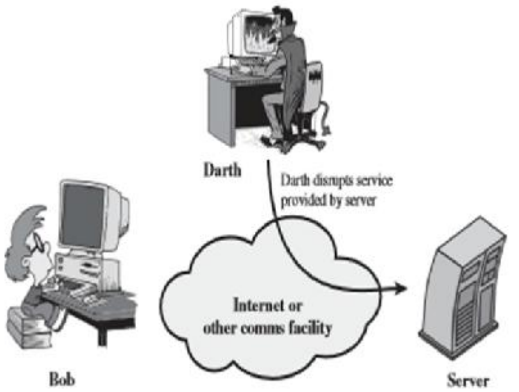

Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

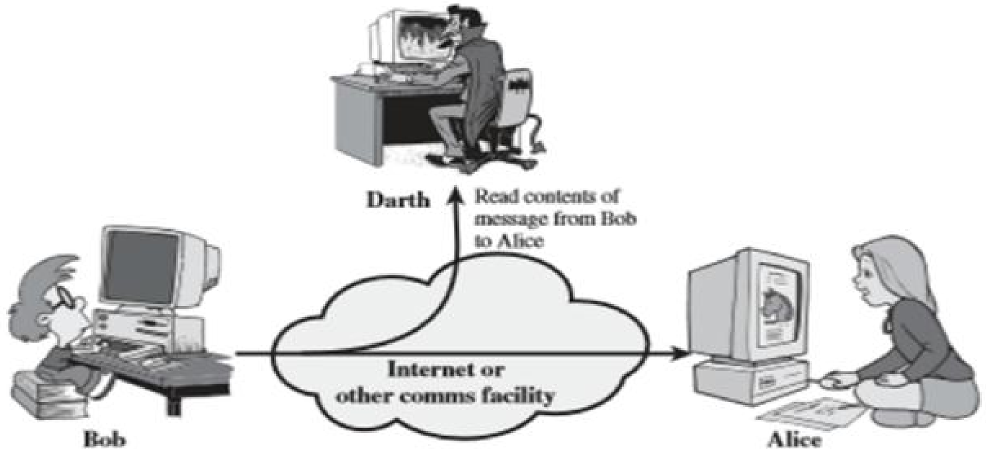
Figure 7 Dos Attack

1.7 Passive Attack

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as following:

Release of message contents

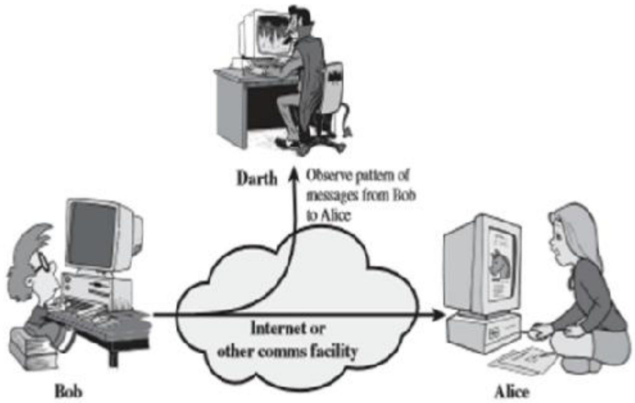
For a release of message content, a telephonic conversation, an E-mail message or a transferred file may contain confidential data. A passive attack monitors the contents of the transmitted data.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

Traffic analysis:

During a traffic analysis attack, the eavesdropper analyzes the traffic, determines the location, identifies communicating hosts and observes the frequency and length of exchanged messages.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

1.8 Security Services

A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service. A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

Example: printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

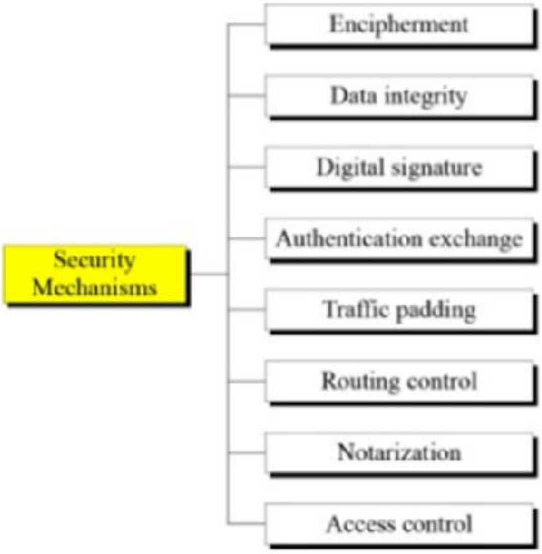
Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

1.9 Security Mechanisms

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are:



Encipherment:

Encipherment is hiding or covering data and can provide confidentiality. It makes use of mathematical algorithms to transform data into a form that is not readily intelligible.

Digital Signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

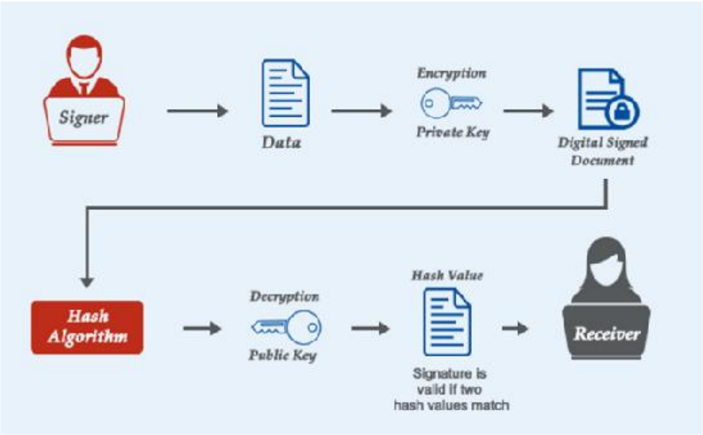


Figure 8 Digital Signature

Access Control:

A variety of mechanisms are used to enforce access rights to resources/data owned by a system, for example, PINS, and passwords.

Data Integrity:

It refers to the accuracy and consistency of data. A good database will enforce data integrity whenever possible.For example, a user could accidentally try to enter a phone number into a date field. If the system enforces data integrity, it will prevent the user from making these mistakes.

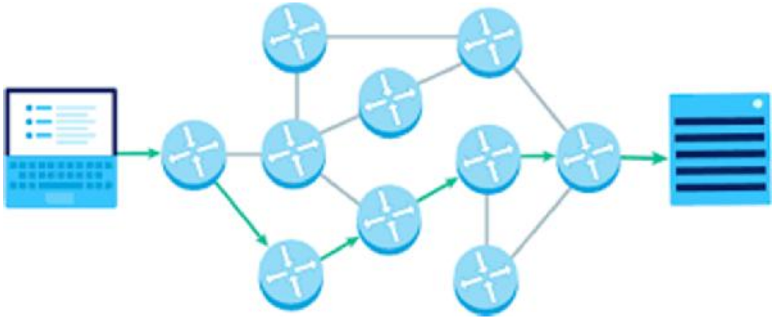
Authentication exchange:

Authentication techniques require that you prove your identity or a program proves its authentication. This can be done by using any one or more of the following:

- A password or character sequence known only to you or the program
- A key card or other physical authorization unique to you
- Your fingerprints, signature, or other item that identifies only you

1.10 Routing control

It enables selection of particular physically secure routes for certain data and allows routing changes which means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from traffic analysis on a particular route.



1.11 A model of Security

A security model is a computer model which is used to identify and impose security policies. It does not require any prior formation it may be founded on the access right model or distributing computing model or computation mode. A security model is a framework in which a security policy is developed. The development of this security policy is geared to a particular setting or instance of a policy, for example, a security policy based upon authentication, but built within the confines of a security model. For example, designing a security model based upon authentication and authorization, one would consider the 4-factor model of security, that is, authentication, authorization, availability, and authenticity. It rigorously defines a security policy. Generally, a security model is a "formal system" used to specify and reason on the security policy (i.e., it is used as a basis for formal specification proofs). It is thus intended to abstract the security policy and handle its complexity; represent the secure states of a system as well as the way in which the system may evolve, verify the consistency of the security policy, detect and resolve possible conflicts.

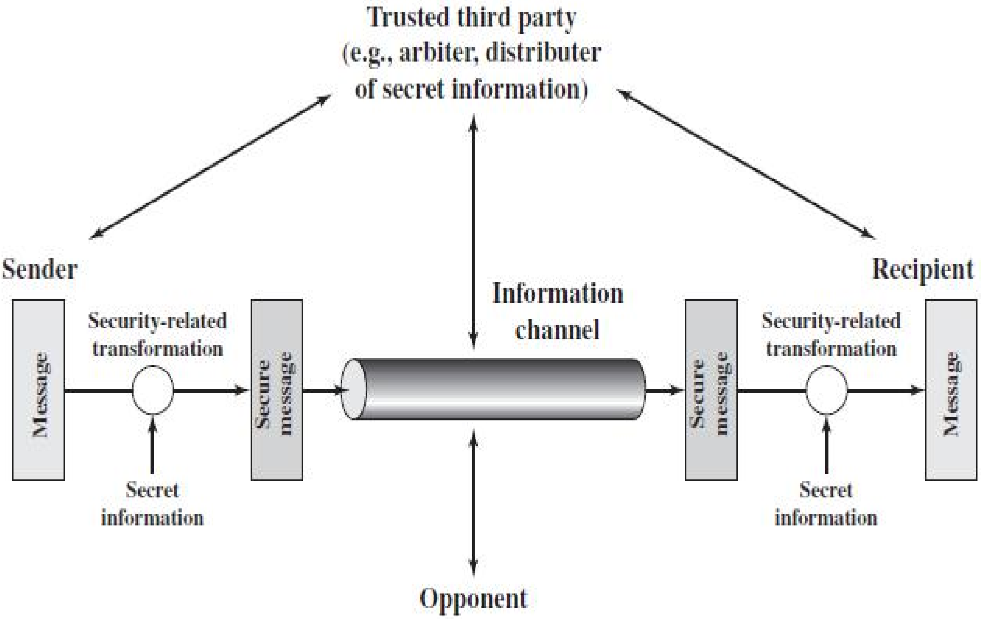


Figure 9 model of security

It includes 4 major tasks:

- Design an algorithm for performing the security-related transformation.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principals that makes use of the security

Summary

- A system is defined as an organized collection of people, machines, procedures, documents, data or any other entities such that they interact with each other as well as with the environment to reach a predefined goal.
- Information system is the study of information production, flows and use within organizations. Information system makes extensive use of information technology means.
- The information system of an organization may be defined as a system that serves to provide information within the organization when and where it is needed at any managerial level.
- An information system is a logically interrelated set of business processes that accomplish organizational goals.
- Telecommunication systems are considered as global. When developing infrastructures, the focus on closed, stand-alone systems has to be replaced by one focusing on the infrastructures as open and global as is the case for development of telecommunication technologies.
- The function of the World Wide Web is offered and assured by the web-hosting organizations. These organizations are the groups of people, who have rooms, full of prevailing computers, named host servers.
- Security information management is a type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusiondetection systems and anti-virus software.
- A Security Information Management, to a great extent, adds value with its capability of finding patterns in network traffic.
- Security Information Managements (SIM) is by its very nature a heterogeneous product, and thus SIM rollouts involve complex technical integration and political negotiations.

Keywords

Information System: An information system is a logically interrelated set of business processes that accomplish organizational goals.

Security Information Management: It is a type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusion-detection systems and anti-virus software.

System: A system is defined as an organized collection of people, machines, procedures, documents, data or any other entities such that they interact with each other as well as with the environment to reach a predefined goal

Self Assessment

1. _______the set of data that has been organized for direct utilization of mankind.

A. Information
B. System
C. Vulnerability
D. Threat

2. Which among these is not the element of Information Security:

A. Collects
B. Manipulates

C. Provides

D. Supplier

3. __________ is the processing system which handles all the customer and employee transaction data so an organization.

A. Office Automation Systems

B. Decision Support Systems

C. Transaction Processing Systems

D. Executive Support System

4. printing documents, mailing paperwork are examples of which types of Information System?

A. Management Information Systems

B. Decision Support Systems

C. Executive Support System

D. Office Automation Systems

5. _______ stores and gathers the information required for management to take the proper actions at the correct time

A. Office Automation Systems

B. Decision Support Systems

C. Executive Support System

D. Knowledge Management Systems

6. _______ manages all the required information needed for enterprise leaders to monitor the growth opportunities.

A. Knowledge Management Systems

B. Transaction Processing Systems

C. Executive Support System

D. Decision Support Systems

7. According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

A. Confidentiality

B. Integrity

C. Authenticity

D. Availability

8. Which of the following security attacks is not an active attack?

A. Masquerade

B. Modification of message

C. Denial of service

D. Traffic analysis

9. Which of the following attacks is a passive attack?

A. Masquerade

B. Modification of message

C. Traffic analysis

D. Replay

10 In this attack one entity pretends to be a different entity?

A. Replay

B. Masquerade

C. Modification of message

D. Denial of service

11. ___________means that a sender must not be able to deny sending a message that it sent.

A. Data Integrity

B. Non- Repudiation

C. Access of Control

D. Data Confidentiality

12. A process that is designed to detect, prevent or recover from security attack is called ________

A. Security Mechanism

B. Security Service

C. Digital Signature

D. Authentication Exchange

13. Encipherment, Digital Signature, Traffic Padding Routing Control are examples of ____

A. Security Service

B. Digital Signature

C. Security Mechanism

D. Access Control

Answers for Self Assessment

1.	A	2.	D	3.	C	4.	D	5.	B
6.	C	7.	C	8.	D	8.	C	10.	B
11.	C	12.	A	13.	C				

Review Questions

1. Explain The OSI security Architecture
2. Explain the types of attack.
3. Define Digital Signature
4. What is information system? Also explain the importance of information system.

Further Reading

https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf

Web Links

https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

Unit 02: Security Design Principles

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand about fundamental of Security Design principles
- Learn about different Standards of Security
- Acquire knowledge about Attack surfaces and attack trees.

Introduction

The security design principles are considered while designing any security mechanism for a system. These principles are review to develop a secure system which prevents the security flaws and also prevents unwanted access to the system.

Fundamental Security Design Principles

Below is the list of fundamental security design principles provided by the National Centers of Academic Excellence in Information Assurance/Cyber Defense, along with the U.S. National Security Agency and the U.S. Department of Homeland SecuritY.

2.1 Fundamental Security Design Principles

- **Economy of Mechanism**: **Economy of Mechanism:**

This fundamental security principle defines that the security measures implemented in the software and the hardware must be simple and small. This would ease the testers to test the security measures thoroughly. If the designed security mechanism is complex then it is likely that the tester would get a chance to exploit the weakness in the design.

So more the design is simple less are the opportunities for the tester to discover the flaws and more the complex is the design more are the chances to exploit flaws in the design. When the security design is simple, it easy to update or modify the design. But when it comes to practice, we cannot consider the economy of a mechanism as the best security design principle. Because there is a continuous demand for adding the security features in both hardware, as well as software.

Adding security features constantly makes the security design complex. What we can do to obey this principle while designing security mechanism is to eliminate the less important complex feature.

- **Fail-safe Defaults:**

This principle says that if any user wants access to any mechanism then whether the access is permitted or denied should be based on authorization rather than elimination.

By default, all the mechanism should have a lack of access and the function of a security mechanism is to identify the condition where the access to the security mechanism should be permitted. This means by default access to all mechanism should be denied, unless any privilege attribute is provided.This principle denies unauthorized access. If there occurs any mistake while designing the security mechanism which grants access based on permission or authorization. That mechanism fails by simply denying access, which is the safest condition.

If there is any mistake while designing the security mechanism which grants access based on exclusion. That mechanism fails by simply granting access which cannot be considered as the safest situation.

- **Complete Mediation:**

Some systems are designed to operate continuously such systems remember access decision. So, there must be an access control mechanism which would check every access occurring on the system.

This principle says that the system should not trust the access decisions it recovers from the system cache. This particular security design principle says that there must be a mechanism in the system that checks each access through the access control mechanism. However, this is an exhaustive approach and is rarely considered while designing a security mechanism.

- **Open Design:**

This security principle suggests that the security mechanism design should be open to the public. Like in the cryptographic algorithm, the encryption key is kept secret while the encryption algorithm is opened for a public investigation.This principle is followed by the NIST (National Institute of Standards and Technology) to standardize the algorithms because it helps in worldwide adoption of NIST approved algorithms.

- **Separation of Privilege:**

This security principle states that whenever a user tries to gain access to a system, the access should not be granted based on a single attribute or condition.Instead, there must be multiple situations or conditions or attribute which should be verified to grant access to the system. We also term this as a multifactor user authentication as this principle says that multiple techniques must be implemented to authenticate a user.

For example, while conducting online money transfer we require user-id, password, transaction password along with OTP.

- **Least Privilege:**

The least privilege security design principle states that each user should be able to access the system with the least privilege. Only those limited privileges should be assigned to the user which are essential to perform the desired task.An example of considering and implementing this principle is role-based access control. The role-based designed security mechanism should discover and describe various roles of the users or processes.

Now, the least set of privileges should be assigned to each role which is essential to perform its functions. So, the access control mechanism enables each role only those privileges for which it is authorized. The least set of privileges assigned to each role describes the resources available each role can access.In this way, unauthentic roles are unable to access the protected resources. Like, the user's accessing database has privilege only to retrieve the data they are not authorized to modify the data.

- **Psychological Acceptability:**

This security design principle says that the security mechanisms design to protect the system should not interfere with the working of the user every now and then.As this would irritate the user ad user may disable this security mechanism on the system. Therefore, it is suggested that the security mechanism should introduce minimum hurdles to the user of the system.

The security mechanism should not be designed such that it becomes difficult for the user to access the resources in the system.

- **Isolation:**

This security design principle is considered in three circumstances. The first condition, the system that has critical data, processes or resources must be isolated such that it restricts public access. It can be done in two ways.

The system with critical resources can be isolated in two ways physical and logical isolation. The physical isolation is one where the system with critical information is isolated from the system with public access information.

In logical isolation, the security services layers are established between the public system and the critical systems. The second isolation condition is that the files or data of one user must be kept isolated with the files or data of another user. Nowadays the new operating system has this functionality. Each user operating the system have an isolated memory space, process space, file space along with the mechanism to prevent unwanted access. And the third isolation condition is where the security mechanism must be isolated from such that they are prevented from unwanted access

- **Encapsulation:**

This security design principle is a form of isolation which is designed on the principle of object-oriented principles. Here the processes of the protected system can only access the data object of the system and these processes can only be invoked from a domain entry point.

- **Least Astonishment:**

This security design principle states that the user interface of the system must not amaze the user while accessing the secure system. He should be able to understand how the security mechanism is essential to protect the system.So, this is all about the security design principles which should be considered while designing the security mechanism for a system.

2.2 Attack Surfaces- What is an Attack Surface?

An attack surface is defined as the total number of all possible entry points for unauthorized access into any system. It includes all vulnerabilities and endpoints that can be exploited to carry out a security attack. The attack surface is also the entire area of an organization or system that is susceptible to hacking.For most modern businesses, the attack surface is complex and massive. The large number of devices, web applications and network nodes create many potential cybersecurity threats.IT leaders, despite their best efforts, can only see a subset of the security risks faced by their organization.

Different types of attack surface

There are three main types of attack surfaces:

- Digital attack surface
- Physical attack surface
- Social engineering attack surface

Anything that houses or has access to sensitive data, business data, personally identifiable information (PII), or protected health information (PHI) should be particularly well examined.

Digital Attack surface:

Your digital attack surface is everything that lives outside of the firewall that is accessible through the Internet. It's often easier for cybercriminals to break into your organization by exploiting poor cybersecurity than it is through physical means.

Your digital attack surface includes:

Known assets: Inventoried and managed assets such as your corporate website, servers, and the dependencies that run on them.

Unknown assets: Also known as shadow IT or orphaned IT that was stood up outside the purview of your security team such as forgotten websites, marketing sites, and employee installed software.

Rogue assets: Malicious infrastructure spun up by threat actors such as malware, a typo squatted domain, or a website or mobile app that is impersonating your organization.

Physical Attack Surface:

Beyond your digital attack surface, there are additional risks that occur when an attacker gets physical access to your office or a device. For one, if they have physical access it doesn't matter whether the device is connected to the Internet or not.

Think of your physical attack surface as all the security vulnerabilities in a given system that would be physically accessible to an attacker if they were able to get access to your office, server room, or other physical location. Physical attack surfaces are typically exploited by insider threats such as rogue employees, social engineering ploys, untrusted or BYOD devices on secure networks, or simply intruders posing as service workers.

For reference, when an attacker gains physical access to a device, they may be able to:

- Map out all the networked devices, ports, and services the device has or is connected to.
- Inspect source code open on or running on the device.
- Check for databases containing sensitive information.
- Install malicious software designed to infect the operating system. This is particularly high-risk if other connected devices have wormable vulnerabilities.
- Use privilege escalation to gain unauthorized access to privileged areas or devices, which is why the principle of least privilege and defense in depth is important.
- Expose sensitive data that is on the computer

Many experts believe if physical security is not considered, a data breach is inevitable. Given that the average cost of a data breach is now nearly $4 million globally, invest in physical security designed to prevent data breaches. This can include swipe bards and biometric access control systems to avoid tailgating, properly disposing of paper files and hardware, as well as a myriad of other physical security controls. With that said, the most common way people gain physical access is through people.

Social Engineering Attack Surface:

People are one of the most dangerous, and often overlooked parts of any organization's attack surface. Think of your social engineering attack surface as the total number of individuals who are susceptible to social engineering. Social engineering exploits human psychology and susceptibility to manipulate victims into divulging confidential information and sensitive data or performing an action that breaks usual security standards.

In general, the success of social engineering relies on a lack of knowledge of the methods attackers use, as well as poor OPSEC. OPSEC or operational security is a process that identifies actions, such as posting to social media, that could be useful for a potential attacker if properly analyzed and grouped with other data. This is why cybersecurity awareness training is the first line of defense in what is frequently the weakest link in otherwise secure organizations that employ sophisticated defense in depth strategies.

Examples of social engineering include:

A whaling attack that targets someone in accounts payable

Media drops where an infected USB is dropped in the lobby of a building and plugged into a computer by an unsuspecting employee

Fake service people like janitors, repair people or electricians gaining access to server closets, computers, or routers.

2.3 Why is Attack Surface Analysis Important?

Attack surface analysis is important because it can:

Identify what parts of your organization need to be reviewed and tested for security vulnerabilities

Identify high-risk areas that require defense in depth

Identify when you have made changes to your infrastructure which have changed your attack surface which may need to do included in the risk assessment process.

This process can help reduce, prevent, and mitigate risks that stem from:

- Legacy, IoT, and shadow IT assets
- Human mistakes and omissions such as phishing and data leaks
- Vulnerable and outdated software
- Unknown open-source software (OSS)
- Large-scale attacks on your industry
- Targeted cyber attacks on your organization
- Intellectual property infringement
- IT inherited from M&A activities
- Vendor managed assets

2.4 How to Define the Attack Surface of Your Organization

Your attack surface is the total number of attack vectors a cybercriminal could use to get into your organization, and what they sensitive data they could extract when they do.

When defining your attack surface think of:

- All the paths sensitive data can take in and out of your organization
- All the security controls that protect those paths including resource connection, authentication, authorization, activity logging, data validation, and encoding
- All the valuable data that is used internally by your organization including secrets and keys, intellectual property, critical business data, personal information, PII, and PHI
- The security controls that protect this data including encryption, checksums, access auditing, data integrity, and operational security controls

2.5 Attack Trees

Attack trees are multi-leveled diagrams consisting of one root, leaves, and children. From the bottom up, child nodes are conditions which must be satisfied to make the direct parent node true; when the root is satisfied, the attack is complete. Each node may be satisfied only by its direct child nodes.

A node may be the child of another node; in such a case, it becomes logical that multiple steps must be taken to carry out an attack. For example, consider classroom computers which are secured to the desks. To steal one, the securing cable must be cut or the lock unlocked. The lock may be unlocked by picking or by obtaining the key. The key may be obtained by threatening a key holder, bribing a keyholder, or taking it from where it is stored (e.g. under a mousemat). Thus a four level attack tree can be drawn, of which one path is (Bribe Keyholder, Obtain Key, Unlock Lock, Steal Computer).

An attack described in a node may require one or more of many attacks described in child nodes to be satisfied. Our above condition shows only OR conditions; however, an AND condition can be created, for example, by assuming an electronic alarm which must be disabled if and only if the cable will be cut. Rather than making this task a child node of cutting the lock, both tasks can simply reach a summing junction. Thus the path ((Disable Alarm, Cut Cable), Steal Computer) is created.

Attack trees are related to the established fault tree formalism. Fault tree methodology employs boolean expressions to gate conditions when parent nodes are satisfied by leaf nodes. By including a priori probabilities with each node, it is possible to perform calculate probabilities with higher nodes using Bayes Rule. However, in reality accurate probability estimates are either unavailable or too expensive to gather. With respect to computer security with active participants (i.e., attackers), the probability distribution of events are probably not independent nor uniformly distributed, hence, naive Bayesian analysis is unsuitable.

Since the Bayesian analytic techniques used in fault tree analysis cannot legitimately be applied to attack trees, analysts instead use other techniques to determine which attacks will be preferred by a particular attacker. These may involve comparing the attacker's capabilities (time, money, skill, equipment) with the resource requirements of the specified attack. Attacks which are near or beyond the attacker's ability to perform are less preferred than attacks that are perceived as cheap and easy. The degree to which an attack satisfies the adversary's objectives also affects the attacker's choices. Attacks that are both within the adversary's capabilities, and which satisfy their goals, are more likely than those that do not.

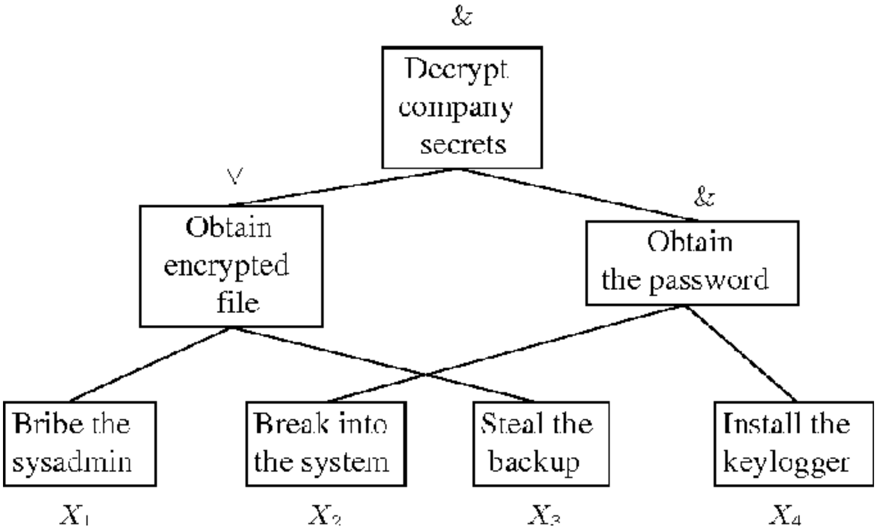


Figure 1 Attack tree example

Computer Security Strategy

An overall strategy for providing security:

- **Policy (specs):** what security schemes are supposed to do

✓ Assets and their values

- ✓ Potential threats
- ✓ Ease of use vs security
- ✓ Cost of security vs cost of failure/recovery
- **Implementation/mechanism: how to enforce**
- ✓ Prevention
- ✓ Detection
- ✓ Response
- ✓ Recovery
- ✓ Correctness/assurance: does it really work (validation/review)

Security Taxonomy

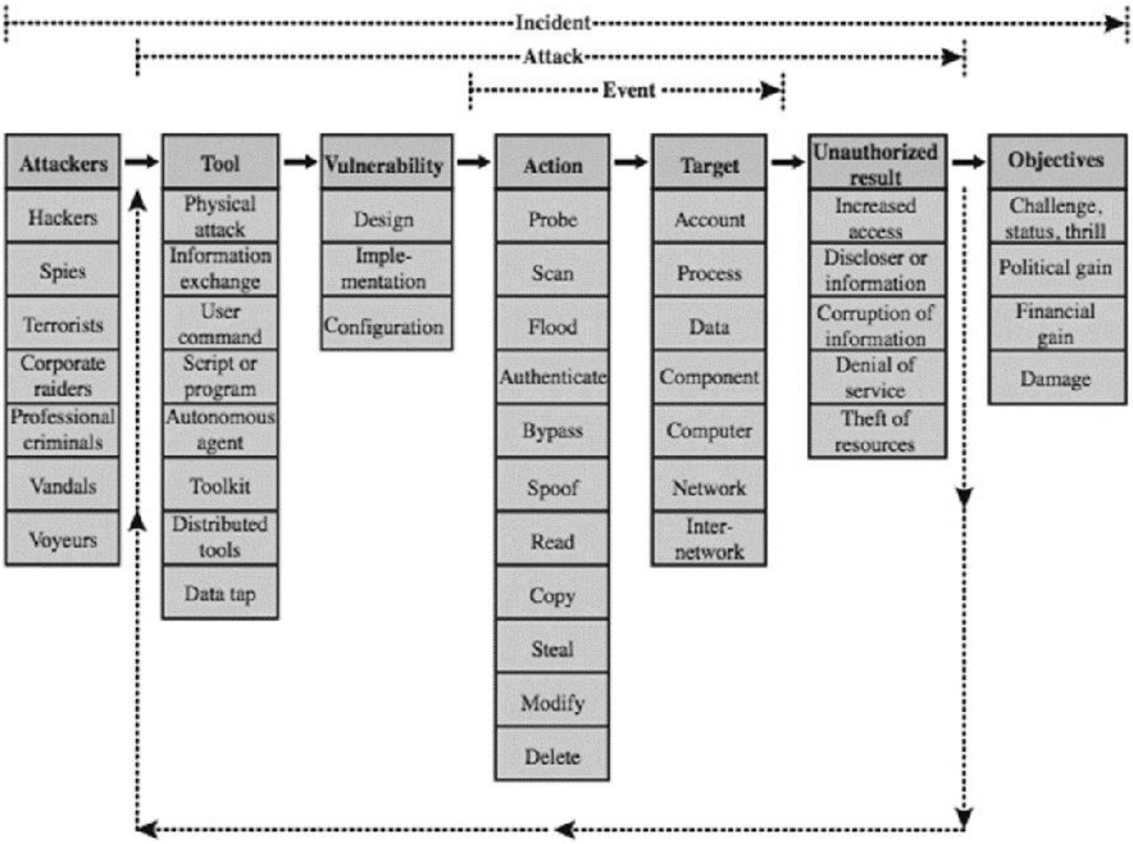


Figure 2Computer Security Taxonomy

The previous figure depicts the overall scope of computer security using this taxonomy. At a top level of detail, an attacker, or group of attackers, achieves their objectives by performing attacks. An incident may be comprised of a single or multiple attacks, as illustrated by the return loop . The key elements are:

- **Action**: A step taken by a user or process to achieve a result
- **Target**: A computer or network logical entity or physical entity
- **Event:** An action directed at a target that is intended to result in a change of state, or status, of the target
- **Tool**: A means of exploiting a computer or network vulnerability
- **Vulnerability**: A weakness in a system allowing unauthorized action
- **Unauthorized result:** An unauthorized consequence of an event
- **Attack:** A series of steps taken by an attacker to achieve an unauthorized result

- **Attacker:** An individual who attempts one or more attacks in order to achieve an objective
- **Objectives:** The purpose or end goal of an incident
- **Incident**: a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.

Notes: The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system

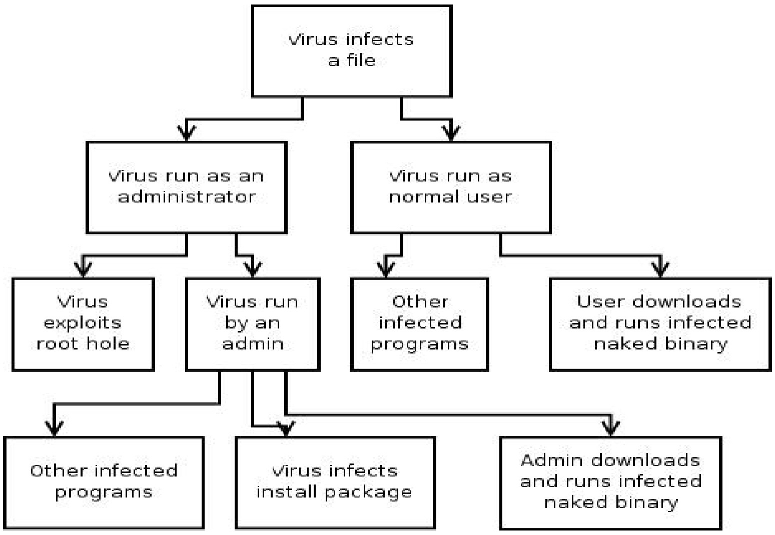

Virus infects a file
Virus run as an administrator
Virus run as normal user
Virus exploits root hole
Virus run by an admin
Other infected programs
User downloads and runs infected naked binary
Other infected programs
Virus infects install package
Admin downloads and runs infected naked binary

Figure 3 Example of Virus attack tree

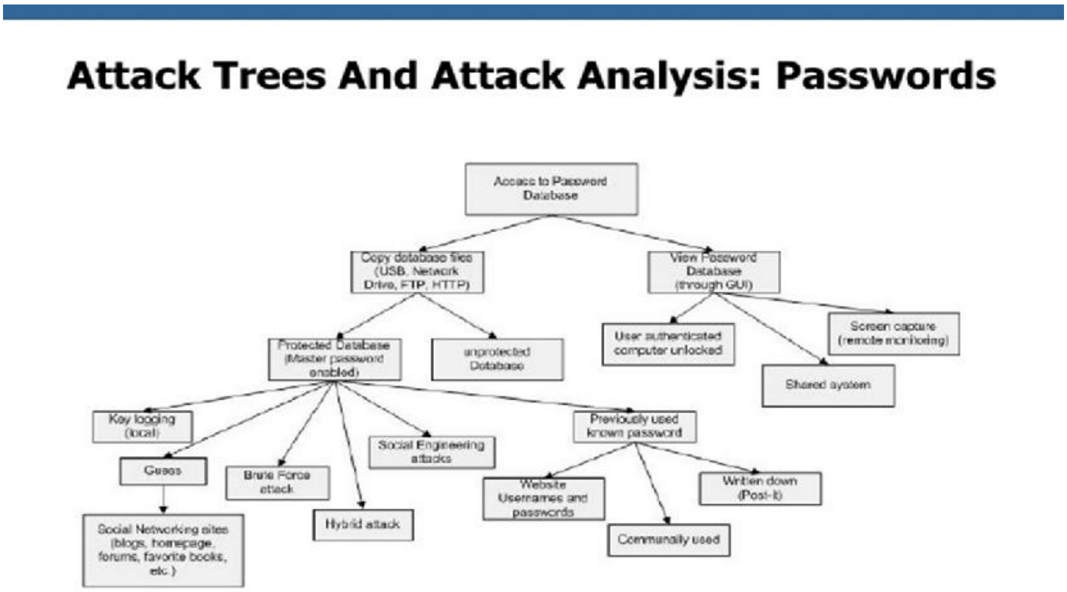

Attack Trees And Attack Analysis: Passwords
Access to Password Database
Copy database files (USB, Network Drive, FTP, HTTP)
View Password Database (through GUI)
Protected Database (Master password enabled)
unprotected Database
User authenticated computer unlocked
Screen capture (remote monitoring)
Shared system
Key logging (local)
Guess
Brute Force attack
Hybrid attack
Social Engineering attacks
Previously used known password
Social Networking sites (blogs, homepage, forums, favorite books, etc.)
Website Usernames and passwords
Communally used
Written down (Post-it)

Figure 4Database Password Attack Trees

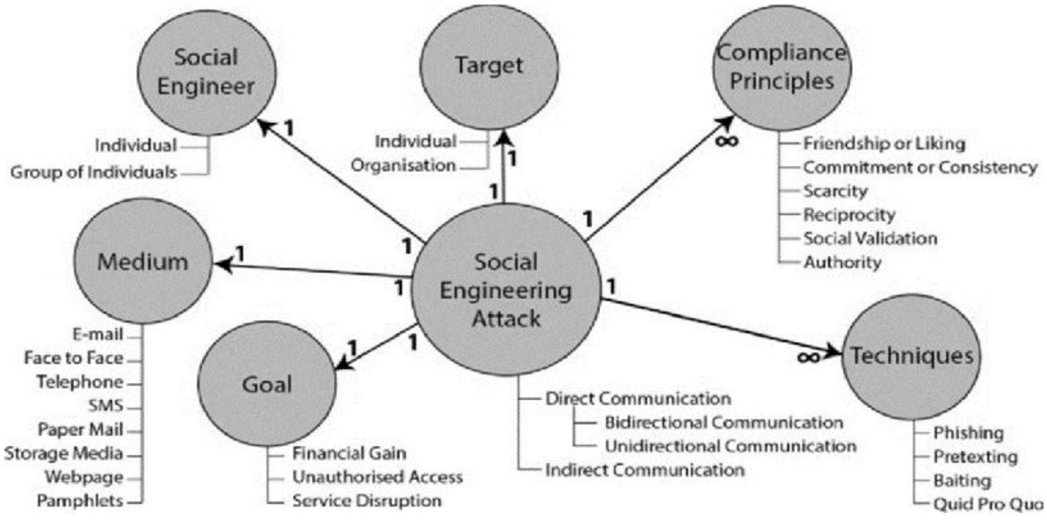


Figure 5 Social Engineering Attack Tree

2.6 Network Access Security Model

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

In this section, we will be discussing the general 'network security model' where we will study how messages are shared between the sender and receiver securely over the network. And we will also discuss the 'network access security model' which is designed to secure your system from unwanted access through the network

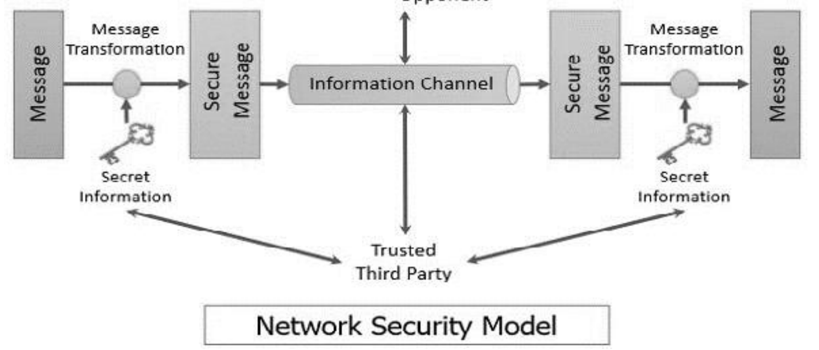
For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. Information channel which is an Internet service.A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.

Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the three components discussed below:

1. **Transformation** of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the **secret information** between sender and receiver of which the opponent must not any clue. Yes, we are talking of the **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a **trusted third party** which should take the responsibility of **distributing the secret information (key)** to both the communicating parties and also prevent it from any opponent.



The network security model presents the two communicating parties**sender** and **receiver** who mutually agrees to exchange the information. The sender has information to share with the receiver.

But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be **transformed** into an unreadable format.

Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

So, considering this general model of network security, one must consider the following four tasks while designing the security model.

1. To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the generation of the secret information which is known as a key.

This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end. At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form.

So, there must be a trusted third party which will distribute the secret information to both sender and receiver. While designing the network security model designer must also concentrate on developing the methods to distribute the key to the sender and receiver.

An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.

It is also taken care that the communication protocols that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

Till now we have discussed the security of the information or message over the network. Now, we will discuss the network access security model which is designed to secure the information system which can be accessed by the attacker through the network.

You are well aware of the attackers who attack your system that is accessible through the internet. These attackers fall into two categories:

1. **Hacker:** The one who is only interested in penetrating into your system. They do not cause any harm to your system they only get satisfied by getting access to your system.

2. **Intruders**: These attackers intend to do damage to your system or try to obtain the information from the system which can be used to attain financial gain.

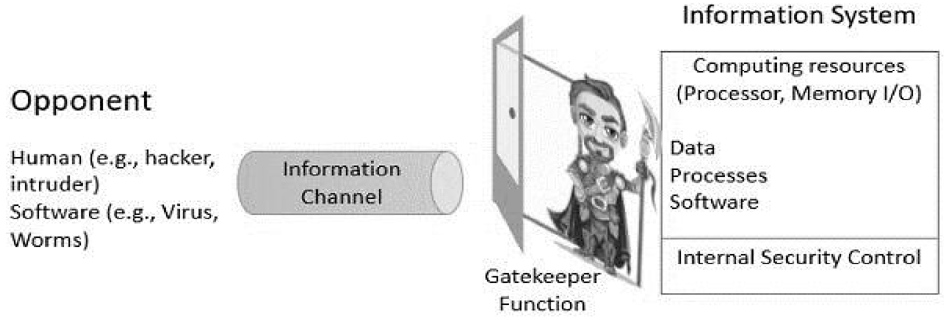
The attacker can place a logical program on your system through the network which can affect the software on your system. This leads to two kinds of risks:

a. **Information threat:** This kind of threats modifies data on the user's behalf to which actually user should not access. Like enabling some crucial permission in the system.

b. **Service threat**: This kind of threat disables the user from accessing data on the system.

Well, these kinds of threats can be introduced by launching worms and viruses and may more like this on your system. Attack with worms and viruses are the software attack that can be introduced to your system through the internet.

The network security model to secure your system is shown in the figure below:


Information System
Computing resources (Processor, Memory I/O)
Data
Processes
Software
Internal Security Control
Opponent
Human (e.g., hacker, intruder)
Software (e.g., Virus, Worms)
Information Channel
Gatekeeper Function

Network Access Security Model

There are two ways to secure your system from attacker of which the first is to introduce the gatekeeper function. Introducing gatekeeper function means introducing login-id and passwords which would keep away the unwanted access.

In case the unwanted user gets access to the system the second way to secure your system is introducing internal control which would detect the unwanted user trying to access the system by analyzing system activities. This second method we call as antivirus which we install on our system to prevent the unwanted user from accessing your computer system through the internet.

So, this is all about the network security model. We have discussed two network security model. One, securing your information over the network during information transmission. Second, securing your information system which can be accessed by the hacker through the network or internet.

2.7 Security Standards

To make cybersecurity measures explicit, the written norms are required. These norms are known as cybersecurity standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common langTo make cybersecurity measures explicit, the written norms are required. These norms are known as cybersecurity standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cybersecurity strategy. usage, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cybersecurity strategy.

2.8 ISO

ISO stands for International Organization for Standardization. International Standards make things to work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard was officially established on 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which cover almost every industry, from information technology to food safety, to agriculture and healthcare.

ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorized into many types. They are-

ISO 27001- This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

ISO 27000- This standard provides an explanation of terminologies used in ISO 27001.

ISO 27002- This standard provides guidelines for organizational information security standards and information security management practices. It includes the selection, implementation, operating and management of controls taking into consideration the organization's information security risk environment(s).

ISO 27005- This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is capable for all kind of organizations such as non-government organization, government agencies, and commercial enterprises**.**

ISO 27032- It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

2.9 IT Act

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of

United Nations. This act is also used to check misuse of cyber network and computer in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitate electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act.

2.10 Copyright Act

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not covers the following-

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic ornamentation, lettering, or coloring

Figure 6 Intellectual Property Rights

2.11 Patent Law

Patent law is a law that deals with new inventions. Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

Not a natural object or process

- New
- Useful
- Not obvious.

2.12 IPR

Intellectual property rights is a right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

Summary

- The security design principles are considered while designing any security mechanism for a system.
- These principles are reviewed to develop a secure system which prevents the security flaws and prevents unwanted access to the system.
- A security standard is "a published specification that establishes a common language and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition.
- Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate.
- ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology to food safety, to agriculture and healthcare.

Keywords

Patent: Patent law is a law that deals with new inventions.

Attack surface: the reachable and exploitable vulnerabilities in a system.

Information access threatsare the threats that Intercept or modify data on behalf of users who should not have access to that data.

Service threats: Exploit service flaws in computers to inhibit use by legitimate users.

Attack Trees: A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

Action: A step taken by a user or process in order to achieve a result.

Incident: a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.

Self Assessment

1. This principle says that the system should not trust the access decisions it recovers from the system cache ______

A. Layering

B. Least privilege

C. Open design

D. Complete Mediation

2. The access is permitted or denied should be based on authorization rather than elimination is stated by which principle_____

A. Fail-Safe Default

B. Economy of Mechanism

C. Isolation

D. Modularity

3. This principle reduces the count of communication paths and therefore further reduces the hardware and software implementation_______

A. Least Common Mechanism

B. Isolation

C. Layering

D. Open Design

4. _________ is the sum of all the possible points in software or system where unauthorized users can enter as well as extract data from the system.

A. Attack vector

B. Attack surface

C. Attack point

D. Attack arena

5. ___________ is a weakness that can be exploited by attackers.

A. System with Virus

B. System without firewall

C. System with vulnerabilities

D. System with a strong password

6. A means of exploiting a computer or network vulnerability_____

A. Target

B. Event

C. Tool

D. Action

7. A series of steps taken by an attacker to achieve an unauthorized result____

A. Vulnerability

B. Objectives

C. Attack

D. Action

8. Which is not an objective of network security?

A. Identification

B. Authentication

C. Access control

D. Lock

9. Exploit service flaws in computers to inhibit use by legitimate users is known as _________

A. Information Access threats

B. Service threats

C. Security Mechanism

D. Encryption

10. _________can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software.

A. Virus/Worm

B. Threats

C. Denial of Service

D. None of these

11. In the model for Network Security, what is the responsibility of the third party____

A. A trusted third party may be needed to achieve secure transmission

B. A third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

C. A third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

D. All the above

12. ISO stands for __________

A. International Organization for Standardization

B. Internet System Order

C. Institutional Security Operation

D. International System Organization

13. This standard proves to managing the best security of their confidential data and information.

A. ISO 27000

B. ISO 27001

C. IT Act

D. Copyright

14. _____ deals with new inventions.

A. Patent Law

B. Copyright

C. Trademark
D. Geographical indication

15. Works that are not fixed in a tangible form is not considered as
A. Trademark
B. Geographical indication
C. Patent Law
D. Copyright

Answers for Self Assessment

1.	D	2.	A	3.	A	4.	B	5.	C
6.	C	7.	C	8.	D	9.	B	10.	A
11.	D	12.	A	13.	B	14.	A	15.	D

Review Questions

1. Explain the fundamentals of Security Design Principles
2. Explain the model of network security with the help of diagram.
3. Discuss the attack surface and attack tree with the help of real-life example.

Further Reading

https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf

Web Links

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Unit 03: Introduction to Number Theory

CONTENTS

Objectives

- Understand the concept of a congruence and use various results related to congruences.
- Identify certain number theoretic functions and their properties.
- Identify how number theory is related to and used in cryptography.
- Identify and apply various properties of and relating to the integers including, primes, unique factorization, the division algorithm and greatest common divisors

Introduction

Theideasthatwewilldevelopinthissectionarebasedonthenotionofdivisibility.Divisionofan integerbyapositiveintegerproducesaquotientandaremainder.Workingwiththeseremainders leads to modular arithmetic, which plays an important role in mathematics, and which is used throughoutcomputerscience.Wewilldiscusssomeimportantapplicationsofmodular arithmetic laterinthischapter,includinggeneratingpseudorandomnumbers, assigningcomputermemory locations to files, constructing check digits, and encrypting messages

Division

When one integer is divided by a second nonzero integer, the quotient may or may not be an integer. For example, 12/3=4 is an integer, whereas 11/4=2.75 is not. This leads to Definition 1.

Definition 1

If a and b are integers with a ≠0, we say that a divides b if there is an integer c such that b = ac,orequivalently, if b/ a isaninteger. Whena dividesb wesaythata isafactor ordivisor of b, and that b is a multiple of a.The notation a | b denotes that a divides b. We write a| b when a does not divide b.

Remark: We can express a | b using quantifiers as∃c(ac = b),where the universe of discourse is the set of integers.

In Figure 1 a number line indicates which integers are divisible by the positive integer d. EXAMPLE 1 Determine whether 3|7 and whether 3|12. Solution: We see that 3| 7, because 7/3 is not an integer. On the other hand, 3|12 because 12/3=4. ▲ EXAMPLE 2 Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution: The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with 0 < dk≤ n, or with 0 <k≤ n/d. Therefore, there are n/dpositive integers not exceeding n that are divisible by d. ▲ Some of the basic properties of divisibility of integers are given in Theorem 1.

Theorem 1

Let a,b, and c be integers, where a ≠0. Then

(i) if a | b and a | c, then a | (b+c);

(ii) (ii) if a | b, then a | bc for all integers c;

(iii) (iii) if a | b and b | c, then a | c.

Proof:

We will give a direct proof of (i). Suppose that a | b and a | c.Then, from the definition of divisibility, it follows that there are integers s and t with b = as and c = at. Hence,

$$b + c = as + at = a(s + t).$$

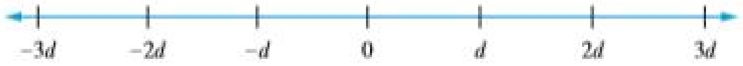


Figure 1 Integers divisible by positive integer d

Therefore, a divides b+c. This establishes part (i) of the theorem. The proofs of parts (ii) and (iii) are left as Exercises 3 and 4.

Theorem 1 has this useful consequence.

If a, b,and c are integers,where a =0,suchthat a | b and a | c,then a | mb+nc whenever m and n are integers.

Proof: We will give a direct proof. By part (ii) of Theorem 1 we see that a | mb and a | nc whenever m and n are integers. By part (i) of Theorem 1 it follows that a | mb+nc.

3.1 The Division Algorithm

Remember in elementary school when you would bring a treat in to share with the class on your birthday? Wasn't that great? Suppose it's your birthday, and you decide to keep tradition alive and bring in 25 pieces of candy to share with your coworkers. You have 6 coworkers in your department to whom to give the candy. You sit down to figure out how many pieces of candy each worker will receive.

You realize this is a simple division problem. You divide the number of pieces of candy by the number of coworkers to solve the problem.

25 / 6 = 4 remainder 1

This tells you that each coworker will get 4 pieces of candy, and you will have 1 piece leftover. In other words:

25 = 6 * 4 + 1

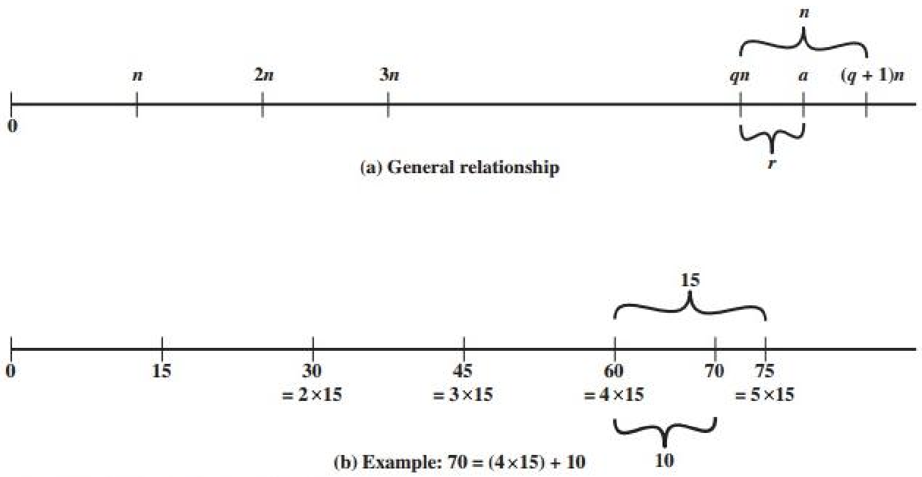
This equation actually represents something called the division algorithm. In the equation, we call 25 the dividend, 6 the divisor, 4 the quotient, and 1 the remainder. The division algorithm is basically just a fancy name for organizing a division problem in a nice equation. It states that for any integer a and any positive integer b, there exists unique integers q and r such that a = bq + r, where r is greater than or equal to 0 and less than b. Does that equation look familiar? It should! It's exactly in the form of the equation we found representing our candy problem! Now, let's talk about a special case of the division algorithm: that is, when we have a remainder equal to 0.

Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad\qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

where |x | is the largest integer less than or equal to x. Equation (4.1) is referred to as the division algorithm.

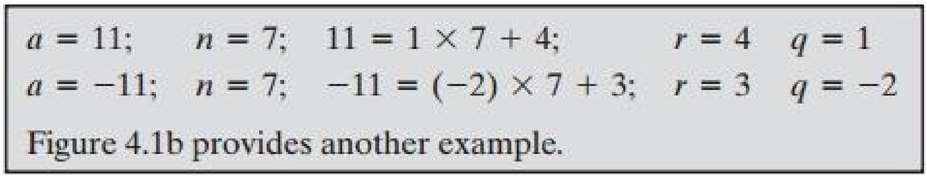
Figure 4.1a demonstrates that, given a and positive n, it is always possible to find q and r that satisfy the preceding relationship. Represent the integers on the number line; a will fall somewhere on that line (positive a is shown, a similar demonstration can be made for negative a). Starting at 0, proceed to n, 2n, up to qn, such that qn<=a and(q + 1)n > a. The distance from qn to a is r, and we have found the unique values of q and r. The remainder r is often referred to as a residue.



(a) General relationship

(b) Example: 70 = (4×15) + 10

Figure 4.1 The Relationship $a = qn + r; 0 \le r < n$



$a = 11$; $n = 7$; $11 = 1 \times 7 + 4$; $r = 4$ $q = 1$

$a = -11$; $n = 7$; $-11 = (-2) \times 7 + 3$; $r = 3$ $q = -2$

Figure 4.1b provides another example.

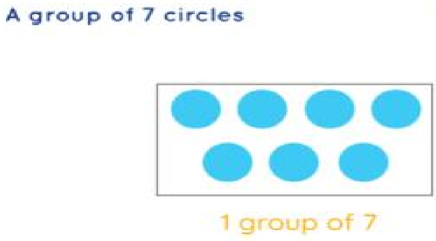
3.2 Prime Numbers

Prime numbers are the numbers that have only two factors, that are, 1 and the number itself. Consider an example of number 5, which has only two factors 1 and 5. This means it is a prime number. Let's take another example of the number 6, which has more than two factors, i.e 1, 2, 3, and 6. This means 6 is not a prime number. Now, if we take the example of the number 1, we know that it has only one factor. So, it cannot be a prime number as a prime number should have exactly two factors. This means 1 is neither a prime nor a composite number, it is a unique number.

What are Prime Numbers?

A number greater than 1 with exactly two factors, i.e. 1 and the number itself is defined as a prime number. In other words, if a number cannot be divided into equal groups, then it is a prime number. We can divide a number into groups with equal numbers of items/elements only if it can be factorized as a product of two numbers. For example, 7 cannot be divided into groups of equal numbers. This is because 7 can only be factorized as follows:

- 7 × 1 = 7
- 1 × 7 = 7



This means 1 and 7 are the only factors of 7. So, 7 is a prime number because it could not be divided into groups of equal numbers.

Definition of a Prime Number: Any whole number greater than 1 that is divisible only by 1 and itself, is defined as a prime number.

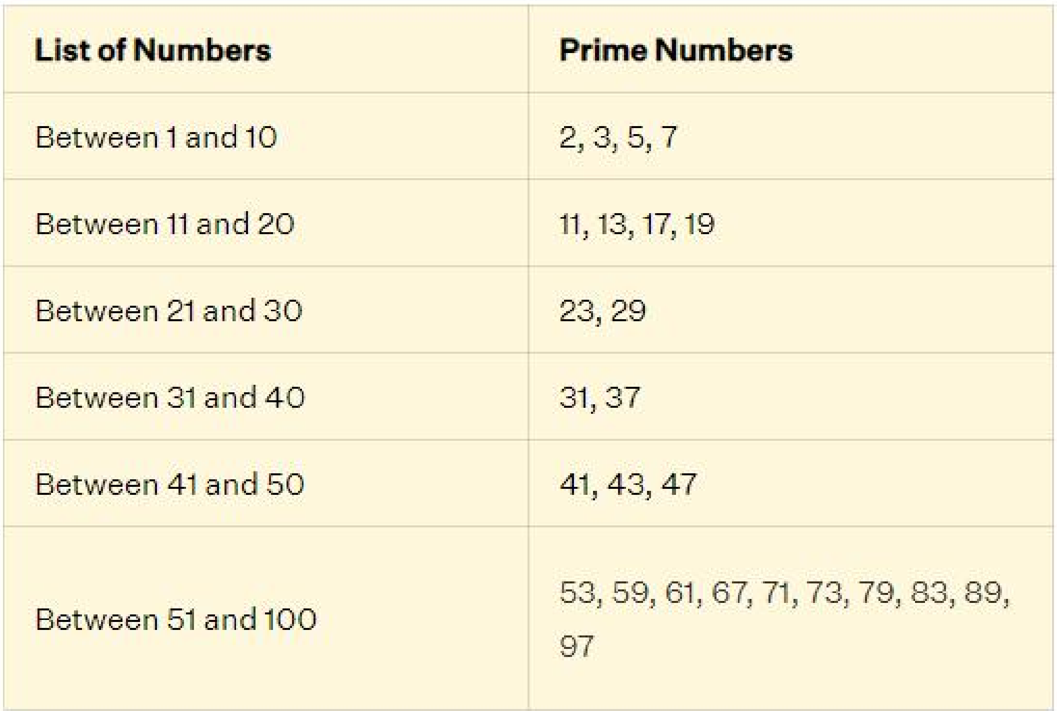
3.3 History of Prime Numbers

Prime numbers created human curiosity since ancient times. Even today, mathematicians are trying to find prime numbers with mystical properties. Euclid proposed the theorem on prime numbers - There are infinitely many prime numbers.

Do you know all the prime numbers from 1 to 100? Did you check if each number is divisible by the smaller numbers? Then, you invested a lot of time and effort. Eratosthenes was one of the greatest scientists, who lived a few decades after Euclid, designed a smart way to determine all the prime numbers up to a given number. This method is called the Sieve of Eratosthenes. Suppose you have to find the prime numbers up to n, we will generate the list of all numbers from 2 to n. Starting from the smallest prime number p = 2, we will strike off all the multiples of 2, except 2 from the list. Similarly, assign the next value of p which is a prime number greater than 2.

List of Prime Numbers

There are 25 prime numbers from 1 to 100. The complete list of prime numbers from 1 to 100 is given below:



List of Numbers	Prime Numbers
Between 1 and 10	2, 3, 5, 7
Between 11 and 20	11, 13, 17, 19
Between 21 and 30	23, 29
Between 31 and 40	31, 37
Between 41 and 50	41, 43, 47
Between 51 and 100	53, 59, 61, 67, 71, 73, 79, 83, 89, 97

3.4 Properties of Prime Numbers

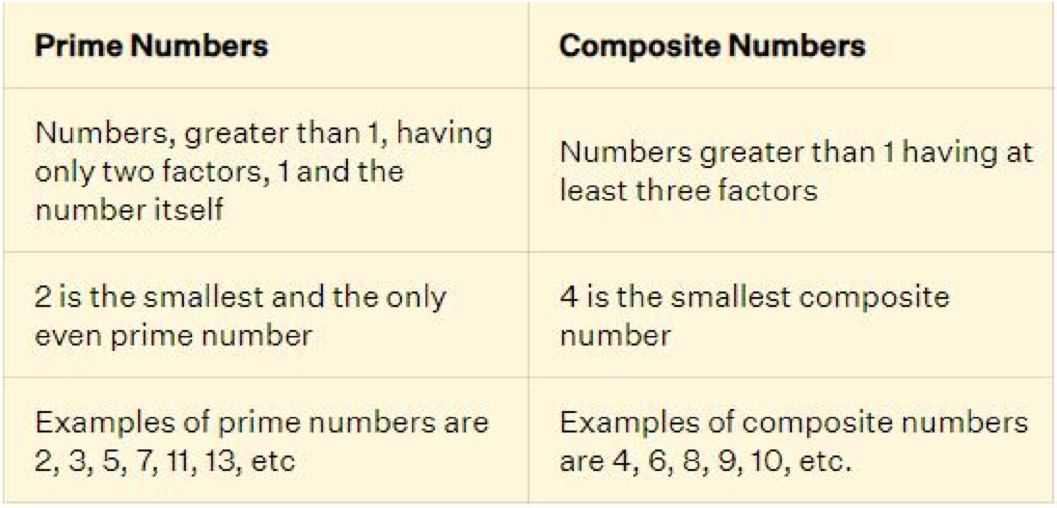
Some of the important properties of prime numbers are given below:

- A prime number is a whole number greater than 1.
- It has exactly two factors, that is, 1 and the number itself.
- There is only one even prime number, that is, 2.
- Any two prime numbers are always co-prime to each other.
- Every number can be expressed as the product of prime numbers.

3.5 Prime Numbers vs Composite Numbers

A prime number is a number greater than 1 that has exactly two factors, while a composite number has more than two factors. For example, 5 can be factorized in only one way, that is, 1 × 5 (OR) 5 × 1. It has only two factors, which are, 1 and 5. Therefore, 5 is a prime number.

A composite number is a number greater than 1 that has more than two factors. For example, 4 can be factorized in multiple ways. So, the factors of 4 are 1, 2, and 4. It has more than two factors. Therefore, 4 is a composite number. Let us understand the difference between prime numbers and composite numbers with the help of a table given below:



Prime Numbers	Composite Numbers
Numbers, greater than 1, having only two factors, 1 and the number itself	Numbers greater than 1 having at least three factors
2 is the smallest and the only even prime number	4 is the smallest composite number
Examples of prime numbers are 2, 3, 5, 7, 11, 13, etc	Examples of composite numbers are 4, 6, 8, 9, 10, etc.

Table 1 Difference between Prime and Composite Number

3.6 Prime Numbers and Co-prime Numbers

There is a difference between prime numbers and co-prime numbers. Co-prime numbers are always considered in pairs, while a single number can be interpreted as a prime number. If a pair of numbers has no common factor apart from 1, then the numbers are called co-prime numbers. Co-prime numbers can be prime or composite, the only criteria to be met is that the GCF of co-prime numbers is always 1.

Examples of co-prime numbers:

5 and 9 are co-primes.

6 and 11 are co-primes.

18 and 35 are co-primes.

Co-prime numbers need not necessarily be prime numbers.

Easy Way to Find Prime Numbers

There are different ways to find prime numbers. Let us go through two of these methods.

Method 1: Substitute whole numbers for n in the formula 'n2 + n + 41'. This formula will give you all the prime numbers greater than 40. Let's substitute a few whole numbers and check.

02 + 0 + 41 = 0 + 41 = 41

12 + 1 + 41 = 2 + 41 = 43

22 + 2 + 41 = 6 + 41 = 47

Continuing like this, you can calculate all the prime numbers greater than 40.

Method 2: Every prime number, apart from 2 and 3, can be written in the form of '6n + 1 or 6n - 1'. So, if you have any number different from 2 and 3, you can check if it is prime or not by trying to express it in the form of 6n + 1 or 6n - 1

6(1) - 1 = 5

6(1) + 1 = 7

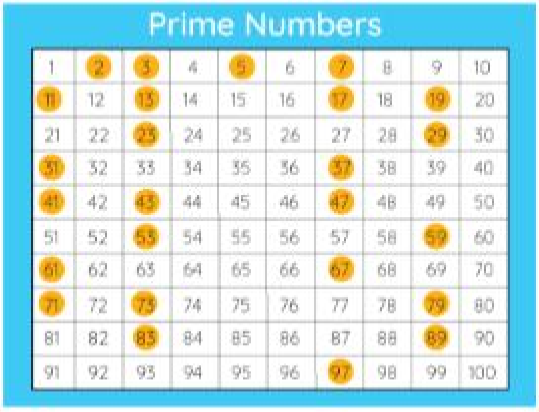
6(2) - 1 = 11

6(2) + 1 = 13

Now, we know that the numbers 5, 7, 11, and 13 are prime.

List of Odd Prime Numbers

A prime number chart is a chart that shows the list of prime numbers in a systematic order. Given below is the prime number chart from numbers 1 to 100 that shows the list of odd prime numbers(highlighted in yellow)



Prime Numbers

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Prime number between 1 to 100

3.7 Least Common Multiple

The abbreviation LCM stands for "Least Common Multiple". The least common multiple of two numbers is the lowest possible number that can be divisible by both numbers. It can be calculated for two or more integers as well as two or more fractions.

There are multiple methods to find the LCM of two numbers. One of the quickest ways to find the LCM of two numbers is to use the prime factorization of each number and then the product of the highest powers of the common prime factors will be the LCM of those numbers.

What is Least Common Multiple (LCM)?

The least common multiple is also known as LCM (or) the lowest common multiple in math. The least common multiple of two or more numbers is the smallest number among all common multiples of the given numbers. Let's take two numbers: say, 2 and 5. Each will have its own set of multiples.

Multiples of 2 are 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, …

Multiples of 5 are 5, 10, 15, 20, …

Let's represent these multiples on the number line and circle the common multiples,

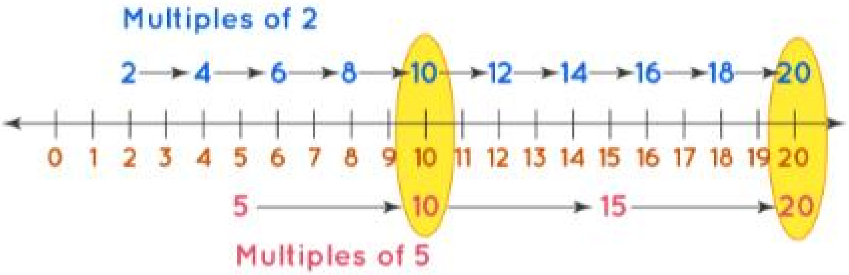


Figure 2 Multiples of 2 and 5

Thus, the common multiples of 2 and 5 are 10, 20, ….. The smallest number among 10, 20, … is 10. So the least common multiple of 2 and 5 is 10. Therefore, LCM (2, 5) = 10.

How to Find the Least Common Multiple?

LCM of numbers can be calculated using various methods. There are 3 methods to find the least common multiple of two numbers. Each method is explained below with some examples of LCM.

- **LCM by Listing Method**
- **LCM using Prime Factorization**
- **LCM using Division Method**

• LCM by Listing Method (Listing Out the Common Multiples)

By using the listing out the common multiples method we can find out the common multiples of two or more numbers. Out of these common multiples, the least common multiple is considered and the LCM of two given numbers can thus be calculated. To calculate the LCM of the two numbers A and B by using the listing method, follow the steps given below:

Step 1 - List a few multiples of A and B.

Step 2 - Mark the common multiples from the multiples of both numbers.

Step 3 - Select the smallest common multiple. That lowest common multiple is the LCM of the two numbers.

Example: Find the least common multiple (LCM) of 4 and 5.

Solution: Multiples of 4 are: 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, ... and the multiples of 5 are: 5, 10, 15, 20, 25, 30, 35, 40, ...

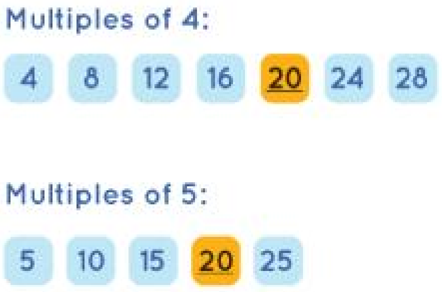


Figure 3 LCM of 4 and 5 by listing out common multiples

Hence, by the definition of least common multiple, the LCM of 4 and 5 is 20.

• LCM using Prime Factorization

By using the prime factorization method we can find out the prime factors of the numbers and these prime factors can be used to find the LCM of those numbers. To calculate the LCM of two numbers using the prime factorization method follow the steps given below:

Step 1 - Represent the numbers in the prime factored form.

Step 2 - The LCM of the given two numbers is the product of all the prime factors. (However, common factors will be included only once)

Let’s learn this method using the example given below.

Example: Find the least common multiple (LCM) of 60 and 90 using prime factorization.

Solution:

Step 1 - The prime factorization of 60 and 90 are: 60 = 2 × 2 × 3 × 5 and 90 = 2 × 3 × 3 × 5.

Step 2 - The product of all the prime factors = 2 × 2 × 3 × 5 × 3 = 180.

Therefore, LCM of 60 and 90 = 2 × 2 × 3 × 5 × 3 = 180.

- **LCM By Division Method**

By the division method, we will divide the numbers by a common prime number, and these prime factors are used to calculate the LCM of those numbers. To calculate the LCM of two numbers using the division method follow the steps given below:

Step 1 - Find a prime number which is a factor of at least one of the given numbers. Write this prime number on the left of the two numbers.

Step 2 - If the prime number in step 1 is a factor of the number, then divide the number by the prime and write the quotient below. If the prime number in step 1 is not a factor of the number, then write the number in the row below as it is. Continue the steps until all prime numbers are left in the last row.

Let's learn this method using the example given below.

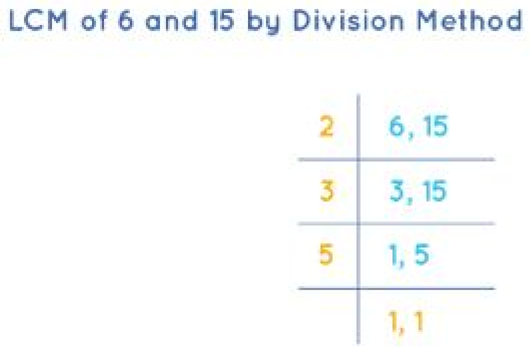
Example: Find the least common multiple (LCM) of 6 and 15 using the division method.

Solution:

Step 1 - 2 is the smallest prime number and it is a factor of 6. Write 2 on the left of the two numbers. For each number in the right column, continue finding out prime numbers which are their factors.

Step 2 - 2 divides 6 but it's not a factor of 15, then write the number 15 in the row below as it is. Continue the steps until 1 is left in the last row.

Step 3 - The LCM is the product of all the prime numbers. LCM of 6 and 15 is, 2 × 3 × 5 = 30.



LCM of 6 and 15 by Division Method

2	6, 15
3	3, 15
5	1, 5
	1, 1

3.8 The Euclidean Algorithm

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. First, we need a simple definition: Two integers are relatively prime if their only common positive integer factor is 1.

Greatest Common factor

Recall that nonzero b is defined to be a divisor of a if a = mb for some m, where a, b, and m are integers. We will use the notation gcd(a, b) to mean the greatest common divisor of a and b. The greatest common divisor of a and b is the largest integer that divides both a and b. We also define gcd(0, 0) = 0.

More formally, the positive integer c is said to be the greatest common divisor of a and b if

1. c is a divisor of a and of b.
2. Any divisor of a and b is a divisor of c. An equivalent definition is the following:

gcd(a, b) = max[k, such that k | a and k | b]

Because we require that the greatest common divisor be positive, gcd(a, b) =

gcd(a, -b) = gcd(-a, b) = gcd(-a,-b). In general, gcd(a, b) = gcd(| a | , | b |).

gcd(60, 24) = gcd(60, -24) = 12

Also, because all nonzero integers divide 0, we have gcd(a, 0) = | a | .

We stated that two integers a and b are relatively prime if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if gcd(a, b) = 1.

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Finding the Greatest Common Factor

We now describe an algorithm credited to Euclid for easily finding the greatest common divisor of two integers. This algorithm has significance subsequently in this chapter. Suppose we have integers a, b such that d = gcd(a, b). Because gcd(| a | , | b |) = gcd(a, b), there is no harm in assuming a >= b > 0. Now dividing a by b and applying the division algorithm, we can state:

$a = q_1 b + r_1$ 0 < , <*b* **(4.2)**

If it happens that r1 = 0,then *bla* and *d* = *gcd(a,* b) = *b.* **But** if r1 *t;* 0,we can state that dlr1.This is due *to* the basic properties of divisibility:the relations *d l a* and *d l b* together imply that *d l (a* - *q1b*),which is the same as dlr1.Before proceeding with the Euclidian algorithm,we need *to* answer the question:What is the *gcd(b,* r1)? We know that *d l b* and dlr1. Now take any arbitrary integer c tha t divides both *b* and r1•

Therefore,*cl(q1b* + *r1)* "'' *a.* Because c divides both *a* and *b,* we must have c <*d,*

which is the greatest common divisor of *a* and *b.*TI1erefore *d* = gcd(b,r1).

Let us now return *to* Equation (4.2) and assume that r1 *t;* 0. Because *b* >*ri,*

we can divide *b* by r1 and apply the division algoritlun to obtain:

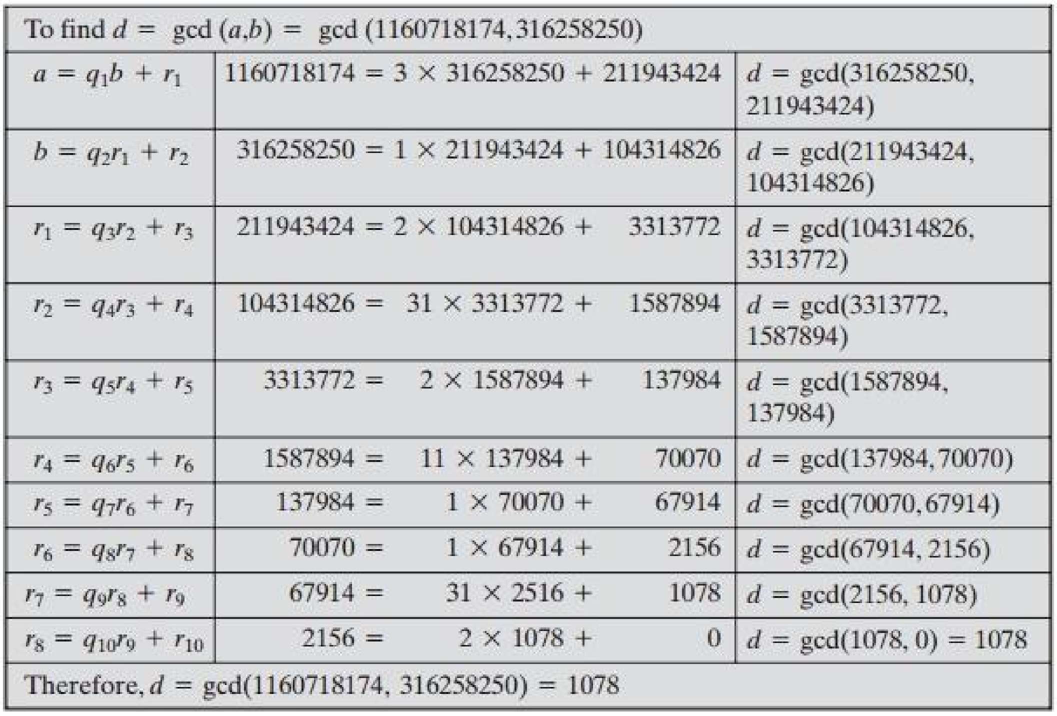
$b = q_2 r_1 + r_2$ 0 < 2 < ,

As before, if *r2* = 0, then *d* = r1 and if *r2* * 0, then *d* = gcd(ri, r2). The division process continues un til some zero remainder appears,say, at the *(n* + l)th stage where *r,,_* 1 is divided by *r,,*. The result is the following system of equations:

At each iteration, we have d = gcd(ri, ri + 1) until finally d = gcd(rn, 0) = rn. Thus, we can find the greatest common divisor of two integers by repetitive application of the division algorithm. This scheme is known as the Euclidean algorithm.

We have essentially argued from the top down that the final result is the gcd(a, b). We can also argue from the bottom up. The first step is to show that rn divides a and b. It follows from the last division in Equation (4.3) that rn divides rn - 1. The next to last division shows that rn divides rn – 2 because it divides both terms on the right. Successively, one sees that rn divides all ri's and finally a and b. It remains to show that rn is the largest divisor that divides a and b. If we take any arbitrary integer that divides a and b, it must also divide r1, as explained previously. We can follow the sequence of equations in Equation (4.3) down and show that c must divide all ri's. Therefore c must divide rn, so that rn = gcd(a, b).

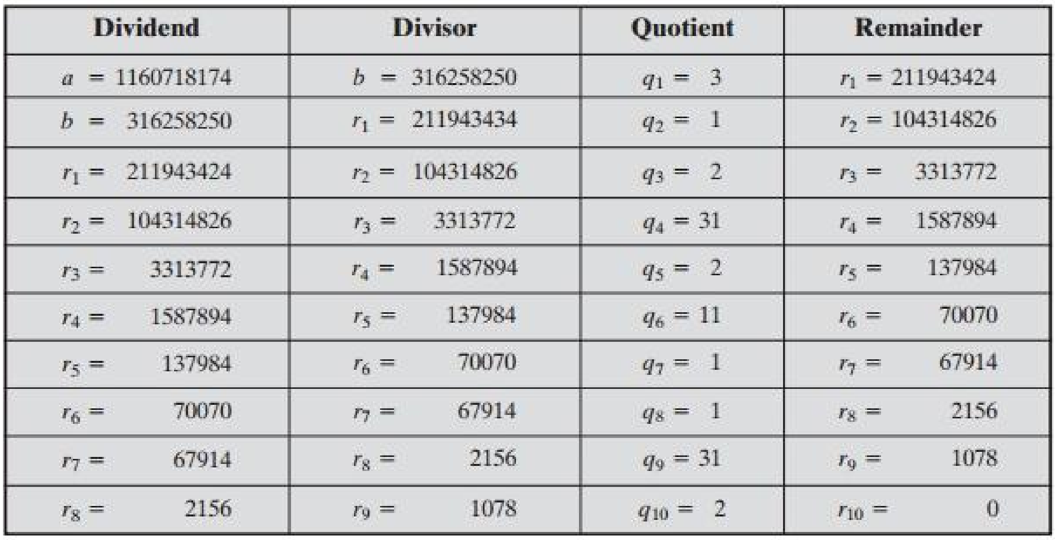
Let us now look at an example with relatively large numbers to see the power of this algorithm:



To find $d = \gcd(a,b) = \gcd(1160718174, 316258250)$		
$a = q_1b + r_1$	1160718174 = 3 × 316258250 + 211943424	$d = \gcd(316258250, 211943424)$
$b = q_2r_1 + r_2$	316258250 = 1 × 211943424 + 104314826	$d = \gcd(211943424, 104314826)$
$r_1 = q_3r_2 + r_3$	211943424 = 2 × 104314826 + 3313772	$d = \gcd(104314826, 3313772)$
$r_2 = q_4r_3 + r_4$	104314826 = 31 × 3313772 + 1587894	$d = \gcd(3313772, 1587894)$
$r_3 = q_5r_4 + r_5$	3313772 = 2 × 1587894 + 137984	$d = \gcd(1587894, 137984)$
$r_4 = q_6r_5 + r_6$	1587894 = 11 × 137984 + 70070	$d = \gcd(137984, 70070)$
$r_5 = q_7r_6 + r_7$	137984 = 1 × 70070 + 67914	$d = \gcd(70070, 67914)$
$r_6 = q_8r_7 + r_8$	70070 = 1 × 67914 + 2156	$d = \gcd(67914, 2156)$
$r_7 = q_9r_8 + r_9$	67914 = 31 × 2516 + 1078	$d = \gcd(2156, 1078)$
$r_8 = q_{10}r_9 + r_{10}$	2156 = 2 × 1078 + 0	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

In this example, we begin by dividing 1160718174 by 316258250, which gives 3 with a remainder of 211943424. Next we take 316258250 and divide it by 211943424. The process continues until we get a remainder of 0, yielding a result of 1078.

It will be helpful in what follows to recast the above computation in tabular form. For every step of the iteration, we have ri - 2 = qiri - 1 + ri, where ri - 2 is the dividend, ri - 1 is the divisor, qi is the quotient, and ri is the remainder. Table 4.1 summarizes the results.



Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943434	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

Table 2Euclidean Algorithm Example

3.9 Modular Arithmetic

The Modulus

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus. Thus, for any integer a, we can rewrite Equation (4.1) as follows:

a =qn + r 0 <= r < n; q = [a/n]

a = [a/n] * n + (a mod n)

11 mod 7 = 4; - 11 mod 7 = 3

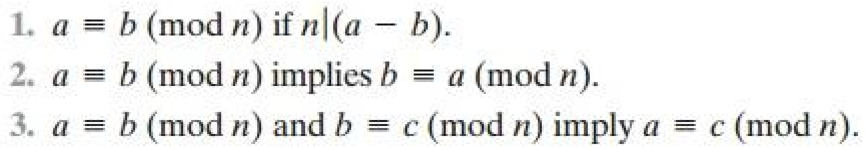
Two integers a and b are said to be congruent modulo n, if (a mod n) = (b mod n). This is written as a K b (mod n).2

73 , 4 (mod 23); 21 , -9 (mod 10)

Note that if a K 0 (mod n), then n | a.

3.10 Properties of Congruences

Congruences have the following properties:



1. $a \equiv b \pmod{n}$ if $n | (a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

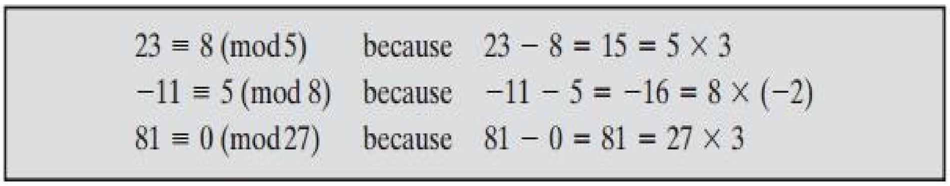
To demonstrate the first point, if n | (a - b), then (a - b) = kn for some k.

So we can write a = b + kn. Therefore, (a mod n) = (remainder when b + kn is divided by n) = (remainder when b is divided by n) = (b mod n).

23 = = 8 (mod 5) because 23 - 8 = 15 = 5 * 3

-11 = = 5 (mod 8) because -11 - 5 = -16 = 8 * (-2)

81 == 0 (mod 27) because 81 - 0 = 81 = 27 * 3



$23 \equiv 8 \pmod{5}$ because $23 - 8 = 15 = 5 \times 3$

$-11 \equiv 5 \pmod{8}$ because $-11 - 5 = -16 = 8 \times (-2)$

$81 \equiv 0 \pmod{27}$ because $81 - 0 = 81 = 27 \times 3$

The remaining points are as easily proved.

3.11 Modular Arithmetic Operations

Note that, by definition (Figure 4.1), the (mod n) operator maps all integers into the set of integers {0, 1, ... , (n - 1)}. This suggests the question: Can we perform arithmetic operations within the confines of this set? It turns out that we can; this technique is known as modular arithmetic.

Modular arithmetic exhibits the following properties:

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n

2. [(a mod n) - (b mod n)] mod n = (a - b) mod n

3. [(a mod n) * (b mod n)] mod n = (a * b) mod n

We demonstrate the first property. Define (a mod n) = ra and (b mod n) = rb.

Then we can write a = ra + jn for some integer j and b = rb + kn for some integer

k. Then

(a + b) mod n = (ra + jn + rb + kn) mod n

= (ra +rb + (k + j)n) mod n

= (ra +rb) mod n

= [(a mod n) + (b mod n)]mod n

The remaining properties are proven as easily. Here are examples of the three properties:

11 mod 8 = 3; 15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) - (15 mod 8)] mod 8 = -4 mod 8 = 4

(11 - 15) mod 8 = -4 mod 8 = 4

[(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.

To find 117 mod 13, we can proceed as follows:

112 = 121 K 4 (mod 13)

114 = (112)2 K 42 K 3 (mod 13)

117 K 11 * 4 * 3 K 132 K 2 (mod 13)

Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

Table 3 provides an illustration of modular addition and multiplication modulo 8. Looking at addition, the results are straightforward, and there is a regular pattern to the matrix. Both matrices are symmetric about the main diagonal in conformance to the commutative property of addition and multiplication. As in ordinary addition, there is an additive inverse, or negative, to each integer in modular arithmetic. In this case, the negative of an integer x is the integer y such that

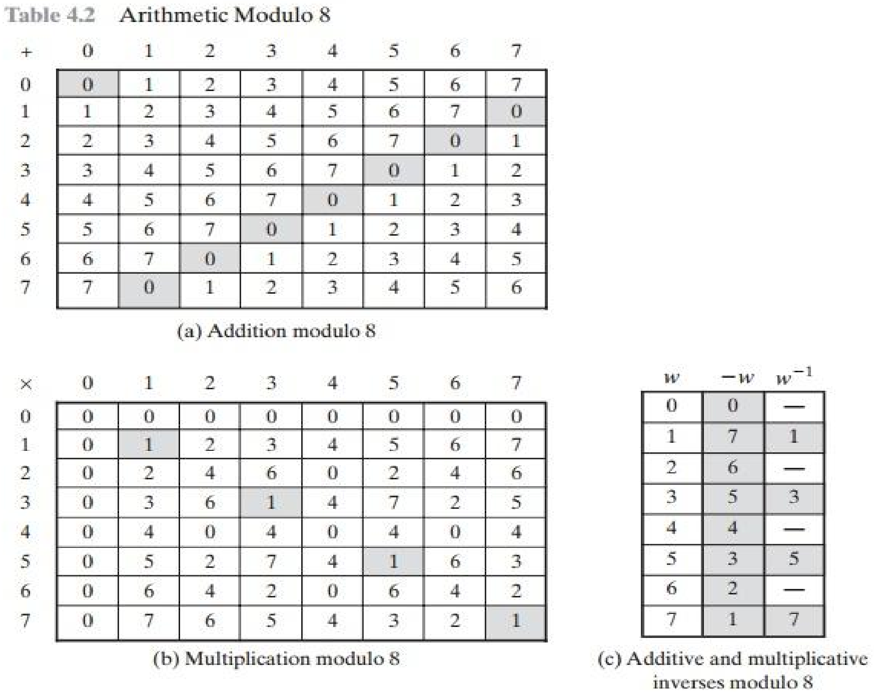


Table 4.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

Table 3Arithmetic Modulo 8

(x + y) mod 8 = 0. To find the additive inverse of an integer in the left-hand column, scan across the corresponding row of the matrix to find the value 0; the integer at the top of that column is the additive inverse; thus, (2 + 6) mod 8 = 0. Similarly, the entries in the multiplication table are straightforward. In ordinary arithmetic, there is a multiplicative inverse, or reciprocal, to each integer. In modular arithmetic mod 8, the multiplicative inverse of x is the integer y such that (x * y) mod 8 = 1 mod 8. Now, to find the multiplicative inverse of an integer from the multiplication table, scan across the matrix in the row for that integer to find the value 1; the integer at the top of that column is the multiplicative inverse; thus, (3 * 3) mod 8 = 1. Note that not all integers mod 8 have a multiplicative inverse; more about that later.

Properties of Modular Arithmetic

Define the set Zn as the set of nonnegative integers less than n:

This is referred to as the set of residues, or residue classes (mod n). To be more precise, each integer in Zn represents a residue class. We can label the residue classes (mod n) as

The residue classes (mod 4) are

[0] = { ... , -16, -12, -8, -4, 0, 4, 8, 12, 16, ... }

[1] = { ... , -15, -11, -7, -3, 1, 5, 9, 13, 17, ... }

[2] = { ... , -14, -10, -6, -2, 2, 6, 10, 14, 18, ... }

[3] = { ... , -13, -9, -5, -1, 3, 7, 11, 15, 19, ... }

Of all the integers in a residue class, the smallest nonnegative integer is the one used to represent the residue class. Finding the smallest nonnegative integer to which k is congruent modulo n is called reducing k modulo n.

If we perform modular arithmetic within Zn, the properties shown in Table 4.3 hold for integers in Zn. We show in the next section that this implies that Zn is a com- mutative ring with a multiplicative identity element.

There is one peculiarity of modular arithmetic that sets it apart from ordinary arithmetic. First, observe that (as in ordinary arithmetic) we can write the following:

if (a + b) K (a + c) (mod n) then b K c (mod n) (4.4)

(5 + 23) K (5 + 7) (mod 8); 23 K 7(mod 8)

Equation (4.4) is consistent with the existence of an additive inverse. Adding the additive inverse of a to both sides of Equation (4.4), we have

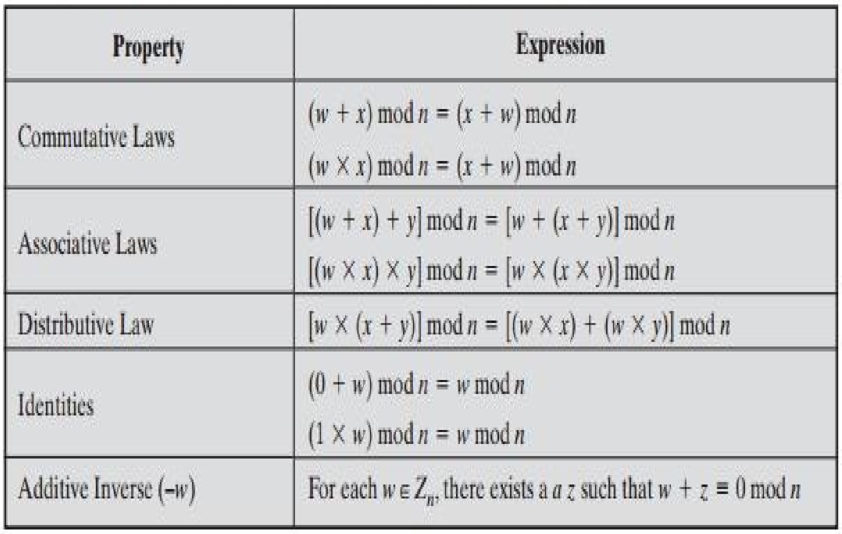
((-a) + a + b) K ((-a) + a + c) (mod n) b K c (mod n)

However, the following statement is true only with the attached condition:

if (a * b) K (a * c) (mod n) then b K c (mod n) if a is relatively prime to n (4.5)

Recall that two integers are relatively prime if their only common positive integer factor is 1. Similar to the case of Equation (4.4), we can say that Equation (4.5) is

Table 4.3 Properties of Modular Arithmetic for Integers in Z_n



Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x + w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse ($-w$)	For each $w \in Z_n$, there exists a a z such that $w + z \equiv 0 \bmod n$

consistent with the existence of a multiplicative inverse. Applying the multiplicative inverse of a to both sides of Equation (4.5), we have

((a - 1)ab) K ((a - 1)ac) (mod n) b K c (mod n)

To see this, consider an example in which the condition of Equation (4.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

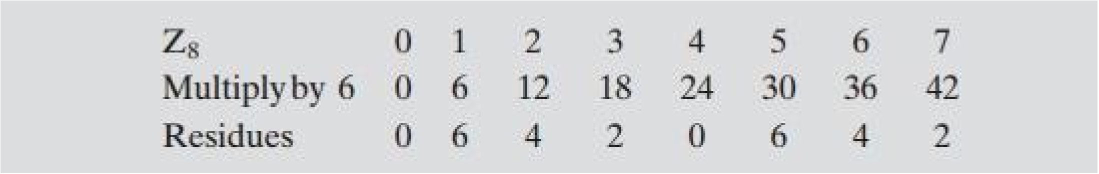
6 * 3 = 18 K 2 (mod 8)

6 * 7 = 42 K 2 (mod 8)

Yet 3 [7 (mod 8).

The reason for this strange result is that for any general modulus n, a multiplier a that is applied in turn to the integers 0 through (n - 1) will fail to produce a complete set of residues if a and n have any factors in common.

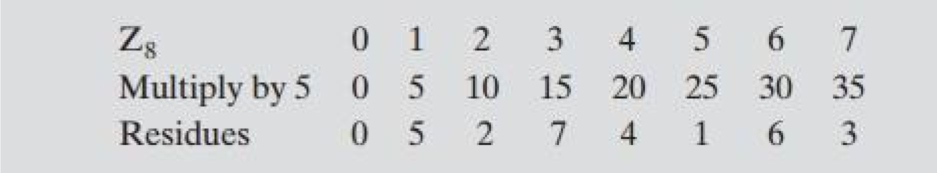
With a = 6 and n = 8,



Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

Because we do not have a complete set of residues when multiplying by 6, more than one integer in Z8 maps into the same residue. Specifically, 6 * 0 mod 8 = 6 * 4 mod 8; 6 * 1 mod 8 = 6 * 5 mod 8; and so on. Because this is a many-to-one mapping, there is not a unique inverse to the multiply operation. However, if we take a = 5 and n = 8, whose only common factor is 1,

However, if we take a = 5 and n = 8, whose only common factor is 1,



Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

The line of residues contains all the integers in Z8, in a different order.

In general, an integer has a multiplicative inverse in Zn if that integer is relatively prime to n. Table 4.2c shows that the integers 1, 3, 5, and 7 have a multiplicative inverse in Z8; but 2, 4, and 6 do not.

Summary

- A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called composite.
- A prime number is a whole number greater than 1.
- It has exactly two factors, that is, 1 and the number itself.
- There is only one even prime number, that is, 2.
- Any two prime numbers are always co-prime to each other.
- Every number can be expressed as the product of prime numbers.

Keywords

***Least common multiple*:** The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

Modular arithmetic: a system of arithmetic for integers, where values reset to zero and begin to increase again, after reaching a certain predefined value, called the modulus (modulo).

Congruence:Congruence is simple, perhaps familiar to you, yet enormously useful and powerful in the study of number theory. If n is a positive integer, we say the integers a and b are congruent modulo n, and write a≡b(modn), if they have the same remainder on division by n.

Self Assessment

1. A Least Common Multiple of a, b is defined as __________

A. It is the smallest integer divisible by both a and b

B. It is the greatest integer divisible by both a and b

C. It is the sum of the number a and b

D. None of the mentioned

2.The LCM of two number 1, b(integer) are _________

A. b + 2

B. 1

C. b

D. None of the mentioned

3. LCM of 6, 10 is?

A. 60

B. 30

C. 10

D. 6

4 The product of two numbers are 12 and their Greatest common divisor is 2 then LCM is?

A. 12

B. 2

C. 6

D. None of the mentioned

5. The number of factors of prime numbers are ___________

A. 2
B. 3
C. Depends on the prime number
D. None of the mentioned

6. What is the number ' 1'?

A. Prime number
B. Composite number
C. Neither Prime nor Composite
D. None of the mentioned

7. Sum of two different prime number is a ____________

A. Prime number
B. Composite number
C. Either Prime or Composite
D. None of the mentioned

8. The product of two numbers are 12 and there LCM is 6 then HCF is?

A. 12
B. 2
C. 6
D. None of the mentioned

9. The HCF of two prime numbers a and b is _________

A. a⁄b
B. ab
C. a + b
D. 1

10. Which one of the following numbers is divisible by 2?

A. 15
B. 29
C. 18
D. 37

11. Which one of the following numbers is divisible by both 2 and 5?

A. 21

B. 30

C. 35

D. 36

12. The greatest common factor of 18, 30, 45 is

A. 3

B. 5

C. 6

D. 9

13. Find the least common multiple l.c.m. of following 3 numbers:

15, 25, 45

A. 125
B. 150
C. 175
D. 225

14. Find the least common multiple l.c.m. of following 3 numbers:

24, 36, 48

A. 96
B. 108
C. 144
D. 172

15. The greatest common factor of 90, 150, 225 is

A. 10

B. 15

C. 18

D. 25

Answers for Self Assessment

1.	A	2.	C	3.	B	4.	B	5.	A
6.	C	7.	C	8.	B	9.	D	10.	C
11.	B	12.	A	13.	D	14.	C	15.	B

Review Questions

1. Explain Divisibility and Divisibility algorithm with help of appropriate example.
2. Differentiate between prime number and composite number with example.
3. What are the properties of prime number?
4. Explain with the help of an example the Euclidean Algorithm for finding Greatest Common factor.

Further Reading

Http://cslabcms.nju.edu.cn/problem_solving/images/3/3e/Discrete_Mathematics_and_Its_Applications_%287th_Edition%29.pdf

Web Links

https://www.math.wustl.edu/~matkerr/NTCbook.pdf

Unit 04: Basic of Cryptography

CONTENTS

Objectives

- understand the basic concept of Cryptography.
- acquire knowledge about types of Cryptography.
- Apply different cryptographic techniques
- Analyze the use of these techniques in Information Security

Introduction

Cryptography, or the art and science of encrypting sensitive information, was once exclusive to the realms of government, academia, and the military. However, with recent technological advancements, cryptography has begun to permeate all facets of everyday life. Everything from your smartphone to your banking relies heavily on cryptography to keep your information safe and your livelihood secure.

And unfortunately, due to the inherent complexities of cryptography, many people assume that this is a topic better left to black hat hackers, multi-billion dollar conglomerates, and the NSA.

But nothing could be further from the truth.With the vast amounts of personal data circulating the Internet, it is more important now than ever before to learn how to successfully protect yourself from individuals with ill intentions.

4.1 What is Cryptography?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Figure 1 Introduction to Cryptography

Cryptography is a technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

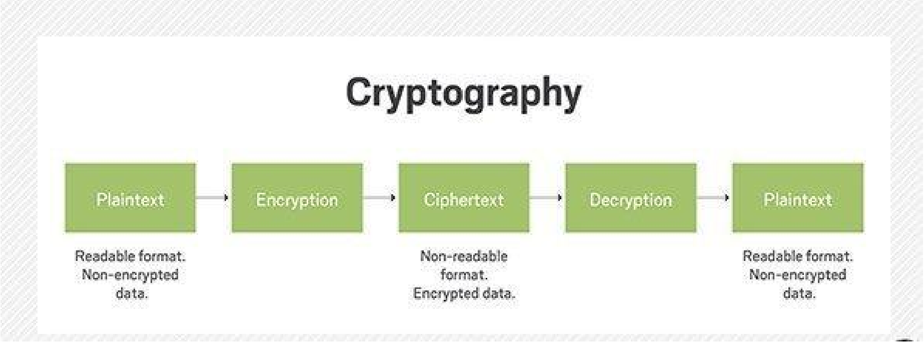

Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

Figure 2 Cryptography process

What is cryptology?

Cryptology is the mathematics, such as number theory and the application of formulas and algorithms,that underpin cryptography and cryptanalysis. Cryptanalysis concepts are highly specialized and complex, so this discussion will concentrate on some of the key mathematical concepts behind cryptography, as well as modern examples of its use.

In order for data to be secured for storage or transmission, it must be transformed in such a manner that it would be difficult for an unauthorized individual to be able to discover its true meaning. To do this, security systems and software use certain mathematical equations that are very difficult to solve unless strict criteria are met. The level of difficulty of solving a given equation is known as its intractability. These equations form the basis of cryptography.

Modern cryptology examples

Today, researchers use cryptology as the basis for encryption in cybersecurity products and systems that protect data and communications. A few examples of modern applications include the following.

Symmetric-key cryptography. Symmetric-key cryptography, sometimes referred to as secret-key cryptography, uses the same key to encrypt and decrypt data. Encryption and decryption are inverse operations, meaning the same key can be used for both steps. Symmetric-key cryptography's most common form is a shared secret system, in which two parties have a shared piece of information, such as a password or passphrase, that they use as a key to encrypt and decrypt information to send to each other.

Public-key cryptography. Public-key cryptography is a cryptographic application that involves two separate keys -- one private and one public. While both keys are mathematically related to one another, only the public key can be used to decrypt what has been encrypted with the private key. The most well-known application of public-key cryptography is for digital signatures, which allow users to prove the authenticity of digital messages and documents. It also makes it possible to establish secure communications over insecure channels.

Cryptanalysis. Cryptanalysis is the practice of analyzing cryptographic systems in order to find flaws and vulnerabilities. For example, cryptanalysts attempt to decrypt ciphertexts without knowledge of the encryption key or algorithm used for encryption. Cryptanalysts use their research results to help to improve and strengthen or replace flawed algorithms.

Cryptographic primitives. A cryptographic primitive in cryptography is a basic cryptographic technique, such as a cipher or hash function, used to construct subsequent cryptographic protocols. In a common scenario, a cryptographic protocol begins by using some basic cryptographic primitives to construct a cryptographic system that is more efficient and secure.

Cryptosystems. Cryptosystems are systems used to encode and decode sensitive information. Cryptosystems incorporate algorithms for key generation, encryption and decryption techniques to keep data secure. The basic principle of a cryptosystem is the use of a ciphertext to transform data held in plaintext into an encrypted message.

4.2 Types of Cryptography

There are four primary types of cryptography in use today, each with its own unique advantages and disadvantages.

They are called hashing, symmetric cryptography, asymmetric cryptography, and key exchange algorithms.

1. Hashing

Hashing is a type of cryptography that changes a message into an unreadable string of text for the purpose of verifying the message’s contents, not hiding the message itself.

This type of cryptography is most commonly used to protect the transmission of software and large files where the publisher of the files or software offers them for download. The reason for this is that, while it is easy to calculate the hash, it is extremely difficult to find an initial input that will provide an exact match for the desired value.

For example, when you download Windows 10, you download the software which then runs the downloaded file through the same hashing algorithm. It then compares the resulting hash with the one provided by the publisher. If they both match, then the download is completed.

However, if there is even the slightest variation in the downloaded file (either through the corruption of the file or intentional intervention from a third party) it will drastically change the resulting hash, potentially nullifying the download.

Currently, the most common hashing algorithms are MD5 and SHA-1, however due to these algorithm’s multiple weaknesses, most new applications are transitioning to the SHA-256 algorithm instead of its weaker predecessors.

2. Symmetric Cryptography

Symmetric Cryptography, likely the most traditional form of cryptography, is also the system with which you are probably most familiar.

This type of cryptography uses a single key to encrypt a message and then decrypt that message upon delivery.Since symmetric cryptography requires that you have a secure channel for delivering the crypto key to the recipient, this type of cryptography is all but useless for transmitting data (after all, if you have a secure way to deliver the key, why not deliver the message in the same manner?).

As such, its primary application is the protection of resting data (e.g. Hard Drives and data bases)

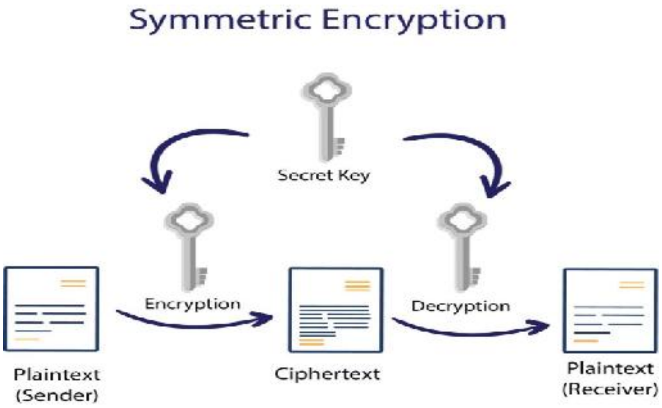


Figure 3Symmetric Encryption and Decryption process

In the Revolutionary War example that I mentioned earlier, Washington's method for transmitting information between his officers would have relied on a symmetric cryptography system. He and all of his officers would have had to meet in a secure location, share the agreed upon key, and then encrypt and decrypt correspondence using that same key. Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypts the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

3. Asymmetric Cryptography

Asymmetric cryptography (as the name suggests) uses two different keys for encryption and decryption, as opposed to the single key used in symmetric cryptography.The first key is a public key used to encrypt a message, and the second is a private key which is used to decrypt them. The great part about this system is that only the private key can be used to decrypt encrypted messages sent from a public key.While this type of cryptography is a bit more complicated, you are likely familiar with a number of its practical applications.

It is used when transmitting email files, remotely connecting to servers, and even digitally signing PDF files. Oh, and if you look in your browser and you notice a URL beginning with "https://", that's a prime example of asymmetric cryptography keeping your information safe.

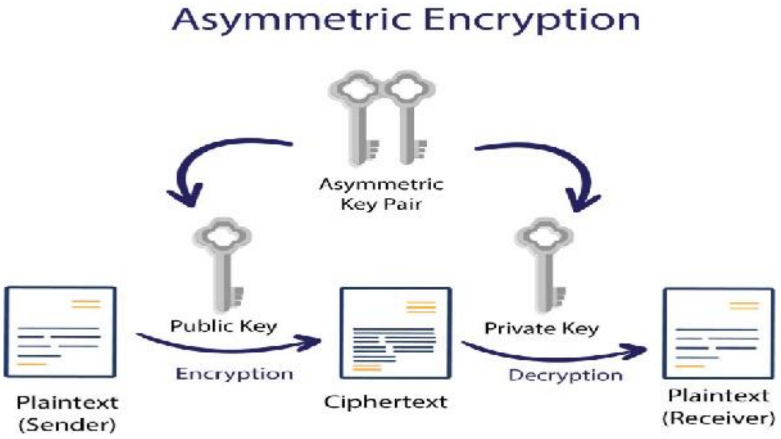


Figure 4Asymmetric Encryption and Decryption

Key Exchange Algorithms

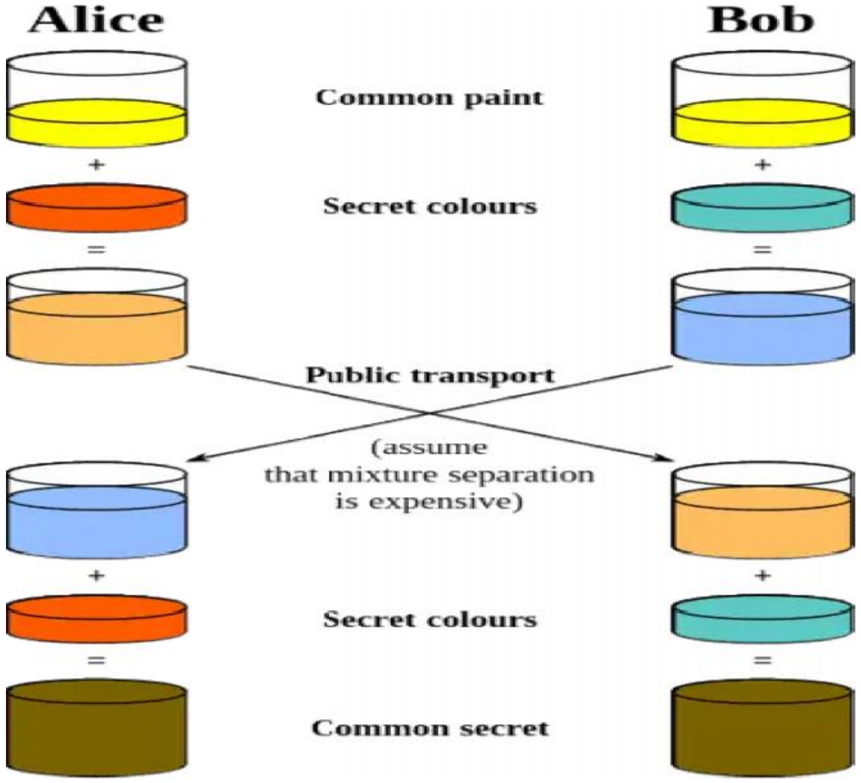
Although this particular type of cryptography isn't particularly applicable for individuals outside of the cyber-security realm, I wanted to briefly mention to ensure you have a full understanding of the different cryptographic algorithms.A key exchange algorithm, like Diffie-Hellman, is used to safely exchange encryption keys with an unknown party.

Unlike other forms of encryption, you are not sharing information during the key exchange. The end goal is to create an encryption key with another party that can later be used with the aforementioned forms of cryptography.

Here's an example from the Diffie-Hellman wiki to explain exactly how this works.

Let's say we have two people, Alice and Bob, who agree upon a random starting color. The color is public information and doesn't need to be kept secret (but it does need to be different each time). Then Alice and Bob each selects a secret color that they do not share with anyone.

Now, Alice and Bob mix the secret color with the starting color, resulting in their new mixtures. They then publicly exchange their mixed colors. Once the exchange is made, they now add their own private color into the mixture they received from their partner, and the resulting in an identical shared mixture.



4.3 The 4 Types of Cryptographic Functions

So now that you understand a little bit more about the different types of cryptography, many of you are probably wondering how it is applied in the modern world.

There are four primary ways that cryptography is implemented in information security. These four applications are called "cryptographic functions".

1. Authentication

When we use the right cryptographic system, we can establish the identity of a remote user or system quite easily. The go-to example of this is the SSL certificate of a web server which provides proof to the user that they are connected to the right server.

The identity in question is not the user, but rather the cryptographic key of that user. Meaning that the more secure the key, the more certain the identity of the user and vice versa.

Here's an example.

Let's say that I send you a message that I have encrypted with my private key and you then decrypt that message using my public key. Assuming that the keys are secure, it is safe to assume that I am the actual sender of the message in question.

If the message contains highly sensitive data, then I can ensure a heightened level of security by encrypting the message with my private key and then with your public key, meaning that you are the only person who can actually read the message and you will be certain the message came from me.The only stipulation here is that the public keys are both associated with their users in a trusted manner, e.g. a trusted directory.

In order to address this weakness, the community created an object called a certificate which contains the issuer's name as well as the name of the subject for whom the certificate is issued. This means that the fastest way to determine if a public key is secure is to note if the certificate issuer also has a certificate too.

An example of this type of cryptography in action is Pretty Good Privacy, or PGP, a software package developed by Phil Zimmerman that provides encryption and authentication for email and file storage applications.

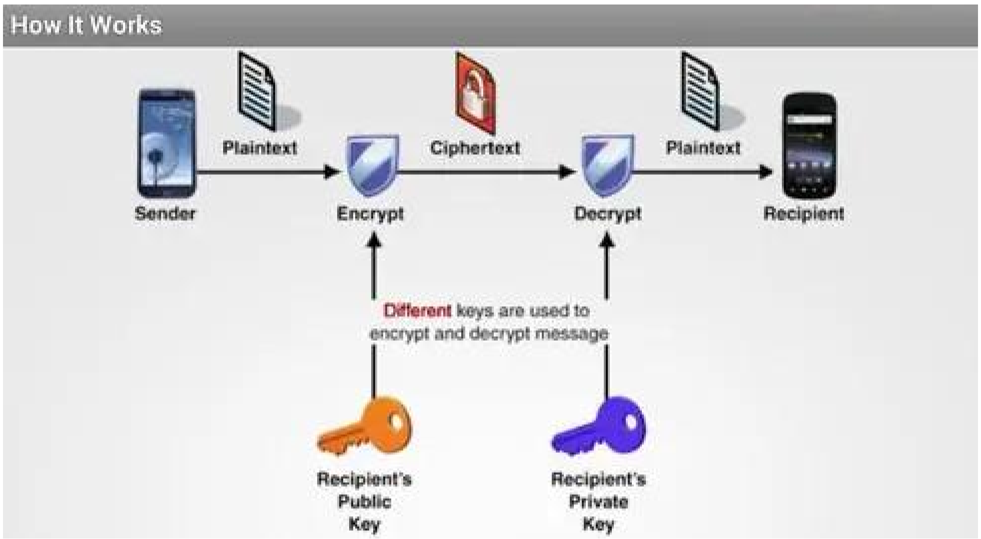


Figure 5 How Pretty Good Privacy

2. Nonrepudiation

This concept is especially important for anyone using or developing financial or e-commerce applications.

One of the big problems that e-commerce pioneers faced was the pervasive nature of users who would refute transactions once they had already occurred. Cryptographic tools were created to ensure that each unique user had indeed made a transaction request that would be irrefutable at a later time.

For example, let's say that a customer at your local bank requests a money transfer to be paid to another account. Later in the week, they claim to have never made the request and demand the full amount be refunded to their account.

However, as long as that bank has taken measures to ensure non-repudiation through cryptography, they can prove that the transaction in question was, in fact, authorized by the user.

3. Confidentiality

With information leaks and a seemingly endless number of privacy scandals making the headlines, keeping your private information, well, private is probably one of your biggest concerns. This is the exact function for which cryptographic systems were originally developed.

With the right encryption tools, users can guard sensitive company data, personal medical records, or just lock their computer with a simple password.

4. Integrity

Another important use of cryptography is to ensure that data is not viewed or altered during transmission or storage.

For example, using a cryptographic system to ensure data integrity ensures that rivaling companies cannot tamper with their competitor’s internal correspondence and sensitive data.

The most common way to do accomplish data integrity through cryptography is by using cryptographic hashes to safeguard information with a secure checksum.

4.4 What is Encryption?

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

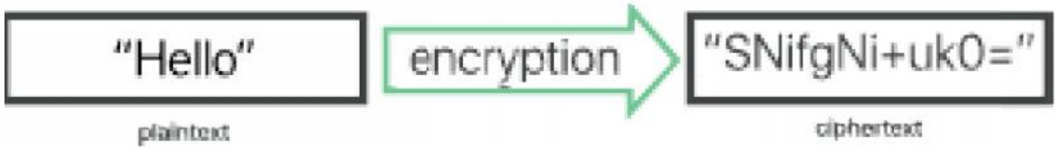


Figure 6 Encryption example

Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by brute force — in other words, by guessing the key.

Data can be encrypted "at rest," when it is stored, or "in transit," while it is being transmitted somewhere

What are Plaintext and Ciphertext? How do they interact?

Plaintext can refer to anything which humans can understand and/or relate to. This may be as simple as English sentences, a script, or Java code. If you can make sense of what is written, then it is in plaintext.

Ciphertext, or encrypted text, is a series of randomized letters and numbers which humans cannot make any sense of. An encryption algorithm takes in a plaintext message, runs the algorithm on the plaintext, and produces a ciphertext. The ciphertext can be reversed through the process of decryption, to produce the original plaintext.

Example: We will encrypt a sentence using Caesar Cipher. The key is 7, which means the letter a becomes h.

Plaintext: This is a plaintext.

Ciphertext: Aopzpz h wshpualea.

What is a key in cryptography?

A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

4.5 What is meant by Decryption?

Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.

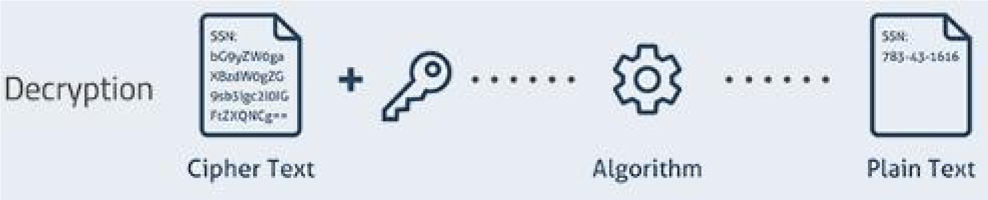


Figure 7 Decryption Process

Key Difference

- Encryption is a process of converting normal data into an unreadable form whereas Decryption is a method of converting the unreadable/coded data into its original form.
- Encryption is done by the person who is sending the data to the destination, but the decryption is done at the person who is receiving the data.
- The same algorithm with the same key is used for both the encryption-decryption processes.

Why use Encryption and Decryption?

Here, are important reasons for using encryption:

- Helps you to protect your confidential data such as passwords and login id
- Provides confidentiality of private information
- Helps you to ensure that that the document or file has not been altered
- Encryption process also prevents plagiarism and protects IP
- Helpful for network communication (like the internet) and where a hacker can easily access unencrypted data.
- It is an essential method as it helps you to securely protect data that you don’t want anyone else to have access.

4.6 Types of Keys

Symmetric Key:

Symmetric-key encryption are algorithms which use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Asymmetric Key:

Asymmetric encryption uses 2 pairs of key for encryption. Public key is available to anyone while the secret key is only made available to the receiver of the message. This boots security.

Public Key:

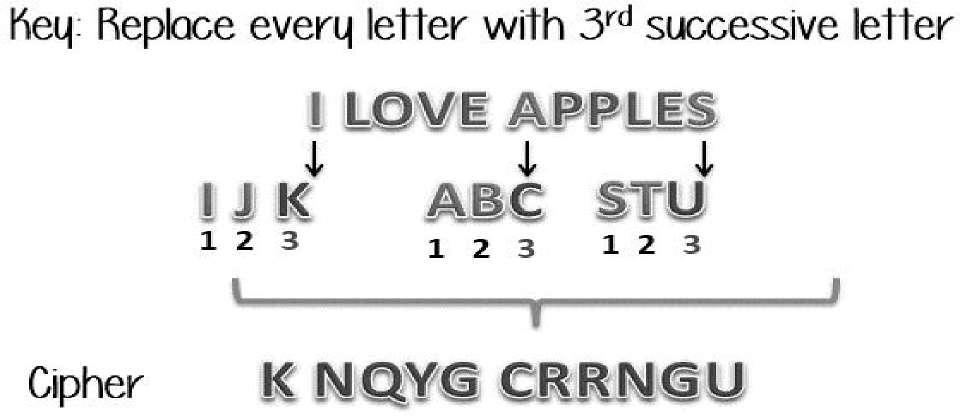
Public key cryptography is an encryption system which is based on two pairs of keys. Public keys are used to encrypt messages for a receiver.

Private Key:

Private key may be part of a public/ private asymmetric key pair. It can be used in asymmetric encryption as you can use the same key to encrypt and decrypt data.

Pre-Shared Key:

In cryptography, a pre-shared key (PSK) is a shared secret which was earlier shared between the two parties using a secure channel before it is used.



4.7 Different Types of Cryptography Attacks

Cryptography involves hiding the information to be transmitted so that only the receiver is able to view it. This is done by encoding the information to be sent at the sender's end and decoding the information on the receiver's end.

The field of cryptography is an old one and dates back to 2000 B.C. in Egypt. Let us have a brief look at the basic working of cryptography before moving onto the different types of attacks:

1. The text that is to be transmitted which can be commonly read is known as **'plaintext'**.
2. This plaintext is converted to unreadable format by the process of encryption and it is then known as '**Ciphertext'.**
3. This ciphertext can now be transmitted over insecure channels confidently without the danger of snooping. Once it has been successfully transmitted, it has to be decrypted at the receiver's end and the '**plaintext**' is again recovered.
4. An algorithm is a complex mathematical formula that aids in encrypting the information along with the "**key".**
5. The **"key"** is a long sequence of bits which is used to encrypt and decrypt the text.

This is the basic and fundamental concept behind cryptography. There are two modes of encryption – symmetric encryption and asymmetric encryption.

In '**Symmetric encryption'** algorithms, the same key which is used to encrypt is used to decrypt a message.

In '**Asymmetric encryption'** algorithms, different keys are used to encrypt and decrypt a message.

Cryptography ensures that the information that is sent safely and securely, preserves the concept of confidentiality, integrity, and authenticity. Having seen, the basics of cryptography and the different types of encryption, let us next view the different types of attacks that are possible.

There are two types of attacks – 'passive attacks' and 'active attacks'. Snooping on data, eavesdropping is simple examples of 'passive attacks'. Passive attacks are not as harmful as they do not cause any altering or modification of data. 'Active attacks' cause data to be altered, system files to be modified and are obviously much more harmful than 'passive attacks'.

These are some examples of 'active attacks':

4.8 Brute Force Attacks

Brute-force attacks involve trying every possible character combination to find the 'key' to decrypt an encrypted message. While brute-force attacks may take a smaller amount of time for smaller keyspaces, it will take an immeasurable amount of time for larger key spaces. Hence it is impractical to try brute-force attacks modern encryption systems.

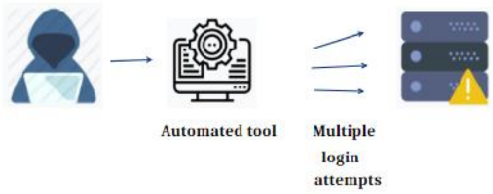
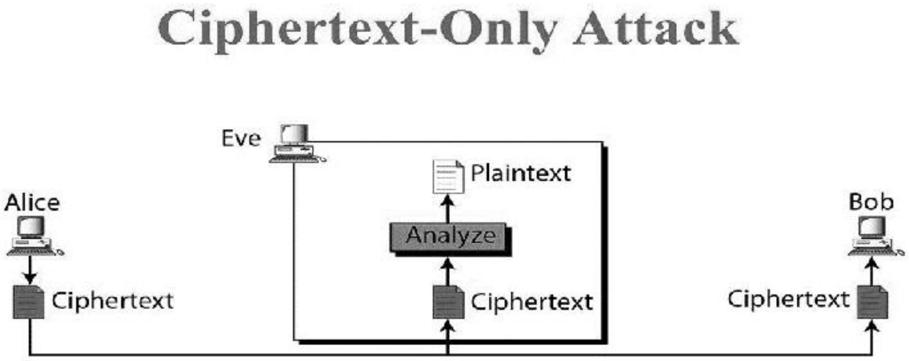


Figure 8 Brute-Force attack

Cipher-only attack

In the 'cipher-only' attack, the attacker knows the ciphertext of various messages which have been encrypted using the same encryption algorithm. The attacker's challenge is to figure the 'key' which can then be used to decrypt all messages.

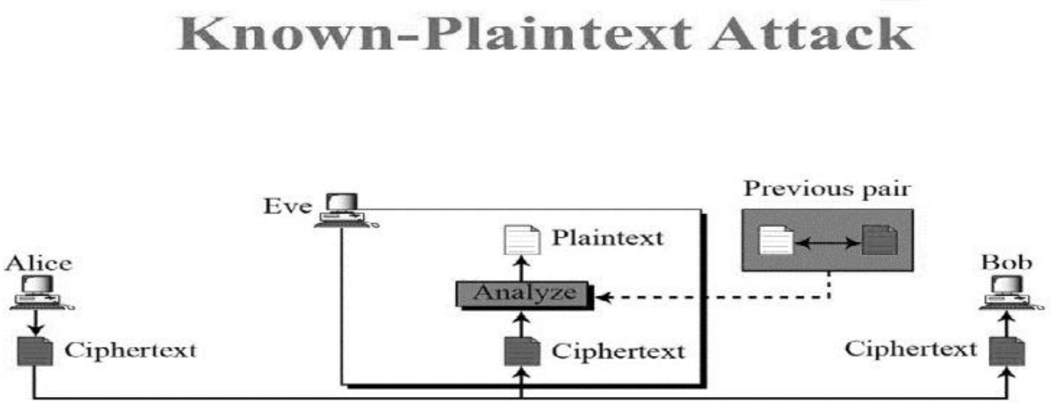
The 'cipher-only' attack is probably one of the easiest attacks to commit since it is easy to capture the ciphertext (by sniffing) but difficult to implement since the knowledge about the encryption process is limited.



Known-plaintext attack

In the 'known-plaintext' attack, the attacker knows some of the plaintext and the ciphertext. He then has to figure the 'key' by reverse engineering and he can decipher other messages which use the same 'key' and algorithm.

The 'known-plaintext' attack was effective against simple ciphers such as the 'substitution cipher'. It was popular for breaking ciphers used during the Second World War.



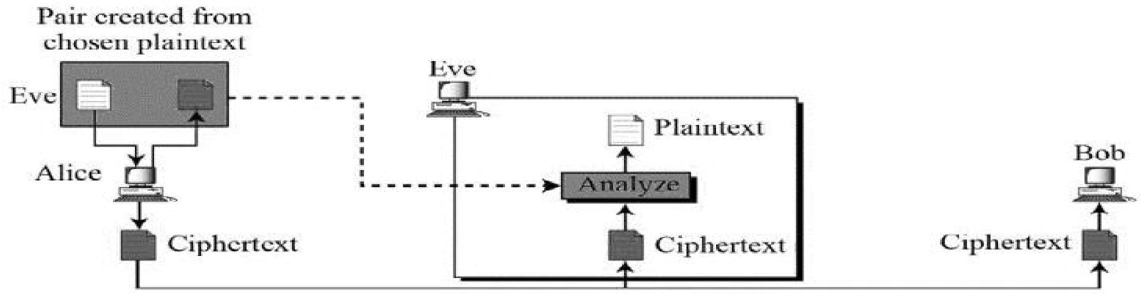
Chosen plaintext attack

The ‘chosen-plaintext’ attack is similar to the ‘known-plaintext’ attack, but here the attacker experiments by choosing his own plaintext (say choosing a word such as ‘cryptography’) for a ‘Vignere cipher’ and with the generated ciphertext he can figure the ‘key’.

Once he figures the ‘key’ he can learn more about the whole encryption process and understand how the ‘key’ is being used.

With this information, he can decrypt other messages.

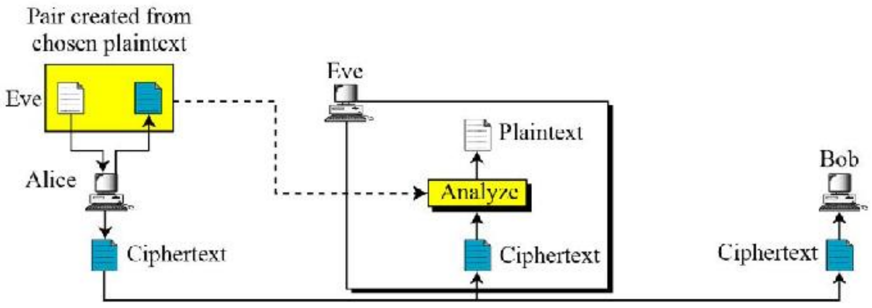
Chosen-Plaintext Attack



Chosen ciphertext attack

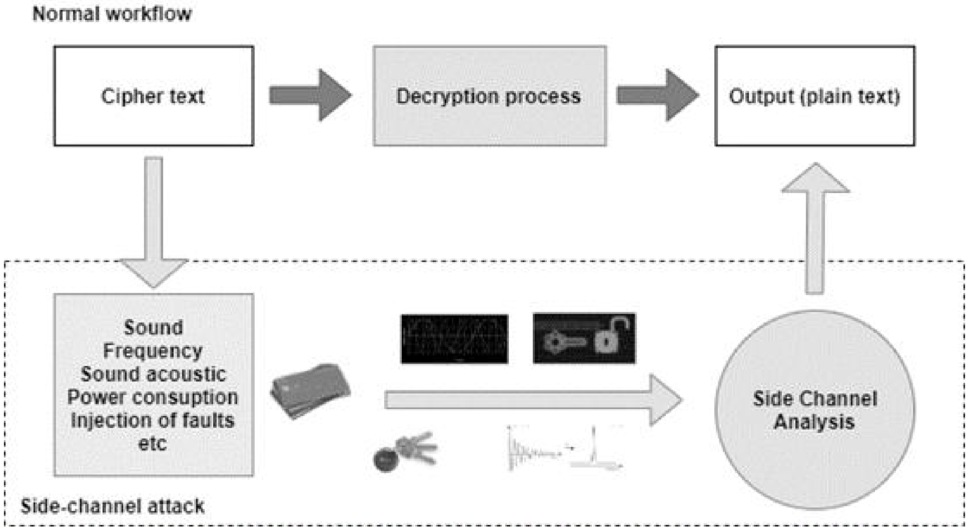
In the ‘chosen ciphertext’ attack, the attacker chooses a portion of the decrypted ciphertext. He then compares the decrypted ciphertext with the plaintext and figures out the key.This is relatively a harder type of attack and earlier versions of RSA were subject to these types of attacks.

Chosen-plaintext attack



Side channel attacks

Apart from just relying on mathematical ways to break into systems, attackers may use other techniques such as observing power consumption, radiation emissions and time for data processing. With this data, the attacker works in a reverse manner to figure the ‘keys’ to an algorithm just by observing the amount of heat released in an attack.



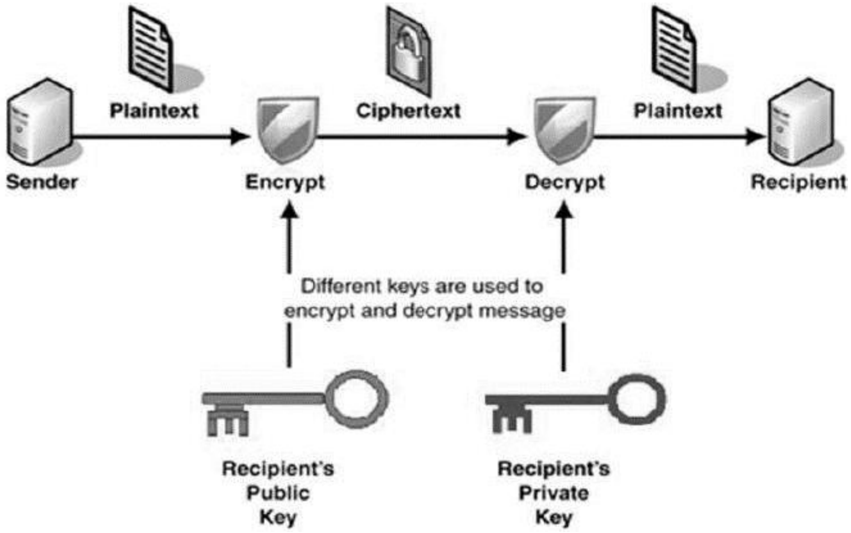
4.9 Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration –



The most important properties of public key encryption scheme are −

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves

trusted third party which certifies that a particular public key belongs to a specific person or entity only.

- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Summary

- Cryptography is used to secure and protect data during communication.
- Encryption is a process which transforms the original information into an unrecognizable form.
- Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer.
- Encryption method helps you to protect your confidential data such as passwords and login id.
- Public, Private, Pre-Shared and Symmetric are important keys used in cryptography.
- An employee is sending essential documents to his/her manager is an example of an encryption method.
- The manager is receiving the essential encrypted documents from his/her employee and decrypting it is an example of a decryption method.

Keywords

- **Cryptography**: Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
- **Encryption:** The process of converting original text into coded form.
- **Decryption:** The method of recovering original text from coded text.
- **Cryptanalysis:** the study of principles/ methods of deciphering ciphertext without knowing key.
- **Symmetric Key :**Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure
- **Asymmetric Key Encryption**:Asymmetric Key Encryption is based on public and private key encryption technique. It uses two different key to encrypt and decrypt the message.
- **Digital signatures -** content is digitally signed with an individual’s private key and is verified by the individual’s public key
- **Authentication –** since the individual’s unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature.
- **Non-repudiation –** since the individual is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn’t him/her who applied the signature.
- **Integrity -** when the signature is verified, it checks that the contents of the document or message match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail.

Self Assessment

1. In cryptography, what is cipher?

A. algorithm for performing encryption and decryption
B. encrypted message
C. both algorithm for performing encryption and decryption and encrypted message
D. decrypted message

2.In asymmetric key cryptography, the private key is kept by __________

A. sender
B. receiver
C. sender and receiver
D. all the connected devices to the network

3. Which of the following is not a principle of data security?

A. Data Confidentiality
B. Data Integrity
C. Authentication
D. None of the above

4. Which of the following options correctly defines the Brute force attack?

A. Brutally forcing the user to share the useful information like pins and passwords.
B. Trying every possible key to decrypt the message.
C. One entity pretends to be some other entity
D. The message or information is modified before sending it to the receiver.

5. A mechanism used to encrypt and decrypt data.

A. Cryptography
B. Algorithm
C. Data flow
D. None of these

6. Security Goals of Cryptography are

A. Confidentiality
B. Authentication
C. Non-repudiation
D. All of these

7. Cipher in cryptography is –

A. Encrypted message
B. Algorithm for performing encryption and decryption
C. Both algorithm for performing encryption and decryption and encrypted message
D. Decrypted message

8.The private key in asymmetric key cryptography is kept by

A. Sender
B. Receiver
C. Sender and receiver
D. All the connected devices to the network

9. Cryptanalysis is used __________

A. to find some insecurity in a cryptographic scheme
B. to increase the speed
C. to encrypt the data
D. to make new cipher

10. In symmetric-key cryptography, the key locks and unlocks the box is

A. same
B. shared
C. c)private
D. public

11. The keys used in cryptography are

A. a)secret key
B. b)private key
C. c)public key
D. d)All of them

12. Cryptography, a word with Greek origins, means

A. Corrupting Data
B. Secret Writing
C. c)Open Writing
D. d)Closed Writing

13. ____ is the message or data that can be readable by the sender.

A. Edited
B. Main Text
C. Plain text
D. All of the mentioned above

14. Cryptography term is used to transforming messages to make them secure and to prevent from

A. Change
B. Defend
C. Idle

D. Attacks

15. What is cipher in Cryptography ?

A. Algorithm for performing encryption
B. Algorithm for performing decryption
C. Encrypted Messages
D. Both algorithm for performing encryption and Decryption and encrypted message

Review Questions

1. Define Cryptography.
2. Discuss different techniques used for Cryptography.
3. Write down the difference between Symmetric and Asymmetric encryption.
4. Explain in detail Symmetric Encryption with the help of diagram
5. Explain in detail Asymmetric Encryption with the help of diagram
6. Explain different types of cryptography attacks.
7. Define Hashing.

Answers for Self Assessment

1.	A	2.	B	3.	D	4.	B	5.	A
6.	D	7.	B	8.	B	9.	A	10.	A
11.	D	12.	B	13.	C	14.	D	15.	D

Further Readings

https://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf

Web Links

https://www.tutorialspoint.com/what-is-cryptography-in-computer-network

Unit 05: Cryptography Techniques

CONTENTS

Objectives

- Understand the concept of Cryptography
- Acquire knowledge about cryptography techniques
- Implement different ciphers using examples
- Evaluate the working of cryptographic techniques

Introduction

The word "cryptography" is derived from the Greek kryptos, meaning hidden. The prefix "crypt-"means "hidden" or "vault," and the suffix "-graphy" stands for "writing."The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few.

The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not want certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems.

However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

5.1 What is cryptography?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

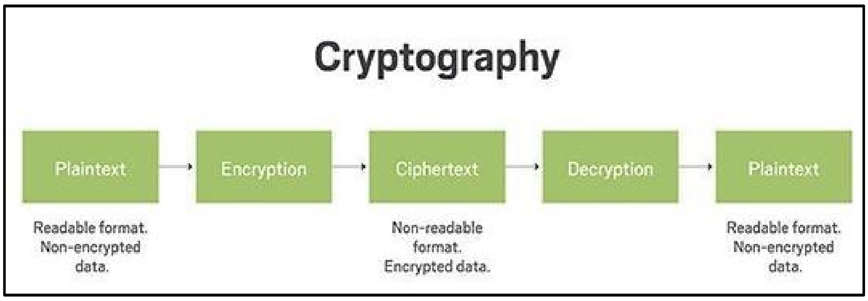
Cryptography deals with various security principles, which are as follows:

Confidentiality – It specifies that only the sender and the recipient or recipients should be able to access the message. Confidentiality will get lost if an authorized person can access a message.

Authentication – It identifies a user or a computer system so that it can be trusted.

Integrity – It checks that a message's contents must not be altered during its transmission from the sender to the recipient.

Non-repudiation – It specifies that the sender of a message cannot be refused having sent it, later on, in the case of a dispute.


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

5.2 Cryptography Techniques

Various cryptography techniques have been developed to provide data security to ensure that the data transferred between communication parties is confidential, not modified by an unauthorized party, to prevent hackers from accessing and using their information. Caesar cipher, monoalphabetic cipher, homophonic substitution cipher, Polyalphabetic Cipher, Playfair cipher, rail fence, One-time pad, hill cipher are some of the examples of cryptography techniques.

Classical Ciphers

Classical ciphers are often divided into transposition ciphers and substitution ciphers.

Substitution Cipher

A well-known example of a substitution cipher is the Caesar cipher. To encrypt a message with the Caesar cipher, each letter of message is replaced by the letter three positions later in the alphabet. Hence, A is replaced by D, B by E, C by F, etc. Finally, X, Y and Z are replaced by A, B and C respectively. Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

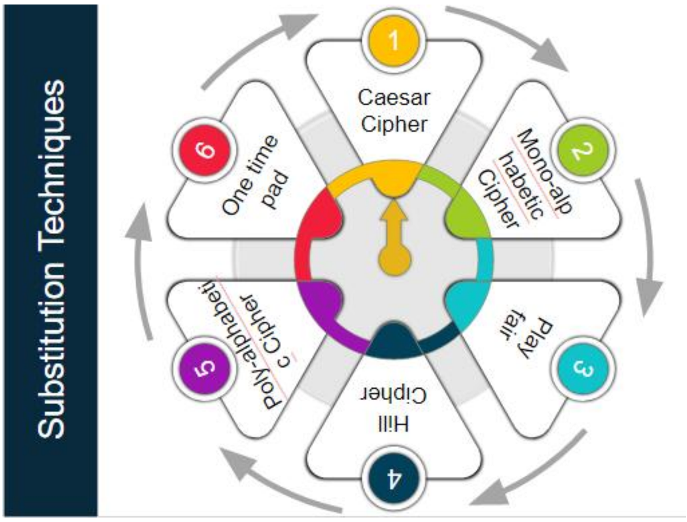


Figure 1 types of Substitution Ciphers

Caesar Cipher

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

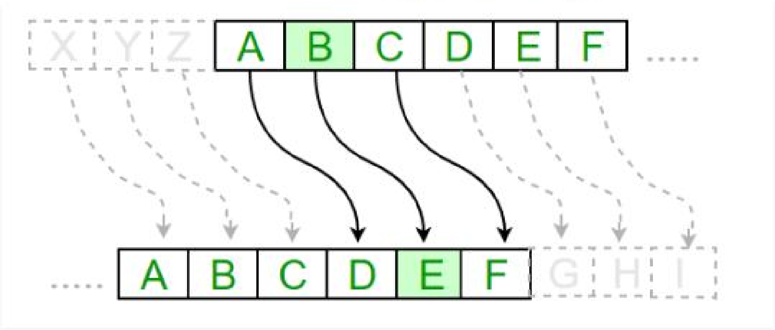
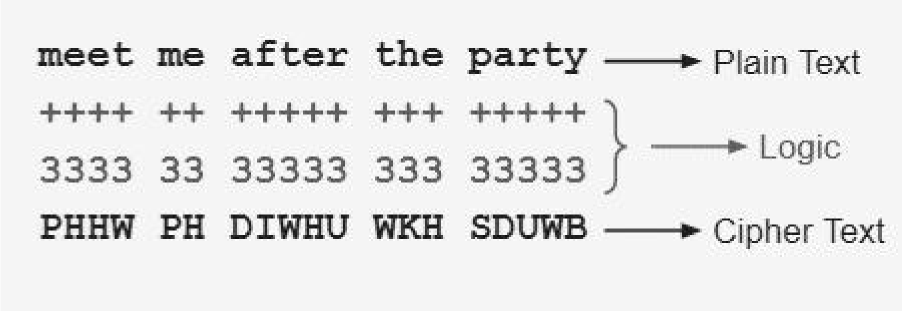


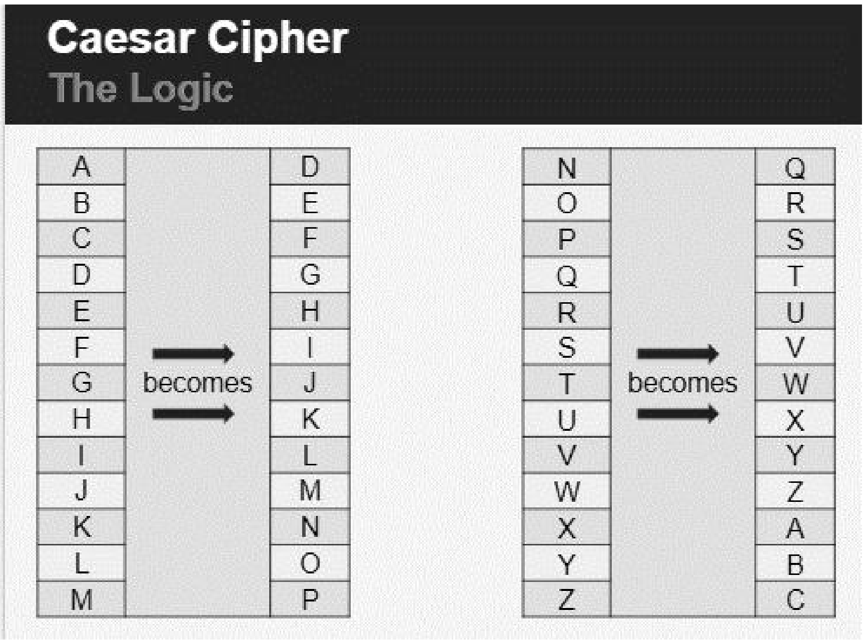
Figure 2 Caesar Cipher

Task: Using Caesar Cipher convert this cipher text into plain text "**Jxhvvzkdw lv zulwwhqehorz**"

Example



```
meet me after the party
++++ ++ +++++ +++ +++++
3333 33 33333 333 33333
PHHW PH DIWHU WKH SDUWB
```



Caesar Cipher

The Logic

A		D	N		Q
B		E	O		R
C		F	P		S
D		G	Q		T
E		H	R		U
F		I	S		V
G	becomes	J	T	becomes	W
H		K	U		X
I		L	V		Y
J		M	W		Z
K		N	X		A
L		O	Y		B
M		P	Z		C

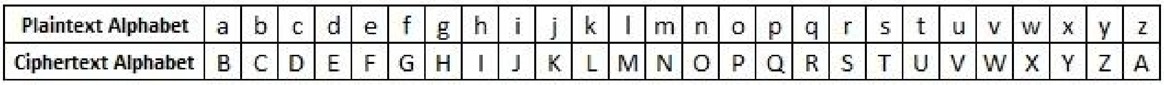
Figure 3 Caesar Cipher Logic

5.3 Monoalphabetic Substitution Ciphers

Substitution ciphers are probably the most common form of cipher. They work by replacing each letter of the plaintext (and sometimes puntuation marks and spaces) with another letter (or possibly even a random symbol).

A monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJNQMF NFTTBHF". In general, when performing a simple substitution manually, it is easiest to generate the ciphertext alphabet first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.

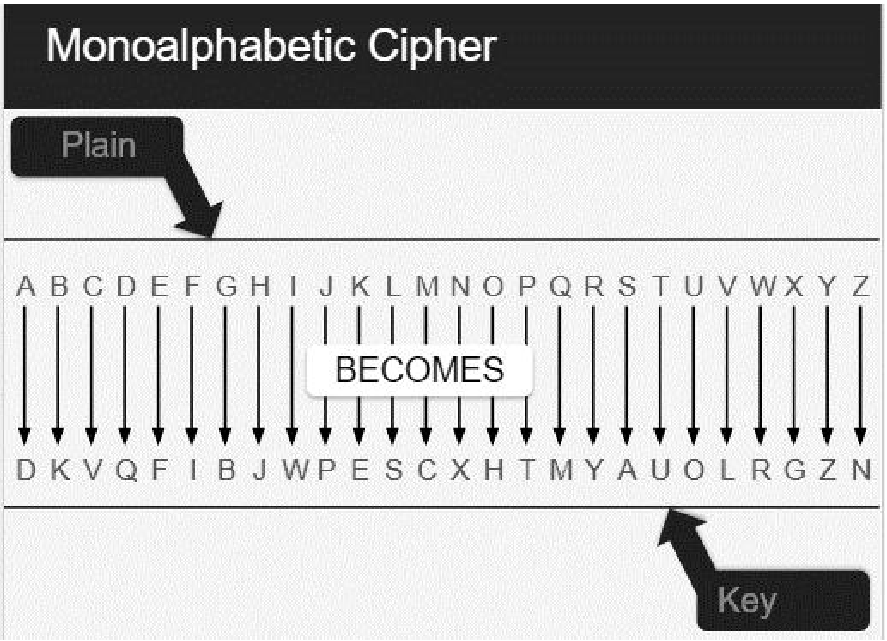


Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

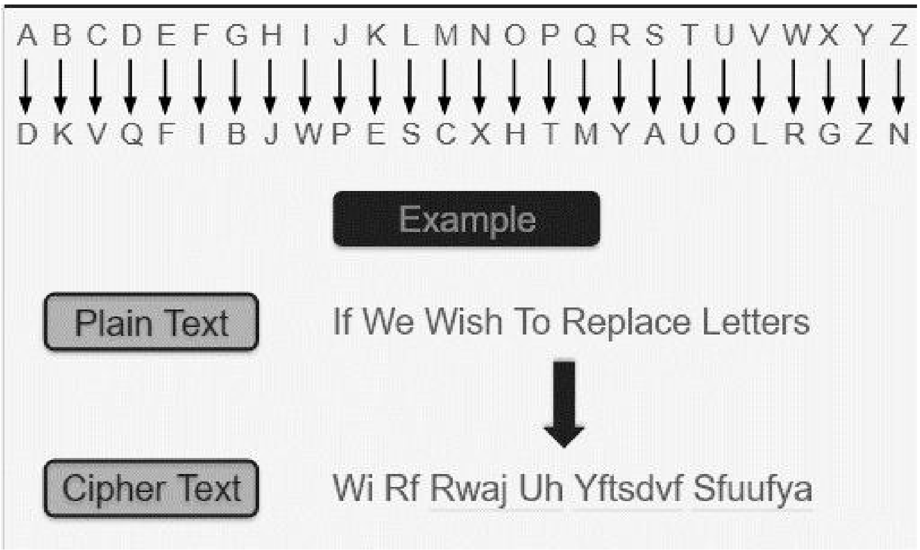
Figure 4The ciphertext alphabet for the cipher where you replace each letter by the next letter in the alphabet

There are many different monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter.

The history of simple substitution ciphers can be traced back to the very earliest civisilisations, and for a long time they were more than adequate for the purposes for which they were needed. By today's standards they are very weak, and incredibly easy to break, but they were a very important step in developing cryptography.


Monoalphabetic Cipher
Plain
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
BECOMES
D K V Q F I B J W P E S C X H T M Y A U O L R G Z N
Key

Example

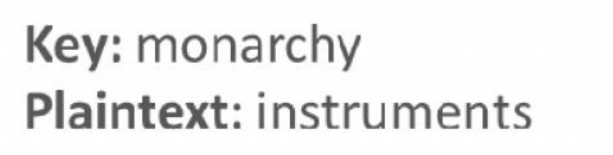

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D K V Q F I B J W P E S C X H T M Y A U O L R G Z N
Example
Plain Text
If We Wish To Replace Letters
Cipher Text
Wi Rf Rwaj Uh Yftsdvf Sfuufya

Playfair Cipher

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

Example:



Key: monarchy
Plaintext: instruments

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1.**Generate the key**Square(5×5): The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2.**Algorithm to encrypt** the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText**: "instruments"**	After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Here ‘x’ is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

Here ‘z’ is the bogus letter.

Rules for Encryption:

1. If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:

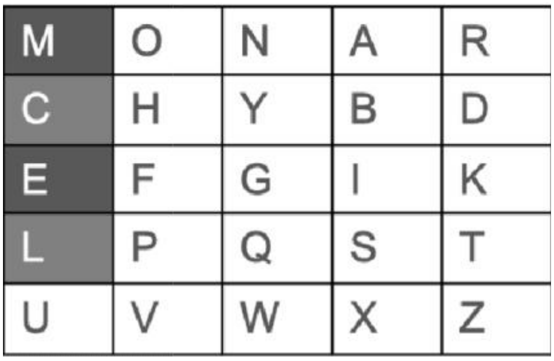
Diagraph: "me"

Encrypted Text: cl

Encryption:

m -> c

e -> l



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:

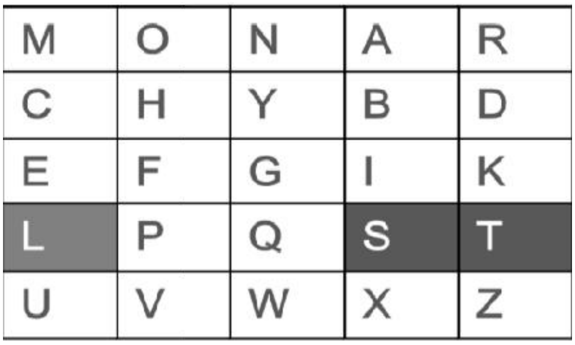
Diagraph: "st"

Encrypted Text: tl

Encryption:

s -> t

t -> l



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizon

For example:

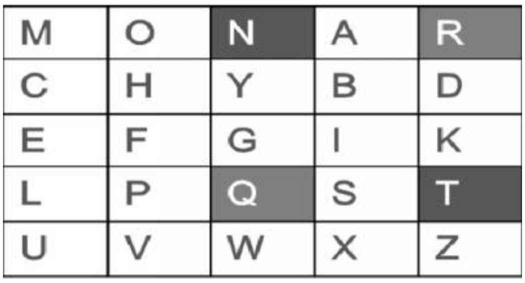
Diagraph: "nt"

Encrypted Text: rq

Encryption:

n -> r

t ->qtal opposite corner of the rectangle



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "instrumentsz"

Encrypted Text: gatlmzclrqtx

Encryption:

i -> g

n -> a

s -> t

t -> l

r -> m

u -> z

m -> c

e -> l

n -> r

t -> q

s -> t

z -> x

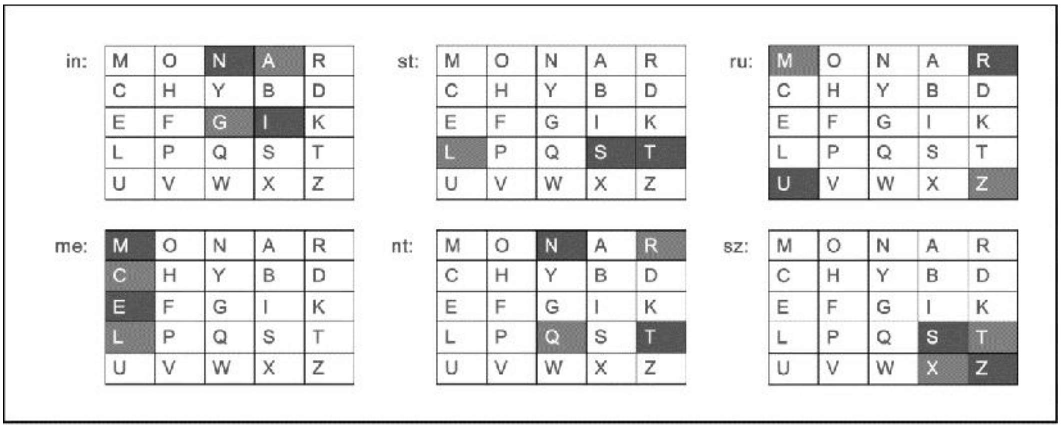


Figure 5Playfair Cipher

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Example

Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

Input : Plaintext: GFG

Key: HILLMAGIC

Output : Ciphertext: SWK

Encryption

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'

Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Vigenère Cipher

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.

The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

The alphabet used at each point depends on a repeating keyword.

Example

Input : Plaintext : GEEKSFORGEEKS

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

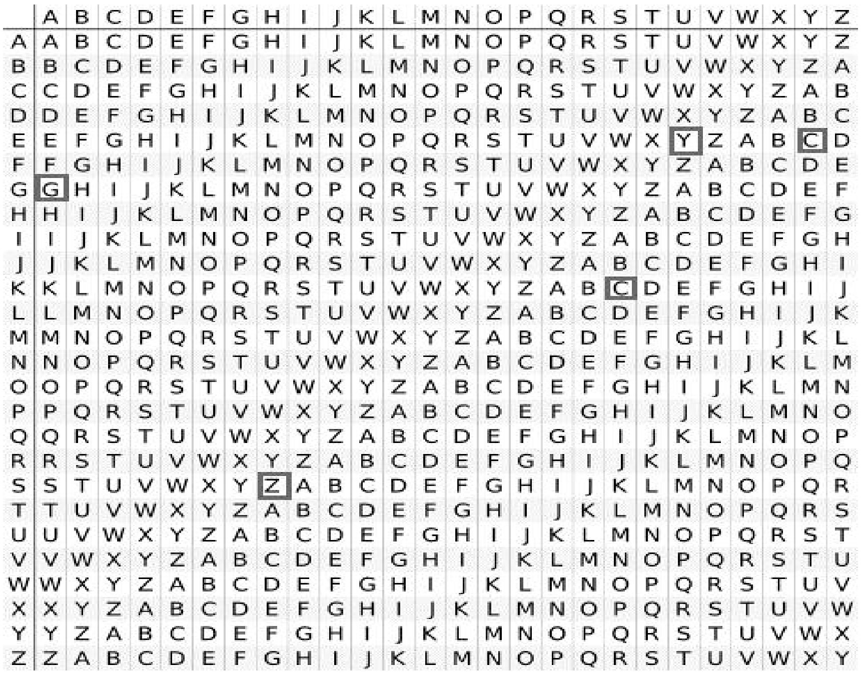
For generating key, the given keyword is repeated
in a circular manner until it matches the length of
the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

The plain text is then encrypted using the process explained below.

Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E, and column Y is C. The rest of the plaintext is enciphered in a similar fashion.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next, we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

A more easy implementation could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

Encryption

The plaintext(P) and key(K) are added modulo 26.

Ei = (Pi + Ki) mod 26

Decryption

Di = (Ei - Ki + 26) mod 26

Note: Di denotes the offset of the i-th character of the plaintext. Like offset of A is 0 and of B is 1 and so on.

Transposition Cipher

Transposition technique is an encryption method which is achieved by performing permutation over the plain text. Mapping plain text into cipher text using transposition technique is called transposition cipher.

In this section, we will discuss variations of transposition technique, and we will also observe how the transposition technique is different from the substitution technique.

On the one hand, the substitution technique substitutes a plain text symbol with a cipher text symbol. On the other hand, the transposition technique executes permutation on the plain text to obtain the cipher text.

5.4 Transposition Techniques

- Rail Fence Transposition
- Columnar Transposition
- Improved Columnar Transposition
- Book Cipher/Running Key Cipher

Rail Fence Cipher

The rail fence cipher is the simplest transposition cipher. The steps to obtain cipher text using this technique are as follow:

Step 1: The plain text is written as a sequence of diagonals.

Step 2: Then, to obtain the cipher text the text is read as a sequence of rows.

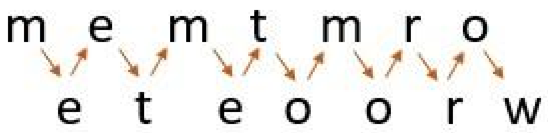
To understand this in a better way, let us take an example:

Plain Text: meet me Tomorrow

Now, we will write this plain text sequence wise in a diagonal form as you can see below:

Looking at the image, you would get it why it got named rail fence because it appears like the rail fence.

Once you have written the message as a sequence of diagonals, to obtain the cipher text out of it you have to read it as a sequence of rows. So, reading the first row the first half of cipher text will be:



Looking at the image, you would get it why it got named rail fence because it appears like the rail fence.

Once you have written the message as a sequence of diagonals, to obtain the cipher text out of it you have to read it as a sequence of rows. So, reading the first row the first half of cipher text will be:

m e m t m r o

reading the second row of the rail fence, we will get the second half of the cipher text:

e t e o o r w

Now, to obtain the complete cipher text combine both the halves of cipher text and the complete cipher text will be:

Cipher Text: M E M T M R O E T E O O R W

Rail fence cipher is easy to implement and even easy for a cryptanalyst to break this technique. So, there was a need for a more complex technique.

Columnar Transposition Technique

The columnar transposition cipher is more complex as compared to the rail fence. The steps to obtain cipher text using this technique are as follow:

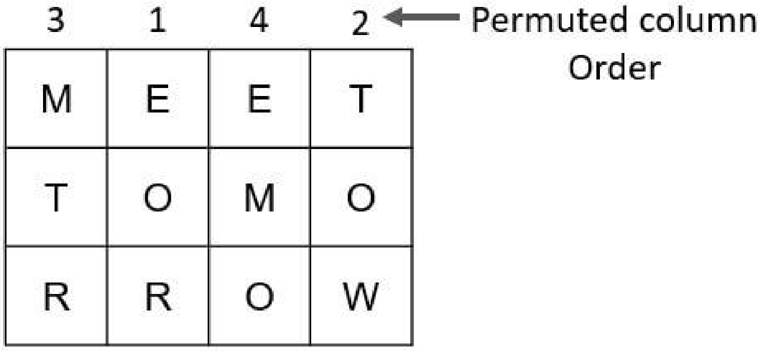
Step 1: The plain text is written in the rectangular matrix of the initially defined size in a row by row pattern.

Step 2: To obtain the cipher text read the text written in a rectangular matrix column by column. But you have to permute the order of column before reading it column by column. The obtained message is the cipher text message.

To understand the columnar transposition let us take an example:

Plain text: meet Tomorrow

Now, put the plain text in the rectangle of a predefined size. For our example, the predefined size of the rectangle would be 3×4. As you can see in the image below the plain text is placed in the rectangle of 3×4. And we have also permuted the order of the column



3	1	4	2
M	E	E	T
T	O	M	O
R	R	O	W

Now, to obtain the cipher text we have to read the plain text column by column as the sequence of permuted column order. So, the cipher text obtained by the columnar transposition technique in this example is:

Cipher Text: MTREOREMOTOW.

Similar to the rail fence cipher, the columnar cipher can be easily broken. The cryptanalyst only has to try few permutation and combination over the order of column to obtain the permuted order of column and the get the original message. So, a more sophisticated technique was required to strengthen the encryption.

5.5 Columnar Transposition Technique with Multiple Rounds

It is similar to the basic columnar technique but is introduced with an improvement. The basic columnar technique is performed over the plain text but more than once. The steps for columnar technique with multiple rounds are as follow:

Step 1: The plain text is written in the rectangle of predetermined size row by row.

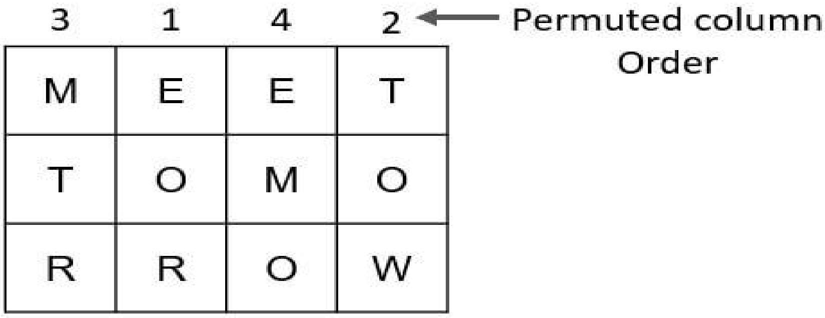
Step 2: To obtain the cipher text, read the plain text in the rectangle, column by column. Before reading the text in rectangle column by column, permute the order of columns the same as in basic columnar technique.

Step 3: To obtain the final cipher text repeat the steps above multiple time.

Let us discuss one example of a columnar transposition technique for better understanding. We will consider the same example of a basic columnar technique which will help in understanding the complexity of the method:

Plain Text: meet Tomorrow

Let us put this plain text in the rectangle of predefined size of 3×4. Proceeding with the next step, the order of the columns of the matrix is permuted as you can see in the image below:



3	1	4	2
M	E	E	T
T	O	M	O
R	R	O	W

Permuted column Order

Now after the first round the cipher text obtained is as follow:

Cipher Text round 1: MTREOREMOTOW

Now, again we have to put the cipher text of round 1 in the rectangle of size 3×4 row by row and permute the order of columns before reading the cipher text for round 2. In the second round, the permuted order of the column is 2, 3, 1, 4.

So, the obtained cipher text for round 2 is MOOTRTREOEMW. In this way, we can perform as many iterations as requires. Increasing the number of iterations increases the complexity of the techniques.

Summary

- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
- Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary
- Based on the security needs and the threats involved, various cryptographic methods such as symmetric key cryptography or public key cryptography can be used during transportation and storage of the data.
- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- monoalphabetic substitution ciphers do not change relative letter frequencies.

Keywords

- **Monoalphabetic Cipher**: A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.
- **Polyalphabetic Cipher :**A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.
- **Caesar Cipher:** It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- **Vignere Cipher:** This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext.
- **Transposition Cipher:**Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text.
- **Plaintext**-text that is not computationally tagged, specially formatted, or written in code.
- **Encryption-**It is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.
- **Cyphertext-**It is the encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.
- **Decryption-**Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

SelfAssessment

1. We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?

A. UWP
B. NUS
C. WUP
D. QSL

2. Which of the following cannot be chosen as a key in the Caesar cipher?

A. An integer
B. An alphabet (A-Z or a-z)
C. A string
D. None of the above

3. Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?

A. Hill Cipher

B. Playfair cipher

C. Both a and b

D. None of the above

4. Which of the following ciphers is a block cipher?

A. Caesar cipher

B. Vernam cipher

C. Playfair cipher

D. None of the above

5. ____ is the message or data that can be readable by the sender.

A. Edited

B. Main Text

C. Plain text

D. All of the mentioned above

6. Shift cipher is also referred to as the

A. Caesar cipher

B. cipher text

C. Shift cipher

D. None of the above

7. Caesar Cipher is an example of

A. Poly-alphabetic Cipher

B. Mono-alphabetic Cipher

C. Multi-alphabetic Cipher

D. Bi-alphabetic Cipher

8. Use Caesar's Cipher to decipher the following

HQFUBSWHG WHAW

A. ABANDONED LOCK

B. ENCRYPTED TEXT

C. ABANDONED TEXT

D. ENCRYPTED LOCK

9. On Encrypting "thepepsiisintherefrigerator" using Vignere Cipher System using the keyword "HUMOR" we get cipher text-

A. abqdnwewuwjphfvrrtrfznsdokvl

B. abqdvmwuwjphfvvyyrfznydokvl

C. tbqyrvmwuwjphfvvyyrfznydokvl

D. baiuvmwuwjphfoeiyrfznydokvl

10. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text

A. nlazeiibljji

B. nlazeiibljii

C. olaaeiibljki

D. mlaaeiibljki

11. Which of the following cipher is created by shuffling the letters of a word?

A. substitution cipher

B. transposition cipher

C. mono alphabetic cipher

D. poly alphabetic cipher

12. Which of the following is not a type of transposition cipher?

A. Rail fence cipher

B. Columnar transposition cipher

C. One time pad cipher

D. Route cipher

13. Which of the following is not a type of mono alphabetic cipher?

A. additive cipher

B. multiplicative cipher

C. afffine cipher

D. hill cipher

14. Which of the following is a type of transposition cipher?

A. Rail Fence cipher

B. Hill cipher

C. Rotor cipher

D. One time pad

15. In which of the following cipher the plain text and the ciphered text have same set of letters?

A. one time pad cipher

B. columnar transposition cipher

C. playfair cipher

D. additive cipher

Answers for Self Assessment

1.	A	2.	C	3.	C	4.	C	5.	C
6.	A	7.	B	8.	B	9.	B	10.	A

11.	B	12.	C	13.	D	14.	A	15.	B

Review Questions

1. Explain different Classical cryptography techniques
2. Discuss Hill Cipher with the help of example
3. Difference between Mono-alphabetic and Polyalphabetic Cipher
4. Using Caesar Cipher technique explain two examples how it works.
5. What are Substitution techniques? Discuss the different techniques with valid example
6. What are transposition Techniques? Discuss the types with the help of valid examples
7. What is a Play Fair Cipher?

Further Readings

https://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf

Web Links

https://www.encryptionconsulting.com/education-center/what-is-cryptography/

Bhanu Sharma, Lovely Professional University

Unit 06: Building Blocks of Information Security

CONTENTS

Objectives

- Understand about Information security
- Learn about the building blocks of IS
- Evaluate what is the importance of these blocks
- Analyze the implementation of the key components

Introduction

Information security is not just about technological controls. Security cannot be achieved solely through the application of software or hardware. Any attempt to implement technology controls without considering the cultural and social attitudes of the corporation is a formula for disaster. The best approach to effective security is a layered approach that encompasses both technological and nontechnological safeguards. Ideally, these safeguards should be used to achieve an acceptable level of protection while enhancing business productivity. While the concept may sound simple, the challenge is to strike a balance between being too restrictive (overly cautious) or too open (not cautious enough). Security technology alone cannot eliminate all exposures. Security managers must integrate themselves with existing corporate support systems. Together with their peers, they will develop the security policies, standards, procedures, and guidelines that form the foundation for security activities. This approach will ensure that security becomes a function of the corporation — not an obstacle to business. A successful layered approach must look at all aspects of security. A layered approach concentrating on technology alone becomes like a house of cards. Without a foundation based on solid policies, the security infrastructure is just cards standing side by side, with each technology becoming a separate card in the house. Adding an extra card (technology layer) to the house (overall security) does not necessarily make the house stronger. Without security policies, standards, procedures, and guidelines, there is no general security framework or foundation. Policies define the behavior that is allowed or not allowed.

They are short because they do not explain how to achieve compliance; such is the purpose of procedures and guidelines. Corporate policy seldom changes because it does not tie to technology, people, or specific processes. Policy establishes technology selection and how it will be configured and implemented. Policies are the consensus between people, especially important between all layers of corporate management. Policy can ensure that the Security Manager and his or her peers apply security technology with the proper emphasis and return on investment for the good of the business as a whole. In most security audits or reviews, checking, maybe even testing, an organization's security policies, standards, procedures, and guidelines is often listed as the first element in assessing security risk. It is easy to see the published hard-copy policy; but to ensure that policy is practiced, it is necessary to observe the workplace in order to evaluate what is really in operation. Lack of general awareness or compliance with a security policy usually indicates a policy that was not developed with the participation of other company management. Whether the organization is global or local, there is still expectation of levels of due diligence. As a spin on the golden rule: “Compute unto others as you would want them to compute unto you.”

6.1 Top 5 Key Elements of an Information Security

An organization that attempts to compose a operating ISP must have well-defined objectives regarding security And strategy. On that management have reached an agreement. Any existing dissonances during this context could render the data security policy project dysfunctional. The foremost necessary factor that a security skilled should bear in mind is that his knowing. The protection management practices would allow him to include them into the documents. He’s entrusted to draft, and that could be a guarantee for completeness, quality and work ability.

Simplification of policy language is one factor that will smooth away the variations and guarantee accord among management workers. Consequently, ambiguous expressions are to be avoid. Beware also of the proper that means of terms or common words. For example, “musts” categorical negotiability, whereas “should” denote certain level of discretion. Ideally, the policy should be shortly developed to the purpose. Redundancy of the policy’s wording (e.g., pointless repetition in writing) ought to be avoided. Moreover, because it would create documents windy and out of correct, with illegibility that encumbers evolution. In the end, a lot of details may impede the entire compliance at the policy level.

So however, management views IT security looks to be one in every of the primary steps. Once someone intends to enforce new rules during this department. Security skilled ought to certify that the ISP has AN equal institutional gravity as different policies enacted within the corporation. In case corporation has size able structure, policies could take issue and so be segregated. So as to define the dealings within the supposed set of this organization.

IS is defined as “a state of well information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable”. It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

1. Confidentiality

Confidentiality is the protection of information in the system so that an unauthorized person cannot access it. This type of protection is most important in military and government organizations that need to keep plans and capabilities secret from enemies. However, it can also be useful to businesses that need to protect their proprietary trade secrets from competitors or prevent unauthorized persons from accessing the company’s sensitive information (e.g., legal, personal, or medical information). Privacy issues have gained an increasing amount of attention in the past few years, place the importance of confidentiality on protecting personal information maintained in automated systems by both government agencies and private-sector organizations. Confidentiality must be well defined, and procedures for maintaining confidentiality must be carefully implemented.

A crucial aspect of confidentiality is user identification and authentication. Positive identification of each system user is essential in order to ensure the effectiveness of policies that specify who is allowed access to which data items.

Threats to Confidentiality:

Confidentiality can be compromised in several ways. The following are some of the commonly encountered threats to information confidentiality –

- Hackers
- Masqueraders
- Unauthorized user activity
- Unprotected downloaded files
- Local area networks (LANs)
- Trojan Horses

Confidentiality Models:

Confidentiality models are used to describe what actions must be taken to ensure the confidentiality of information. These models can specify how security tools are used to achieve the desired level of confidentiality. The most commonly used model for describing the enforcement of confidentiality is the Bell-LaPadula model.

- In this model the relationship between objects (i.e, the files, records, programs and equipment that contain or receive information) and subjects (i.e, the person, processes, or devices that cause the information to flow between the objects).
- The relationships are described in terms of the subject's assigned level of access or privilege and the object's level of sensitivity. In military terms, these would be described as the security clearance of the subject and security classification of the object.

Another type of model that is commonly used is **Access control model.**

- It organizes the system into objects (i.e, resources being acted on), subjects (i.e, the person or program doing the action), and operations (i.e, the process of interaction).
- A set of rules specifies which operation can be performed on a object by which subject.

2. Integrity

Integrity is the protection of system data from international or accidental unauthorized changes. The challenges of the security program are to ensure that data is maintained in the state that is expected by the users. Although the security program cannot improve the accuracy of the data that is put into the system by users. It can help ensure that any changes are intended and correctly applied. An additional element of integrity is the need to protect the process or program used to manipulate the data from unauthorized modification.

A critical requirement of both commercial and government data processing is to ensure the integrity of data to prevent fraud and errors. It is imperative; therefore, no user be able to modify data in a way that might corrupt or lose assets or financial records or render decision making information unreliable.

Examples of government systems in which integrity is crucial include air traffic control system, military fire control systems, social security and welfare systems.

Examples of commercial systems that require a high level of integrity include medical prescription system, credit reporting systems, production control systems and payroll systems.

This principle seeks to ensure the accuracy, trustworthiness and validity of information throughout its life cycle. Information only holds its value if it's truthful, therefore effective measures need to be taken to prohibit the alteration of data whether at rest or in transit by unauthorised individuals or processes.

To prevent unwanted modifications and to ensure that information can be restored if altered, the implementation of regular backups is essential as well as effective access privileges, version controls and input validation.

Challenges that could affect the integrity of your information are:

- Human error
- Compromising a server where end to end encryption isn't present
- Physical compromise to device

Protecting again threats to Integrity

Like confidentiality, integrity can also be arbitrated by hackers, masqueraders, unprotected downloaded files, LANs, unauthorized user activities, and unauthorized programs like Trojan Horse and viruses, because each of these threads can lead to unauthorized changes to data or programs.

For example, unauthorized user can corrupt or change data and programs intentionally or accidentally if their activities on the system are not properly controlled.

Generally, three basic principles are used to establish integrity controls:

- **Need-to-know access:** User should be granted access only on to those files and programs that they need in order to perform their assigned jobs functions.
- **Separation of duties:** To ensure that no single employee has control of a transaction from beginning to end, two or more people should be responsible for performing it.
- **Rotation of duties**: Job assignment should be changed periodically so that it becomes more difficult for the users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes.

Integrity Models

Integrity models are used to describe what needs to be done to enforce the information integrity policy. There are three goals of integrity, which the models address in various ways:

- Preventing unauthorized users from making modifications to data or programs.
- Preventing authorized users from making improper or unauthorized modifications.
- Maintaining internal and external consistency of data and programs.

Integrity models includes five models that suggests different approaches to achieving integrity, they are –

- Biba
- Goguen-Meseguer
- Sutherland
- Clark-Wilson
- Brewer-Nash

Keeping the information intact, complete and correct, and IT systems operational; Integrity is the trustworthiness of data or resources in the prevention of improper and unauthoriz changes the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only the authorized people can update, add, and delete data to protect its integrity). Integrity involves maintaining the consistency, accuracy, and trustworthiness of information over its entire life cycle.

Information should not be modified in transit, and steps should be taken to confirm that information can't be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version management maybe won't be able to prevent incorrect changes or accidental deletion by licensed users becoming a problem. Additionally, some means that should be in place to discover any changes in information that may occur as a result of non-human-caused events like an electromagnetic pulse (EMP) or server crash. Some information would possibly include checksum, even cryptographic checksum, for verification of integrity. Backups or redundancies should be offered to revive the affected information to its correct state.

3. Availability

Availability is one of the three basic functions of security management that are present in all systems. Availability is the assertion that a computer system is available or accessible by an authorized user whenever it is needed. Systems have high order of availability to ensures that the system operates as expected when needed. Availability provides building of fault tolerance system in the products. It also ensures the backup processing by including hot and cold sites in the disaster recovery planning.

There are mainly two threats to availability of the system which are as follows:

1. Denial of Service

2. Loss of Data Processing Capabilities

The above two facets of availability are explained as following below:

1. Denial of Service:

Denial of Service specifies to actions that lock up computing services in a way that the authorized users is unable to use the system whenever needed. Availability is also blocked in case, if a security office unintentionally locks up an access control of database during the routine maintenance of the system thus for a period of time authorized users are block to access. In the computer systems, internet worm overloaded about 10% of the system on the network, causing them to be non responsive to the need of users is an example of denial of service.

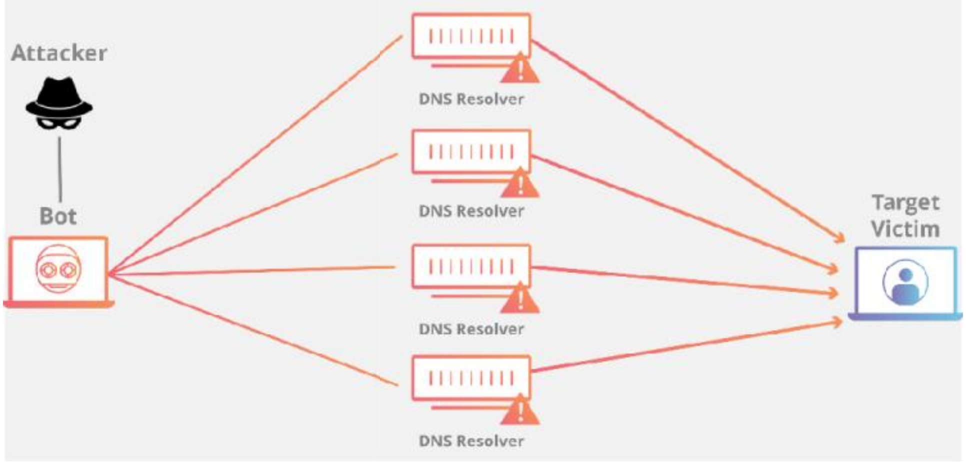


Figure 1 Denial of Service attack

2. Loss of Data Processing Capabilities:

The loss of data processing capabilities are generally caused by the natural disasters or human actions is perhaps more common. Contingency planning is the measure to counter such type of losses, which helps in minimizing the time for that a data processing capability remains unavailable. Contingency planning provides an alternative means of processing which involves business resumption planning, alternative site processing or simply disaster recovery planning thereby ensures data availability.

Security aspects of Availability:

Generally, three basic issues are aspects of security initiatives that are used to address availability, they are:

Physical issues:

The physical issues includes access controls that prevent unauthorized persons from coming into contact with computing resources, various fire and water control mechanisms, hot and cold sites for use in alternative site processing, and backup storage facilities.

Technical issues:

Technical issues includes the fault-tolerance mechanisms, electronic vaulting (automatically backup to a secure location) and access control software to restrict unauthorized users from disrupting services. Fault tolerance mechanisms involves hardware redundancy, disk mirroring and application checkpoint restart.

Administrative issues:

The issues comes in the administrative aspect of availability are access control policies, operating procedures, contingency planning and user training. Proper training of operators, programmers and security personnel can help avoid many computing stages that leads to the loss of availability.

An objective indicating that data or system is at disposal of license users once require. Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Availability means data is accessible by licensed users.

If AN attacker isn't able to compromise the primary components of data security (see above) they'll try and execute attacks like denial of service that will bring down the server, creating the web site unavailable to legitimate users because of lack of availability. Measures to maintain data availability can include redundant systems' disk arrays and clustered Machines, anti-virus software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

4. Authenticity

Authenticity is assurance that a message, transaction, or other exchange of information is from the source it claims to be from. Authenticity involves proof of identity.

We can verify authenticity through authentication. The process of authentication usually involves more than one "proof" of identity (although one may be sufficient). The proof might be something a user knows, like a password. Or, a user might prove their identity with something they have, like a keycard. Modern (biometric) systems can also provide proof based on something a user is. Biometric authentication methods include things like fingerprint scans, hand geometry scans, or retinal scans.

A security policy includes a hierarchical pattern. It means inferior workers is typically certain to not share the small quantity of data they need unless explicitly approved. Conversely, a senior manager might have enough authority to create a choice what information is shared and with whom, which implies that they're not tied down by an equivalent data security policy terms. That the logic demands that ISP ought to address each basic position within the organization with specifications which will clarify their authoritative standing. Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or corrupted. The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as bio metrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.

The user should prove access rights and identity. Commonly, usernames and passwords are used for this method. However, this kind of authentication may be circumvented by hackers. a much better form of authentication is bio metrics, as a result of it depends on the user's presence and biological features (retina or fingerprints). The PKI (Public Key Infrastructure) authentication methodology uses digital certificates to prove a user's identity. Different authentication tools will be key cards or USB tokens. The best authentication threat occurs with unsecured emails that seem legitimate.

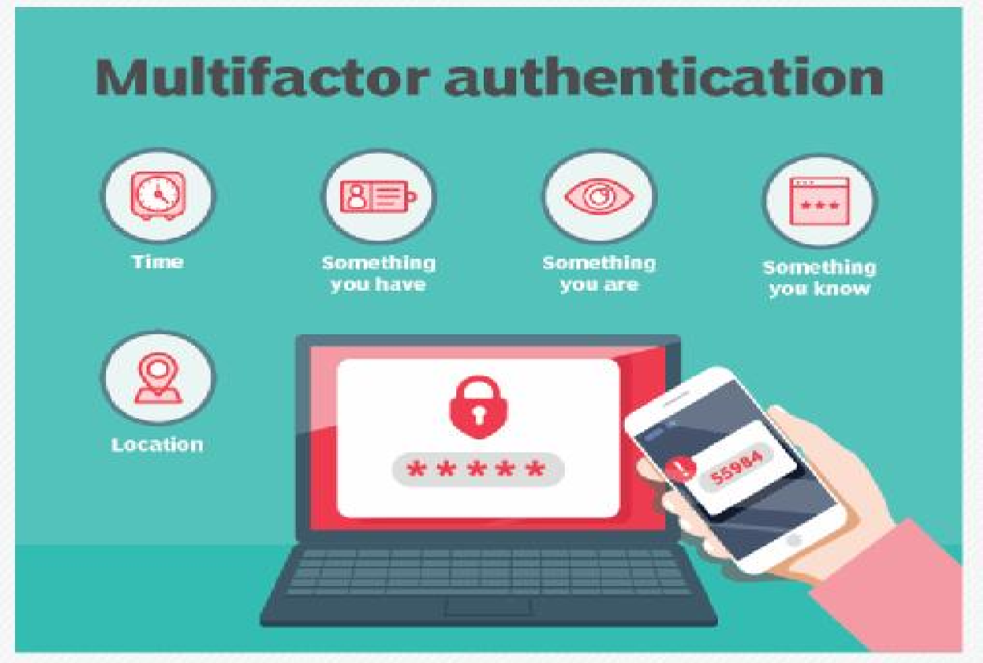


Figure 2 Authentication method

Ensuring Authenticity

For user interaction with systems, programs, and each other, authentication is critical. User ID and password input is the most prevalent method of authentication. It also seems to present the most problems. Passwords can be stolen or forgotten. Cracking passwords can be simple for hackers if the passwords aren't long enough or not complex enough. Remembering dozens of passwords for dozens of applications can be frustrating for home users and business users alike. Single Sign On (SSO) solutions

Two-factor or multi-factor authentication is more common in the enterprise for mission critical applications and systems. Mulit-factor authentication systems may use Key cards, smart cards, or USB tokens. Public Key Infrastructure (PKI) Authentication uses digital certificates issued by a central or 3rd party authority. Secure Socket Layer (SSL) connections to web sites provide not only encryption for the session, but also (usually) provide verification that the web site is authentically the site it claims to be.

The main objective of authentication is to allow authorized users to access the computer and to deny access to the unauthorized users. Operating Systems generally identifies/authenticates users using following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.

Passwords:Passwords verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In password based system, each user is assigned a valid username and password by the system administrator.

System stores all username and Passwords. When a user logs in, its username and password is verified by comparing it with stored login name and password. If the contents are same, then the user is allowed to access the system otherwise it is rejected.

Physical Identification: This technique include machine readable badges(symbols), card or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many systems, identification is combined with the use of password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATM. Smart card can enhance this scheme by keeping the user password within the card itself. This allow the authentication without storage of password in the computer system. The loss of such card can be dangerous.

Biometrics:This method of authentication is based on the unique biological characteristics of each user such as fingerprints, voice or face recognition, signatures, and eyes.

Biometric devices often consist of –

- A scanner or other devices to gather the necessary data about user.
- Software to convert the data into a form that can be compared and stored.
- A database that stores information for all authorized users.

A number of different types of physical characteristics are –

Facial Characteristics –Humans are differentiated based on facial characteristics such as eyes, nose, lips, eyebrows, and chin shape.

Fingerprints –Fingerprints are believed to be unique across the entire human population.

Hand Geometry –Hand geometry systems identify features of hand that includes shape, length, and width of fingers.

Retinal pattern –It is concerned with the detailed structure of the eye.

Signature –Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.

Voice –This method records the frequency pattern of the voice of an individual speaker.

One Time passwords: One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time passwords are implemented in various ways. Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

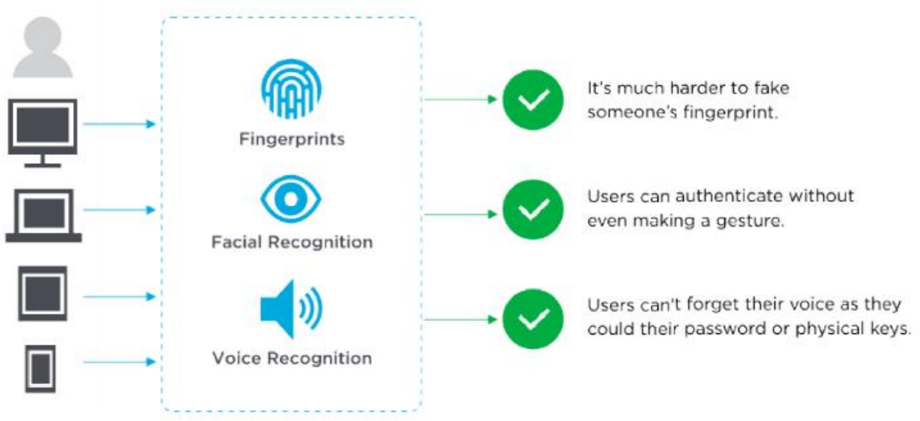

Fingerprints
Facial Recognition
Voice Recognition
It's much harder to fake someone's fingerprint.
Users can authenticate without even making a gesture.
Users can't forget their voice as they could their password or physical keys.

Figure 3 Example of authentication

5. Non-Repudiation

It is the assurance that somebody cannot deny the validity of one thing. It may be a legal thought that's widely used in data security and refers to a service that provides proof of the origin of information and also the integrity of the information. In different words, non-repudiation makes it very difficult to successfully deny who/where a message came from also as the authenticity of that message.Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

Digital signatures (combined with other measures) can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place. In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

Nonrepudiation provides proof of the origin, authenticity and integrity of data. It provides assurance to the sender that its message was delivered, as well as proof of the sender's identity to the recipient. This way, neither party can deny that a message was sent, received and processed.

Nonrepudiation is like authentication, particularly with respect to implementation. For instance, a public key signature can be a nonrepudiation device if only one party can produce signatures.

In general, nonrepudiation combines both authentication and integrity.

Nonrepudiation, message authentication code and digital signatures

Nonrepudiation is achieved through cryptography, like digital signatures, and includes other services for authentication, auditing and logging.

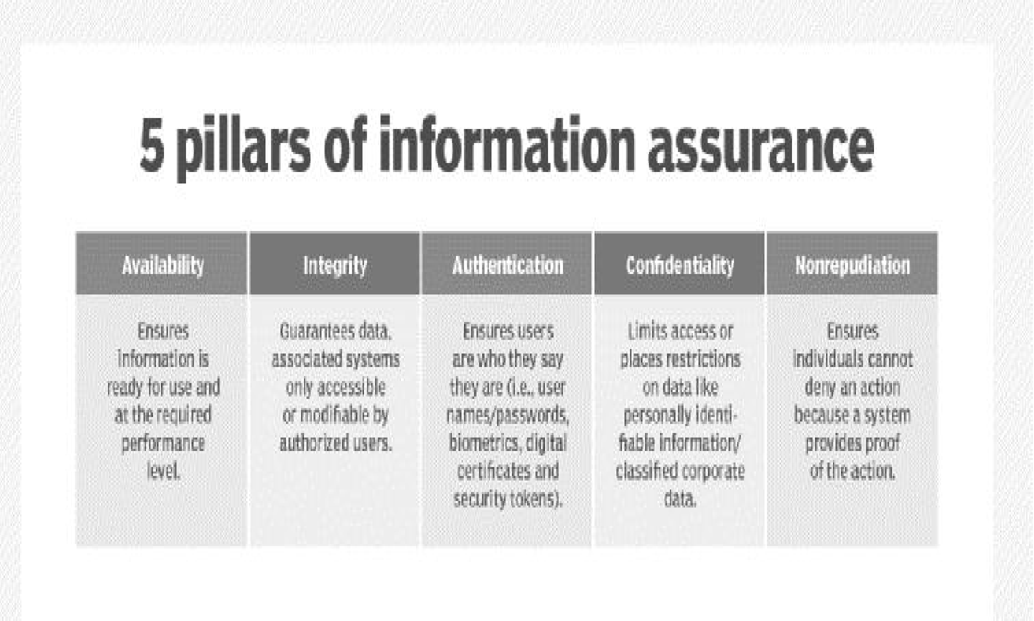
In online transactions, digital signatures ensure that a party cannot later deny sending information or deny the authenticity of its signature. A digital signature is created using the private key of an asymmetric key pair, which is public key cryptography, and verified with a corresponding public key.

Only the private key holder can access this key and create this signature, proving that a document was electronically signed by that holder. This ensures that a person cannot later deny that they furnished the signature, providing nonrepudiation.

In cryptography, a message authentication code (MAC), also known as a tag, is used to authenticate a message or confirm that the message came from the stated sender and was not changed along the way. Unlike digital signatures, MAC values are generated and verified using the same secret key, which the sender and recipient must agree on before initiating communications.

A MAC can protect against message forgery by anyone who doesn't know the shared secret key, providing both integrity and authentication. However, MAC algorithms, like cipher-based MAC and hash-based MAC, cannot provide nonrepudiation.

In addition to digital signatures, nonrepudiation is also used in digital contracts and email. Email nonrepudiation involves methods such as email tracking.



5 pillars of information assurance

Availability	Integrity	Authentication	Confidentiality	Nonrepudiation
Ensures information is ready for use and at the required performance level.	Guarantees data, associated systems only accessible or modifiable by authorized users.	Ensures users are who they say they are (i.e., user names/passwords, biometrics, digital certificates and security tokens).	Limits access or places restrictions on data like personally identifiable information/ classified corporate data.	Ensures individuals cannot deny an action because a system provides proof of the action.

Figure 4 Pillars of Information Security

6.2 Information Classification in Information Security

In today's world, Information is one of the essential parts of our life. In this, we will discuss the categorization of information on the basis of different organizations and different parameters. Information in an organization should be categorized and must be kept confidential and that's why information security comes into the picture, and it plays a vital role for any organization.

The main reason for classifying information is that not all data/information has the same level of importance or the same level of relevance/critical to an organization. Some data are more valuable to people who make strategic decisions (senior management) because they aid them in making long-run or short-range business direction decisions. Some data such as trade secrets, formulas (used by scientific and/or research organizations), and new product information (such as the use by marketing staff and sales force) are so valuable that their loss could create significant problems for the enterprise in the market. Thus, it is obvious that information is used to prevent unauthorized disclosure and the resultant failure of confidentiality.

Schemes for Information Classifications as follows.

- **Government Organization**
- **Private Organizations**

Levels in Government organization for Information Classification:

Unclassified –Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.

Sensitive but Unclassified –Information that has been designed as a major secret but may not create serious damage if disclosed.

Confidential –The unauthorized disclosure of confidential information could cause some damage to the country's national security

Secret –The unauthorized disclosure of this information could cause serious damage to the country's national security.

Task: Considering any organization discuss information classification with relevant example.

Top Secret –his is the highest level of information classification. Any unauthorized disclosure of top-secret information will cause grave damage to the country's national security.

Levels in Private Organizations for Information Classification:

Public –Information that is similar to unclassified information. However, if it is disclosed, it is not expected to seriously impact the company.

Sensitive –Information that required a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from loss of integrity owing to an unauthorized alteration.

Private –Typically, this is the information i.e., considered of a personal nature and is intended for company use only, its disclosure could adversely affect the company or its employee salary levels and medical information could be considered as examples of "private information".

Criteria for Information Classification:

Value –It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization, it needs to be classified.

Age –The classification of the information may be lowered if the information value decreases over time.

Useful Life –Information will be more useful if it will be available to make the changes as per requirements than, it will be more useful.

Personal association –If the information is personally associated with a specific individual or is addressed by a privacy law then it may need to be classified.

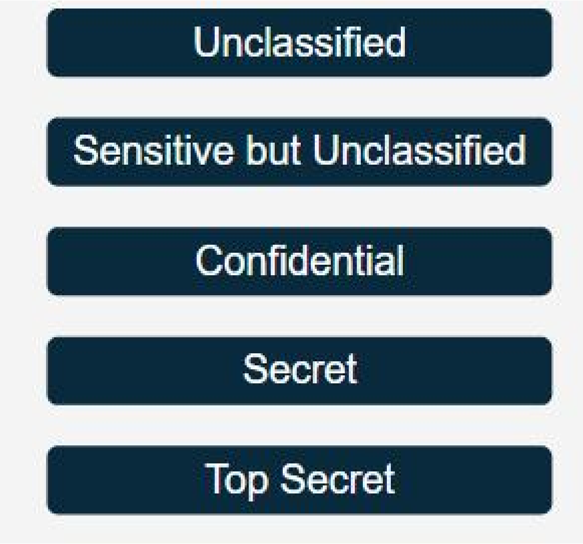


Figure 5 Information Classification

Summary

- Information security can be said to be a branch of cybersecurity, even though, sometimes the two terms are used interchangeably.

- Data is any information relating to personal, organizational, security, defence, financial, commercial, and others in every possible area of operation.
- The Information Security Objectives are to protect data in computers, networks and servers across different organizations in every sector
- The confidentiality of information related to an organization is integral to any information security policy.
- This principally means that the sender of a message can not deny transmitting the message. Similarly, the receiver can not deny receiving the message that was sent.
- All organizations have clearly defined information security policies in place which enumerate the company's approach to Information security principles and practices.

Keywords

- **Unclassified:** Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.
- **Sensitive but Unclassified:**Information that has been designed as a major secret but may not create serious damage if disclosed.
- **Top Secret:** This is the highest level of information classification. Any unauthorized disclosure of top-secret information will cause grave damage to the country's national security.
- **Digital Signatures**: A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit(integrity).
- **Confidentiality:**Prevents sensitive information from reaching the wrong people, while making sure that the right people can use it.
- **Integrity:**Maintains the consistency, accuracy and trustworthiness of information over its lifecycle.
- **Availability:** Ensures that the information is available when it is needed.

SelfAssessment

1. _______ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

A. Network Security
B. Database Security
C. Information Security
D. Physical Security

2. From the options below, which of them is not a threat to information security?

A. Disaster
B. Eavesdropping
C. Information leakage
D. Unchanged default password

3. From the options below, which of them is not a vulnerability to information security?

A. flood

B. without deleting data, disposal of storage media

C. unchanged default password

D. latest patches and updates not done

4. The CIA triad is often represented by which of the following?

A. triangle

B. diagonal

C. ellipse

D. circle

5. CIA triad is also known as

A. nic (non-repudiation, integrity, confidentiality)

B. aic (availability, integrity, confidentiality)

C. ain (availability, integrity, non-repudiation)

D. aic (authenticity, integrity, confidentiality)

6. Which of the following contains the primary goals and objectives of security?

A. A network's border perimeter

B. The CIA Triad

C. A stand-alone system

D. The Internet

7. Vulnerabilities and risks are evaluated based on their threats against which of the following?

A. One or more of the CIA Triad principles

B. Data usefulness

C. Due care

D. Extent of liability

8. Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

A. Identification

B. Availability

C. Encryption

D. Layering

9. Which of the following is not considered a violation of confidentiality?

A. Stealing passwords

B. Eavesdropping

C. Hardware destruction

D. Social engineering

10. Which of the following is not true?

A. Violations of confidentiality include human error.

B. Violations of confidentiality include management oversight.

C. Violations of confidentiality are limited to direct intentional attacks.

D. Violations of confidentiality can occur when a transmission is not properly encrypted.

11. Confidentiality is dependent upon which of the following?

A. Accountability

B. Availability

C. Nonrepudiation

D. Integrity

12. If a security mechanism offers availability, then it offers a high level of assurance that the data, objects, and resources are _______________ by authorized subjects.

A. Controlled

B. Audited

C. Accessible

D. Repudiated

13. Which of the following describes the freedom from being observed, monitored, or examined without consent or knowledge?

A. Integrity

B. Privacy

C. Authentication

D. Accountability

14. All but which of the following items require awareness for all individuals affected?

A. The restriction of personal e-mail

B. Recording phone conversations

C. Gathering information about surfing habits

D. The backup mechanism used to retain e-mail messages

15. Which of the following is typically not used as an identification factor?

A. Username

B. Smart card swipe

C. Fingerprint scan

D. A challenge/response token device

Answers for Self Assessment

1.	C	2.	D	3.	A	4.	A	5.	B
6.	B	7.	A	8.	B	9.	C	10.	C
11.	D	12.	C	13.	B	14.	D	15.	D

Review Questions

1. What is confidentiality availability and integrity?
2. What does confidentiality integrity and availability have to do with security?
3. What is confidentiality in information security?
4. What are the 3 principles of information security?
5. What are Top 5 Key Elements of an Information Security?
6. Discuss different information classification with the help of example.

Further Readings

https://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf

Web Links

https://www.encryptionconsulting.com/education-center/what-is-cryptography/

Unit 07: User Authentication

CONTENTS

Objectives

- Understand the concept of User Authentication
- Acquire knowledge about different types of User Authentication
- Identify the usage of biometric authentication along with its application in real world

Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security.

There are several authentication types. For purposes of user identity, users are typically identified with a user ID, and authentication occurs when the user provides credentials such as a password that matches their user ID. The practice of requiring a user ID and password is known as single-factor authentication (SFA). In recent years, companies have strengthened authentication by asking for additional authentication factors, such as a unique code that is provided to a user over a mobile device when a sign-on is attempted or a biometric signature, like a facial scan or thumbprint. This is known as two-factor authentication (2FA).

Authentication factors can even go further than SFA, which requires a user ID and password, or 2FA, which requires a user ID, password and biometric signature. When three or more identity verification factors are used for authentication -- for example, a user ID and password, biometric signature and perhaps a personal question the user must answer -- it is called multifactor authentication (MFA).

7.1 What is user authentication?

User authentication verifies the identity of a user attempting to gain access to a network or computing resource by authorizing a human-to-machine transfer of credentials during interactions on a network to confirm a user's authenticity. The term contrasts with machine authentication, which is an automated authentication method that does not require user input.

Authentication helps ensure only authorized users can gain access to a system by preventing unauthorized users from gaining access and potentially damaging systems, stealing information, or causing other problems. Almost all human-to-computer interactions -- other than guest and automatically logged-in accounts -- perform a user authentication. It authorizes access on both wired and wireless networks to enable access to network and internet-connected systems and resources.

A straightforward process, user authentication consists of three tasks:

1. **Identification.** Users must prove who they are.
2. **Authentication**. Users must prove they are who they say they are.
3. **Authorization.** Users must prove they're allowed to do what they are trying to do.

User authentication can be as simple as requiring a user to type a unique identifier, such as a user ID, along with a password to access a system. It can also be more complex, however -- for example, requiring a user to provide information about physical objects or the environment or even take actions, such as placing a finger on a fingerprint reader.

Why is authentication important in cybersecurity?

Authentication enables organizations to keep their networks secure by permitting only authenticated users or processes to gain access to their protected resources. This may include computer systems, networks, databases, websites and other network-based applications or services.

Once authenticated, a user or process is usually subjected to an authorization process to determine whether the authenticated entity should be permitted access to a specific protected resource or system. A user can be authenticated but not be given access to a specific resource if that user was not granted permission to access it.

The terms authentication and authorization are often used interchangeably. While they are often implemented together, they are two distinct functions. Authentication is the process of validating the identity of a registered user or process before enabling access to protected networks and systems. Authorization is a more granular process that validates that the authenticated user or process has been granted permission to gain access to the specific resource that has been requested. The process by which access to those resources is restricted to a certain number of users is called access control. The authentication process always comes before the authorization process.

How does authentication work?

During authentication, credentials provided by the user are compared to those on file in a database of authorized users' information either on the local operating system server or through an authentication server. If the credentials entered match those on file and the authenticated entity is authorized to use the resource, the user is granted access. User permissions determine which resources the user gains access to and also any other access rights that are linked to the user, such as during which hours the user can access the resource and how much of the resource the user is allowed to consume.

Traditionally, authentication was accomplished by the systems or resources being accessed. For example, a server would authenticate users using its own password system, login IDs, or usernames and passwords.

However, the web's application protocols -- Hypertext Transfer Protocol and HTTP Secure -- are stateless, meaning that strict authentication would require end users to reauthenticate each time they access a resource using HTTPS. To simplify user authentication for web applications, the authenticating system issues a signed authentication token to the end-user application; that token is appended to every request from the client. This means that users do not have to sign on every time they use a web application.

What is authentication used for?

User and process authentication are used to ensure that only authorized individuals or processes are allowed to access company IT resources. Depending on the use cases for which authentication is used, authentication can consist of either SFA, 2FA or MFA.

The most common implementation of authentication is SFA, which requires a user ID and a password for sign-on and access. However, since banks and many companies now use online banking and e-commerce to conduct business and store customer Social Security and credit and debit card numbers, there is an increased use of 2FA and even MFA, which requires users and customers to enter not only a user ID and password, but also additional authentication information.

From an IT standpoint, organizations use authentication to control who has access to corporate networks and resources, as well as to identify and control which machines and servers have access. Companies also use authentication to enable remote employees to securely access their applications and networks.

For enterprises and other large organizations, authentication may also be accomplished using a simplified single sign-on system, which grants access to multiple systems with a single set of login credentials.

What are Authentication factors?

Authenticating a user with a user ID and a password is usually considered the most basic type of authentication, and it depends on the user knowing two pieces of information -- the user ID or username, and the password. Since this type of authentication relies on just one authentication factor, it is a type of SFA.

Strong authentication is a term that is typically used to describe a type of authentication that is more reliable and resistant to attack. Strong authentication typically uses at least two different types of authentication factors and often requires the use of strong passwords containing at least eight characters, a mix of small and capital letters, special symbols and numbers.

An authentication factor represents a piece of data or attribute that can be used to authenticate a user requesting access to a system. An old security adage has it that authentication factors can be something you know, something you have or something you are. Additional factors have been proposed and put into use in recent years, with location serving in many cases as the fourth factor and time serving as the fifth factor.

Currently used authentication factors include the following:

Knowledge factor. The knowledge factor, or something you know, may be any authentication credentials that consist of information that the user possesses, including a personal identification number (PIN), a username, a password or the answer to a secret question.

Possession factor. The possession factor, or something you have, may be any credential based on items that the user can own and carry with them, including hardware devices, like a security token or a mobile phone used to accept a text message or to run an authentication app that can generate a one-time password (OTP) or PIN.

Inherence factor. The inherence factor, or something you are, is typically based on some form of biometric identification, including fingerprints or thumbprints, facial recognition, retina scan or any other form of biometric data.

Location factor. Where you are may be less specific, but the location factor is sometimes used as an adjunct to the other factors. Location can be determined to reasonable accuracy by devices equipped with the Global Positioning System or with less accuracy by checking network addresses and routes. The location factor cannot usually stand on its own for authentication, but it can supplement the other factors by providing a means of ruling out some requests. For example, it can prevent an attacker located in a remote geographical area from posing as a user who normally logs in only from their home or office in the organization's home country.

Time factor. Like the location factor, the time factor, or when you are authenticating, is not sufficient on its own, but it can be a supplemental mechanism for weeding out attackers who attempt to access a resource at a time when that resource is not available to the authorized user. It may also be used together with location. For example, if the user was last authenticated at noon in the U.S., an attempt to authenticate from Asia one hour later would be rejected based on the combination of time and location.

Despite being used as supplemental authentication factors, user location and current time by themselves are not sufficient, without at least one of the first three factors, to authenticate a user.

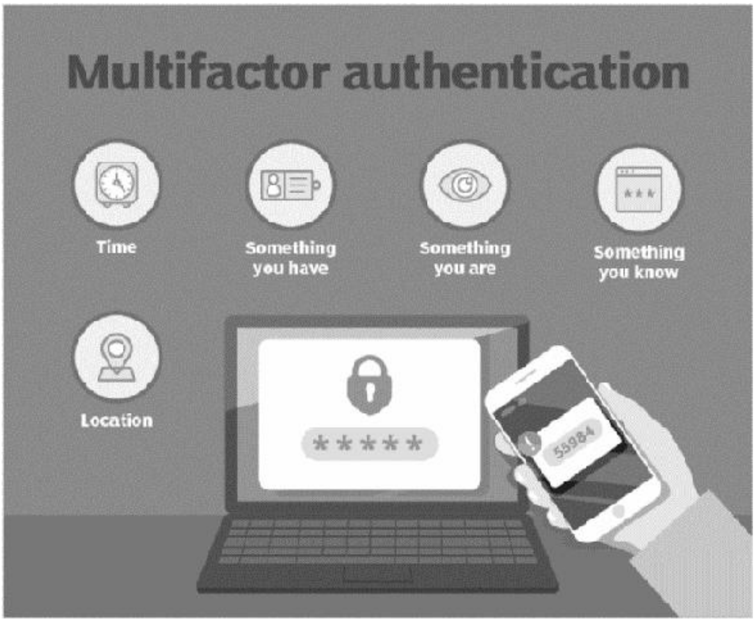


Figure 1 Multifactor Authentication

Authentication vs. authorization

Authorization includes the process through which an administrator grants rights to authenticated users, as well as the process of checking user account permissions to verify that the user has been granted access to those resources. The privileges and preferences granted for an authorized account depend on the user's permissions, which are either stored locally or on an authentication server. The settings defined for all these environment variables are established by an administrator.

7.2 User Authentication Methods

The main factors used in user authentication include the following:

Knowledge factors include all things users must know in order to log in to gain access to a system. Usernames, IDs, passwords and personal identification numbers (PINs) all fall under this category.

Possession factors consist of anything users must have in their possession in order to log in. This category includes one-time password tokens, key fobs, smartphone apps, and employee ID cards.

Inherence factors include characteristics inherent to individuals that confirm their identity. This category includes the scope of biometrics, such as retina scans, fingerprint scans, facial recognition and Voice authentication.

Other factors include location and time factors, which are typically used together or in conjunction with another authentication factor:

Location factors are a method of confirming users' identity through their location. User authentication systems accomplish this by using the built-in Global Positioning System (GPS) functionality of most smartphones to identify a person's location or combine Wi-Fi and cell tower triangulation to estimate a location. Authentication systems typically do not use location on its own to confirm identity. For example, if an attacker logs in with a user's password, the location factor can prevent the attacker in a different geographical area from posing as the user, who typically logs in only from a specific location. Here, location and password are used together to confirm identity.

Time factors add time-based access characteristics to confirm identity. Similar to the location factor, the time factor is not adequate on its own but can be helpful when used with another factor. For example, if a system last authenticated a user at noon in the U.S., an attempt to log in an hour later from Asia would be rejected based on the combination of time and location. A time factor can also only permit access within a scheduled time interval.

Single-factor authentication vs. multifactor authentication

Single-factor authentication (SFA) requires verification of one piece of information from a user, such as a password. Because SFA commonly employs knowledge factors, which require only a single piece of information, it can't stop an attacker who has stolen a user's password from accessing a user's system.

Multifactor authentication (MFA) uses more than one method of authentication to verify the identity of a user. For example, a user may be required to provide a password in combination with a security question. Two-factor authentication (2FA) uses factors from two of the authentication categories, while four-factor authentication (4FA) uses at least one factor from four categories of factors. The latter is considered far more secure due to the additional layers of security that come with more factors.

7.3 Types of Authentications

Traditional authentication depends on the use of a password file, in which user IDs are stored together with hashes of the passwords associated with each user. When logging in, the password submitted by the user is hashed and compared to the value in the password file. If the two hashes match, the user is authenticated.

This approach to authentication has several drawbacks, particularly for resources deployed across different systems. For one thing, attackers who are able to gain access to the password file for a system can use brute-force attacks against the hashed passwords to extract the passwords. In addition, this method would require multiple authentications for modern applications that access resources across multiple systems.

Password-based authentication weaknesses can be addressed to some extent with smarter usernames and passwords based on rules such as minimum length and complexity using capital letters and symbols. However, password-based authentication and knowledge-based authentication are more vulnerable than systems that require multiple independent methods.

Other authentication methods include the following:

2FA

This type of authentication adds an extra layer of protection to the process by requiring users to provide a second authentication factor in addition to the password. 2FA systems often require the user to enter a verification code received via text message on a preregistered mobile phone or mobile device, or a code generated by an authentication application.

MFA

This type of authentication requires users to authenticate with more than one authentication factor, including a biometric factor, such as a fingerprint or facial recognition; a possession factor, like a security key fob; or a token generated by an authenticator app.

OTP

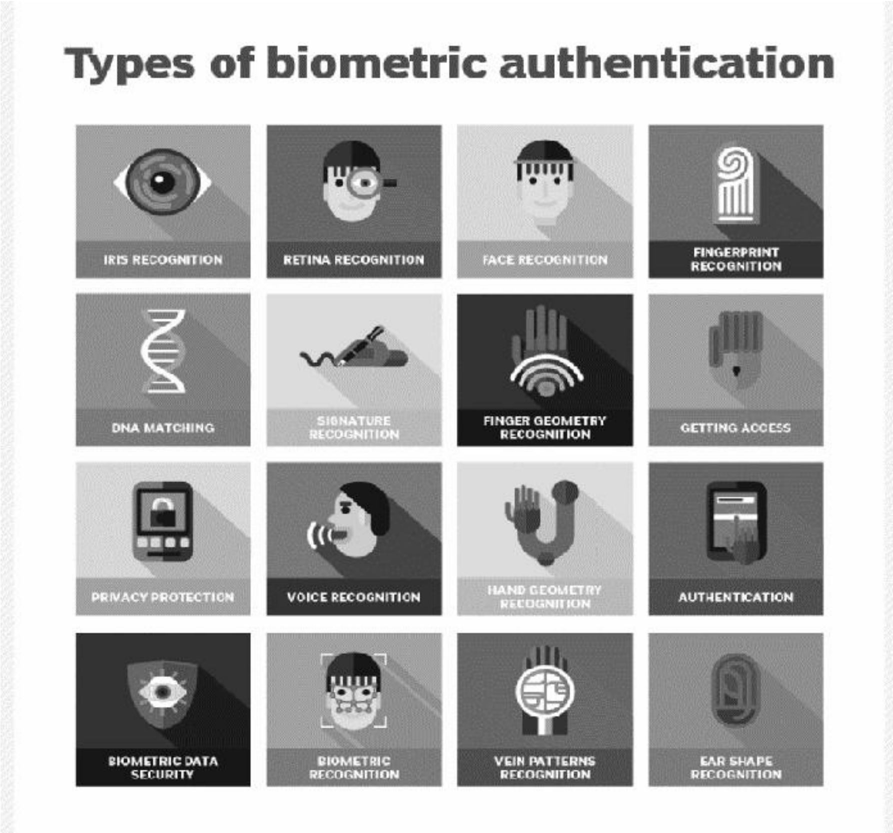
An OTP is an automatically generated numeric or alphanumeric string of characters that authenticates a user. This password is only valid for one login session or transaction and is typically employed for new users or for users who lost their passwords and are given an OTP to log in and change to a new password.

Three-factor authentication.

This type of MFA uses three authentication factors -- usually, a knowledge factor, such as a password, combined with a possession factor, such as a security token, and an inherence factor, such as a biometric.

Biometrics

While some authentication systems depend solely on biometric identification, biometrics are usually used as a second or third authentication factor. The more common types of biometric authentication available include fingerprint scans, facial or retina scans, and voice recognition.



Mobile authentication.

Mobile authentication is the process of verifying users via their devices or verifying the devices themselves. This enables users to log into secure locations and resources from anywhere. The mobile authentication process involves MFA that can include OTPs, biometric authentication or Quick Response code

Continuous authentication.

With continuous authentication, instead of a user being either logged in or out, a company's application continually computes an authentication score that measures how sure it is that the account owner is the individual who is using the device.

Application programming interface (API) authentication.

The standard methods of managing API authentication are HTTP basic authentication, API keys and Open Authorization (OAuth).

In HTTP basic authentication, the server requests authentication information, such as a username and password, from a client. The client then passes the authentication information to the server in an authorization header.

In the API key authentication method, a first-time user is assigned a unique generated value that indicates that the user is known. Then, each time the user tries to enter the system again, their unique key is used to verify they are the same user who entered the system previously.

OAuth is an open standard for token-based authentication and authorization on the internet. It enables a user's account information to be used by third-party services, such as Facebook, without exposing the user's password. OAuth acts as an intermediary on behalf of the user, providing the service with an access token that authorizes specific account information to be shared.

7.4 5 Common Authentication Types

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. This is why companies are starting to implement more sophisticated incident response strategies, including authentication as part of the process. The list below reviews some common authentication methods used to secure modern systems.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication:

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication technologies:

- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

Facial recognition—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.

Fingerprint scanners—match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.

Speaker Recognition —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.

Eye scanners—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.

5. Token-based authentication

Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission. Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

7.5 User Authentication vs. Machine Authentication

Machines also need to authorize their automated actions within a network. Online backup services, patching and updating systems, and remote monitoring systems, such as those used in telemedicine and smart grid technologies, all need to securely authenticate to verify that it is the authorized system involved in an interaction and not a hacker.

Machine authentication can be carried out with machine credentials, similar to a user's ID and password but submitted by the device in question. Machine authentication may also use digital certificates issued and verified by a certificate authority as part of a public key infrastructure to prove identification while exchanging information over the internet.

With the increasing number of internet-enabled devices, reliable machine authentication is crucial to enable secure communication for home automation and other internet of things applications, where almost any entity may be made addressable and able to exchange data over a network. It is important to realize that each access point is a potential intrusion point. Each networked device needs strong machine authentication, and despite their normally limited activity, these devices must be configured for limited permissions access to restrict what can be done even if they are breached.

Did you Know?

Longer passwords are more secure than shorter passwords or the passwords with your name or dob.

User authentication limitations and improvements

A number of issues affect the security of an authentication system. In addition to the number of factors involved, the specific technologies used and the way they are implemented affect reliability. Well-designed and appropriately enforced implementation rules can help ensure the security of user authentication.

For example, passwords -- among the most vulnerable methods of authentication -- are relatively insecure because hackers can typically easily guess and crack them. To alleviate the problem, several industries and organizations have implemented strong password standards, which insist users create passwords that meet minimum length and other requirements, such as including at least one number and letter plus a symbol.

The ubiquity of mobile devices and cloud computing today has greatly affected how enterprises implement authentication. In the past, a simple password authentication system was sufficient to keep networks secure. However, increased risk of data breaches has made companies reevaluate their authentication strategies. Modern authentication processes should involve more than a single factor in order to ensure the highest level of security.

While MFA provides added layers of security for confirming a user's identity, it is also important not to overburden users with difficult authentication routines, which can lead to noncompliance that undermines the purpose of the authentication system in the first place. For instance, MFA with automatic processes can enhance security, while minimizing the effort required by the user.

MFA is especially important for organizations that offer cloud-based services, as the cloud itself provides secondary authentication if a user has a password breach.

Summary

- User authentication is a security process that covers all of the human-to-computer interactions that require the user to register and log in. Said more simply, authentication asks each user, “who are you?” and verifies their response.
- When your user authentication isn’t secure, however, cybercriminals can hack the system and gain access, taking whatever information the user is authorized to access.
- a password less login system is an authentication method that doesn’t require a password. In the past couple of years, these types of authentication methods have become more popular—and you’ve probably experienced a few.
- Biometrics can also provide a user experience that is convenient and easy to understand. For example, with fingerprint authentication, the user only needs to complete one step—the rest is the system’s responsibility

Keywords

Email authentication is one of the most universally accessible types of password less user authentication, largely because anyone with an email account can use this method.

Certificate Based Authentication:A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.

E-Token Based Authentication: An authentication token is a small device that generates a new random value every time it is used. This random value becomes the basis for authentication{an alternative to a password}.

Biometric authentication: refers to the identification of humans by their characteristics such as fingerprint, voice, Iris pattern of the eye, vein pattern, etc.

Multi-factor Authentication: Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user.

Self Assessment

1. Biometric authentication:

A. is inexpensive.
B. is used widely in Europe for security applications.
C. can use a person's face as a unique, measurable trait.
D. only uses physical traits as a measurement.

2. Includes pieces of information used to verify a person's identity for security purposes. (15)

A. Authorization
B. Authenticate
C. Authentication
D. Authentication Factors

3. A biometric modality that uses an individual's speech-a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual-for recognition purposes.

A. Access Control
B. Voice Recognition
C. Pattern Recognition
D. Face Recognition

4. Offers reasonable accuracy but can be affected by poor lighting, glasses, facial hair, and aging.

A. Voice Recognition
B. Pattern Recognition
C. Face Recognition
D. Access Control

5. Defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security.

A. Identity
B. Identifier
C. Integrity
D. Confidentiality

6. Finger Scanning, Finger Geometry, Hand Geometry, Palm Imaging, Iris Imaging, Retina Recognition, Face Recognition, Voice Recognition, and Signature Verification are examples of

A. Biometrics
B. Biometric Methods
C. Biometric Verification
D. Biometric Technologies

7. The process of granting access to information system resources only to authorized users, programs, processes, or other systems

A. Face Recognition
B. Accessibility
C. Voice Recognition
D. Access Control

8. This system examines the dynamics of the signing process, rather than the signature.

A. Covert Screening
B. Signature Scanning
C. Palm Scanning
D. Retina Scanning

9. Provides very high accuracy, provided the user's eye is properly focused.

A. Retina Scanning
B. Matching
C. Palm Scanning
D. Covert Screening

10. Voice recognition is nothing but ___________ recognition.

A. vocal
B. iris
C. sound
D. face

11. Which of the following is used in hand-free computing, map, or menu navigation?

A. Speaker Recognition
B. Vocal Recognition
C. Speech Recognition
D. None of the above

12. The objective of voice recognition is to recognize _________ is speaking.

A. What
B. Why
C. Whom
D. Who

13. Which of the following Demerits of Voice Recognition?

A. It is susceptible to quality of microphone and noise

B. The inability to control the factors affecting the input system can significantly decrease performance.

C. Some speaker verification systems are also susceptible to spoofing attacks through recorded voice.

D. All of the above

14. Consists of some method of determining "something you are," "something you have," and "something you know."

A. Authorization

B. Authentication

C. Three Factor Authentication

D. Biometric Verification

15. Acronym for confidentiality, integrity, and accessibility.

A. Matching

B. Trust

C. CIA

D. Token

Answers for Self Assessment

1.	C	2.	D	3.	B	4.	C	5.	D
6.	B	7.	D	8.	B	9.	A	10.	C
11.	C	12.	D	13.	D	14.	C	15.	C

Review Questions

1. Explain the difference between Authentication and Authorization.
2. Explain the different types of user authentication methods with the help of there use in real world.
3. Explain the properties for setting a secure password

Further Reading

https://www.securid.com/content/dam/en/e-book/user-authentication-trends.pdf

Web Links

https://www.usenix.org/system/files/conference/ase17/ase17_supplement_stobert.pdf

Unit 08: Access Control

CONTENTS

Objectives

- Understand about the concept of Access Control
- Acquire the knowledge about different types of Access Control Models
- Learn about the basics of identity, credentials, and Access management
- Evaluate how to implement different Authentication method

Introduction

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

8.1 Why is access control important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information (PII) and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

How access control works?

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address. Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology (IT) they are trying to protect.

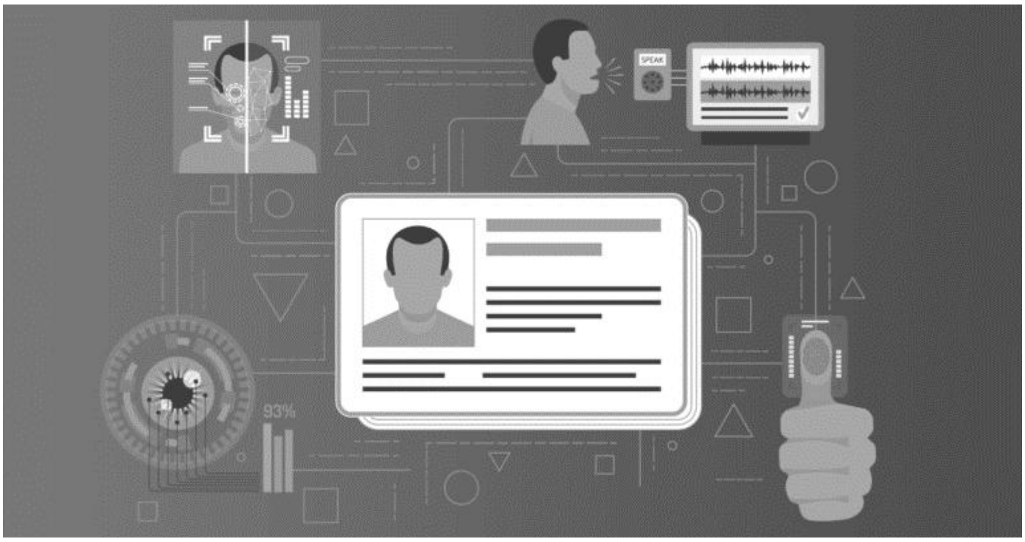
8.2 Elements of Access Control

Effective security starts with understanding the principles involved. Simply going through the motions of applying some memory set of procedures isn't sufficient in a world where today's "best practices" are tomorrow's security failures. IT security is a fast-moving field, and knowing how to perform the actions necessary for accepted practices isn't enough to ensure the best security possible for your systems.

Among the most basic of security concepts is access control. It's so fundamental that it applies to security of any type -- not just IT security. Everything from getting into your car to launching nuclear missiles is protected, at least in theory, by some form of access control. Because of its universal applicability to security, access control is one of the most important security concepts to understand.

The key to understanding access control security is to break it down. There are three core elements to access control. Of course, we're talking in terms of IT security here, but the same concepts apply to other forms of access control.

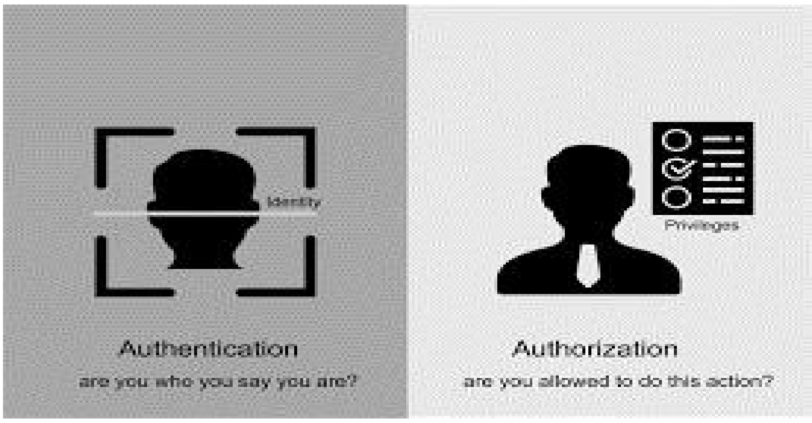
Identification: For access control to be effective, it must provide some way to identify an individual. The weakest identification capabilities will simply identify someone as part of a vague, poorly defined group of users who should have access to the system. Your TechRepublic username, a PGP e-mail signature, or even the key to the server closet provides some form of identification.



Authentication: Identification requires authentication. This is the process of ensuring that the identity in use is authentic -- that it's being used by the right person. In its most common form in IT security, authentication involves validating a password linked to a username. Other forms of authentication also exist, such as fingerprints, smartcards, and encryption keys.

your SMS code:
24 - 55 - 14 - 20
2-STEP AUTHENTICATION
It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged.
login
name
password
sms code
next

Authorization: The set of actions allowed to a particular identity makes up the meat of authorization. On a computer, authorization typically takes the form of read, write, and execution permissions tied to a username.


Identity
Authentication
are you who you say you are?
Privileges
Authorization
are you allowed to do this action?

These three elements of access control combine to provide the protection you need -- or at least they do when implement so they cannot be circumvented. For the example of simple access to basic system utilities on a workstation or server, identification is necessary for accounting (i.e., tracking user behavior) and providing something to authenticate. Authentication is necessary to ensure the identity isn't being used by the wrong person, and authorization limits an identified, authenticated user from engaging in prohibited behavior (such as deleting all your backups).

Depending on the type of security you need, various levels of protection may be more or less important in a given case. Access to a meeting room may need only a key kept in an easily broken lockbox in the receptionist's area, but access to the servers probably requires a bit more care.

Multi-factor authentication has recently been getting a lot of attention. Things are getting to the point where your average, run-of-the-mill IT professional right down to support technicians knows what "multi-factor authentication" means. Sadly, the same security awareness doesn't extend to the bulk of end users, who often think that passwords are "just another bureaucratic annoyance."

However, even many IT departments aren't as aware of the importance of access control as they would like to think. Sure, they may be using two-factor security to protect their laptops by combining standard password authentication with a fingerprint scanner. But if all you need to physically get to the servers is a key, and even the janitors have copies of the key, the fingerprint scanner on the laptop isn't going to mean much.

The same is true if you have important data on your laptops and there isn't any notable control on where the employees take them. There are ways around fingerprint scanners, including the ability to boot from a LiveCD operating system or even physically remove a hard drive and access it from a system that does not provide biometric access control. Some corporations and government agencies have learned the lessons of laptop control the hard way in recent months.

Remember that the fact you're working with high-tech systems doesn't rule out the need for protection from low-tech thieves. Understand the basics of access control, and apply them to every aspect of your security procedures. You shouldn't stop at access control, but it's a good place to start.

8.3 Types of Access Control

The main models of access control are the following:

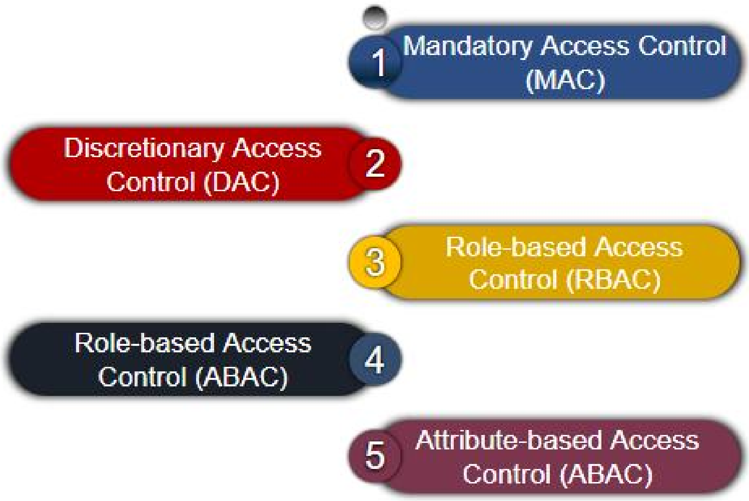
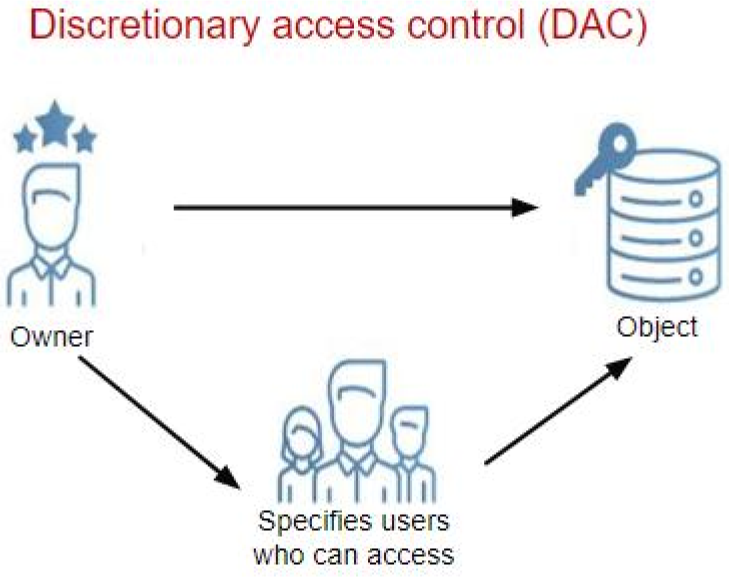

1 Mandatory Access Control (MAC)
2 Discretionary Access Control (DAC)
3 Role-based Access Control (RBAC)
4 Role-based Access Control (ABAC)
5 Attribute-based Access Control (ABAC)

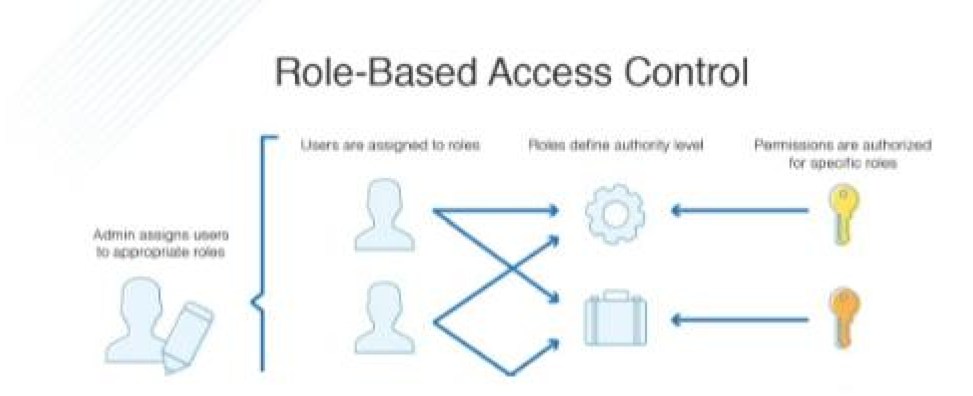
Figure 1 Types of Access Control

Mandatory access control (MAC). This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system (OS) or security kernel. It grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux (SELinux) is an implementation of MAC on the Linux OS.

Discretionary access control (DAC). This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

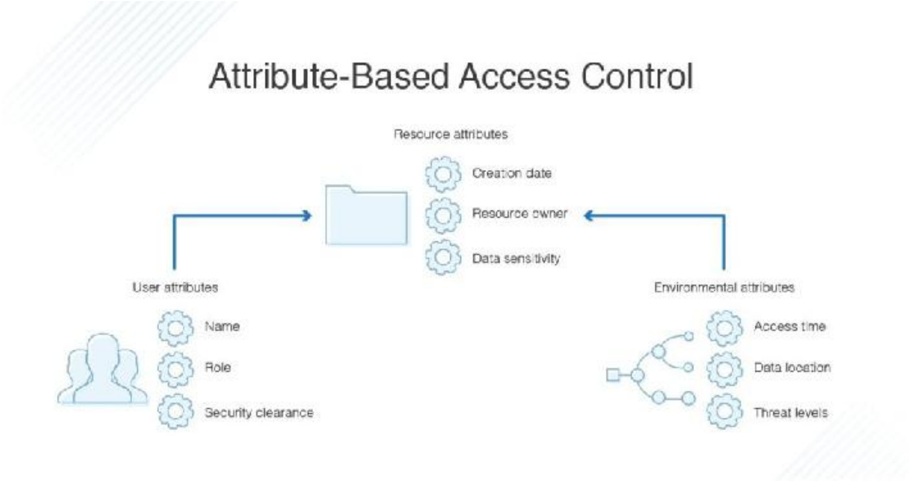

Discretionary access control (DAC)
Owner
Object
Specifies users who can access

Role-based access control (RBAC). This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.


Role-Based Access Control
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

Rule-based access control. This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.

Attribute-based access control (ABAC). This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.



8.4 Implementing Access Control

Access control is a process that is integrated into an organization's IT environment. It can involve identity management and access management systems. These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.

When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.

The best practice of least privilege restricts access to only resources that employees require to perform their immediate job functions.

Challenges of access control

Many of the challenges of access control stem from the highly distributed nature of modern IT. It is difficult to keep track of constantly evolving assets as they are spread out both physically and logically. Some specific examples include the following:

- dynamically managing distributed IT environments;
- password fatigue;
- compliance visibility through consistent reporting;
- centralizing user directories and avoiding application-specific silos; and
- data governance and visibility through consistent reporting.

Modern access control strategies need to be dynamic. Traditional access control strategies are more static because most of a company's computing assets were held on premises. Modern IT environments consist of many cloud-based and hybrid implementations, which spreads assets out over physical locations and over a variety of unique devices. A singular security fence that protects on-premises assets is becoming less useful because assets are becoming more distributed.

To ensure data security, organizations must verify individuals' identities because the assets they use are more transient and distributed. The asset itself says less about the individual user than it used to.

Organizations often struggle with authorization over authentication. Authentication is the process of verifying an individual is who they say they are through the use of biometric identification and MFA. The distributed nature of assets gives organizations many avenues for authenticating an individual.

The process that companies struggle with more is authorization, which is the act of giving individuals the correct data access based on their authenticated identity. One example of where this might fall short is if an individual leaves a job but still has access to that company's assets. This can create security holes because the asset the individual uses for work -- a smartphone with company software on it, for example -- is still connected to the company's internal infrastructure but is no longer being monitored because the individual is no longer with the company. Left unchecked, this can cause problems for an organization.

If the ex-employee's device were to be hacked, the hacker could gain access to sensitive company data unbeknownst to the company because the device is no longer visible to the company in many ways but still connected to company infrastructure. The hacker may be able to change passwords, view sensitive information or even sell employee credentials or consumer data on the dark web for other hackers to use.

One solution to this problem is strict monitoring and reporting on who has access to protected resources so that, when a change occurs, it can be immediately identified and access control lists (ACLs) and permissions can be updated to reflect the change.

Another often overlooked challenge of access control is the user experience (UX) design of access control technologies. If a particular access management technology is difficult to use, an employee may use it incorrectly or circumvent it entirely, which creates security holes and compliance gaps. If a reporting or monitoring application is difficult to use, then the reports themselves may be compromised due to an employee mistake, which then would result in a security gap because an important permissions change or security vulnerability went unreported.

8.5 Access Control Software

There are many types of access control software and technology, and often, multiple components are used together to maintain access control. The software tools may be on premises, in the cloud or a hybrid of both. They may focus primarily on a company's internal access management or may focus outwardly on access management for customers. Some of the types of access management software tools include the following:

- reporting and monitoring applications
- password management tools
- provisioning tools
- identity repositories
- security policy enforcement tools

Microsoft Active Directory (AD) is one example of software that includes most of the tools listed above in a single offering. Other vendors with popular products for identity and access management (IAM) include IBM, Idaptive and Okta.

8.6 Authentication methods to prevent Breach

There is a growing demand for different types of user authentication technologies for both online and in physical systems. The motivation to authenticate users ranges from access control reasons to business development purposes like adding e-commerce elements.

Organizations need to understand that passwords are not the only way to authenticate users. There is a wide variety of authentication technologies and an even greater range of activities that require authentication methods.

What is Authentication?

Authentication is the process of identifying users that request access to a system, network, or device. Access control often determines user identity according to credentials like username and password. Other authentication technologies like biometrics and authentication apps are also used to authenticate user identity.

Why Is User Authentication Important?

User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User A only has access to relevant information and cannot see the sensitive information of User B.

Cybercriminals can gain access to a system and steal information when user authentication is not secure. The data breaches companies like Adobe, Equifax, and Yahoo faced are examples of what happens when organizations fail to secure their user authentication.

5 Common Authentication Types

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. This is why companies are starting to implement more sophisticated incident response strategies, including authentication as part of the process. The list below reviews some common authentication methods used to secure modern systems.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

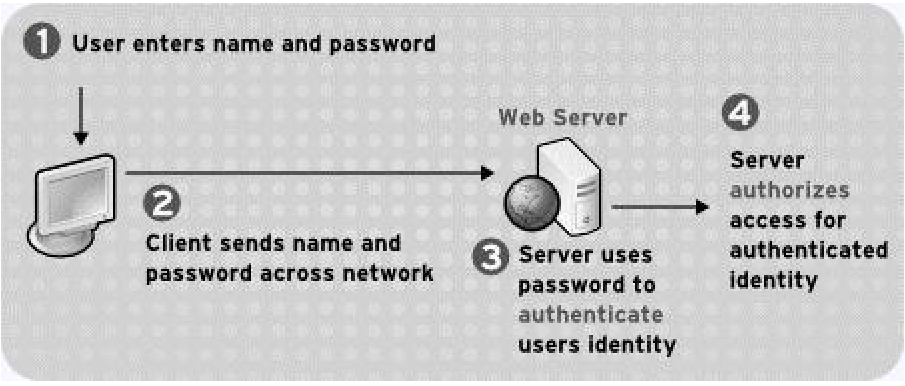

1 User enters name and password
Web Server
4
Server authorizes access for authenticated identity
2
Client sends name and password across network
3 Server uses password to authenticate users identity

Figure 2 Password Authentication Process

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.

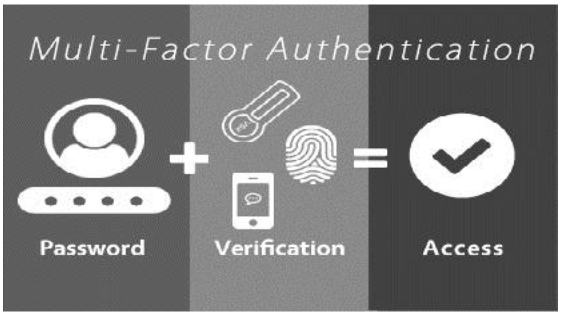


Figure 3 Defining multi Factor Authentication

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

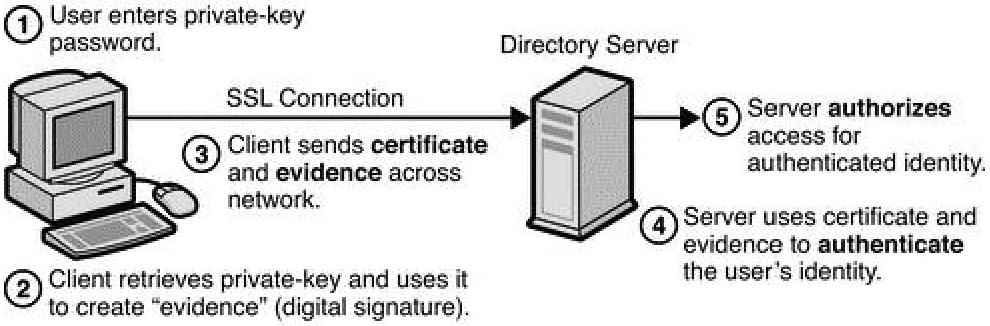

1 User enters private-key password.
Directory Server
SSL Connection
3 Client sends certificate and evidence across network.
5 Server authorizes access for authenticated identity.
4 Server uses certificate and evidence to authenticate the user's identity.
2 Client retrieves private-key and uses it to create "evidence" (digital signature).

Figure 4 Certificate based Authentication process

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication technologies:

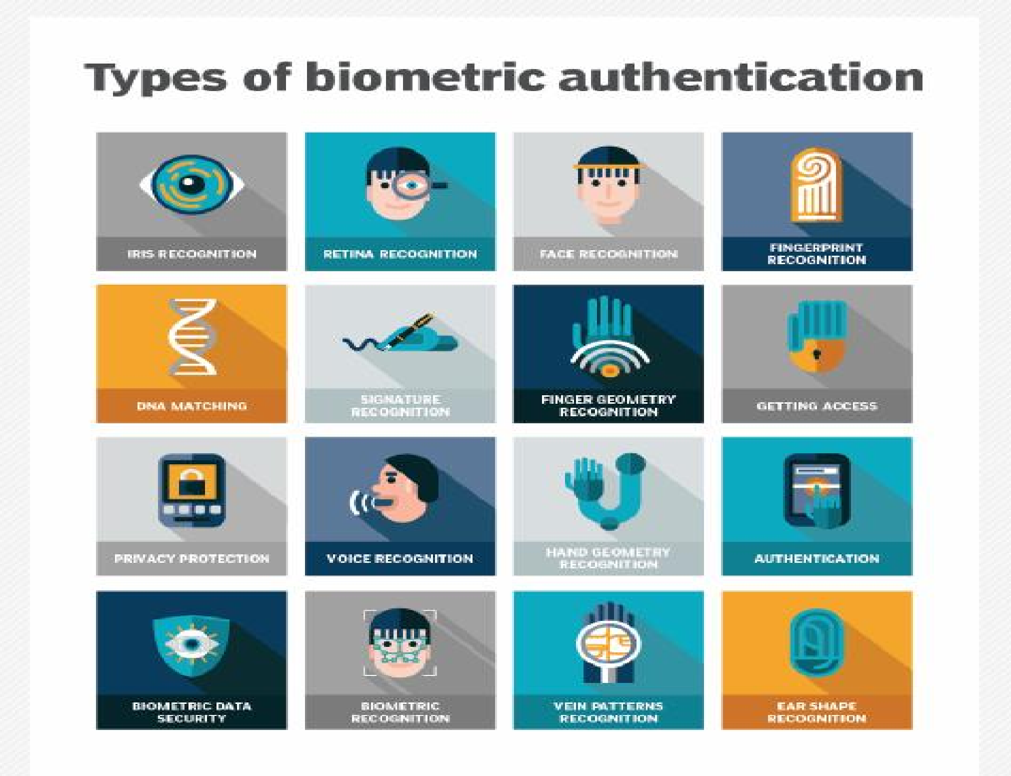
- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

- **Facial recognition—**matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners—**match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.

Task: You all are using latest technology Gadgets, right? Identify different Biometric authentication and password authentication that you people have used. Discuss them in detail.

- **Speaker Recognition —**also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.
- **Eye-scanners—**include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses



Summary

- Access control is a security technique that regulates who or what can view or use resources in a computing environment.
- To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers.
- Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.
- Access control systems perform identification, authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.

Keywords

- **Physical Access Control:**limits access to campuses, buildings, rooms and physical IT assets.
- **Logical Access Control**: limits connections to computer networks, system files and data.
- **Authentication**: This is the process of ensuring that the identity in use is authentic -- that it's being used by the right person.
- **Authorization:**The set of actions allowed to a particular identity makes up the meat of authorization.
- **Identity:** In computer technology, the unique name of a person, device, or the combination of that is recognized by a system.

- **Credential:**A credential is a piece of any document that details a qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so.

Self Assessment

1. The process of verifying the identity of a user.

A. Authentication
B. Identification
C. Validation
D. Verification

2. Which of the following does authentication aim to accomplish?

A. Restrict what operations/data the user can access
B. Determine if the user is an attacker
C. Flag the user if he/she misbehaves
D. Determine who the user is

3. Which of the following does authorization aim to accomplish?

A. Restrict what operations/data the user can access
B. Determine if the user is an attacker
C. Flag the user if he/she misbehaves
D. Determine who the user is

4. Which of the following is an authentication method?

A. Secret question
B. Biometric
C. Password
D. SMS code

5. What is the first step of access control?

A. Accountability logging

B. ACL verification

C. Subject authorization

D. Subject identification

6. ___________________ is the process of verifying or testing the validity of a claimed identity.

A. Identification

B. Authentication

C. Authorization

D. Accountability

7. Which of the following is an example of a Type 2 authentication factor?

A. Something you have, such as a smart card, ATM card, token device, and memory card

B. Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, and hand geometry

C. Something you do, such as type a pass phrase, sign your name, and speak a sentence

D. Something you know, such as a password, personal identification number (PIN), lock combination, pass phrase, mother's maiden name, and favorite color

8. Which of the following is not a reason why using passwords alone is a poor security mechanism?

A. When possible, users choose easy-to-remember passwords, which are therefore easy to guess or crack.

B. Randomly generated passwords are hard to remember, thus many users write them down.

C. Short passwords can be discovered quickly in brute force attacks only when used against a stolen password database file.

D. Passwords can be stolen through many means, including observation, recording and playback, and security database theft.

9. Which of the following is not a valid means to improve the security offered by password authentication?

A. Enabling account lockout controls

B. Enforcing a reasonable password policy

C. Using password verification tools and password cracking tools against your own password database file

D. Allowing users to reuse the same password

10. ___________________ access controls rely upon the use of labels.

A. Discretionary

B. Role-based

C. Mandatory

D. Nondiscretionary

11. What is the most important aspect of a biometric device?

A. Accuracy

B. Acceptability

C. Enrollment time

D. Invasiveness

12. _________is the measurement of things such as fingerprints and retinal scans used for security access.

A. Biometrics

B. Bio measurement

C. Computer security

D. Smart weapon machinery

13. __________Predefined set of capabilities and access to information (who can share what to who)

A. Mandatory Access Control(MAC)

B. Discretionary Access Control (DAC)

C. Attribute-based Access Control (ABAC)

D. Rule-based Access Control (RBAC)

14. ____________Access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource.

A. Mandatory Access Control(MAC)

B. Discretionary Access Control (DAC)

C. Attribute-based Access Control (ABAC)

D. Rule-based Access Control (RBAC)

15. This is a security model in which the system administrator defines the rules that govern access to resource objects______________

A. Mandatory Access Control(MAC)

B. Discretionary Access Control (DAC)

C. Attribute-based Access Control (ABAC)

D. Rule-based Access Control (RBAC)

Answers for Self Assessment

1.	A	2.	B	3.	C	4.	A	5.	D
6.	B	7.	A	8.	C	9.	D	10.	C
11.	A	12.	A	13.	A	14.	B	15.	D

Review Questions

1. Define the terms Identification, Authentication and Authorization.
2. Discuss different types of Access based authentical model with the help of examples
3. Explain 5 common times of Authentication.
4. Give some real life examples of Biometric authentication and password authentication that you use.
5. Discuss the process of Multi-Factor Authentication with the help of real life example.

Further Readings

https://www.dhs.gov/sites/default/files/publications/ACT-HB_0915-508.pdf

Web Links

https://www.youtube.com/watch?v=KKAoPqB1uxo

Unit 09: System Security

CONTENTS

Objectives

- Understand about the concept of Intruders
- Learn about Intrusion detection system
- Implement different methods for Password management
- Acquire knowledge about Intrusion Prevention System

Introduction

A significant security problem for networked systems is hostile, or at leastunwanted, trespass by users or software. User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized. Software trespass can take the form of a virus, worm, or Trojan horse.

All these attacks relate to network security because system entry can be achieved by means of a network. However, these attacks are not confined to network-based attacks. A user with access to a local terminal may attempt trespass without using an intermediate network. A virus or Trojan horse may be introduced into a system by means of an optical disc. Only the worm is a uniquely network phenomenon. Thus, system trespass is an area in which the concerns of network security and computer security overlap. Because the focus of this book is network security, we do not attempt a comprehensive analysis of either the attacks or the security countermeasures related to system trespass. Instead, in this Part we present a broad overview of these concerns. This chapter covers the subject of intruders. First, we examine the nature of the attack and then look at strategies intended for prevention and, failing that, detection. Next we examine the related topic of password management.

9.1 INTRUDERS

One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker. In an important early study of intrusion, Anderson [ANDE80] identified three classes of intruders:

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Figure 1 Masquerade Intruder

- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.Intruder attacks range from the benign to the serious.At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

Lists the following examples of intrusion:

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information,

without authorization

- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated

software and music files

- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail

password, and learning the new password

- Using an unattended, logged-in workstation without permission

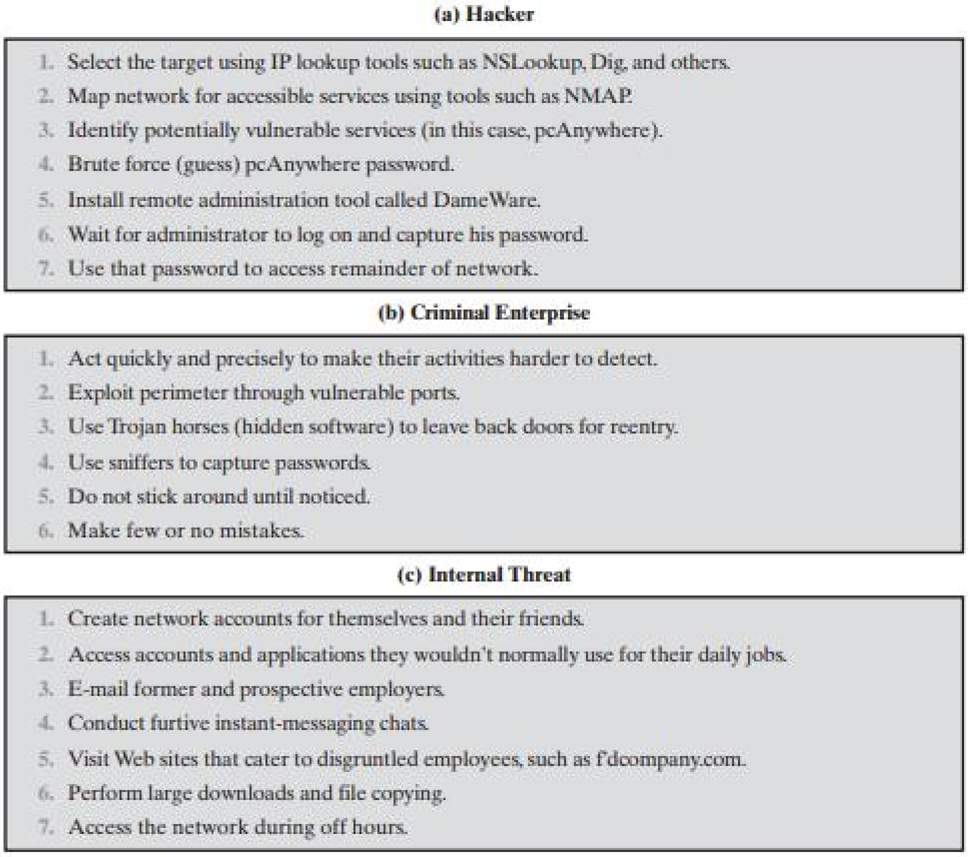
9.2 Intruder Behavior Patterns

The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures. Even

so, intruders typically follow one of a number of recognizable behavior patterns, and

these patterns typically differ from those of ordinary users. In the following, we look at three broad examples of intruder behavior patterns, to give the reader some feel for the challenge facing the security administrator. Table 20.1, based on [RADC04], summarizes the behavior.

HACKERSTraditionally, those who hack into computers do so for the thrill of it or for status. The hacking community is a strong meritocracy in which status is determined by level of competence. Thus, attackers often look for targets of opportunity and then share the information with others. A typical example is a break-in at a large financial institution reported in [RADC04]. The intruder took advantage of the fact that the corporate network was running unprotected services, some of which were not even needed. In this case, the key to the break-in was thepc. Anywhere application. The manufacturer, Symantec, advertises this program as aremote-control solution that enables secure connection to remote devices. But theattacker had an easy time gaining access to PCAnywhere; the administrator used thesame three-letter username and password for the program. In this case, there was nointrusion detection system on the 700-node corporate network. The intruder wasonly discovered when a vice president walked into her office and saw the cursormoving files around on her Windows workstation.



(a) Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

(b) Criminal Enterprise

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

(c) Internal Threat

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

Figure 2 Example of Intruders Pattern behavior

Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users. However, there is no way in advance to know whether an intruder will be benign or malign. Consequently, even for systems with no particularly sensitive resources, there is a motivation to control this problem. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are designed to counter this type of hacker threat. In addition to using such systems, organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network technology.One of the results of the growing awareness of the intruder problem has beenthe establishment of a number of computer emergency response teams (CERTs).These cooperative ventures collect information about system vulnerabilities anddisseminate it to systems managers. Hackers also routinely read CERT reports.Thus, it is important for system administrators to quickly insert all software patchesto discovered vulnerabilities. Unfortunately, given the complexity of many IT

systems, and the rate at which patches are released, this is increasingly difficult toachieve without automated updating. Even then, there are problems caused byincompatibilities resulting from the updated software. Hence the need for multiplelayers of defense in managing security threats to IT systems.

Criminals

Organized groups of hackers have become a widespread and common threat to Internet-based systems. These groups can be in the employ of a corporation or government but often are loosely affiliated gangs of hackers. Typically, these gangs are young, often Eastern European, Russian, or southeast Asian hackers who do business on the Web [ANTE06]. They meet in underground forums with names like DarkMarket.org and theftservices.com to trade tips and data and coordinate attacks. A common target is a credit card file at an e-commerce server. Attackers attempt to gain root access. The card numbers are used by organized crime gangs to purchase expensive items and are then posted to carder sites, where others can access and use the account numbers; this obscures usage patterns and complicates investigation. Whereas traditional hackers look for targets of opportunity, criminal hackers usually have specific targets, or at least classes of targets in mind. Once a site is penetrated, the attacker acts quickly, scooping up as much valuable information as possible and exiting. IDSs and IPSs can also be used for these types of attackers, but may be less effective because of the quick in-and-out nature of the attack. For e-commerce sites, database encryption should be used for sensitive customer information, especially credit cards. For hosted e-commerce sites (provided by an outsider service), the e-commerce organization should make use of a dedicated server (not used to support multiple customers) and closely monitor the provider’s security services.

INSIDER

ATTACKS Insider attacks are among the most difficult to detect and prevent. Employees already have access and knowledge about the structure and content of corporate databases. Insider attacks can be motivated by revenge or simply a feeling of entitlement. An example of the former is the case of Kenneth Patterson, fired from his position as data communications manager for American Eagle Outfitters. Patterson disabled the company’s ability to process credit card purchases during five days of the holiday season of 2002. As for a sense of entitlement, there have always been many employees who felt entitled to take extra office supplies for home use, but this now extends to corporate data. An example is that of a vice president of sales for a stock analysis firm who quit to go to a competitor. Before she left, she copied the customer database to take with her. The offender reported feeling no animus toward her former employee; she simply wanted the data because it would be useful to her. Although IDS and IPS facilities can be useful in countering insider attacks, other more direct approaches are of higher priority. Examples include the following:

- Enforce least privilege, only allowing access to the resources employees need

to do their job.

- Set logs to see what users access and what commands they are entering.
- Protect sensitive resources with strong authentication.
- Upon termination, delete employee’s computer and network access.
- Upon termination, make a mirror image of employee’s hard drive before reissuing it. That evidence might be needed if your company information turns up at a competitor.

9.3 Different types of Intrusion Detection Systems

IDSes come in different flavors and detect suspicious activities using different methods, including the following:

A network intrusion detection system(NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

A host intrusion detection system (HIDS) runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A HIDS has an advantage over an NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that an NIDS has failed to detect. A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

A signature-based intrusion detection system (SIDS) monitors all the packets traversing the network and compares them against a database of attack signatures or attributes of known malicious threats, much like antivirus software.

An anomaly-based intrusion detection system (AIDS) monitors network traffic and compares it against an established baseline to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type often uses machine learning to establish a baseline and accompanying security policy. It then alerts IT teams to suspicious activity and policy violations. By detecting threats using a broad model instead of specific signatures and attributes, the anomaly-based detection method improves upon the limitations of signature-based methods, especially in the detection of novel threats.

Historically, intrusion detection systems were categorized as passive or active. A passive IDS that detected malicious activity would generate alert or log entries but would not take action. An active IDS, sometimes called an intrusion detection and prevention system (IDPS), would generate alerts and log entries but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Snort -- one of the most widely used intrusion detection systems -- is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems (OSes), with a version available for Windows as well.

9.4 Capabilities of Intrusion Detection Systems

Intrusion detection systems monitor network traffic in order to detect when an attack is being carried out by unauthorized entities. IDSes do this by providing some -- or all -- of the following functions to security professionals:

- monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing, or recovering from cyberattacks.
- providing administrators, a way to tune, organize and understand relevant OS audit trails and other logs that are otherwise difficult to track or parse.
- providing a user-friendly interface so nonexpert staff members can assist with managing system security.
- including an extensive attack signature database against which information from the system can be matched.
- recognizing and reporting when the IDS detects that data files have been altered.
- generating an alarm and notifying that security has been breached; and
- reacting to intruders by blocking them or blocking the server.

9.5 Intrusion Techniques

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a back door into the system. Alternatively, the intruder attempts to acquire information that should have been protected. In some cases, this information is in the form of a user password. With knowledge of some other user's password, an intruder can log in to a system and

exercise all the privileges accorded to the legitimate user. Typically, a system must maintain a file that associates a password with each authorized user. If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords. The password file can be protected in one of two ways:

- **One-way function:** The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.

- **Access control**: Access to the password file is limited to one or a very few accounts.

If one or both of these countermeasures are in place, some effort is needed for a potential intruder to learn passwords. On the basis of a survey of the literature and interviews with a number of password crackers, [ALVA90] reports the following techniques for learning passwords:

1. Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.

2. Exhaustively try all short passwords (those of one to three characters).

3. Try words in the system's online dictionary or a list of likely passwords. Examples of the latter are readily available on hacker bulletin boards.

4. Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.

5. Try users' phone numbers, Social Security numbers, and room numbers

. 6. Try all legitimate license plate numbers for this state.

7. Use a Trojan horse to bypass restrictions on access.

8. Tap the line between a remote user and the host system. The first six methods are various ways of guessing a password. If an intruder has to verify the guess by attempting to log in, it is a tedious and easily countered means of attack.

For example, a system can simply reject any login after three password attempts, thus requiring the intruder to reconnect to the host to try again. Under these circumstances, it is not practical to try more than a handful of passwords. However, the intruder is unlikely to try such crude methods. For example, if an intruder can gain access with a low level of privileges to an encrypted password file, then the strategy would be to capture that file and then use the encryption mechanism of that particular system at leisure until a valid password that provided greater privileges was discovered.

Guessing attacks are feasible, and indeed highly effective, when a large number of guesses can be attempted automatically and each guess verified, without the guessing process being detectable.

The seventh method of attack listed earlier, the Trojan horse, can be particularly difficult to counter. An example of a program that bypasses access controls was cited in [ALVA90]. A low-privilege user produced a game program and invited the system operator to use it in his or her spare time.The program did indeed play a game, but in the background it also contained code to copy the password file, which was unencrypted but access protected, into the user's file. Because the game was running under the operator's high-privilege mode, it was able to gain access to the password file. The eighth attack listed, line tapping, is a matter of physical security. Other intrusion techniques do not require learning a password.

Intruders can get access to a system by exploiting attacks such as buffer overflows on a program that runs with certain privileges. Privilege escalation can be done this way as well. We turn now to a discussion of the two principal countermeasures: detection and prevention. Detection is concerned with learning of an attack, either before or after its success. Prevention is a challenging security goal and an uphill battle at all times.The difficulty stems from the fact that the defender must attempt to thwart all possible attacks, whereas the attacker is free to try to find the weakest link in the defense chain and attack at that point.

9.6 Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) is a network security and threat prevention tool. The idea behind intrusion prevention is to create a preemptive approach to network security so potential threats can be identified and responded to swiftly. Intrusion prevention systems are thereby used to examine network traffic flows in order to find malicious software and to prevent vulnerability exploits.

An IPS is used to identify malicious activity, record detected threats, report detected threats and take preventative action to stop a threat from doing damage. An IPS tool can be used to continually monitor a network in real time.

Intrusion prevention is a threat detection method that can be utilized in a security environment by system and security administrators. These tools are useful for systems as a prevention action for observed events. In addition, with many potential ways that suspicious activity can occur, it is important to have a plan in place for detecting potential attacks.

An intrusion prevention system is made to expand on the base capabilities found in intrusion detection systems (IDSes).

How do intrusion prevention systems work?

An intrusion prevention system will work by scanning through all network traffic. To do this, an IPS tool will typically sit right behind a firewall, acting as an additional layer that will observe events for malicious content. In this way, IPS tools are placed in direct communication paths between a system and network, enabling the tool to analyze network traffic.

The following are three common approaches for an IPS tool to protect networks:

signature-based detection in which the IPS tool uses previously defined attack signatures of known network threats to detect threats and take action;

anomaly-based detection in which the IPS searches for unexpected network behavior and blocks access to the host if an anomaly is detected; and

Task: Discover the companies that are using IDS and IPS softwares.

policy-based detection in which the IPS first requires administrators to make security policies -- when an event occurs that breaks a defined security policy, an alert is sent to system administrators.

If any threats are detected, an IPS tool is typically capable of sending alerts to the administrator, dropping any malicious network packets, and resetting connections by reconfiguring firewalls, repackaging payloads and removing infected attachments from servers.

IPS tools can help fend off denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, worms, viruses or exploits, such as a zero-day exploit. According to Michael Reed, formerly of Top Layer Networks (acquired by Corero), an effective intrusion prevention system should perform more complex monitoring and analysis, such as watching and responding to traffic patterns, as well as individual packets. "Detection mechanisms can include address matching, HTTP [Hypertext Transfer Protocol] string and substring matching, generic pattern matching, TCP [Transmission Control Protocol] connection analysis, packet anomaly detection, traffic anomaly detection and TCP/UDP [User Datagram Protocol] port matching."

9.7 Types of Intrusion Detection System

Three types of intrusion prevention systems appear commonly. These types are the following:

- network behavior analysis (NBA), which analyzes network behavior for abnormal traffic flow -- commonly used for detecting DDoS attacks;

- network-based intrusion prevention system (NIPS), which analyzes a network to look for suspicious traffic -- typically surrounding protocols;
- host-based intrusion prevention system (HIPS), which are installed in a single host and used to analyze suspicious activity in one specific host.

In addition, there are other types of IPS tools, including ones that analyze wireless networks. Broadly speaking, however, an intrusion prevention system can be said to include any product or practice used to keep attackers from gaining access to your network, such as firewalls and antivirus software.

Benefits of intrusion prevention systems

Benefits of intrusion prevention systems include the following:

- lowering the chances of security incidents;
- providing dynamic threat protection;
- automatically notifying administrators when suspicious activity is found.
- mitigating attacks such as zero-day threats, DoS attacks, DDoS attacks and brute-force attack attempts;
- reducing maintenance of networks for IT staff; and
- allowing or denying specific incoming traffic to a network.

Disadvantages of intrusion prevention systems

Disadvantages to intrusion prevention systems include the following:

- When a system blocks abnormal activity on a network assuming it is malicious, it may be a false positive and lead to a DoS to a legitimate user.
- If an organization does not have enough bandwidth and network capacity, an IPS tool could slow a system down.
- If there are multiple IPSes on a network, data will have to pass through each to reach the end user, causing a loss in network performance.
- IPS may also be expensive.

9.8 IPS vs. IDS

IDSes are software tools made to detect and monitor network traffic. Both IPS and IDS tools will read network packets and compare their contents with known threats. However, IDS differs in what actions are taken next. An IDS tool will not take any action on its own. An IDS requires a human to analyze results and make decisions on what to do next. This is why IPS is seen as an extension to IDS.

An IDS is designed to monitor a network and to send alerts to administrators if a threat is found. However, an IPS is designed to control network access and to protect a network from harm.

Like an IDS, an IPS will monitor network traffic. However, because an exploit may be carried out quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that Internet Protocol (IP) address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

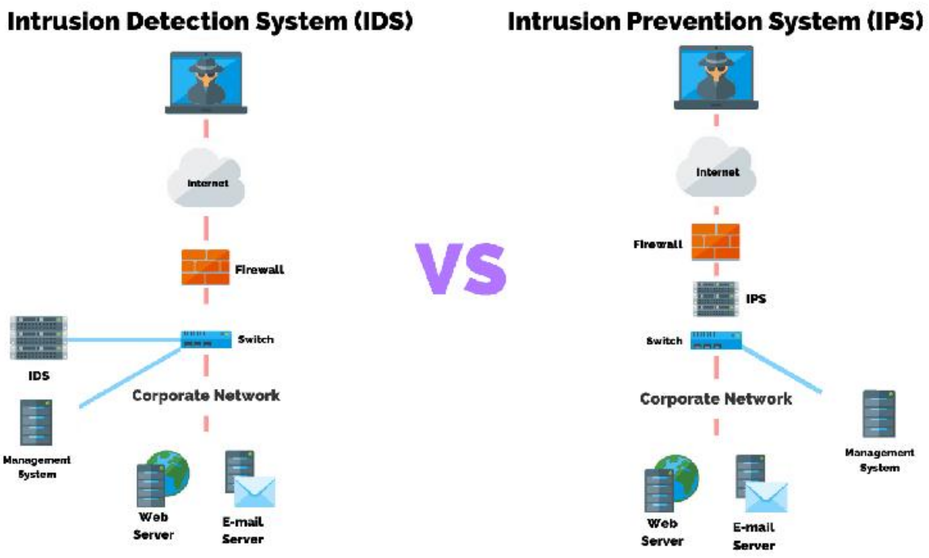


Figure 3 Difference between IDS vs IPS

9.9 Approaches to Intrusion Detection and Prevention

IDS stands for Intrusion Detection System (IDS)is device or software application that monitors network or systems for malicious activity or policy violations. There are six basic approaches to Intrusion Detection and Prevention. Some of these methods are implemented inside various software packages, and others are simply strategies that an organisation can employ to decrease the likelihood of successful intrusion. Historically when IDs were first developed, Hubs were used very frequently.

Today, Switches are used rather than Hubs because with Hub after packet has travelled from its Source network to its Destination network (being routed by its destination IP Address), it finally arrives at network segment on which target is located. After it gets to that final segment, MAC Address is used to find target.

All the computers on that segment can see packet but because Destination MAC address does not match MAC address of their Network Interface Card, it ignores packet. At some point, enterprise individuals realise that if they simply chose not to ignore the packets not destined for their network card, they could see all traffic on network segment. In other words, one could look at all packets on that network segment. Thus packet sniffer was born. After that, it was simply matter of time before idea came about analysing those packets for indications of an attack. Thereby giving rise to Intrusion Detection System.

Approaches to Intrusion Detection and Prevention :

1. **Pre-emptive Blocking :**

It is also called Banishment vigilance. It seeks to prevent intrusion from happening before they occur.

The above method is done by observing any danger signs of imminent threats and then blocking user or IP address from which these signs originate.

Example –

This technique includes attempts to detect early foot-printing of an imminent intrusion then blocking IP or user that is source of foot-printing activity. If Admin finds that particular IP address is source of frequent port scans and other scans of their system then they will block that IP address at firewall.

The above intrusion detection and avoidance can be quite complicated which could potentially block legitimate user by mistake. The complexity arises from distinguishing legitimate traffic from that indicative of an impending attack. This can lead to problem of false positives, in which system mistakenly identifies legitimate traffic as some form of attack.

- A software system will simply alert administrator that suspicious activity has taken place. The human admin then makes decision whether or not to block traffic.
- If software automatically blocks any addresses it deems suspicious, you run risk of blocking out legitimate users.
- It should also be noted that nothing prevents offending user from moving to different machine to continue attack.

This sort of approach should only be one part of an overall intrusion-detection strategy and not entire strategy.

2. Anomaly Detection:

It involves actual software that works to detect intrusion attempts and to then notify the administrator.

The general process is simple, system looks for any abnormal behavior. Any activity that does not match pattern of normal user access is noted and logged. The software compares observed activity against expected normal usages profiles.

Profiles are usually developed for specific user, group of users, or applications. Any activity that does not match definition of normal behaviour is considered an anomaly and is logged.

Sometimes above situation is referred to as “traceback” detection or “traceback” process. We are able to establish from where this packet was delivered.

The specific ways in which an anomaly is detected includes : Threshold Monitoring, Resource Profiling, User/Group Work Profiling, and Executable Profiling. These are explained as following below.

3. Threshold Monitoring :

Threshold monitoring pre-sets acceptable behaviour levels and observes whether these levels are exceeded. This could include something as simple as finite number of failed login attempts or something as complex as monitoring the time user is connected and amount of data user downloads.

Threshold monitoring provide definition of acceptable behaviour.

Characterizing intrusive behaviour only by threshold limits can be somewhat challenging. It is often quite difficult to establish proper threshold values or proper time frames at which to check those threshold values. This can result in high rate of false positives in which system misidentifies normal usage as probable attack.

4. Resource Profiling:

It measures the system-wide use of resources and develops historic usage profile. Abnormal readings can be indicative of illicit activity underway. It might be difficult to interpret meaning of changes in overall system usages.

An increase in usage might simply indicate something benign like an increased workflow rather than an attempt to breach security.

5. User/Group Work Profiling:

Here, the IDS maintains individual work profiles about user and groups. These users and groups are expected to obey these profiles. As the user changes his/her activities, his/her expected work profile is updated to reflect those changes. Some systems attempt to monitor interaction of short-term versus long-term profiles.

The short-term profiles capture recent changing work patterns, whereas long-term profiles provide view of usages over an extended period of time.

However, it can be difficult to profile an irregular or dynamic user base. Profiles that are defined too broadly enable any activity to pass review, whereas profiles that are defined too narrowly may inhibit user work.

6. Executable Profiling:

Executable profiling seeks to measure and monitor how programs use system resources, paying particular attention to those whose activity can always be traced to specific originating user.

Example – system services usually cannot be traced to specific user launching them.

Viruses, Trojan horses, worms, Tap-doors and other software attacks are addressed by profiling how system objects such as files and printers are normally used, not only by the user but also by other system subjects on the part of users.

If the viruses inherit all of privileges of user executing software. Software is not limited by the principle of least privilege but to only those privileges needed to properly execute. This openness architecture permits viruses to covertly change and infect totally unrelated parts of system.

Executable profiling enables IDS to identify activity that might indicate an attack. Once potential danger is identified, method of notifying administrator, such as by network message or email, is specific to individual IDS.

Summary

- Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.
- Intrusion detection systems have been developed to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.
- One important element of intrusion prevention is password management, with the goal of preventing unauthorized users from having access to the passwords of others.

Keywords

- **System Security:** Systems security refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.
- **Intruder:**An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data.
- **Clandestine user:**An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection (either).
- **Intrusion Detection System:** Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
- **Host Based Intrusion Detection:**Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
- **Network Based Intrusion Detection**: A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.
- **Honeypot:** Are decoy servers or systems setup to gather information regarding an attacker of intruder into networks or systems. It Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.

Self Assessment

1. What are strengths of Network based IDS?

A. Cost of ownership reduced
B. Malicious intent detection
C. Real time detection and response
D. All of the mentioned

2. What are the different ways to classify an IDS?

A. Zone based
B. Host & Network based
C. Network & Zone based
D. Level based

3. What are characteristics of Network based IDS ?

A. They look for attack signatures in network traffic
B. Filter decides which traffic will not be discarded or passed
C. It is programmed to interpret a certain series of packet
D. It models the normal usage of network as a noise characterization

4. What are strengths of the host based IDS?

A. Attack verification
B. System specific activity
C. No additional hardware required
D. All of the mentioned

5. A method used by an IDS that involves checking for a pattern to identify unauthorized activity

A. Pattern Matching
B. Session Splicing
C. Protocol Decoding
D. State Table

6. A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.

A. Anomaly Detection
B. Access Control List (ACL)
C. Intrusion Detection System (IDS)
D. Session Splicing

7. Your password should be ?

A. at least six characters

B. at least seven characters

C. at least eight characters

D. at most eight characters

8. Which of the following is true regarding secure password?

A. use the same password for each account.

B. use personal information

C. Random passwords are the strongest

D. None of the above

9. Does swimming1 use as secure password?

A. Yes

B. No

C. Maybe

D. Don't know

10. Which of the following is used to crack the security of a system and gain access for stealing data?

A. System hacking

B. hacking methodologies

C. online attack

D. offline attack

11. The ________ needs _________ to the system that is having a password file or the hacker needs to crack the system by other means.

A. Physical access, Offline attack

B. Offline attack, Physical access

C. Physical access, Online attack

D. Online attack, Physical access

12. Ideally, what characters should you use in a password to make it strong?

A. Letters and Numbers only

B. Mixed Case (Upper and Lower) Characters

C. Special Characters

D. All of the above

13. What can you do to avoid forgetting the strong passwords as they can be difficult to remember?

A. Use mnemonics

B. Develop a password strategy

C. Use password management software with encryption

D. All of the above

14. Which one of the following statements about a password is TRUE?

A. It must be changed only if it is compromised.

B. It cannot contain special character symbols.

C. It must be registered with the system administrator.

D. It should be changed regularly.

15. When it's time to change your password, what's the best way to choose a new one?

A. Add a number or special character to the end of your old password.

B. Pick something easy to remember, such as a football team or your birthday.

C. Choose something quick and easy to type in so nobody can see it.

D. Choose something you can remember, but modify it with a complex pattern that only you know.

Answers for Self Assessment

1.	D	2.	B	3.	A	4.	D	5.	A
6.	C	7.	A	8.	C	9.	B	10.	A
11.	B	12.	D	13.	D	14.	D	15.	D

Review Questions

1. What are Intruders?
2. Discuss Intrusion Detection System.
3. Explain different types of Intrusion Detection System.
4. Explain the difference between Host based detection and Network based detection.
5. Define Honeypots.
6. Discuss Signature Based IDS.
7. Discuss the concept of Intrusion Prevention System.
8. Differentiate between IPS and IDS.
9. Explain Wireless Intrusion Prevention System.

Furter Reading

https://heimdalsecurity.com/pdf/cyber_security_for_beginners_ebook.pdf

Web Links

https://phoenixnap.com/blog/intrusion-detection-system

Unit 10: Risk Analysis

CONTENTS

Objective

- Discuss about Risk analysis
- Understand the concept of Risk Management and why it is important?
- Acquire knowledge about Risk Assessment steps
- Learn about how to avoid risk with the help of risk assessments steps

Introduction

Risk analysis refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis. Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage.

What is risk analysis?

Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks.

Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur.

Why is risk analysis important?

Enterprises and other organizations use risk analysis to:

- anticipate and reduce the effect of harmful results from adverse events;
- evaluate whether the potential risks of a project are balanced by its benefits to aid in the decision process when evaluating whether to move forward with the project;
- plan responses for technology or equipment failure or loss from adverse events, both natural and human-caused; and
- identify the impact of and prepare for changes in the enterprise environment, including the likelihood of new competitors entering the market or changes to government regulatory policy.

What are the benefits of risk analysis?

Organizations must understand the risks associated with the use of their information systems to effectively and efficiently protect their information assets.Risk analysis can help an organization improve its security in a number of ways. Depending on the type and extent of the risk analysis, organizations can use the results to help:

- identify, rate and compare the overall impact of risks to the organization, in terms of both financial and organizational impacts.
- identify gaps in security and determine the next steps to eliminate the weaknesses and strengthen security.
- enhance communication and decision-making processes as they relate to information security.
- improve security policies and procedures and develop cost-effective methods for implementing these information security policies and procedures.
- put security controls in place to mitigate the most important risks.
- increase employee awareness about security measures and risks by highlighting best practices during the risk analysis process; and
- understand the financial impacts of potential security risks.

Done well, risk analysis is an important tool for managing costs associated with risks, as well as for aiding an organization's decision-making process.

10.1 Steps in Risk Analysis Process

The risk analysis process usually follows these basic steps:

Conduct a risk assessment survey: This first step, getting input from management and department heads, is critical to the risk assessment process. The risk assessment survey is a way to begin documenting specific risks or threats within each department.

1. **Identify the risks**: The reason for performing risk assessment is to evaluate an IT system or other aspect of the organization and then ask: What are the risks to the software, hardware, data and IT employees? What are the possible adverse events that could occur, such as human error, fire, flooding or earthquakes? What is the potential that the integrity of the system will be compromised or that it won't be available?
2. **Analyze the risks**: Once the risks are identified, the risk analysis process should determine the likelihood that each risk will occur, as well as the consequences linked to each risk and how they might affect the objectives of a project.
3. **Develop a risk management plan:** Based on an analysis of which assets are valuable and which threats will probably affect those assets negatively, the risk analysis should produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.

4. **Implement the risk management plan**: The ultimate goal of risk assessment is to implement measures to remove or reduce the risks. Starting with the highest-priority risk, resolve or at least mitigate each risk so it's no longer a threat.
5. **Monitor the risks:** The ongoing process of identifying, treating and managing risks should be an important part of any risk analysis process.

The focus of the analysis, as well as the format of the results, will vary depending on the type of risk analysis being carried out.

10.2 Qualitative vs. Quantitative Risk Analysis

The two main approaches to risk analysis are qualitative and quantitative. Qualitative risk analysis typically means assessing the likelihood that a risk will occur based on subjective qualities and the impact it could have on an organization using predefined ranking scales. The impact of risks is often categorized into three levels: low, medium or high. The probability that a risk will occur can also be expressed the same way or categorized as the likelihood it will occur, ranging from 0% to 100%.

Quantitative risk analysis, on the other hand, attempts to assign a specific financial amount to adverse events, representing the potential cost to an organization if that event actually occurs, as well as the likelihood that the event will occur in a given year. In other words, if the anticipated cost of a significant cyberattack is $10 million and the likelihood of the attack occurring during the current year is 10%, the cost of that risk would be $1 million for the current year.

A qualitative risk analysis produces subjective results because it gathers data from participants in the risk analysis process based on their perceptions of the probability of a risk and the risk's likely consequences. Categorizing risks in this way helps organizations and/or project teams decide which risks can be considered low priority and which have to be actively managed to reduce the effect on the enterprise or the project.

A quantitative risk analysis, in contrast, examines the overall risk of a project and generally is conducted after a qualitative risk analysis. The quantitative risk analysis numerically analyzes the probability of each risk and its consequences.

The goal of a quantitative risk analysis is to associate a specific financial amount to each risk that has been identified, representing the potential cost to an organization if that risk actually occurs. So, an organization that has done a quantitative risk analysis and is then hit with a data breach should be able to easily determine the financial impact of the incident on its operations.

A quantitative risk analysis provides an organization with more objective information and data than the qualitative analysis process, thus aiding in its value to the decision-making process.

10.3 Risk Management

Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These risks stem from a variety of sources including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents and natural disasters.

A successful risk management program helps an organization consider the full range of risks it faces. Risk management also examines the relationship between risks and the cascading impact they could have on an organization's strategic goals.

This holistic approach to managing risk is sometimes described as enterprise risk management because of its emphasis on anticipating and understanding risk across an organization. In addition to a focus on internal and external threats, enterprise risk management (ERM) emphasizes the importance of managing positive risk. Positive risks are opportunities that could increase business value or, conversely, damage an organization if not taken. Indeed, the aim of any risk management program is not to eliminate all risk but to preserve and add to enterprise value by making smart risk decisions.

We don't manage risks so we can have no risk. We manage risks so we know which risks are worth taking, which ones will get us to our goal, which ones have enough of a payout to even take them," said Forrester Research senior analyst Alla Valente, a specialist in governance, risk and compliance.

Thus, a risk management program should be intertwined with organizational strategy. To link them, risk management leaders must first define the organization's risk appetite -- i.e., the amount of risk it is willing to accept to realize its objectives.

The formidable task is to then determine "which risks fit within the organization's risk appetite and which require additional controls and actions before they are acceptable," explained Notre Dame University Senior Director of IT Mike Chapple in his article on risk appetite vs. risk tolerance. Some risks will be accepted with no further action necessary. Others will be mitigated, shared with or transferred to another party, or avoided altogether.

Every organization faces the risk of unexpected, harmful events that can cost it money or cause it to close. Risks untaken can also spell trouble, as the companies disrupted by born-digital powerhouses, such as Amazon and Netflix, will attest. This guide to risk management provides a comprehensive overview of the key concepts, requirements, tools, trends and debates driving this dynamic field.

Why is risk management important?

Risk management has perhaps never been more important than it is now. The risks modern organizations face have grown more complex, fueled by the rapid pace of globalization. New risks are constantly emerging, often related to and generated by the now-pervasive use of digital technology. Climate change has been dubbed a "threat multiplier" by risk experts.

A recent external risk that manifested itself as a supply chain issue at many companies -- the coronavirus pandemic -- quickly evolved into an existential threat, affecting the health and safety of their employees, the means of doing business, the ability to interact with customers and corporate reputations.

Businesses made rapid adjustments to the threats posed by the pandemic. But, going forward they are grappling with novel risks, including how or whether to bring employees back to the office and what should be done to make their supply chains less vulnerable to crises.

As the world continues to reckon with COVID-19, companies and their boards of directors are taking a fresh look at their risk management programs. They are reassessing their risk exposure and examining risk processes. They are reconsidering who should be involved in risk management. Companies that currently take a reactive approach to risk management -- guarding against past risks and changing practices after a new risk causes harm -- are considering the competitive advantages of a more proactive approach. There is heightened interest in supporting sustainability, resiliency and enterprise agility. Companies are also exploring how artificial intelligence technologies and sophisticated governance, risk and compliance (GRC) platforms can improve risk management.

10.4 Risk Management Process

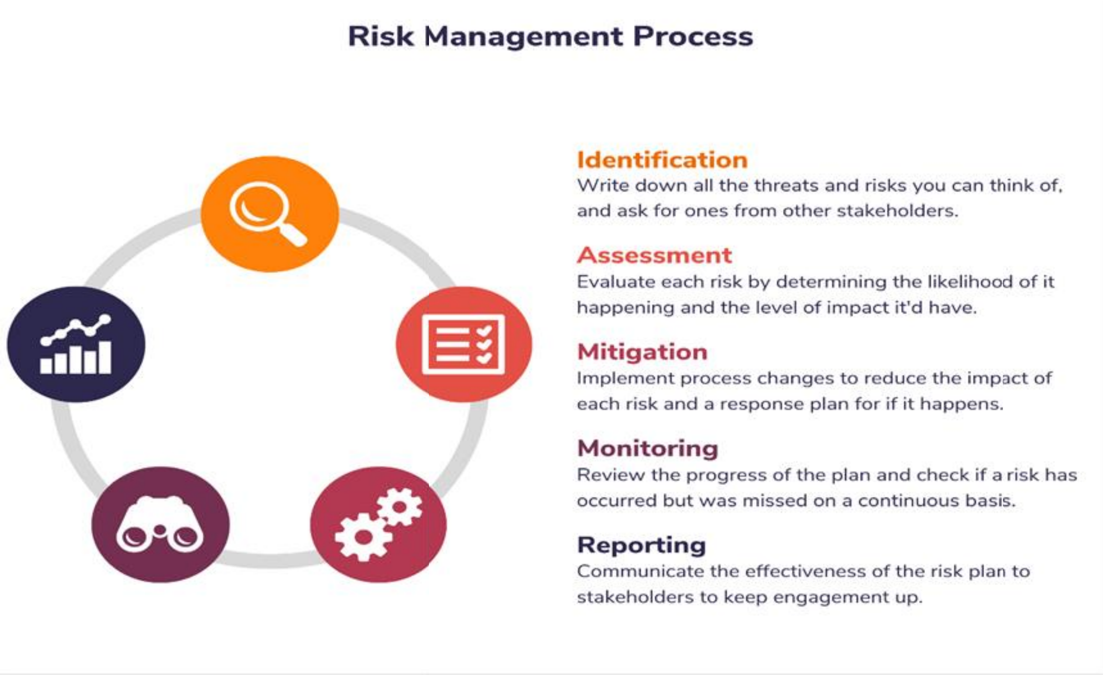
The risk management discipline has published many bodies of knowledge that document what organizations must do to manage risk. One of the best-known sources is the ISO 31000 standard, Risk Management -- Guidelines, developed by the International Organization for Standardization, a standards body commonly known as ISO.

ISO's five-step risk management process comprises the following and can be used by any type of entity:

1. Identify the risks.
2. Analyze the likelihood and impact of each one.
3. Prioritize risks based on business objectives.

4. Treat (or respond to) the risk conditions.
5. Monitor results and adjust as necessary.

Figure 1 Risk Management Steps



Risk Management Process

Identification
Write down all the threats and risks you can think of, and ask for ones from other stakeholders.

Assessment
Evaluate each risk by determining the likelihood of it happening and the level of impact it'd have.

Mitigation
Implement process changes to reduce the impact of each risk and a response plan for if it happens.

Monitoring
Review the progress of the plan and check if a risk has occurred but was missed on a continuous basis.

Reporting
Communicate the effectiveness of the risk plan to stakeholders to keep engagement up.

Task:

- Are there any new or recently updated legal and/or compliance laws we need to prepare to manage?
- Does this risk have an impact on other parts of the business? (If yes, be sure to include the risks to that department.)

	• What events have caught us off guard in the past?

Step 1: Risk identification

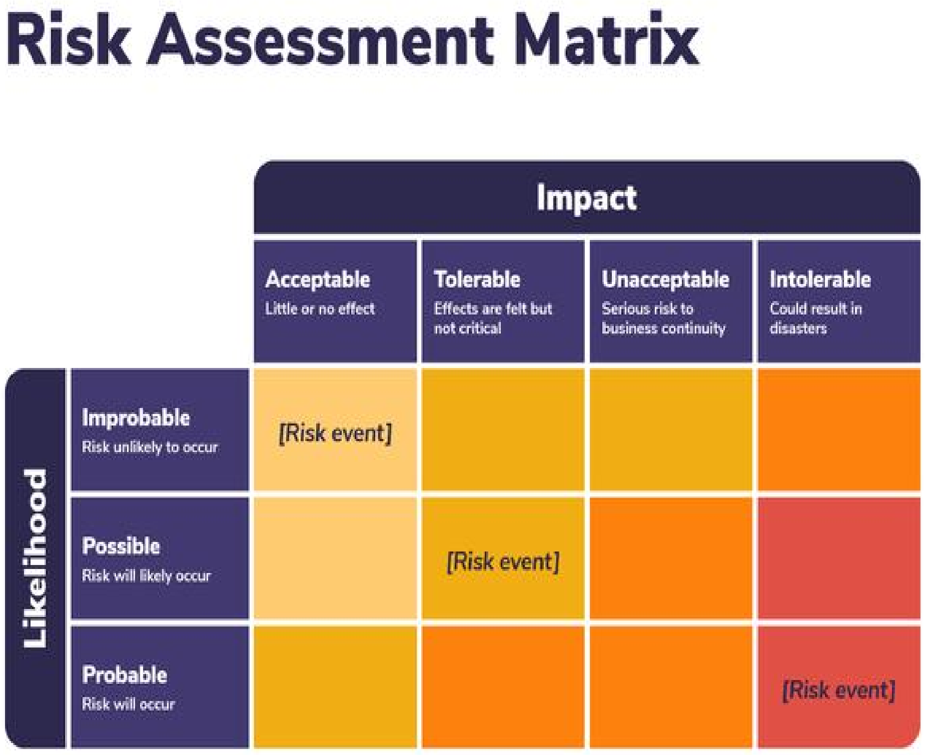
To start this process, list out any and all events that would have a negative impact on your business. Expect to add risks to your list over days, maybe even a couple weeks, and know that you won't think of all possible risks.

Be sure to ask leaders in other departments to identify risks, too. You want your plan to be as holistic and comprehensive as possible.

Step 2: Risk assessment

Now that you have a list of potential or existing threats and risks, it's time to assess the likelihood of the event happening and the level of impact. Doing this risk analysis helps determine the priority levels of each risk so you don't over- or under-allocate resources for mitigation in the next step.

Your assessment can be performed using a matrix like the one below. For each identified risk, determine both the likelihood of it happening and the level of negative impact it would have on your business. Write each risk in the corresponding box. This exercise is also best done in collaboration with leaders of each department.



Risk Assessment Matrix

		Impact			
		Acceptable Little or no effect	Tolerable Effects are felt but not critical	Unacceptable Serious risk to business continuity	Intolerable Could result in disasters
Likelihood	Improbable Risk unlikely to occur	[Risk event]			
	Possible Risk will likely occur		[Risk event]		
	Probable Risk will occur				[Risk event]

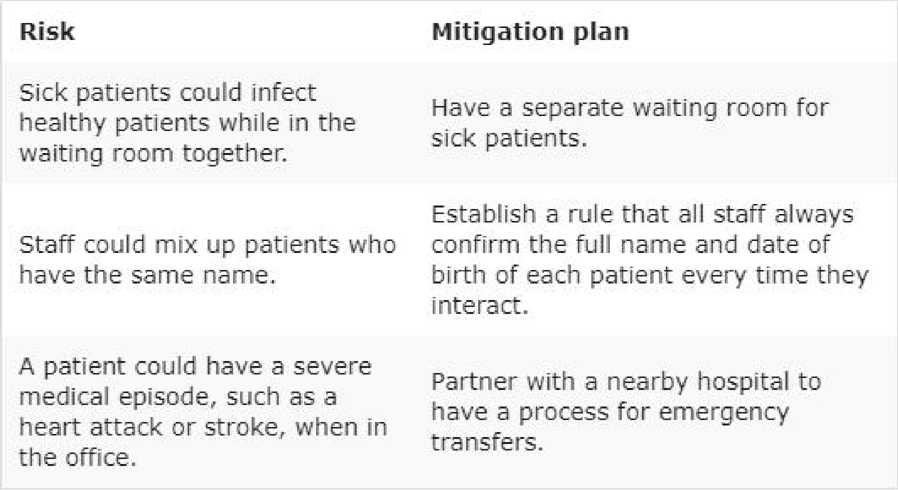
Task: Give yourself a timebox for identifying risks, otherwise you'll get stuck in analysis paralysis and never move on to the next steps. Keep in mind that this entire process is an ongoing one, so you'll continue to add risks over time.

Step 3: Risk mitigation

Risk mitigation is where you will create and begin to implement the plan for the best way to reduce the likelihood and/or impact of each risk. You may not be able to come up with a mitigation plan for each and every risk, but it's important to try to identify what changes in your current processes can be adjusted to reduce risk.

Start with the risks you placed in the red boxes of your assessment matrix. Create a mitigation plan document where you name an owner for each risk and describe the steps to be taken if/when the risk event happens. You'll do this for each risk.

As this step is rather complex, let's use a medical office as an example for risk mitigation efforts:



Risk	Mitigation plan
Sick patients could infect healthy patients while in the waiting room together.	Have a separate waiting room for sick patients.
Staff could mix up patients who have the same name.	Establish a rule that all staff always confirm the full name and date of birth of each patient every time they interact.
A patient could have a severe medical episode, such as a heart attack or stroke, when in the office.	Partner with a nearby hospital to have a process for emergency transfers.

Design your risk mitigation plans to be a natural part of business operations, wherever possible. To do this, collaborate with the other leaders in your business to coordinate mitigation efforts as seamlessly as possible into daily operations and strategic planning meetings.

Step 4: Risk monitoring

Now that you have identified, assessed, and made a mitigation plan, you need to monitor for both the effectiveness of your plan and the occurrence of risk events. Monitoring the status of risks, monitoring the effectiveness of mitigation plans implemented, and consulting with key stakeholders are all parts of the risk monitoring step. Risk monitoring should happen throughout the risk management process.

Step 5: Risk reporting

You need to document, analyze, and share the progress of your risk management plan. Reporting on risks serves two key purposes: It helps you analyze and evaluate your risk management plan and helps keep stakeholders engaged in mitigating risks by sharing the progress made.

When you first start out, reporting can be done by manually entering the status of each risk into your mitigation plan on a regular basis. Then email the report, or at least the highlights, to the other department leads.

Risk reporting is where risk management software really shines as it can gather all the data points and create an easy-to-read dashboard. If reporting on risk is an important facet of managing your risk, we strongly recommend considering investing in software.

10.5 What are the Benefits and Challenges of Risk Management?

Effectively managing risks that could have a negative or positive impact on capital and earnings brings many benefits. It also presents challenges, even for companies with mature governance, risk and compliance strategies.

Benefits of risk management include the following:

- increased awareness of risk across the organization;
- more confidence in organizational objectives and goals because risk is factored into strategy;
- better and more efficient compliance with regulatory and internal compliance mandates because compliance is coordinated;

- improved operational efficiency through more consistent application of risk processes and control;
- improved workplace safety and security for employees and customers; and
- a competitive differentiator in the marketplace.

The following are some of the challenges risk management teams should expect to encounter:

- Expenditures go up initially, as risk management programs can require expensive software and services.
- The increased emphasis on governance also requires business units to invest time and money to comply.
- Reaching consensus on the severity of risk and how to treat it can be a difficult and contentious exercise and sometimes lead to risk analysis paralysis.
- Demonstrating the value of risk management to executives without being able to give them hard numbers is difficult.

10.6 Risk Assessment

Risk assessment is the identification of hazards that could negatively impact an organization's ability to conduct business. These assessments help identify these inherent business risks and provide measures, processes and controls to reduce the impact of these risks to business operations.

Companies can use a risk assessment framework (RAF) to prioritize and share the details of the assessment, including any risks to their information technology (IT) infrastructure. The RAF helps an organization identify potential hazards and any business assets put at risk by these hazards, as well as potential fallout if these risks come to fruition.

In large enterprises, the risk assessment process is usually conducted by the Chief Risk Officer (CRO) or a Chief Risk Manager.

Risk assessment steps

How a risk assessment is conducted varies widely depending on the risks unique to the type of business, the industry that business is in and the compliance rules applied to that given business or industry. However, there are five general steps that companies can follow regardless of their business type or industry.

Step 1: Identify the hazards. The first step in a risk assessment is to identify any potential hazards that, if they were to occur, would negatively influence the organization's ability to conduct business. Potential hazards that could be considered or identified during risk assessment include natural disasters, utility outages, cyberattacks and power failure.

Step 2: Determine what, or who, could be harmed. After the hazards are identified, the next step is to determine which business assets would be negatively influenced if the risk came to fruition. Business assets deemed at risk to these hazards can include critical infrastructure, IT systems, business operations, company reputation and even employee safety.

Step 3: Evaluate the risks and develop control measures. A risk analysis can help identify how hazards will impact business assets and the measures that can be put into place to minimize or eliminate the effect of these hazards on business assets. Potential hazards include property damage, business interruption, financial loss and legal penalties.

Step 4: Record the findings. The risk assessment findings should be recorded by the company and filed as easily accessible, official documents. The records should include details on potential hazards, their associated risks and plans to prevent the hazards.

Step 5: Review and update the risk assessment regularly. Potential hazards, risks and their resulting controls can change rapidly in a modern business environment. It is important for companies to update their risk assessments regularly to adapt to these changes.

Risk assessment tools, such as risk assessment templates, are available for different industries. They might prove useful to companies developing their first risk assessments or updating older assessments.

The goal of risk assessments

Similar to risk assessment steps, the specific goals of risk assessments will likely vary based on industry, business type and relevant compliance rules. An information security risk assessment, for example, should identify gaps in the organization's IT security architecture, as well as review compliance with infosec-specific laws, mandates and regulations.

Some common goals and objectives for conducting risk assessments across industries and business types include the following:

- Developing a risk profile that provides a quantitative analysis of the types of threats the organization faces.
- Developing an accurate inventory of IT assets and data assets.
- Justifying the cost of security countermeasures to mitigate risks and vulnerabilities.
- Developing an accurate inventory of IT assets and data assets.
- Identifying, prioritizing and documenting risks, threats and known vulnerabilities to the organization's production infrastructure and assets.
- Determining budgeting to remediate or mitigate the identified risks, threats and vulnerabilities.
- Understanding the return on investment, if funds are invested in infrastructure or other business assets to offset potential risk.
- The ultimate goal of the risk assessment process is to evaluate hazards and determine the inherent risk created by those hazards. The assessment should not only identify hazards and their potential effects, but should also identify potential control measures to offset any negative impact on the organization's business processes or assets.

Summary

- Information security risk management, or ISRM, is the process of managing risks associated with the use of information technology.
- Organizations should regularly undertake comprehensive, focused assessment of potential risks to the organization
- It is important that all aspects of the activity workflow be represented on the team, including human resources, administrative processes, automated systems, and physical security.
- It is important that all aspects of the activity workflow be represented on the team, including human resources, administrative processes, automated systems, and physical security.
- Vulnerability is a weakness which a threat will exploit to attack the assets.
- Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset.
- Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.
- Risk management can be divided into four steps: risk identification, risk assessment, risk control, and risk records.

- Risk transfer involves transferring the weight or the consequence of a risk on to some other party
- A risk assessment is an examination of a given task that you undertake at work, that could potentially cause harm to people.

Keywords

1. **Vulnerabilities:**vulnerabilities are weaknesses in security that can expose assets to threats. Conduct internal audits, penetration testing, etc, to find vulnerabilities in your organization.
2. **Risk assessment**: is to analyze and measure the size of risks in order to provide information to risk control.
3. **Risk acceptance**: is also known by the name of risk retention. It is simply accepting the identified risk without taking any measures to prevent loss or the probability of the risk happening.
4. **Risk mitigation**: is where you will create and begin to implement the plan for the best way to reduce the likelihood and/or impact of each risk.
5. **Internal risks:**are from within the organization and arise during normal operation. Internal risks are often forecastable, and therefore can be avoided or mitigated. Internal risks are typically generated by one (or some combination) of human, technical or physical factors.
6. **External risks:** come from outside the organization or project and outside of the team's control. External risks tend to only be forecastable in retrospect, and therefore efforts need to be focused on recognition and reaction.
7. **Asset:**Asset is what we are trying to protect, and a threat is what we are trying to protect against.
8. **Threat**: is anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an asset.
9. **Threat Source:** is a method to exploit a vulnerability or a situation either intentionally or unintentionally.
10. **Quantitative Risk Assessment**: Mostly used by the organizations except for the financial institutions and insurance companies. Quantitative risk is Mathematically expressed as Annualized Loss Expectancy (ALE).

SelfAssessment

1. What all has to be identified as per risk identification?

A. Threats
B. Vulnerabilities
C. Consequences
D. All of the mentioned

2. Which one is not a risk management activity?

A. Risk assessment
B. Risk generation

C. Risk control

D. None of the mentioned

3. Risk management is one of the most important jobs for a

A. Client

B. Investor

C. Production team

D. Project manager

4.risk assessment is the combined effort of?

A. identifying and analyzing potential (future) events

B. making judgments on the tolerability of the risk on the basis of a risk analysis

C. Both A and B

D. None of the above

5. Risk assessment is an inherent part of a broader risk management strategy to help reduce any potential risk-related consequences.

A. True

B. False

C. Can be true or false

D. Cannot say

6. What assess the risk and your plans for risk mitigation and revise these when you learn more about the risk?

A. Risk monitoring

B. Risk planning

C. Risk analysis

D. Risk identification

7. Which of the following strategies means that the impact of the risk will be reduced?

A. Avoidance strategies

B. Minimization strategies

C. Contingency plans

D. All of the mentioned

8. A process that involves prioritizing risks for further action or analysis by assessing the impact and the probability of occurrence is called

A. Qualitative Risk Analysis

B. Risk Brainstorming

C. Quantitative Risk Analysis

D. Risk Retrospective

9. When do you perform Risk Identification?

A. At the beginning of a project.

B. During project planning.

C. During the whole lifetime of a project.

D. During project execution.

10. "Least privilege" is defined as:

A. The level of authorization granted to a user that is under investigation

B. Access to, knowledge of, or possession of information based on need to perform assigned job duties

C. Only most restrictive privileges granted based on need for job performance

D. Level of trust that is granted to system users

11. When should a risk be avoided?

A. When the risk event has a low probability of occurrence and low impact

B. When the risk event is unacceptable -- generally one with a very high probability of occurrence and high impact

C. When it can be transferred by purchasing insurance

D. A risk event can never be avoided

12. . Risk mitigation involves all but which of the following:

A. Developing system standards (policies, procedures, responsibility standards)

B. Obtaining insurance against loss

C. Identification of project risks

D. Performing contingent planning

13. Suppose a project has many hazards that could easily injure one or more persons and there is no method of avoiding the potential for damages. The project manager should consider __________ as a means of deflecting the risk.

A. abandoning the project

B. buying insurance for personal bodily injury

C. establishing a contingency fund

D. establishing a management reserve

14. Risk management can be defined as the art and science of _________ risk factors throughout the life cycle of a project.

A. researching, reviewing, and acting on

B. identifying, analyzing, and responding to

C. reviewing, monitoring, and managing

D. identifying, reviewing, and avoiding

15. When should a risk be avoided?

A. When the risk event has a low probability of occurrence and low impact

B. When the risk event is unacceptable -- generally one with a very high probability of occurrence and high impact

C. When it can be transferred by purchasing insurance

D. A risk event can never be avoided

Answers for Self Assessment

1.	D	2.	B	3.	D	4.	C	5.	A
6.	A	7.	B	8.	A	9.	C	10.	C
11.	B	12.	C	13.	B	14.	A	15.	B

Review Questions

1. What is risk management? What factors of risk are addressed by managing risk?
2. What is risk avoidance? Give an example.
3. How does the risk management process start?
4. How is risk reduction or minimization used in the process of risk management?
5. What is a risk management statement?
6. Who is responsible for compiling the risk management statement?
7. How do you decide on items of priority? What factors are considered when deciding priority?

Further Readings

https://www.files.ethz.ch/isn/47029/hb_riskanalysis&management.pdf

Web Links

https://assets.publishing.service.gov.uk/media/57a08bd1ed915d3cfd000f68/WKS081002_Annex5.pdf

Unit 11: Malicious Software

CONTENTS

Objectives

- Understanding of Malicious Software
- Acquire knowledge about different types of Malwares
- Analysis of how these malwares effect the computer system.
- Learn how to avoid various viruses to get into system.

Introduction

The words “Malicious Software” coin the word “Malware” and the meaning remains the same. Malicious Software refers to any malicious program that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.

Their mission is often targeted at accomplishing unlawful tasks such as robbing protected data, deleting confidential documents or add software without the user consent.

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malwares include computer viruses, worms, Trojan horses, ransomware, and spyware. These malicious programs steal, encrypt, and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.

What does malware do?

Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way.

Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous.

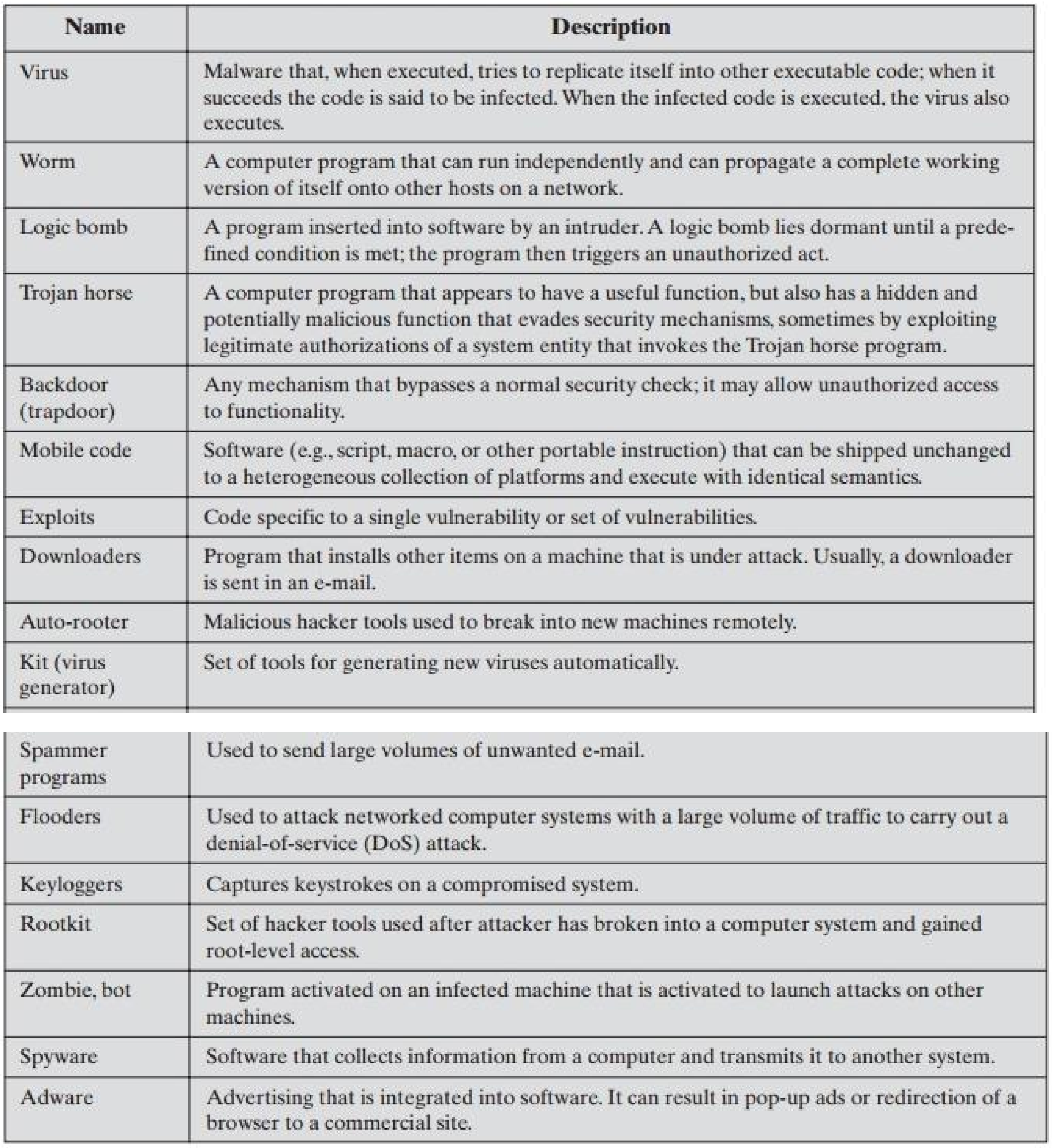
No matter the method, all types of malwares are designed to exploit devices at the expense of the user and to the benefit of the hacker -- the person who has designed and/or deployed the malware.

11.1 Types of Malicious Software

The terminology in this area presents problems because of a lack of universal agreement on all of the terms and because some of the categories overlap. Table 21.1 is a useful guide.

Malicious software can be divided into two categories: those that need a host program, and those that are independent. The former, referred to as parasitic, are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs,and backdoors are examples. Independent malware is a self-contained program that can be scheduled and run by the operating system. Worms and bot programs are examples.

We can also differentiate between those software threats that do not repli-cate and those that do. The former are programs or fragments of programs that are activated by a trigger. Examples are logic bombs, backdoors, and bot pro- grams. The latter consist of either a program fragment or an independent program that, when executed, may produce one or more copies of itself to be activated later on the same system or some other system. Viruses and worms are examples.



Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

Figure 1 Terminologies of Malicious Programs

11.2 Backdoor

A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures. Programmers have used backdoors legitimately for many years to debug and test programs; such a backdoor is called a maintenance hook. This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application. To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication. The programmer may also want to ensure that there is a method of activating the program should something be wrong with the authentication procedure that is being built into the application. The backdoor is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

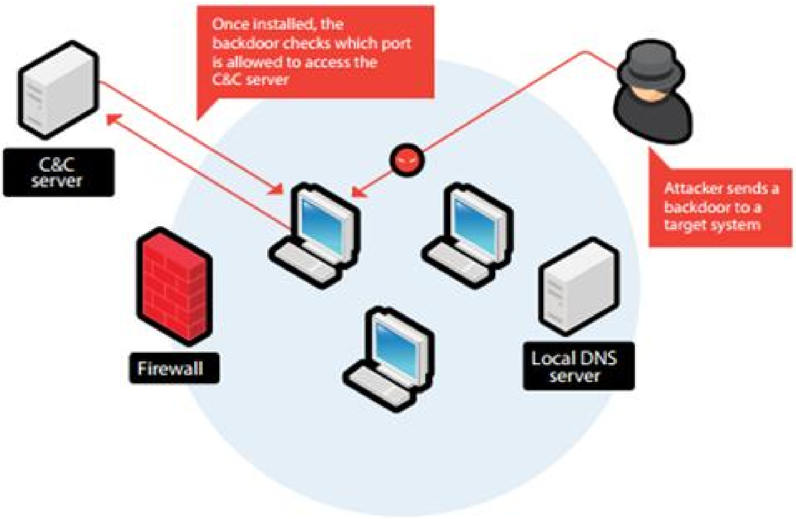

Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

Figure 2: Typical targeted attack on a corporate network

Backdoors become threats when unscrupulous programmers use them to gain unauthorized access. The backdoor was the basic idea for the vulnerability portrayed in the movie War Games. Another example is that during the development of Multics, penetration tests were conducted by an Air Force "tiger team" (simulating adversaries). One tactic employed was to send a bogus operating system update to a site running Multics. The update contained a Trojan horse (described later) that could be activated by a backdoor and that allowed the tiger team to gain access. The threat was so well implemented that the Multics developers could not find it, even after they were informed of its presence [ENGE80].

It is difficult to implement operating system controls for backdoors. Security measures must focus on the program development and software update activities.

11.3 Virus

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. A virus spreads between systems after some type of human intervention. Viruses replicate by creating their own files on an infected system, attaching themselves to a legitimate program, infecting a computer's boot process or infecting user documents. The virus requires someone to knowingly or unknowingly spread the infection. In contrast, a computer worm is standalone programming that does not require human interaction to spread. Viruses and worms are two examples of malware, a broad category that includes any type of malicious code.

A virus can be spread when a user opens an email attachment, runs an executable file, visits an infected website or views an infected website advertisement, known as malvertising. It can also be spread through infected removable storage devices, such as Universal Serial Bus (USB) drives. Once a virus has infected the host, it can infect other system software or resources, modify or disable core functions or applications, and copy, delete or encrypt data. Some viruses begin replicating as soon as they infect the host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system.

Many viruses also include evasion or obfuscation capabilities designed to bypass modern antivirus and antimalware software and other security defenses. The rise of polymorphic malware development, which can dynamically change its code as it spreads, has made viruses more difficult to detect and identify.

11.4 Types of Computer Viruses

File infectors. Some file infector viruses attach themselves to program files, usually selected COM or EXE files. Others can infect any program for which execution is requested, including SYS, OVL, PRG and MNU files. When the infected program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programs or scripts sent as an attachment to an email note.

Macro viruses. These viruses specifically target macro language commands in applications such as Microsoft Word and other programs. In Word, macros are saved sequences for commands or keystrokes that are embedded in the documents. Macro viruses, or scripting viruses, can add their malicious code to the legitimate macro sequences in a Word file. Microsoft disabled macros by default in more recent versions of Word; as a result, hackers have used social engineering schemes to convince targeted users to enable macros and launch the virus.

Overwrite viruses. Some viruses are designed specifically to destroy a file or application's data. After infecting a system, an overwrite virus begins overwriting files with its own code. These viruses can target specific files or applications or systematically overwrite all files on an infected device. An overwrite virus can install new code in files and applications that programs them to spread the virus to additional files, applications and systems.

Polymorphic viruses. A polymorphic virus is a type of malware that has the ability to change or apply updates to its underlying code without changing its basic functions or features. This process helps a virus evade detection from many antimalware and threat detection products that rely on identifying signatures of malware; once a polymorphic virus's signature is identified by a security product, the virus can then alter itself so it will no longer be detected using that signature.

Resident viruses. This type of virus embeds itself in the memory of a system. The original virus program isn't needed to infect new files or applications. Even if the original virus is deleted, the version stored in memory can be activated when the operating system (OS) loads a specific application or service. Resident viruses are problematic because they can evade antivirus and antimalware software by hiding in the system's random access memory (RAM).

Rootkit viruses. A rootkit virus is a type of malware that installs an unauthorized rootkit on an infected system, giving attackers full control of the system with the ability to fundamentally modify or disable functions and programs. Rootkit viruses were designed to bypass antivirus software, which typically scanned only applications and files. More recent versions of major antivirus and antimalware programs include rootkit scanning to identify and mitigate these types of viruses.

System or boot sector viruses. These viruses infect executable code found in certain system areas on a disk. They attach to the disk OS (DOS) boot sector on diskettes and USB thumb drives or the master boot record (MBR) on hard disks. In a typical attack scenario, the victim receives a storage device that contains a boot disk virus. When the victim's OS is running, files on the external storage device can infect the system; rebooting the system will trigger the boot disk virus. An infected storage device connected to a computer can modify or even replace the existing boot code on the infected system so that, when the system is booted next, the virus will be loaded and run immediately as part of the MBR. Boot viruses are less common now as today's devices rely less on physical storage media.

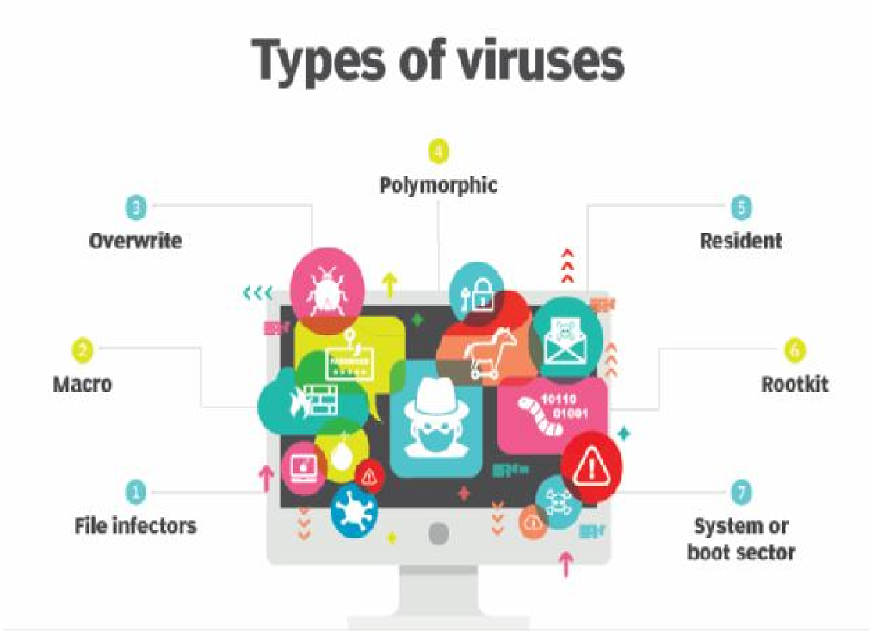


Figure 2 Types of Virus

11.5 Trojan

In computing, a Trojan horse is a program downloaded and installed on a computer that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.

Typically, the Trojan horse is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware that is hidden inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

How a Trojan horse works?

Before a Trojan horse can infect a machine, the user must download the server side of the malicious application. The Trojan horse cannot manifest by itself. The executable file (exe file) must be implemented and the program must be installed in order for the attack to be unleashed on the system. Social engineering tactics are often used to convince end users to download the malicious application. The download trap may be found in banner ads, website links or pop-up advertisements.

However, the most popular tactic for spreading Trojan horses is through seemingly unthreatening emails and email attachments. Trojan horse developers frequently use spamming techniques to send their emails to hundreds or thousands of people. As soon as the email has been opened and the attachment has been downloaded, the Trojan server will be installed and will automatically run each time the computer turns on.

It is also possible for an infected computer to continue spreading the Trojan horse to other computers.This is sometimes accomplished by turning an innocent computer into a zombie computer, meaning the person using the infected computer has no idea it is being controlled by somebody else. Hackers use these zombie computers to continue dispersing additional malware in order to create a network of zombie computers. This network is called a botnet.

Laptop and desktop computer users are not the only ones who are at risk of a Trojan horse infection. Trojans can also attack mobile devices, such as smartphones and tablets with mobile malware. This form of infection could result in an attacker redirecting traffic on these Wi-Fi connected devices and using them to commit cybercrimes.

Here is one example of how a Trojan horse might be used to infect a personal computer:

The victim receives an official-looking email with an attachment. The attachment contains malicious code that is executed as soon as the victim clicks on the attachment. Because nothing bad happens and the computer continues to work as expected, the victim does not suspect that the attachment is actually a Trojan horse and his computing device is now infected.

The malicious code resides undetected until a specific date or until the victim carries out a specific action, such as visiting a banking website. At that time, the trigger activates the malicious code and carries out its intended action. Depending upon how the Trojan has been created, it may delete itself after it has carried out its intended function, it may return to a dormant state or it may continue to be active.

Uses of a Trojan horse

When a Trojan horse becomes active, it puts sensitive user data at risk and can negatively impact performance. Once a Trojan has been transferred, it can:

- give the attacker backdoor control over the computing device;
- record keyboard strokes to steal the user's account data and browsing history;
- download and install a virus or worm to exploit a vulnerability in another program;
- install ransomware to encrypt the user's data and extort money for the decryption key;
- activate the computing device's camera and recording capabilities;
- turn the computer into a zombie computer that can be used to carry out click fraud schemes or illegal actions;
- legally capture information relevant to a criminal investigation for law enforcement.

11.6 What is spyware?

Spyware is a type of malicious software -- or malware -- that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.

Any software can be classified as spyware if it is downloaded without the user's authorization. Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused.

Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

But spyware can also be used to track a person's location, as is the case with stalker ware. Often installed secretly on mobile phones by jealous spouses, ex-partners and even concerned parents, this type of spyware can track the physical location of the victim, intercept their emails and texts, eavesdrop on their phone calls and record conversations, and access personal data, such as photos and videos.

Spyware can be difficult to detect; often, the first indication a user has that a computing device has been infected with spyware is a noticeable reduction in processor or network connection speeds and -- in the case of mobile devices -- data usage and battery life. Antispyware tools can be used to prevent or remove spyware. They can either provide real-time protection by scanning network data and blocking malicious data, or they can execute scans to detect and remove spyware already on a system.

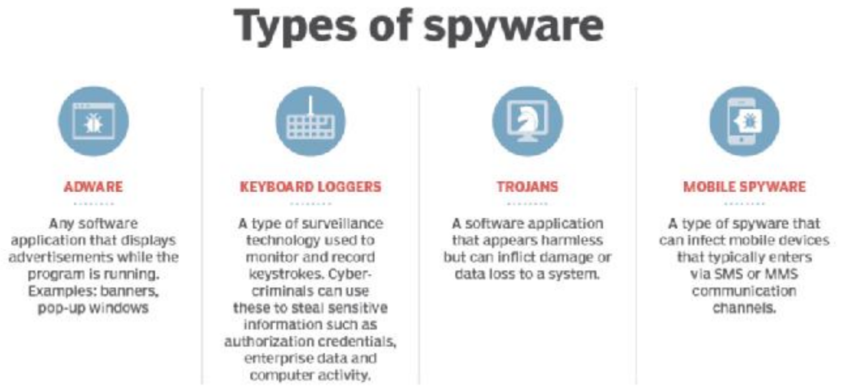
How do spyware infections occur?

Spyware infections can affect any personal computer, Mac, iOS or Android device. Some of the most common ways for computers to become infected include the following:

- pirating media such as games, videos and music by downloading and distributing copyrighted digital content without permission;
- downloading materials from unknown sources;
- accepting pop-up advertisements; and

- opening email attachments from unknown senders.

Spyware is most commonly distributed by getting potential victims to click on a link. The link can be in an email, pop-up window or ad. Malicious code can also be embedded on legitimate websites as an advertisement. Other ways for spyware to infect a machine include via drive-by download -- where spyware is downloaded just by visiting a website or viewing a HyperText Markup Language email message -- phishing links or physical devices.



Any software application that displays advertisements while the program is running. Examples: banners, pop-up windows

A type of surveillance technology used to monitor and record keystrokes. Cyber-criminals can use these to steal sensitive information such as authorization credentials, enterprise data and computer activity.

A software application that appears harmless but can inflict damage or data loss to a system.

A type of spyware that can infect mobile devices that typically enters via SMS or MMS communication channels.

Figure 3 Types of Spyware

11.7 Ransomware

Ransomware is a subset of malware in which the data on a victim's computer is locked -- typically by encryption -- and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is usually monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity is not known.

Ransomware malware can be spread through malicious attachments found in emails or in infected malicious software apps, infected external storage devices and compromised websites. Attacks have also used Remote Desktop Protocol and other approaches that do not rely on any form of user interaction.

11.8 Types of Ransomware

Attackers may use one of several different approaches to extort digital currency from their victims:

Scareware. This malware poses as security software or tech support. Ransomware victims may receive pop-up notifications saying malware has been discovered on their system. Security software that the user does not own would not have access to this information. Not responding to this will not do anything except lead to more pop-ups.

Screen lockers. Also known simply as lockers, these are a type of ransomware designed to completely lock users out of their computers. Upon starting up the computer, a victim may see what looks to be an official government seal, leading the victim into believing they are the subject of an official inquiry. After being informed that unlicensed software or illegal web content has been found on the computer, the victim is given instructions on how to pay an electronic fine. However, official government organizations would not do this; they instead would go through proper legal channels and procedures.

Encrypting ransomware. Otherwise known as data kidnapping attacks, these give the attacker access to and encrypt the victim's data and ask for a payment to unlock the files. Once this happens, there is no guarantee that the victim will get access to their data back -- even if they negotiate for it. The attacker may also encrypt files on infected devices and make money by selling a product that promises to help the victim unlock files and prevent future malware attacks.

Doxware. With this malware, an attacker may threaten to publish victim data online if the victim does not pay a ransom.

Master boot record ransomware. With this, the entire hard drive is encrypted, not just the user's personal files, making it impossible to access the operating system.

Mobile ransomware. This ransomware affects mobile devices. An attacker can use mobile ransomware to steal data from a phone or lock it and require a ransom to return the data or unlock the device.

11.9 Rootkit

A rootkit is a program or a collection of malicious software tools that give a threat actor remote access to and control over a computer or other system. Although this type of software has some legitimate uses, such as providing remote end-user support, most rootkits open a backdoor on victims' systems to introduce malicious software -- including viruses, ransomware, keylogger programs or other types of malware -- or to use the system for further network security attacks. Rootkits often attempt to prevent detection of malicious software by deactivating endpoint antimalware and antivirus software.

Rootkits, which can be purchased on the dark web, can be installed during phishing attacks or employed as a social engineering tactic to trick users into giving the rootkits permission to be installed on their systems, often giving remote cybercriminals administrator access to the system. Once installed, a rootkit gives the remote actor access to and control over almost every aspect of the operating system (OS). Older antivirus programs often struggled to detect rootkits, but today, most antimalware programs can scan for and remove rootkits hiding within a system.

Symptoms of rootkit infection

A primary goal of a rootkit is to avoid detection to remain installed and accessible on the victim's system. Although rootkit developers aim to keep their malware undetectable and there are not many easily identifiable symptoms that flag a rootkit infection, here are four indicators that a system has been compromised:

1. **Antimalware stops running**. An antimalware application that just stops running indicates an active rootkit infection.
2. **Windows settings change by themselves.** If Windows settings change without any apparent action by the user, the cause may be a rootkit infection. Other unusual behavior, such as background images changing or disappearing in the lock screen or pinned items changing on the taskbar, could also indicate a rootkit infection.
3. **Performance issues**. Unusually slow performance or high central processing unit usage and browser redirects may also point to the presence of a rootkit infection.
4. **Computer lockups**. These occur when users cannot access their computer or the computer fails to respond to input from a mouse or keyboard.

What is a keylogger?

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data.

Some uses of keyloggers could be considered ethical or appropriate in varying degrees. Keylogger recorders may also be used by:

- employers to observe employees' computer activities;
- parents to supervise their children's internet usage;
- device owners to track possible unauthorized activity on their devices; or

- law enforcement agencies to analyze incidents involving computer use.

Task: List down the best anti-virus software's that you would recommend your friends and your organization.

11.10 Advanced persistent threat (APT)

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.

APT attacks are initiated to steal data rather than cause damage to the target organization's network.

The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible. Because a great deal of effort and resources can go into carrying out APT attacks, hackers typically select high-value targets, such as nation-states and large corporations, with the goal of stealing information over a long period of time.

To gain access, APT groups often use advanced attack methods, including advanced exploits of zero-day vulnerabilities, as well as highly-targeted spear phishing and other social engineering techniques. To maintain access to the targeted network without being discovered, threat actors will continuously rewrite malicious code to avoid detection and other sophisticated evasion techniques. Some APTs are so complex that they require full-time administrators to maintain the compromised systems and software in the targeted network.

The motives of advanced persistent threat actors are varied. For example, attackers sponsored by nation-states may target intellectual property to gain a competitive advantage in certain industries. Other targets may include power distribution and telecommunications utilities and other infrastructure systems, social media, media organizations, and electoral and other political targets. Organized crime groups may sponsor advanced persistent threats to gain information they can use to carry out criminal acts for financial gain.

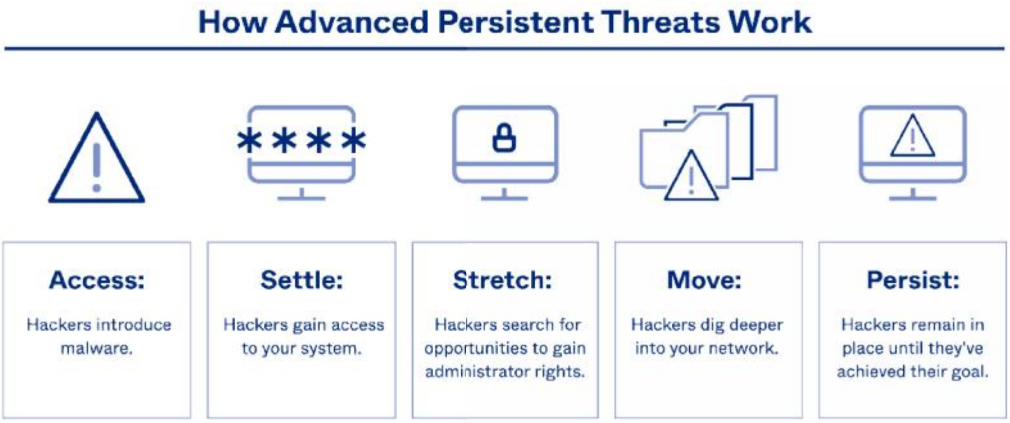
Although APT attacks can be difficult to identify, data theft is never completely undetectable. However, the act of exfiltrating data from an organization may be the only clue defenders have that their networks are under attack. Cybersecurity professionals often focus on detecting anomalies in outbound data to see if the network has been the target of an APT attack.

How an APT attack works?

Attackers executing APTs typically take the following sequential approach to gain and maintain ongoing access to a target:

- Gain access. APT groups gain access to a target by targeting systems through the internet. Normally, through spear phishing emails or via an application vulnerability with the intention of leveraging any access by inserting malicious software into the target.
- Establish a foothold. After gaining access to the target, threat actors use their access to do further reconnaissance. They use the malware they've installed to create networks of backdoors and tunnels to move around unnoticed. APTs may use advanced malware techniques such as code rewriting to cover their tracks.
- Gain even greater access. Once inside the targeted network, APT actors may use methods such as password cracking to gain administrative rights. This gives them more control of the system and get even deeper levels of access.
- Move laterally. Once threat actors have breached their target systems, including gaining administrator rights, they can then move around the enterprise network at will. They can also attempt to access other servers, as well as other secure areas of the network.

- Stage the attack. At this point, the hackers centralize, encrypt and compress the data so they can exfiltrate it.
- Take the data. The attackers harvest the data and transfer it to their own system.
- Remain until they're detected. Cybercriminals can repeat this process for long periods of time until they're detected, or they can create a backdoor so they can access the system again later.



How Advanced Persistent Threats Work

Access: Hackers introduce malware.

Settle: Hackers gain access to your system.

Stretch: Hackers search for opportunities to gain administrator rights.

Move: Hackers dig deeper into your network.

Persist: Hackers remain in place until they've achieved their goal.

11.11 What is a Denial of Service Attack?

The results of a successful DoS attack are characterized by a particular website or online service being unusually slow or entirely unreachable. This could be likened to large groups of Black Friday shoppers cramming themselves into a store, blocking entry to the people behind them, and slowing down customer traffic.

What are the symptoms of one?

When a client attempts to connect with a service that's influenced by an effective DoS attack, they may experience the following:

- Excessive load times with partially loaded data or a total failure to connect
- Inability to connect to one particular website or its services
- In the case that an ISP is targeted, all of its users may be unable to access the web
- Sudden loss of internet connection, whether to one service or all of them.

Unwitting (and unwilling) participants of a poorly controlled DDoS attack can lose their own internet connection as the attack jumps from one IP to the next in a spread sequence, knocking entire geographical locations offline. This is usually not intended, as DoS attackers are generally more interested in disabling a specific target.

A recent example of this is when the Australian Bureau of Statistics (ABS) conducted their Census, which had received over $500,000 in stress testing for quality assurance — only to be subjected to a series of DDoS attacks that resulted in multiple interruptions of service. At the time, sites like Google and Yahoo! would have worked fine — only the ABS website was down.

Motives of a DoS attack

Not all cases of mitigated or failed connection is due to DoS; however, it's a distinct possibility if the affected service has garnered a great deal of publicity lately. This is because perpetrators frequently use DoS software to temporarily disable websites, network providers, web-based services and video game hosts in order to make a statement, gain publicity, exact revenge, or simply as a show of power.

In the case of the ABS being attacked, the Census was a matter of high publicity. As with other high-profile web-based situations, such as the launch of an anticipated site or video game, the attention of unsavory individuals was captured. Attacks were administered for what was guessed to be no other reason than “because they can”.

Denial of service attacks has been used for benevolent causes as well, shutting down criminal enterprises or even singular IP addresses of criminal perpetrators. Hacktivist group Anonymous has gained traction for administering DoS attacks against organizations and people that are thought to have engaged in illicit activities.

Circumvention

Unfortunately, DoS is an effective method of briefly shutting down almost any host whose services are provided over the Internet in any form. An attack can last for minutes or hours, depending on how long the offending IP addresses continue to send superfluous requests. Hosts and legitimate clients usually have to wait it out until it’s over. There are countermeasures to mitigate the effectiveness of an attack, but there’s no surefire way to avoid it altogether.

Typically, hosts with more bandwidth and server support are more difficult to crash, but this isn’t an especially effective means of directly combating such attacks, since the scale has been rising rapidly over the years in proportion to advancements in the technology that can handle it. The volume of an attack nowadays can exceed 400Gbit/s, which could effectively bring large-scale providers to their knees.

There are other well-known methods that are implemented to mitigate the severity of DoS attacks, listed as follows.

1. **Blackholing** routes the offending traffic to a “black hole” or null server where it causes no harm.
2. **DNS sinkholing** routes all traffic to a working IP that checks packets and rejects the ones that are faulty. This is not effective for severe attacks, however.
3. **Firewalls** are effective because they can block the offending IP addresses or the ports they’re attacking. This has the drawback of also blocking legitimate requests through those ports, however.
4. **Intrusion prevention systems (IPS**) are designed to detect server requests that are not legitimate and deny them. There are multiple types of IPS, but generally speaking, DoS requests that mimic legitimate ones can bypass this countermeasure.
5. **DoS defense systems (DDS)** are similar to IPS and are designed to block malicious requests that appear legitimate.
6. **Routers** offer limitation settings and ACL features but are easily overpowered regardless. They can still mitigate the effects of an attack.
7. **Upstream filtering** routes data through numerous means of network cleaning systems that identify malicious traffic and separate it from the traffic that’s legitimate. This is offered as a service by companies such as Arbor Networks, AT&T, Verizon, Cloudflare, Radware, and more.

The problem with preventing malicious requests is that there’s no effective way to know what the request will be until it’s already in the system and pulling on its resources. Blocking malicious traffic tends to be much like blocking an entire highway: The bad traffic is halted, but so is the good.

Summary

- Malware is a broad term that refers to a variety of malicious programs.
- Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.
- Worms have probably been around the longest, though when they first started surfacing they were hardly as malicious as today's malware. A worm, as well as a virus for that matter, is a self-propagating computer program.
- The most recent trends in malware are related to the increasing criminalization of online threats. One of these threats, bots, is either on the rise or people are just starting to realize the dangers of being infected by one.
- Bot makers and distributors infect multiple systems to create massive botnets that can be used to launch Distributed Denial of Service attacks or as spam distributors -- which is, unfortunately, a lucrative endeavor.
- Scareware is malware that scares people into making some purchase. One common example is malware that displays a message on a device that the device is infected with some virus that only a particular security package can remove, with a link to purchase that "security software."
- Zero Day malware is any malware that exploits a vulnerability not previously known to the public or to the vendor of the technology containing the vulnerability.

Keywords

- **BOT**: Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc), it is becoming increasingly common to see bots being used maliciously.
- **BUG**:a bug is a flaw produces an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program**.**
- **Worms:** A computer worm is a standalone piece of malware that replicates itself without the need for any host in order to spread. Worms often propagate over networks by exploiting security vulnerabilities on target computers and networks. Because they normally consume network bandwidth, worms can inflict harm even without modifying systems or stealing data.
- **Spyware** –Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
- **Rootkits** –A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Viruses –**A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
- **Trojan horse –**A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.
- **Backdoors –**A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Self Assessment

1. Computer virus is simply meaning is _______________

A. hardware component

B. disease

C. set of computer instructions or code

D. Type of bacteria

2. What is the name of the viruses that fool a user into downloading and/or executing them by pretending to be useful applications?

A. Cracker

B. Worm

C. Trojan horses

D. Keylogger

3. What kind of attempts is made by individuals to obtain confidential information from a person by falsifying their identity?

A. Computer viruses

B. Spyware scams

C. Phishing scams

D. None of the above

4. Delayed payload of some viruses is also called as

A. Time

B. Bomb

C. Anti-virus

D. None of the above

5. The difference between a virus and a self-replicating program which is like a virus is that rather than creating copies of itself on only one system it propagate through computer network. What is the self replicating program called?

A. Keylogger

B. Cracker

C. Worm

D. All of the above

6. Which one of the following can be considered as the class of computer threats?

A. Dos Attack

B. Phishing

C. Soliciting

D. Both A and C

7. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

A. Malware

B. Spyware

C. Adware

D. All of the above

8. _______ is a type of software designed to help the user's computer detect viruses and avoid them.

A. Malware

B. Adware

C. Antivirus

D. Both B and C

9. Which one of the following is a type of antivirus program?

A. Quick heal

B. Mcafee

C. Kaspersky

D. All of the above

10. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_______:

A. Antivirus

B. Firewall

C. Cookies

D. Malware

11. In system hacking, which of the following is the most crucial activity?

A. Information gathering

B. Covering tracks

C. Cracking passwords

D. None of the above

12. Rootkit is

A.an application that captures TCP/IP data packets, which can maliciously be used to capture passwords and other data while it is in transit either within the computer or over the network.

B. a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining illegitimate access.

C. a toolkit for hiding the fact that a computer's security has been compromised, is a general description of a set of programs which work to subvert control of an operating system from its legitimate (in accordance with established rules) operators.

D. None of these

13. A ___________ is a small malicious program that runs hidden on infected system.

A. Virus

B. Trojan

C. Shareware

D. Adware

14. Trojans do not do one of the following. What is that?

A. Deleting Data
B. Protecting Data
C. Modifying Data
D. Copying Data

15. When a logic bomb is activated by a time-related event, it is known as a:

A. Time-related bomb sequence
B. Virus
C. Time bomb
D. Trojan horse.

Answers for Self Assessment

1.	C	2.	C	3.	C	4.	B	5.	C
6.	A	7.	B	8.	C	9.	D	10.	B
11.	C	12.	B	13.	B	14.	B	15.	C

Review Questions

1. Explain Malware and Malware Softwares.
2. Discuss Phishing attack in detail.
3. Explain the different between DoS and DDOS.
4. Discuss different types of Malware in detail.
5. What is the effect of Rootkit?
6. Define Advance Persistent Threat.
7. What do you mean by Spam? Give some example of it.
8. Show the working of DDos attack along with the help of the diagram.
9. List done some of the parameters to avoid Rootkit attack.
10. What do mean by Bots? How it is different from Dos.

Further Reading

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf

Web Links

https://ftms.edu.my/v2/wpcontent/uploads/2019/02/csca0101_ch08.pdf

Unit 12: Software Level Security

CONTENTS

Objectives

- Understand the concept of Operating System Security
- Learn about System hardening along with its different types
- Acquire knowledge about Security Maintenance steps
- Identify the concept of Virtualization and Para Virtualization

Introduction

Security of computing systems is a vital topic whose importance only keeps increasing. Much money has been lost and many people's lives have been harmed when computer security has failed. Attacks on computer systems are so common as to be inevitable in almost any scenario where you perform computing. Generally, all elements of a computer system can be subject to attack, and flaws in any of them can give an attacker an opportunity to do something you want to prevent. But operating systems are particularly important from a security perspective.

Why? To begin with, pretty much everything runs on top of an operating system. As a rule, if the software you are running on top of, whether it be an operating system, a piece of middleware, or something else, is insecure, what's above it is going to also be insecure. It's like building a house on sand. You may build a nice solid structure, but a flood can still wash away the base underneath your home, totally destroying it despite the care you took in its construction. Similarly, your application might perhaps have no security flaws of its own, but if the attacker can misuse the software underneath you to steal your information, crash your program, or otherwise cause you harm, your own efforts to secure your code might be for naught.

This point is especially important for operating systems. You might not care about the security of a particular web server or database system if you don't run that software, and you might not care about the security of some middleware platform that you don't use, but everyone runs an operating system, and there are relatively few choices of which to run. Thus, security flaws in an operating system, especially a widely used one, have an immense impact on many users and many pieces of software.

Another reason that operating system security is so important is that ultimately all of our software relies on proper behavior of the underlying hardware: the processor, the memory, and the peripheral devices. What has ultimate control of those hardware resources? The operating system.

Thinking about what you have already studied concerning memory management, scheduling, file systems, synchronization, and so forth, what would happen with each of these components of your operating system if an adversary could force it to behave in some arbitrarily bad way? If you understand what you've learned so far, you should find this prospect deeply disturbing1 . Our computing lives depend on our operating systems behaving as they have been defined to behave, and particularly on them not behaving in ways that benefit our adversaries, rather than us. The task of securing an operating system is not an easy one, since modern operating systems are large and complex. Your experience in writing code should have already pointed out to you that the more code you've got, and the more complex the algorithms are, the more likely your code is to contain flaws. Failures in software security generally arise from these kinds of flaws. Large, complex programs are likely to be harder to secure than small, simple programs. Not many other programs are as large and complex as a modern operating system.

Another challenge in securing operating systems is that they are, for the most part, meant to support multiple processes simultaneously. As you've learned, there are many mechanisms in an operating system meant to segregate processes from each other, and to protect shared pieces of hardware from being used in ways that interfere with other processes. If every process could be trusted to do anything it wants with any hardware resource and any piece of data on the machine without harming any other process, securing the system would be a lot easier. However, we typically don't trust everything equally. When you download and run a script from a web site you haven't visited before, do you really want it to be able to wipe every file from your disk, kill all your other processes, and start using your network interface to send spam email to other machines? Probably not, but if you are the owner of your computer, you have the right to do all those things, if that's what you want to do. And unless the operating system is careful, any process it runs, including the one running that script you downloaded, can do anything you can do.

Consider the issue of operating system security from a different perspective. One role of an operating system is to provide useful abstractions for application programs to build on. These applications must rely on the OS implementations of the abstractions to work as they are defined. Often, one part of the definition of such abstractions is their security behavior. For example, we expect that the operating system's file system will enforce the access restrictions it is supposed to enforce. Applications can then build on this expectation to achieve the security goals they require, such as counting on the file system access guarantees to ensure that a file they have specified as un-writeable does not get altered. If the applications cannot rely on proper implementation of security guarantees for OS abstractions, then they cannot use these abstractions to achieve their own security goals. At the minimum, that implies a great deal more work on the part of the application developers, since they will need to take extra measures to achieve their desired security goals. Taking into account our earlier discussion, they will often be unable to achieve these goals if the abstractions they must rely on (such as virtual memory or a well-defined scheduling policy) cannot be trusted. Obviously, operating system security is vital, yet hard to achieve. So what do we do to secure our operating system? Addressing that question has been a challenge for generations of computer scientists, and there is as yet no complete answer. But there are some important principles and tools we can use to secure operating systems. These are generally built into any general-purpose operating system you are likely to work with, and they alter what can be done with that system and how you go about doing it. So you might not think you're interested in security, but you need to understand what your OS does to secure itself to also understand how to get the system to do what you want.

What Are We Protecting?

We aren't likely to achieve good protection unless we have a fairly comprehensive view of what we're trying to protect when we say our operating system should be secure. Fortunately, that question is easy to answer for an operating system, at least at the high level: everything. That answer isn't very comforting, but it is best to have a realistic understanding of the broad implications of operating system security. A typical commodity operating system has complete control of all (or almost all) hardware on the machine and is able to do literally anything the hardware permits. That means it can control the processor, read and write all registers, examine any main memory location, and perform any operation one of its peripherals supports.

As a result, among the things the OS can do are:

• examine or alter any process's memory

• read, write, delete or corrupt any file on any writeable persistent storage medium, including hard disks and flash drives

• change the scheduling or even halt execution of any process

• send any message to anywhere, including altered versions of those a process wished to send

• enable or disable any peripheral device

In essence, processes are at the mercy of the operating system. It is nearly impossible for a process to 'protect' any part of itself from a malicious operating system. We typically assume our operating system is not actually malicious2 , but a flaw that allows a malicious process to cause the operating system to misbehave is nearly as bad, since it could potentially allow that process to gain any of the powers of the operating system itself. This point should make you think very seriously about the importance of designing secure operating systems and, more commonly, applying security patches to any operating system you are running. Security flaws in your operating system can completely compromise everything about the machine the system runs on, so preventing them and patching any that are found is vitally important.

Task: In the face of multiple possibly concurrent and interacting processes running on the same machine, how can we ensure that the resources each process is permitted to access are exactly those it should access, in exactly the ways we desire? What primitives are needed from the OS? What mechanisms should be provided by the hardware? How can we use them to solve the problems of security?

12.1 Security Goals and Policies

What do we mean when we say we want an operating system, or any system, to be secure? That's a rather vague statement. What we really mean is that there are things we would like to happen in the system and things we don't want to happen, and we'd like a high degree of assurance that we get what we want. As in most other aspects of life, we usually end up paying for what we get, so it's worthwhile to think about exactly what security properties and effects we actually need and then pay only for those, not for other things we don't need. What this boils down to is that we want to specify the goals we have for the security-relevant behavior of our system and choose defense approaches likely to achieve those goals at a reasonable cost.

Researchers in security have thought about this issue in broad terms for a long time. At a high conceptual level, they have defined three big security-related goals that are common to many systems, including operating systems. They are:

• Confidentiality – If some piece of information is supposed to be hidden from others, don't allow them to find it out. For example, you don't want someone to learn what your credit card number is – you want that number kept confidential.

• Integrity – If some piece of information or component of a system is supposed to be in a particular state, don't allow an adversary to change it. For example, if you've placed an online order for delivery of one pepperoni pizza, you don't want a malicious prankster to change your order to 1000 anchovy pizzas. One important aspect of integrity is authenticity. It's often important to be sure not only that information has not changed, but that it was created by a particular party and not by an adversary. • Availability – If some information or service is supposed to be available for your own or others' use, make sure an attacker cannot prevent its use. For example, if your business is having a big sale, you don't want your competitors to be able to block off the streets around your store, preventing your customers from reaching you.

An important extra dimension of all three of these goals is that we want controlled sharing in our systems. We share our secrets with some people and not with others. We allow some people to change our enterprise's databases, but not just anyone. Some systems need to be made available to a particular set of preferred users (such as those who have paid to play your on-line game) and not to others (who have not). Who's doing the asking matters a lot, in computers as in everyday life. Another important aspect of security for computer systems is we often want to be sure that when someone told us something, they cannot later deny that they did so. This aspect is often called non-repudiation. The harder and more expensive it is for someone to repudiate their actions, the easier it is to hold them to account for those actions, and thus the less likely people are to perform malicious actions. After all, they might well get caught and will have trouble denying they did it.

These are big, general goals. For a real system, you need to drill down to more detailed, specific goals. In a typical operating system, for example, we might have a confidentiality goal stating that a process's memory space cannot be arbitrarily read by another process. We might have an integrity goal stating that if a user writes a record to a particular file, another user who should not be able to write that file can't change the record. We might have an availability goal stating that one process running on the system cannot hog the CPU and prevent other processes from getting their share of the CPU. If you think back on what you've learned about the process abstraction, memory management, scheduling, file systems, IPC, and other topics from this class, you should be able to think of some other obvious confidentiality, integrity, and availability goals we are likely to want in our operating systems.

For any particular system, even goals at this level are not sufficiently specific. The integrity goal alluded to above, where a user's file should not be overwritten by another user not permitted to do so, gives you a hint about the extra specificity we need in our security goals for a particular system. Maybe there is some user who should be able to overwrite the file, as might be the case when two people are collaborating on writing a report. But that doesn't mean an unrelated third user should be able to write that file, if he is not collaborating on the report stored there. We need to be able to specify such detail in our security goals. Operating systems are written to be used by many different people with many different needs, and operating system security should reflect that generality. What we want in security mechanisms for operating systems is flexibility in describing our detailed security goals.

Ultimately, of course, the operating system software must do its best to enforce those flexible security goals, which implies we'll need to encode those goals in forms that software can understand. We typically must convert our vague understandings of our security goals into highly specific security policies. For example, in the case of the file described above, we might want to specify a policy like 'users A and B may write to file X, but no other user can write it.' With that degree of specificity, backed by carefully designed and implemented mechanisms, we can hope to achieve our security goals.

Note an important implication for operating system security: in many cases, an operating system will have the mechanisms necessary to implement a desired security policy with a high degree of assurance in its proper application, but only if someone tells the operating system precisely what that policy is. With some important exceptions (like maintaining a process's address space private unless specifically directed otherwise), the operating system merely supplies general mechanisms that can implement many specific policies. Without intelligent design of policies and careful application of the mechanisms, however, what the operating system should or could do may not be what your operating system will do.

12.2 Designing Secure Systems

Few of you will ever build your own operating system, nor even make serious changes to any existing operating system, but we expect many of you will build large software systems of some kind. Experience of many computer scientists with system design has shown that there are certain design principles that are helpful in building systems with security requirements. These principles were originally laid out by Jerome Saltzer and Michael Schroeder in an influential paper [SS75], though some of them come from earlier observations by others. While neither the original authors nor later commentators would claim that following them will guarantee that your system is secure, paying attention to them has proven to lead to more secure systems, while you ignore them at your own peril. We'll discuss them briefly here. If you are actually building a large software system, it would be worth your while to look up this paper (or more detailed commentaries on it) and study the concepts carefully.

1. **Economy of mechanism** – This basically means keep your system as small and simple as possible. Simple systems have fewer bugs and it's easier to understand their behavior. If you

don't understand your system's behavior, you're not likely to know if it achieves its security goals.

2. **Fail-safe defaults –** Default to security, not insecurity. If policies can be set to determine the behavior of a system, have the default for those policies be more secure, not less.
3. **Complete mediation –** This is a security term meaning that you should check if an action to be performed meets security policies every single time the action is taken .
4. **Open design –** Assume your adversary knows every detail of your design. If the system can achieve its security goals anyway, you're in good shape. This principle does not necessarily mean that you actually tell everyone all the details but base your security on the assumption that the attacker has learned everything. He often has, in practice.
5. **Separation of privilege** – Require separate parties or credentials to perform critical actions. For example, two-factor authentication, where you use both a password and possession of a piece of hardware to determine identity, is more secure than using either one of those methods alone.
6. **Least privilege –** Give a user or a process the minimum privileges required to perform the actions you wish to allow. The more privileges you give to a party, the greater the danger that they will abuse those privileges. Even if you are confident that the party is not malicious, if they make a mistake, an adversary can leverage their error to use their superfluous privileges in harmful ways.
7. **Least common mechanism –** For different users or processes, use separate data structures or mechanisms to handle them. For example, each process gets its own page table in a virtual memory system, ensuring that one process cannot access another's pages.
8. **Acceptability –** A critical property not dear to the hearts of many programmers. If your users won't use it, your system is worthless. Far too many promising secure systems have been abandoned because they asked too much of their users.

These are not the only useful pieces of advice on designing secure systems out there. There is also lots of good material on taking the next step, converting a good design into code that achieves the security you intended, and other material on how to evaluate whether the system you have built does indeed meet those goals. These issues are beyond the scope of this course but are extremely important when the time comes for you to build large, complex systems. For discussion of approaches to secure programming, you might start with Seacord [SE13], if you are working in C. If you are working in another language, you should seek out a similar text specific to that language, since many secure coding problems are related to details of the language.

12.3 The Basics of OS Security

In a typical operating system, then, we have some set of security goals, centered around various aspects of confidentiality, integrity, and availability. Some of these goals tend to be built into the operating system model, while others are controlled by the owners or users of the system. The built-in goals are those that are extremely common or must be ensured to make the more specific goals achievable. Most of these built-in goals relate to controlling process access to pieces of the hardware. That's because the hardware is shared by all the processes on a system, and unless the sharing is carefully controlled, one process can interfere with the security goals of another process. Other built-in goals relate to services that the operating system offers, such as file systems, memory management, and interprocess communications. If these services are not carefully controlled, processes can subvert the system's security goals.

Clearly, a lot of system security is going to be related to process handling. If the operating system can maintain a clean separation of processes that can only be broken with the operating system's help, then neither shared hardware nor operating system services can be used to subvert our security goals. That requirement implies that the operating system needs to be careful about allowing use of hardware and of its services. In many cases, the operating system has good opportunities to apply such caution. For example, the operating system controls virtual memory, which in turn completely controls which physical memory addresses each process can access. Hardware support prevents a process from even naming a physical memory address that is not mapped into its virtual memory space. (The software folks among us should remember to regularly thank the hardware folks for all the great stuff they've given us to work with.)

System calls offer the operating system another opportunity to provide protection. In most operating systems, processes access system services by making an explicit system call.As you have learned, system calls switch the execution mode from the processor's user mode to its supervisor mode, invoking an appropriate piece of operating system code as they do so. That code can determine which process made the system call and what service the process requested. Earlier, we only talked about how this could allow the operating system to call the proper piece of system code to perform the service, and to keep track of who to return control to when the service had been completed. But the same mechanism gives the operating system the opportunity to check if the requested service should be allowed under the system's security policy. Since access to peripheral devices is through device drivers, which are usually also accessed via system call, the same mechanism can ensure proper application of security policies for hardware access.

When a process performs a system call, then, the operating system will use the process identifier in the process control block or similar structure to determine the identity of the process. The OS can then use access control mechanisms to decide if the identified process is authorized to perform the requested action. If so, the OS either performs the action itself on behalf of the process or arranges for the process to perform it without further system intervention. If the process is not authorized, the OS can simply generate an error code for the system call and return control to the process, if the scheduling algorithm permits.

12.4 Virtualization

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine.**

Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1. Hardware Virtualization:

When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage: Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2. Operating System Virtualization:

When the virtual machine software or virtual machine manager (VMM) is installed on the Host operating system instead of directly on the hardware system is known as operating system virtualization.

Usage: Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3. Server Virtualization:

When the virtual machine software or virtual machine manager (VMM) is directly installed on the Server system is known as server virtualization.

Usage: Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4. Storage Virtualization:

Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device.

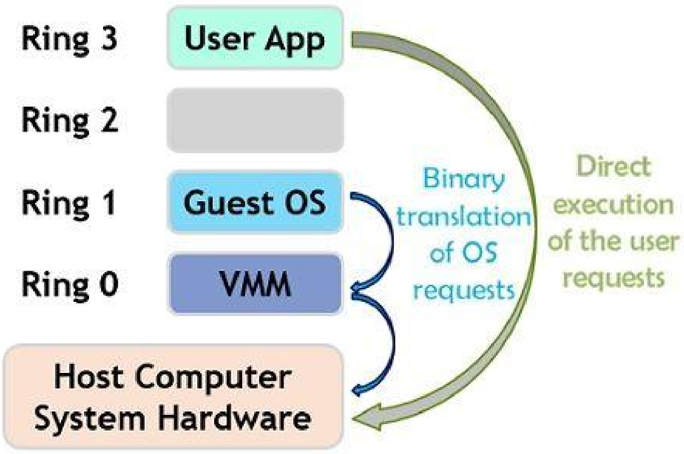
Storage virtualization is also implemented by using software applications.

Usage: Storage virtualization is mainly done for back-up and recovery purposes

12.5 Full Virtualization

Full virtualization is the first generation of the software solution regarding server virtualization and developed in the year of 1966 by IBM. It works by merging the binary translation and the direct execution where the guest OS is entirely separated from the elementary hardware and virtualization layer. Therefore, whatever the virtual machines are producing a dynamic translator rewrites to the underlining hardware. It involves a lack of awareness at the guest OS end about its virtualization and modification is inevitable.

The technologies provide full virtualization support are VMWare, ESXi and Microsoft virtual servers. Each time an OS instruction is generated the hypervisor translates it during run-time quickly and caches the outcome for the future references. While the user-level instructions are executed without modification at native speed.


Ring 3
User App
Ring 2
Ring 1
Guest OS
Ring 0
VMM
Host Computer System Hardware
Binary translation of OS requests
Direct execution of the user requests

Full Virtualization

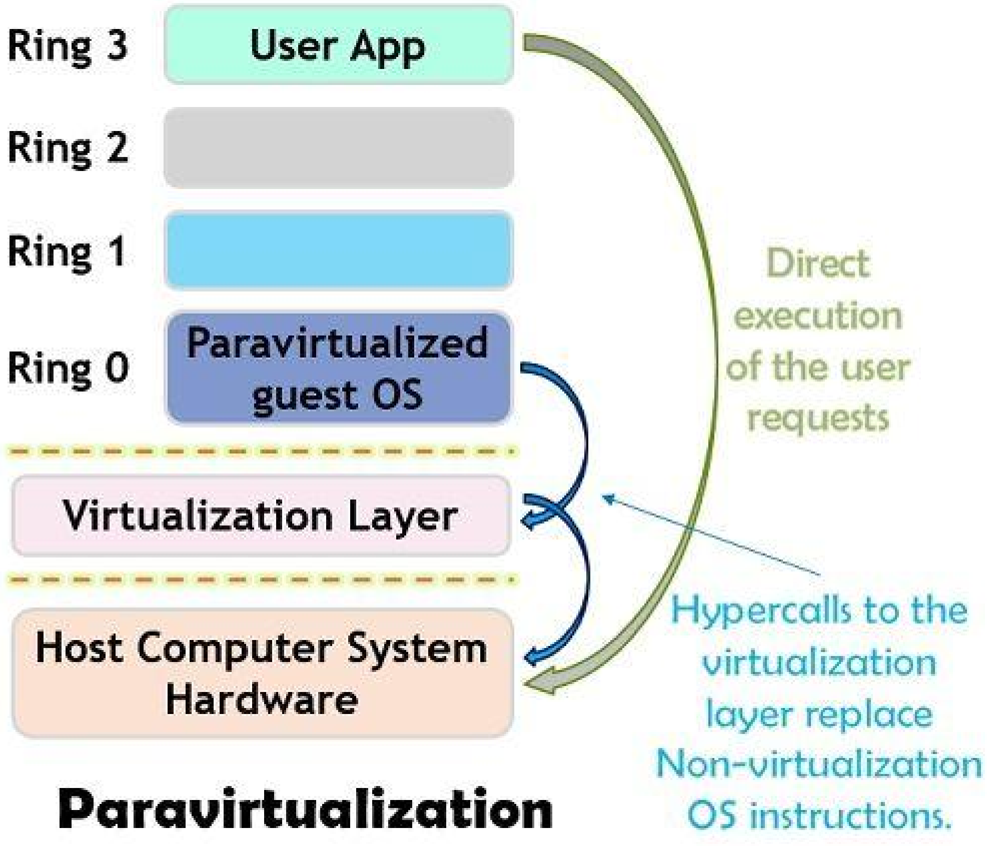
However, the storage of the translated instructions during the binary translation is intended to improve performance but this result in an increase in the cost of memory consumption.

Another demerit of the full virtualization is binary translation also takes much time and can achieve a huge performance overhead. I/O intensive applications are very challenging to employ full virtualization.

12.6 Paravirtualization

Paravirtualization is nothing but the interaction of the guest OS to the hypervisor in order to boost performance and productivity. Unlike full virtualization, paravirtualization does not implement complete isolation; instead, partial isolation is implemented in the approach. It also alters OS kernel to substitute the hypercalls in place of non-virtualizable instructions. The purpose of hypercalls is to interact with the virtualization layer hypervisor directly.

In paravirtualization, there are various functions performed by hypervisor such as the arrangement of hypercalls interface for other crucial kernel functions like memory management, time keeping and interrupt handling. The major merit of paravirtualization is that it can easily reduce the virtualization overhead.


Ring 3
User App
Ring 2
Ring 1
Ring 0
Paravirtualized guest OS
Virtualization Layer
Host Computer System Hardware
Direct execution of the user requests
Hypercalls to the virtualization layer replace Non-virtualization OS instructions.
Paravirtualization

However, most user space workloads gain very less, and close native performance which is not obtained for all workloads.

Furthermore, it is less compatible and portable as it does not support the unmodified OS. It could also arise some crucial support and maintainability problems in the production environ due to the need for deep OS kernel modifications.

Summary

- Internet Information Services (IIS) is a flexible, general-purpose web server from Microsoft that runs on Windows systems to serve requested HTML pages or files.
- An IIS web server accepts requests from remote client computers and returns the appropriate response.
- Microsoft SQL Server is one of the market leaders for database technology.

- It's a relational database management system that supports several applications, including business intelligence, transaction processing and analytics.
- WSH provides an environment for scripts to run – it invokes the appropriate script engine and provides a set of services and objects for the script to work with.
- These scripts may be run in GUI mode (WScript.exe) or command line mode (CScript.exe), or from a COM object (wshom.ocx), offering flexibility to the user for interactive or non-interactive scripts. Windows Management Instrumentation is also scriptable by this means.
- Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system:
- The instruction set, also called ISA (instruction set architecture), is part of a computer that pertains to programming, which is more or less machine language.

Keywords

- **Confidentiality –** If some piece of information is supposed to be hidden from others, don't allow them to find it out. For example, you don't want someone to learn what your credit card number is – you want that number kept confidential.
- **Integrity –** If some piece of information or component of a system is supposed to be in a particular state, don't allow an adversary to change it. For example, if you've placed an online order for delivery of one pepperoni pizza, you don't want a malicious prankster to change your order to 1000 anchovy pizzas. One important aspect of integrity is authenticity. It's often important to be sure not only that information has not changed, but that it was created by a particular party and not by an adversary.
- **Availability –** If some information or service is supposed to be available for your own or others' use, make sure an attacker cannot prevent its use. For example, if your business is having a big sale, you don't want your competitors to be able to block off the streets around your store, preventing your customers from reaching you.
- **Virtualization:**Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.
- **Hardware Virtualization:** When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization.

SelfAssessment

1. What is an operating system?

A. interface between the hardware and application programs
B. collection of programs that manages hardware resources
C. system service provider to the application programs
D. all of the mentioned

2. What are the services operating System provides to both the users and to the programs?

A. File System manipulation

B. Error Detection

C. Program execution

D. Resource Allocation

3. Which of the following few common services provided by an operating system?

A. Protection

B. Program execution

C. I/O operations

D. All of the above

4. What are security controls ?

A. Controls that are intended to ensure that attacks are unsuccessful

B. Controls that are intended to detect and repel attacks

C. Controls that are intended to support recovery from problems

D. All of the mentioned

5. Controls that are intended to repel attacks is analogous to ____________ in dependability engineering.

A. Fault avoidance

B. Fault tolerance

C. Fault detection

D. None of the mentioned

6. Controls that are intended to ensure that attacks are unsuccessful is analogous to ____________ in dependability engineering.

A. Fault avoidance

B. Fault tolerance

C. Fault detection

D. Fault Recovery

7. Which of the following are good account security practices?

A. Least Privilege

B. Multi-Factor Authentication

C. Automatic Account Login

D. Require password on wake/boot

8. Which of the following is considered OS hardening?

A. Turning on the latest OS features

B. Using a cable lock

C. Keeping all applications updated

D. Disabling the guest account

9. __________ is a general system hardening process that involves securing the data, ports, components, functions, and permissions of a server using advanced security measures.

A. Server hardening
B. Software application hardening
C. Operating system hardening
D. Database hardening

10 ____________ involves updating or implementing additional security measures to protect both standard and third-party applications installed on your server.

A. Operating system hardening
B. Database hardening
C. Server hardening
D. Software application hardening

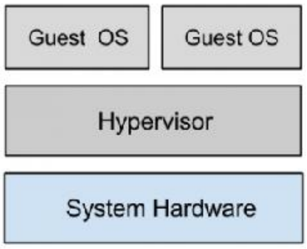
11. ____________ involves securing both the contents of a digital database and the database management system (DBMS), which is the database application users interact with to store and analyze information within a database

A. Operating system hardening
B. Database hardening
C. Server hardening
D. Software application hardening

12. ___________ involves securing the basic communication infrastructure of multiple servers and computer systems operating within a given network.

A. Database hardening
B. Server hardening
C. Software application hardening
D. Network Hardening

13. Which type of Hypervisor is shown in the following figure?



A. Type 1
B. Type 2
C. Type 3
D. All of the mentioned

14. Which of the following provide system resource access to virtual machines?

A. VMM
B. VMC
C. VNM
D. All of the mentioned

15. An operating system running on a Type ______ VM is full virtualization.

A. 1
B. 2
C. 3
D. All of the mentioned

Review Questions

1. Explain the concept of Operating System Security.
2. Explain different types of Operating System Hardening.
3. Define System hardening.
4. Discuss different steps for to ensure Security Maintenance.
5. Explain Virtualization with the help of diagram
6. Differentiate between Full Virtualizations and Para Virtualization.
7. What is Hypervisor and discuss its types.

Answers for Self Assessment

1.	D	2.	C	3.	D	4.	D	5.	B
6.	A	7.	C	8.	D	9.	A	10.	D
11.	B	12.	D	13.	A	14.	A	15.	A

Further Reading

http://www.cs.fsu.edu/~lacher/courses/COP4610/lectures_9e/ch15.pdf

Web Links

https://www.cs.colostate.edu/~massey/Teaching/cs356/RestrictedAccess/Slides/356lecture26.pdf

Unit 13: Database and Cloud Security

CONTENTS

Objectives

- Understand the concept of Database Security and Cloud Security
- Discuss about Database security Policies
- Learn how to secure Mobile database
- Acquire the knowledge about Cloud Computing Concepts

Introduction

Databases have been largely secured against hackers through network security measures such as firewalls, and network-based intrusion detection systems. While network security controls remain valuable in this regard, securing the database systems themselves, and the programs/functions and data within them, has arguably become more critical as networks are increasingly opened to wider access, in particular access from the Internet. Furthermore, system, program, function and data access controls, along with the associated user identification, authentication and rights management functions, have always been important to limit and in some cases log the activities of authorized users and administrators. In other words, these are complementary approaches to database security, working from both the outside-in and the inside-out as it were.

Many organizations develop their own "baseline" security standards and designs detailing basic security control measures for their database systems. These may reflect general information security requirements or obligations imposed by corporate information security policies and applicable laws and regulations (e.g. concerning privacy, financial management and reporting systems), along with generally accepted good database security practices (such as appropriate hardening of the underlying systems) and perhaps security recommendations from the relevant database system and software vendors. The security designs for specific database systems typically specify further security administration and management functions (such as administration and reporting of user access rights, log management and analysis, database replication/synchronization and backups) along with various business-driven information security controls within the database programs and functions (e.g. data entry validation and audit trails). Furthermore, various security-related activities (manual controls) are normally incorporated into the procedures, guidelines etc. relating to the design, development, configuration, use, management and maintenance of databases.

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical.

Database security includes a variety of measures used to secure database management systems from malicious cyber-attacks and illegitimate use. Database security programs are designed to protect not only the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion. Database security encompasses tools, processes, and methodologies which establish security inside a database environment.

13.1 What is database security?

Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability. This article will focus primarily on confidentiality since it's the element that's compromised in most data breaches.

Database security must address and protect the following:

- The data in the database
- The database management system (DBMS)
- Any associated applications
- The physical database server and/or the virtual database server and the underlying hardware
- The computing and/or network infrastructure used to access the database

Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices. It's also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.

13.2 Why is it important?

By definition, a data breach is a failure to maintain the confidentiality of data in a database. How much harm a data breach inflicts on your enterprise depends on a number of consequences or factors:

Compromised intellectual property: Your intellectual property—trade secrets, inventions, proprietary practices—may be critical to your ability to maintain a competitive advantage in your market. If that intellectual property is stolen or exposed, your competitive advantage may be difficult or impossible to maintain or recover.

Damage to brand reputation: Customers or partners may be unwilling to buy your products or services (or do business with your company) if they don't feel they can trust you to protect your data or theirs.

Business continuity (or lack thereof): Some business cannot continue to operate until a breach is resolved.

Fines or penalties for non-compliance: The financial impact for failing to comply with global regulations such as the Sarbannes-Oxley Act (SAO) or Payment Card Industry Data Security Standard (PCI DSS), industry-specific data privacy regulations such as HIPAA, or regional data privacy regulations, such as Europe's General Data Protection Regulation (GDPR) can be devastating, with fines in the worst cases exceeding several million dollars per violation.

Costs of repairing breaches and notifying customers: In addition to the cost of communicating a breach to customer, a breached organization must pay for forensic and investigative activities, crisis management, triage, repair of the affected systems, and more.

Database security is the technique that protects and secures the database against intentional or accidental threats.

- Theft and fraudulent.
- Loss of confidentiality or secrecy.
- Loss of data privacy.
- Loss of data integrity.
- Loss of availability of data.

13.3 Common Threats and Challenges

Many software misconfigurations, vulnerabilities, or patterns of carelessness or misuse can result in breaches. The following are among the most common types or causes of database security attacks and their causes.

Insider threats

An insider threat is a security threat from any one of three sources with privileged access to the database:

A malicious insider who intends to do harm

A negligent insider who makes errors that make the database vulnerable to attack

An infiltrator—an outsider who somehow obtains credentials via a scheme such as phishing or by gaining access to the credential database itself

Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials.

Human error

Accidents, weak passwords, password sharing, and other unwise or uninformed user behaviors continue to be the cause of nearly half (49%) of all reported data breaches.(Link resides outside IBM)

Exploitation of database software vulnerabilities

Hackers make their living by finding and targeting vulnerabilities in all kinds of software, including database management software. All major commercial database software vendors and open source database management platforms issue regular security patches to address these vulnerabilities, but failure to apply these patches in a timely fashion can increase your exposure.

SQL/NoSQL injection attacks

A database-specific threat, these involve the insertion of arbitrary SQL or non-SQL attack strings into database queries served by web applications or HTTP headers. Organizations that don't follow secure web application coding practices and perform regular vulnerability testing are open to these attacks.

Buffer overflow exploitations

Buffer overflow occurs when a process attempts to write more data to a fixed-length block of memory than it is allowed to hold. Attackers may use the excess data, stored in adjacent memory addresses, as a foundation from which to launch attacks.

Denial of service (DoS/DDoS) attacks

In a denial of service (DoS) attack, the attacker deluges the target server—in this case the database server—with so many requests that the server can no longer fulfill legitimate requests from actual users, and, in many cases, the server becomes unstable or crashes.

In a distributed denial of service attack (DDoS), the deluge comes from multiple servers, making it more difficult to stop the attack.

Malware

Malware is software written specifically to exploit vulnerabilities or otherwise cause damage to the database. Malware may arrive via any endpoint device connecting to the database's network.

Attacks on backups

Organizations that fail to protect backup data with the same stringent controls used to protect the database itself can be vulnerable to attacks on backups.

These threats are exacerbated by the following:

Growing data volumes: Data capture, storage, and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.

Infrastructure sprawl: Network environments are becoming increasingly complex, particularly as businesses move workloads to multicloud or hybrid cloud architectures, making the choice, deployment, and management of security solutions ever more challenging.

Increasingly stringent regulatory requirements: The worldwide regulatory compliance landscape continues to grow in complexity, making adhering to all mandates more difficult.

Cybersecurity skills shortage: Experts predict there may be as many as 8 million unfilled cybersecurity positions by 2022.

13.4 How Can You Secure Your Database Server?

A database server is a physical or virtual machine running the database. Securing a database server, also known as "hardening", is a process that includes physical security, network security, and secure operating system configuration.

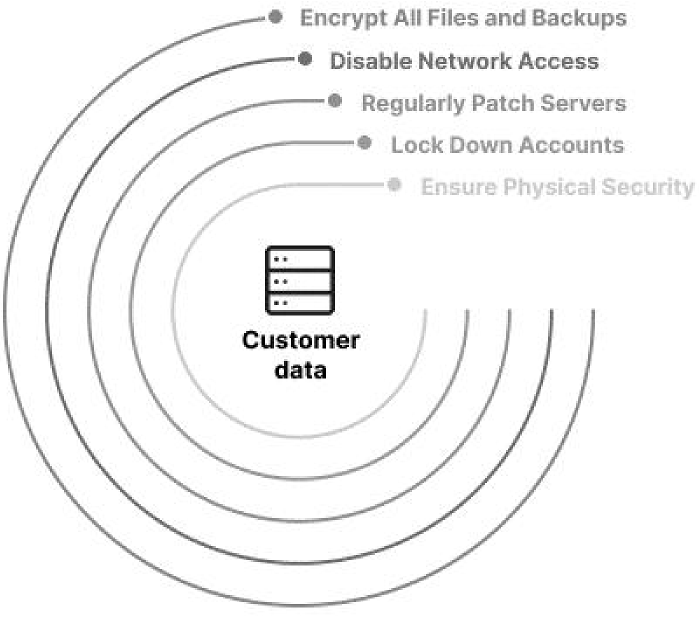


Figure 1 Countermeasure to secure database server

13.5 Ensure Physical Database Security

Refrain from sharing a server for web applications and database applications, if your database contains sensitive data. Although it could be cheaper, and easier, to host your site and database together on a hosting provider, you are placing the security of your data in someone else's hands.

If you do rely on a web hosting service to manage your database, you should ensure that it is a company with a strong security track record. It is best to stay clear of free hosting services due to the possible lack of security.

If you manage your database in an on-premise data center, keep in mind that your data center is also prone to attacks from outsiders or insider threats. Ensure you have physical security measures, including locks, cameras, and security personnel in your physical facility. Any access to physical servers must be logged and only granted to authorized individuals.

In addition, do not leave database backups in locations that are publicly accessible, such as temporary partitions, web folders, or unsecured cloud storage buckets.

13.6 Lock Down Accounts and Privileges

Let's consider the Oracle database server. After the database is installed, the Oracle database configuration assistant (DBCA) automatically expires and locks most of the default database user accounts.

If you install an Oracle database manually, this doesn't happen and default privileged accounts won't be expired or locked. Their password stays the same as their username, by default. An attacker will try to use these credentials first to connect to the database.

It is critical to ensure that every privileged account on a database server is configured with a strong, unique password. If accounts are not needed, they should be expired and locked.

For the remaining accounts, access has to be limited to the absolute minimum required. Each account should only have access to the tables and operations (for example, SELECT or INSERT) required by the user. Avoid creating user accounts with access to every table in the database.

Regularly Patch Database servers

Ensure that patches remain current. Effective database patch management is a crucial security practice because attackers are actively seeking out new security flaws in databases, and new viruses and malware appear on a daily basis.

A timely deployment of up-to-date versions of database service packs, critical security hotfixes, and cumulative updates will improve the stability of database performance.

Disable Public Network Access

Organizations store their applications in databases. In most real-world scenarios, the end-user doesn't require direct access to the database. Thus, you should block all public network access to database servers unless you are a hosting provider. Ideally, an organization should set up gateway servers (VPN or SSH tunnels) for remote administrators.

Encrypt All Files and Backups

Irrespective of how solid your defenses are, there is always a possibility that a hacker may infiltrate your system. Yet, attackers are not the only threat to the security of your database. Your employees may also pose a risk to your business. There is always the possibility that a malicious or careless insider will gain access to a file they don't have permission to access.

Encrypting your data makes it unreadable to both attackers and employees. Without an encryption key, they cannot access it, this provides a last line of defense against unwelcome intrusions. Encrypt all-important application files, data files, and backups so that unauthorized users cannot read your critical data.

13.7 Database Security Best Practices

Because databases are nearly always network-accessible, any security threat to any component within or portion of the network infrastructure is also a threat to the database, and any attack impacting a user's device or workstation can threaten the database. Thus, database security must extend far beyond the confines of the database alone.

When evaluating database security in your environment to decide on your team's top priorities, consider each of the following areas:

Physical security: Whether your database server is on-premise or in a cloud data center, it must be located within a secure, climate-controlled environment. (If your database server is in a cloud data center, your cloud provider will take care of this for you.)

Administrative and network access controls: The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

End user account/device security: Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.

Encryption: ALL data—including data in the database, and credential data—should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best-practice guidelines.

Database software security: Always use the latest version of your database management software, and apply all patches as soon as they are issued.

Application/web server security: Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.

Backup security: All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.

Auditing: Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

Actively Manage Passwords and User Access

If you have a large organization, you must think about automating access management via password management or access management software. This will provide permitted users with a short-term password with the rights they need every time they need to gain access to a database.

It also keeps track of the activities completed during that time frame and stops administrators from sharing passwords. While administrators may feel that sharing passwords is convenient, however, doing so makes effective database accountability and security almost impossible.

In addition, the following security measures are recommended:

- Strong passwords must be enforced
- Password hashes must be salted and stored encrypted
- Accounts must be locked following multiple login attempts
- Accounts must be regularly reviewed and deactivated if staff move to different roles, leave the company, or no longer require the same level of access

Test Your Database Security

Once you have put in place your database security infrastructure, you must test it against a real threat. Auditing or performing penetration tests against your own database will help you get into the mindset of a cybercriminal and isolate any vulnerabilities you may have overlooked.

To make sure the test is comprehensive, involve ethical hackers or recognized penetration testing services in your security testing. Penetration testers provide extensive reports listing database vulnerabilities, and it is important to quickly investigate and remediate these vulnerabilities. Run a penetration test on a critical database system at least once per year.

Use Real-Time Database Monitoring

Continually scanning your database for breach attempts increases your security and lets you rapidly react to possible attacks.

In particular, File Integrity Monitoring (FIM) can help you log all actions carried out on the database's server and to alert you of potential breaches. When FIM detects a change to important database files, ensure security teams are alerted and able to investigate and respond to the threat.

Use Web Application and Database Firewalls

You should use a firewall to protect your database server from database security threats. By default, a firewall does not permit access to traffic. It needs to also stop your database from starting outbound connections unless there is a particular reason for doing so.

As well as safeguarding the database with a firewall, you must deploy a web application firewall (WAF). This is because attacks aimed at web applications, including SQL injection, can be used to gain illicit access to your databases.

A database firewall will not stop most web application attacks, because traditional firewalls operate at the network layer, while web application layers operate at the application layer (layer 7 of the OSI model). A WAF operates at layer 7 and is able to detect malicious web application traffic, such as SQL injection attacks, and block it before it can harm your database.

13.8 Controls and Policies

In addition to implementing layered security controls across your entire network environment, database security requires you to establish the correct controls and policies for access to the database itself. These include:

Administrative controls to govern installation, change, and configuration management for the database.

Preventative controls to govern access, encryption, tokenization, and masking.

Detective controls to monitor database activity monitoring and data loss prevention tools. These solutions make it possible to identify and alert on anomalous or suspicious activities.

Database security policies should be integrated with and support your overall business goals, such as protection of critical intellectual property and your cybersecurity policies and cloud security policies. Ensure you have designated responsibility for maintaining and auditing security controls within your organization and that your policies complement those of your cloud provider in shared responsibility agreements. Security controls, security awareness training and education programs, and penetration testing and vulnerability assessment strategies should all be established in support of your formal security policies.

13.9 What is Cloud Computing?

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into three main categories or types of cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

A cloud can be private or public. A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Cloud infrastructure involves the hardware and software components required for proper implementation of a cloud computing model. Cloud computing can also be thought of as utility computing or on-demand computing.

The name cloud computing was inspired by the cloud symbol that's often used to represent the internet in flowcharts and diagrams.

13.10 How does Cloud work?

Cloud computing works by enabling client devices to access data and cloud applications over the internet from remote physical servers, databases and computers.

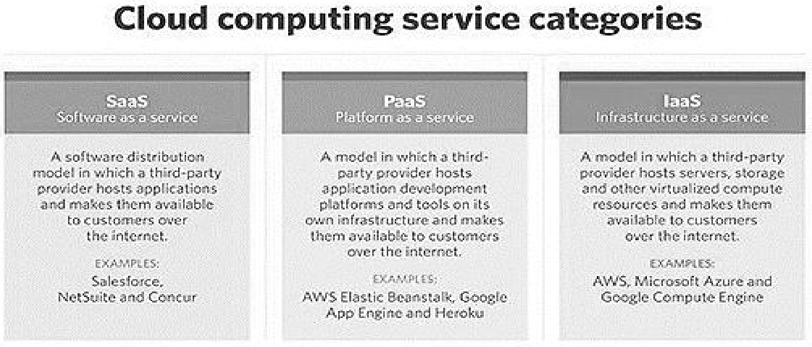
An internet network connection links the front end, which includes the accessing client device, browser, network and cloud software applications, with the back end, which consists of databases, servers and computers. The back end functions as a repository, storing data that is accessed by the front end.

Communications between the front and back ends are managed by a central server. The central server relies on protocols to facilitate the exchange of data. The central server uses both software and middleware to manage connectivity between different client devices and cloud servers. Typically, there is a dedicated server for each individual application or workload.

Cloud computing relies heavily on virtualization and automation technologies. Virtualization enables the easy abstraction and provisioning of services and underlying cloud systems into logical entities that users can request and utilize. Automation and accompanying orchestration capabilities provide users with a high degree of self-service to provision resources, connect services and deploy workloads without direct intervention from the cloud provider's IT staff.

13.11 Types of Cloud Computing Services

Cloud computing can be separated into three general service delivery categories or forms of cloud computing:



Cloud computing service categories

SaaS Software as a service	PaaS Platform as a service	IaaS Infrastructure as a service
A software distribution model in which a third-party provider hosts applications and makes them available to customers over the internet.	A model in which a third-party provider hosts application development platforms and tools on its own infrastructure and makes them available to customers over the internet.	A model in which a third-party provider hosts servers, storage and other virtualized compute resources and makes them available to customers over the internet.
EXAMPLES: Salesforce, NetSuite and Concur	EXAMPLES: AWS Elastic Beanstalk, Google App Engine and Heroku	EXAMPLES: AWS, Microsoft Azure and Google Compute Engine

Notes: Cloud security refers broadly to measures undertaken to protect digital assets and data stored online via cloud services providers

1. **IaaS.** IaaS providers, such as Amazon Web Services (AWS), supply a virtual server instance and storage, as well as application programming interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and can start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to enabling customization of instances, for various workload needs. The IaaS cloud model is closest to a remote data center for business users.

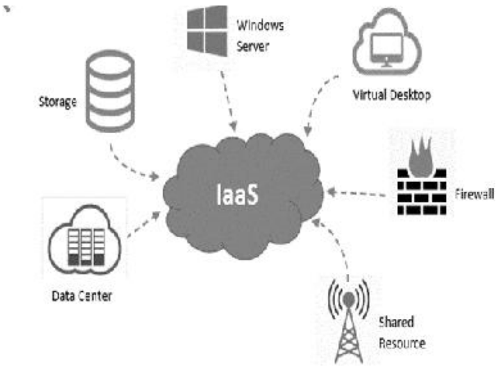


Figure 2: Infrastructure as a Service

2. **PaaS**. In the PaaS model, cloud providers host development tools on their infrastructures. Users access these tools over the internet using APIs, web portals or gateway software. PaaS is used for general software development, and many PaaS providers host the software after it's developed. Common PaaS products include Salesforce's Lightning Platform, AWS Elastic Beanstalk and Google App Engine.

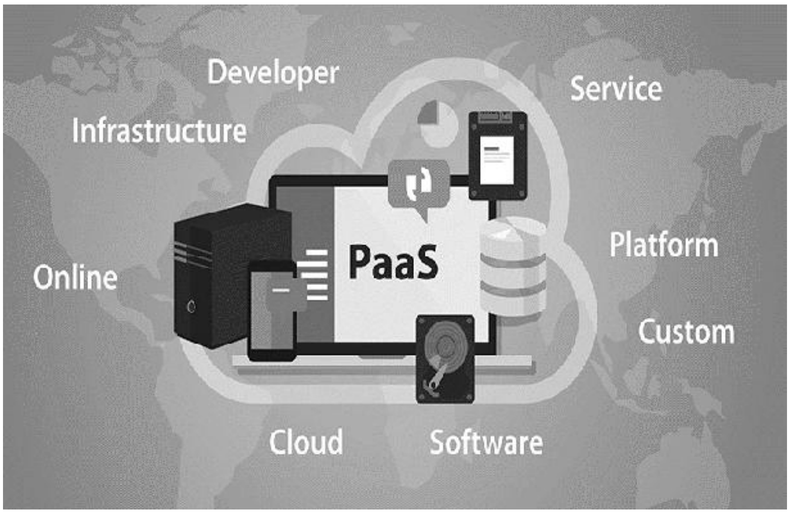


Figure 3 Platform as a Service

3. **SaaS**. SaaS is a distribution model that delivers software applications over the internet; these applications are often called web services. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access. In the SaaS model, users gain access to application software and databases. One common example of a SaaS application is Microsoft 365 for productivity and email services.

Figure 4 Software as a Service

13.12 Cloud Computing Deployment Models

Private Cloud services are delivered from a business's data center to internal users. With a private cloud, an organization builds and maintains its own underlying cloud infrastructure. This model offers the versatility and convenience of the cloud, while preserving the management, control and security common to local data centers. Internal users might or might not be billed for services through IT chargeback. Common private cloud technologies and vendors include VMware and OpenStack.

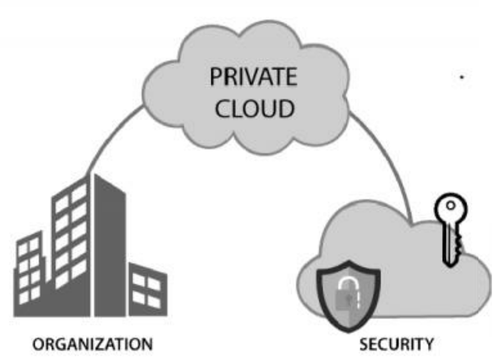


Figure 5 Example of Private Cloud

In the **public cloud** model, a third-party cloud service provider (CSP) delivers the cloud service over the internet. Public cloud services are sold on demand, typically by the minute or hour, though long-term commitments are available for many services. Customers only pay for the central processing unit cycles, storage or bandwidth they consume. Leading public CSPs include AWS, Microsoft Azure, IBM and Google Cloud Platform (GCP), as well as IBM, Oracle and Tencent.

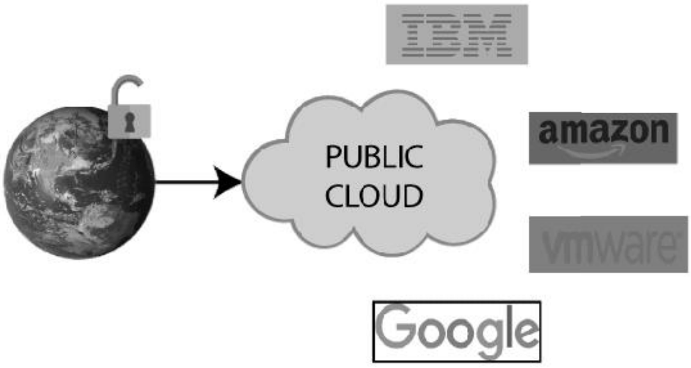


Figure 6 Example of Public Cloud

A **hybrid cloud** is a combination of public cloud services and an on-premises private cloud, with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud and use the public cloud to handle workload bursts or spikes in demand. The goal of a hybrid cloud is to create a unified, automated, scalable environment that takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

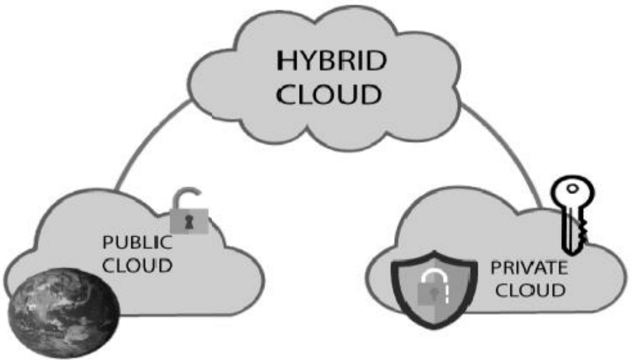
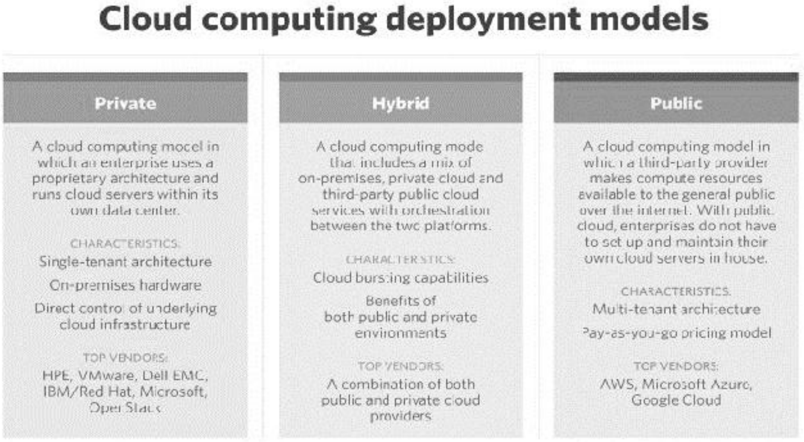


Figure 7: Example of Hybrid Cloud



Cloud computing deployment models

Private	Hybrid	Public
A cloud computing model in which an enterprise uses a proprietary architecture and runs cloud servers within its own data center.	A cloud computing mode that includes a mix of on-premises, private cloud and third-party public cloud services with orchestration between the two platforms.	A cloud computing model in which a third-party provider makes compute resources available to the general public over the internet. With public cloud, enterprises do not have to set up and maintain their own cloud servers in house.
CHARACTERISTICS: Single-tenant architecture On-premises hardware Direct control of underlying cloud infrastructure	CHARACTERISTICS: Cloud bursting capabilities Benefits of both public and private environments	CHARACTERISTICS: Multi-tenant architecture Pay-as-you-go pricing model
TOP VENDORS: HPE, VMware, Dell EMC, IBM/Red Hat, Microsoft, OpenStack	TOP VENDORS: A combination of both public and private cloud providers	TOP VENDORS: AWS, Microsoft Azure, Google Cloud

In addition, organizations are increasingly embracing a multi-cloud model, or the use of multiple IaaS providers. This enables applications to migrate between different cloud providers or to even operate concurrently across two or more cloud providers.

Organizations adopt multi-cloud for various reasons. For example, they could do so to minimize the risk of a cloud service outage or to take advantage of more competitive pricing from a particular provider. Multi-cloud implementation and application development can be a challenge because of the differences between cloud providers' services and APIs.

Multi-cloud deployments should become easier, however, as providers' services and APIs converge and become more standardized through industry initiatives such as the Open Cloud Computing Interface.

A community cloud, which is shared by several organizations, supports a particular community that shares the same concerns -- e.g., the same mission, policy, security requirements and compliance considerations. A community cloud is either managed by these organizations or a third-party vendor and can be on or off premises.

Cloud Computing Security

Security remains a primary concern for businesses contemplating cloud adoption -- especially public cloud adoption. Public CSPs share their underlying hardware infrastructure between numerous customers, as the public cloud is a multi-tenant environment. This environment demands significant isolation between logical compute resources. At the same time, access to public cloud storage and compute resources is guarded by account login credentials.

Many organizations bound by complex regulatory obligations and governance standards are still hesitant to place data or workloads in the public cloud for fear of outages, loss or theft. However, this resistance is fading, as logical isolation has proven reliable and the addition of data encryption and various identity and access management tools have improved security within the public cloud.

Ultimately, the responsibility for establishing and maintaining a secure cloud environment falls to the individual business user that is responsible for building the workload's architecture -- the combination of cloud resources and services in which the workload runs -- and implementing the security features that the cloud provider offers.

Characteristics and Advantages of Cloud Computing

Cloud computing has been around for several decades now, and today's cloud computing infrastructure demonstrates an array of characteristics that have brought meaningful benefits for businesses of all sizes. Some of the main characteristics of cloud computing are the following:

Self-service provisioning. End users can spin up compute resources for almost any type of workload on demand. An end user can provision computing capabilities, such as server time and network storage, eliminating the traditional need for IT administrators to provision and manage compute resources.

Elasticity. Companies can freely scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure, which might or might not remain active.

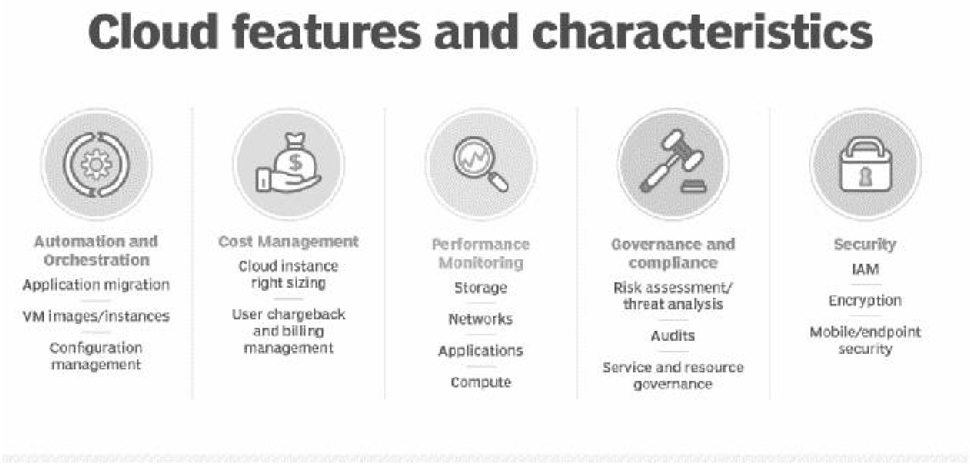
Pay per use. Compute resources are measured at a granular level, enabling users to pay only for the resources and workloads they use.

Workload resilience. CSPs often implement redundant resources to ensure resilient storage and to keep users' important workloads running -- often across multiple global regions.

Migration flexibility. Organizations can move certain workloads to or from the cloud -- or to different cloud platforms -- as desired or automatically for better cost savings or to use new services as they emerge.

Broad network access. A user can access cloud data or upload data to the cloud from anywhere with an internet connection using any device.

Multi-tenancy and resource pooling. Multi-tenancy lets numerous customers share the same physical infrastructures or the same applications yet still retain privacy and security over their own data. With resource pooling, cloud providers service numerous customers from the same physical resources. The resource pools of the cloud providers should be large and flexible enough so they can service the requirements of multiple customers.


Cloud features and characteristics
Automation and Orchestration
Application migration
VM images/instances
Configuration management
Cost Management
Cloud instance right sizing
User chargeback and billing management
Performance Monitoring
Storage
Networks
Applications
Compute
Governance and compliance
Risk assessment/ threat analysis
Audits
Service and resource governance
Security
IAM
Encryption
Mobile/endpoint security

13.13 Disadvantages of Cloud Computing

Despite the clear upsides to relying on cloud services, cloud computing carries its own challenges for IT professionals:

Cloud security. Security is often considered the greatest challenge facing cloud computing. When relying on the cloud, organizations risk data breaches, hacking of APIs and interfaces, compromised credentials and authentication issues. Furthermore, there is a lack of transparency regarding how and where sensitive information entrusted to the cloud provider is handled. Security demands careful attention to cloud configurations and business policy and practice.

Cost unpredictability. Pay-as-you-go subscription plans for cloud use, along with scaling resources to accommodate fluctuating workload demands, can make it tough to define and predict final costs. Cloud costs are also frequently interdependent, with one cloud service often utilizing one or more other cloud services -- all of which appear in the recurring monthly bill. This can create additional unplanned cloud costs.

Lack of capability and expertise. With cloud-supporting technologies rapidly advancing, organizations are struggling to keep up with the growing demand for tools and employees with the proper skill sets and knowledge needed to architect, deploy, and manage workloads and data in a cloud.

IT governance. The emphasis on do-it-yourself capability in cloud computing can make IT governance difficult, as there is no control over provisioning, deprovisioning and management of infrastructure operations. This can make it challenging to properly manage risks and security, IT compliance and data quality.

Compliance with industry laws. When transferring data from on-premises local storage into cloud storage, it can be difficult to manage compliance with industry regulations through a third party. It's important to know where data and workloads are actually hosted in order to maintain regulatory compliance and proper business governance.

Management of multiple clouds. Every cloud is different, so multi-cloud deployments can disjoint efforts to address more general cloud computing challenges.

Cloud performance. Performance -- such as latency -- is largely beyond the control of the organization contracting cloud services with a provider. Network and provider outages can interfere with productivity and disrupt business processes if organizations are not prepared with contingency plans.

Building a private cloud. Architecting, building and managing private clouds -- whether for its own purpose or for a hybrid cloud goal -- can be a daunting task for IT departments and staff.

Cloud migration. The process of moving applications and other data to a cloud infrastructure often causes complications. Migration projects frequently take longer than anticipated and go over budget. The issue of workload and data repatriation -- moving from the cloud back to a local data center -- is often overlooked until unforeseen cost or performance problems arise.

Vendor lock-in. Often, switching between cloud providers can cause significant issues. This includes technical incompatibilities, legal and regulatory limitations and substantial costs incurred from sizable data migrations.

Cloud computing examples and use cases

Cloud computing has evolved and diversified into a wide array of offerings and capabilities designed to suit almost any conceivable business need. Examples of cloud computing capabilities and diversity include the following:

Google Docs, Microsoft 365. Users can access Google Docs and Microsoft 365 through the internet. Users can be more productive because they can access work presentations and spreadsheets stored in the cloud at anytime from anywhere on any device.

Email, Calendar, Skype, WhatsApp. Emails, calendars, Skype and WhatsApp take advantage of the cloud's ability to provide users with access to data remotely so they can access their personal data on any device, whenever and wherever they want.

Zoom. Zoom is a cloud-based software platform for video and audio conferencing that records meetings and saves them to the cloud, enabling users to access them anywhere and at any time. Another common communication and collaboration platform is Microsoft Teams.

AWS Lambda. Lambda enables developers to run code for applications or back-end services without having to provision or manage servers. The pay-as-you-go model constantly scales with an organization to accommodate real-time changes in data usage and data storage. Other major cloud providers also support serverless computing capabilities, such as Google Cloud Functions and Azure Functions.

Task: Search out for the latest organization who have their own cloud and other who are using cloud services.

Figure 7 Examples of Cloud computing

Summary

- A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields.
- Database security is the technique that protects and secures the database against intentional or accidental threats.
- Business intelligence environments consist of a variety of technologies, applications, processes, strategies, products, and technical architectures used to enable the collection, analysis, presentation, and dissemination of internal and external business information.
- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections.
- Cloud security refers broadly to measures undertaken to protect digital assets and data stored online via cloud services providers.
- Cloud computing is the delivery of different services through the Internet, including data storage, servers, databases, networking, and software.
- Measures to protect this data include two-factor authorization (2FA), the use of VPNs, security tokens, data encryption, and firewall services, among others.

- Database users may have different privileges. However, users may abuse them and here are the major types of privilege abuses: excessive privilege abuse, legitimate privileges abuse and unused privilege abuse

Keywords

- **Cloud Computing:** Cloud computing is a general term for anything that involves delivering hosted services over the internet.
- **Database:** A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields.
- **Database Security**: Database security is the technique that protects and secures the database against intentional or accidental threats.
- **Physical database integrity.** The data of a database are immune from physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.
- **Logical database integrity**: The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields, for example.
- **SaaS:** Provides service to customers in the form of application software. Clients can access application via various platforms thru a simple interface (often a browser).
- **PaaS**: Provides service to customers in the form of a platform on the which the customer apps can run.
- **IaaS:** Provides clients access to the underlying cloud infrastructure. It provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets.

Self Assessment

1. What is used for database security?

A. Data encryption

B. A view

C. Fingerprint

D. All of the above

2. Which of the following is not a type of hacking any smart-phone.

A. Target mobile hardware vulnerabilities

B. Target apps’ vulnerabilities

C. Snatching

D. Setup Keyloggers

3. Mobile phone operating systems contain open ________ that or may be vulnerable to different attacks.

A. OS

B. APIs

C. Keyloggers

D. spyware

4. Malware gets propagated through networks and technologies like?

A. SMS

B. Bluetooth

C. Wireless

D. All of the above

5. ____________ is the protection of smart-phones, phablets, tablets, and other portable tech-devices, & the networks to which they connect to, from threats & bugs.

A. OS Security

B. Database security

C. Cloud security

D. Mobile security

6. Try not to keep ________________ passwords, especially fingerprint for your smart-phone, because it can lead to physical hacking if you're not aware or asleep.

A. Biometric

B. PIN-based

C. Alphanumeric

D. Short

7. What type of computing technology refers to services and applications that typically run on a distributed network through virtualized resources?

A. Distributed Computing

B. Cloud Computing

C. Soft Computing

D. Parallel Computing

8. Cloud computing is a kind of abstraction which is based on the notion of combining physical resources and represents them as _______resources to users.

A. Real

B. Cloud

C. Virtual

D. none of the mentioned

9. Which one of the following is Cloud Platform by Amazon?

A. Azure

B. AWS

C. Cloudera

D. All of the mentioned

10. Which of the following statement is not true?

A. Through cloud computing, one can begin with very small and become big in a rapid manner.

B. All applications benefit from deployment in the Cloud.

C. Cloud computing is revolutionary, even though the technology it is built on is evolutionary.

D. None of the mentioned

11. Which of the following is not a type of cloud server?

A. Public Cloud Servers

B. Private Cloud Servers

C. Dedicated Cloud Servers

D. Merged Cloud Servers

12. Which of the following are the features of cloud computing?

A. Security

B. Availability

C. Large Network Access

D. All of the mentioned

13. Which of the following is a type of cloud computing service?

A. Service-as-a-Software (SaaS)

B. Software-and-a-Server (SaaS)

C. Software-as-a-Service (SaaS)

D. Software-as-a-Server (SaaS)

14. Which of the following is an example of the cloud?

A. Amazon Web Services (AWS)

B. Dropbox

C. Cisco WebEx

D. All of the above

15. When you add operating system and applications to the service, the model called as ____________.

A. PaaS

B. CaaS

C. SaaS

D. IaaS

Answers for Self Assessment

1.	D	2.	C	3.	B	4.	D	5.	D
6.	A	7.	B	8.	C	9.	B	10.	B
11.	C	12.	D	13.	C	14.	D	15.	C

Review Questions

1. Explain Database Security.
2. Explain the points to control database security along with its policies
3. Discuss different characteristics of Cloud Computing.
4. Explain the difference Between SaaS,PaaS and IaaS with the help of example.
5. What is the Cloud Deployment Model?
6. Illustrate the difference between Public, Private and Hybrid Model in cloud computing

Further Reading

https://mu.ac.in/wp-content/uploads/2021/01/Cloud-Computing.pdf

Web Links

https://www.researchgate.net/publication/229014450_Database_Security_What_Students_Need_to_Know

Unit 14: Firewalls

CONTENTS

Objectives

- Understand the concept of Digital Signature
- Acquire the knowledge about of Digital Signature works
- Learn about Firewalls and its different types
- Apply different design principles of Firewalls

Introduction

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

14.1 How Digital Signature works?

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.

Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder

Part 1 Public Key and Private Key in Digital Signature Example

To be effective in ensuring the security of the message, digital signatures have two types of keys:

- **public key**: The public key is an encryption that is given to the receiving computer by the host computer to enable the other person access to information being sent. But to access the information, the receiving computer must use the public key from the host computer as well as their own private key.
- **private key**: A private key on the other hand is vitally different. It is a secret code that allows a computer to encrypt a message before it can be sent over a network. For two computers to gain access to this information or connect on the same network, they must have this private key installed on them. It is essentially a coded language that only the computer with the private key can understand. It is therefore a lot more secure.

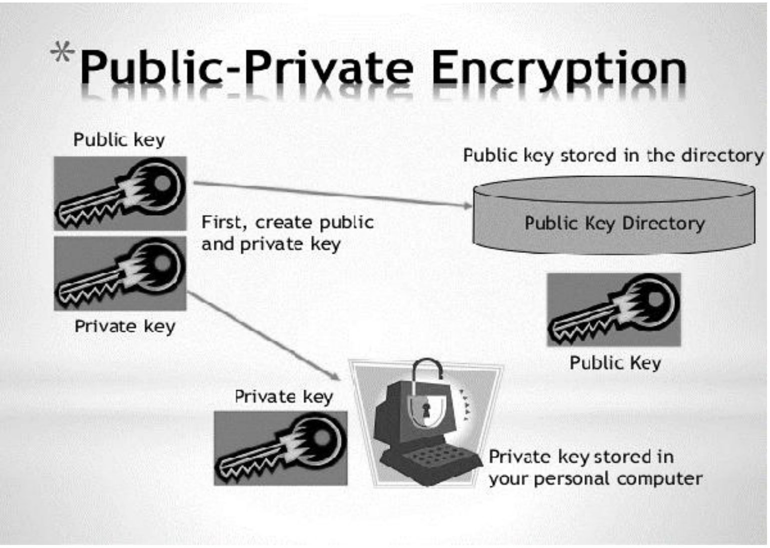

*Public-Private Encryption
Public key
Public key stored in the directory
First, create public and private key
Public Key Directory
Private key
Public Key
Private key
Private key stored in your personal computer

Figure 1 Public-Private Encryption

What are the benefits of digital signatures?

Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. Security features and methods used in digital signatures include the following:

- **Personal identification numbers (PINs), passwords and codes.** Used to authenticate and verify a signer's identity and approve their signature. Email, username and password are the most common methods used.
- **Asymmetric cryptography.** Employs a public key algorithm that includes private and public key encryption and authentication.
- **Checksum.** A long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. A checksum acts as a data fingerprint.

- **Cyclic redundancy check (CRC).** An error-detecting code and verification feature used in digital networks and storage devices to detect changes to raw data.
- **Certificate authority (CA) validation**. CAs issue digital signatures and act as trusted third parties by accepting, authenticating, issuing and maintaining digital certificates. The use of CAs helps avoid the creation of fake digital certificates.
- **Trust service provider (TSP) validation.** A TSP is a person or legal entity that performs validation of a digital signature on a company's behalf and offers signature validation reports.

Other benefits to using digital signatures include the following:

Timestamping. By providing the data and time of a digital signature, timestamping is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings.

Globally accepted and legally compliant. The public key infrastructure (PKI) standard ensures vendor-generated keys are made and stored securely. Because of the international standard, a growing number of countries are accepting digital signatures as legally binding.

Time savings. Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.

Cost savings. Organizations can go paperless and save money previously spent on the physical resources and on the time, personnel and office space used to manage and transport them.

Positive environmental impact. Reducing paper use also cuts down on the physical waste generated by paper and the negative environmental impact of transporting paper documents.

Traceability. Digital signatures create an audit trail that makes internal record-keeping easier for business. With everything recorded and stored digitally, there are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something.

14.2 Firewalls

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

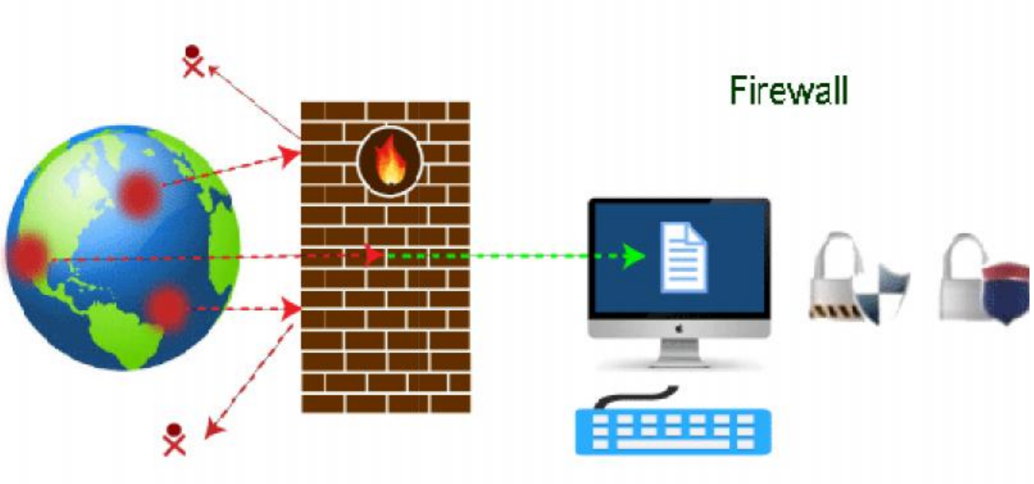


Figure 2 Structure of Firewalls

Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Why Firewall?

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

Open Access

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

Network Crashes

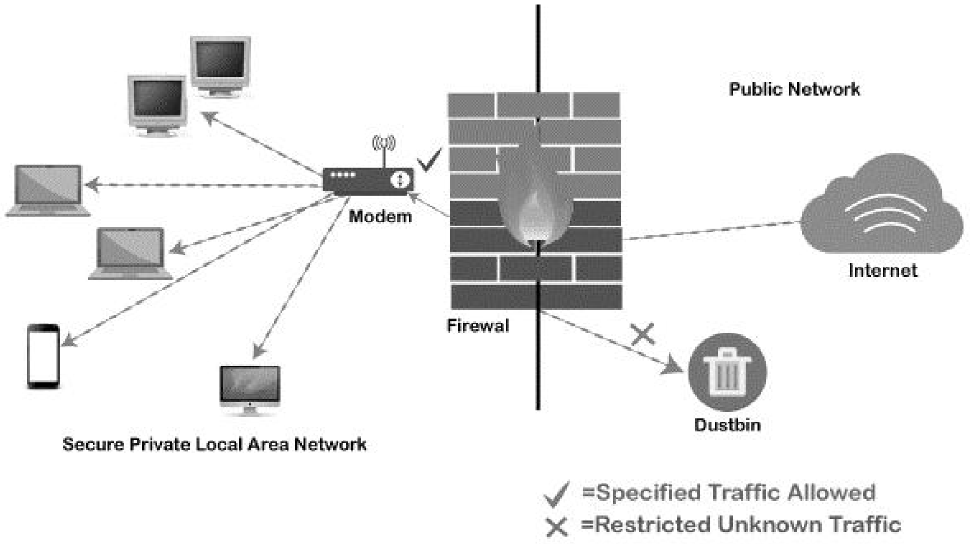
In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.

Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

14.3 How does Firewall Works?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.


Public Network
Modem
Firewal
Internet
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✕ =Restricted Unknown Traffic

Functions of Firewalls

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

14.4 Limitations of Firewalls

When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks. The answer may be "no". The best practice is to use a firewall system when using the Internet. However, it is important to use other defense systems to help protect the network and data stored on the computer. Because cyber threats are continually evolving, a firewall should not be the only consideration for protecting the home network.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.

- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Therefore, it is recommended to keep all Internet-enabled devices updated. This includes the latest operating systems, web browsers, applications, and other security software (such as anti-virus). Besides, the security of wireless routers should be another practice. The process of protecting a router may include options such as repeatedly changing the router's name and password, reviewing security settings, and creating a guest network for visitors.

14.5 Types of Firewalls

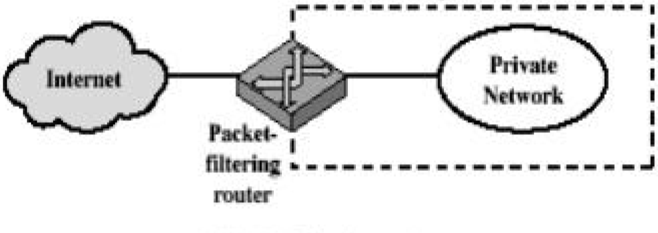
There are 3 common types of firewalls.

- Packet filters
- Application-level gateways
- Circuit-level gateways

Packet Filters

A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions. Filtering rules are based on the information contained in a network packet:

- Source IP address – IP address of the system that originated the IP packet. Destination IP address – IP address of the system, the IP is trying to reach. Source and destination transport level address – transport level port number. IP protocol field – defines the transport protocol.
- Interface – for a router with three or more ports, which interface of the router the packet come from or which interface of the router the packet is destined for.



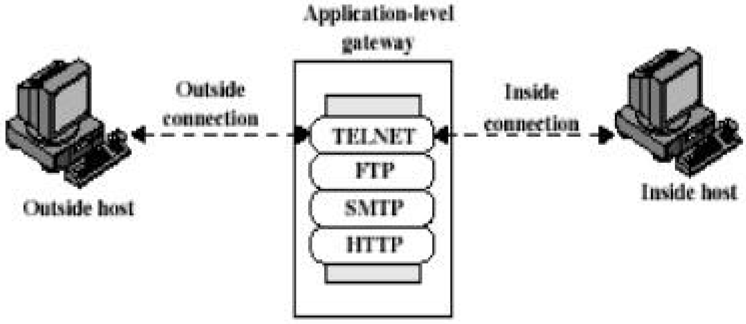
(a) Packet-filtering router

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

14.6 Application-Level Gateways

An Application level gateway, also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

Application level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level. A prime disadvantage is the additional processing overhead on each connection.

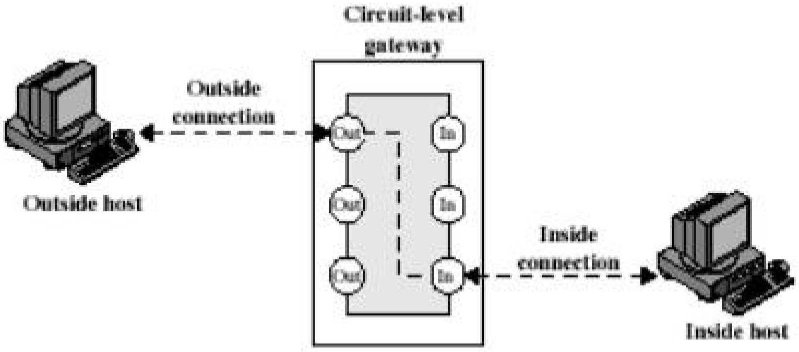


(b) Application-level gateway

14.7 Circuit Level Gateways

Circuit level gateway can be a stand-alone system or it can be a specified function performed by an application level gateway for certain applications. A Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.



(c) Circuit-level gateway

14.8 Firewall Design Principles

Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.

The firewall is inserted between the premise network and internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from internet-based attacks and to provide a single choke point where security and audit can be imposed. The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

14.9 Firewall Characteristics

All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.

- Various configurations are possible.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system. This implies that use of a trusted system with a secure operating system.

  Four techniques that firewall use to control access and enforce the site"s security policy is as follows:

  1. **Service control** – determines the type of internet services that can be accessed, inbound or outbound. The firewall may filter traffic on this basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as web or mail service.
  2. **Direction control** – determines the direction in which particular service request may be initiated and allowed to flow through the firewall.
  3. **User control** – controls access to a service according to which user is attempting to access it.
  4. **Behavior control** – controls how particular services are used.

Capabilities of firewall

A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

A firewall provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system.

A firewall is a convenient platform for several internet functions that are not security related.

A firewall can serve as the platform for IPsec.

Limitations of Firewalls

The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.

- The firewall does not protect against internal threats. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

14.10 How to Disable Firewalls?

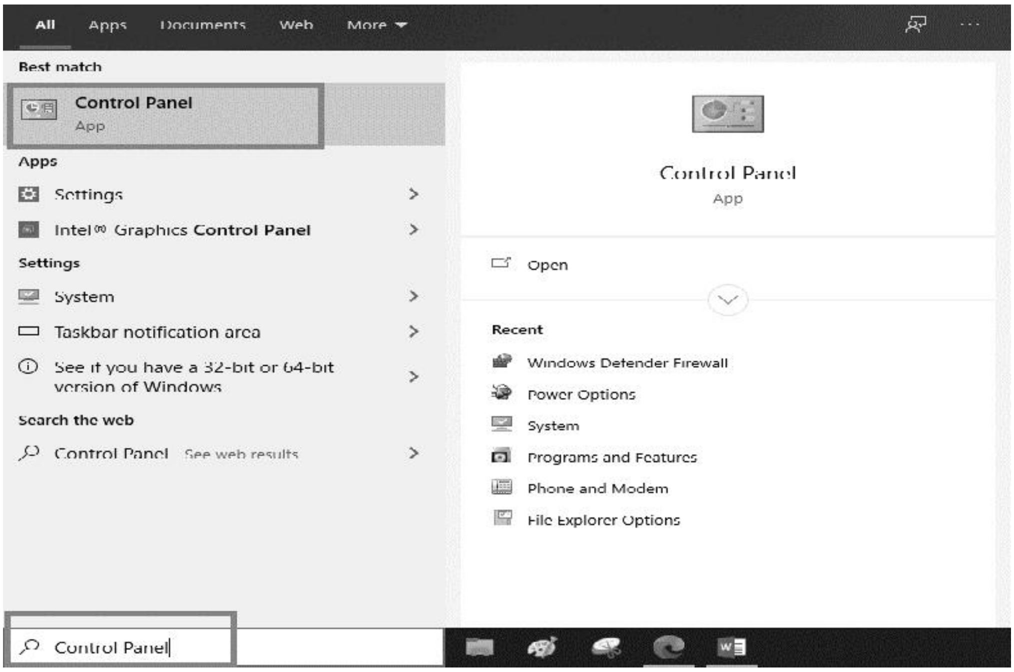
A firewall is the first line of control when it comes to the security of computers. It is designed to keep unauthorized users away from accessing files and resources stored on the computer system.

There can be several reasons why a user might want to disable the firewall, especially when a user wants to try another firewall program.

Disabling the Windows Firewall is quite easy, and it hardly takes around 10 minutes. Let's proceed with the steps to disable a firewall:

Step 1: First, we need to open the Control Panel. There are several ways to do this, but the easiest way is to use a search bar. Therefore, we need to click on the Windows search bar and enter the 'Control Panel'. It will look like the following screen:

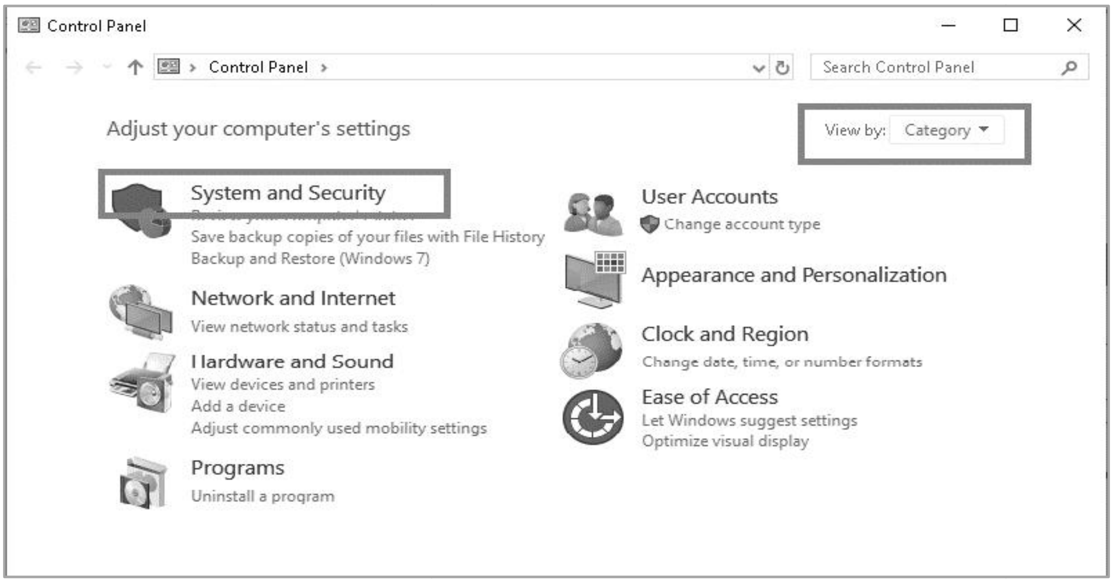
> ***Notes:*** It is not good to disable Windows Firewall unless there is another security program (with additional firewall support) running on the computer.



Control Panel

Figure 3 Step 1 Open Control Panel

Step 2: After that, we are required to click on the Control Panel to open its settings. The control panel contains the following options:

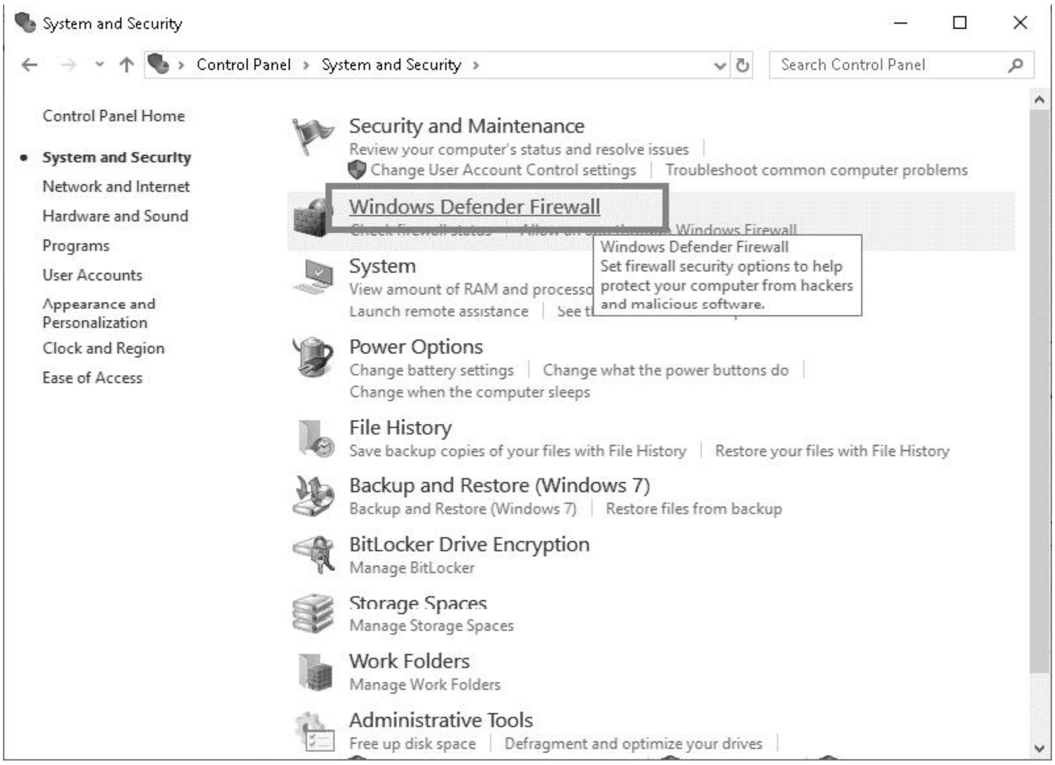

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

View by: Category

Figure 4 Step 2 Open System and Security Option

Here, we need to click on 'System and Security'. This option is only visible if the 'view by:' option is set as 'Category'.

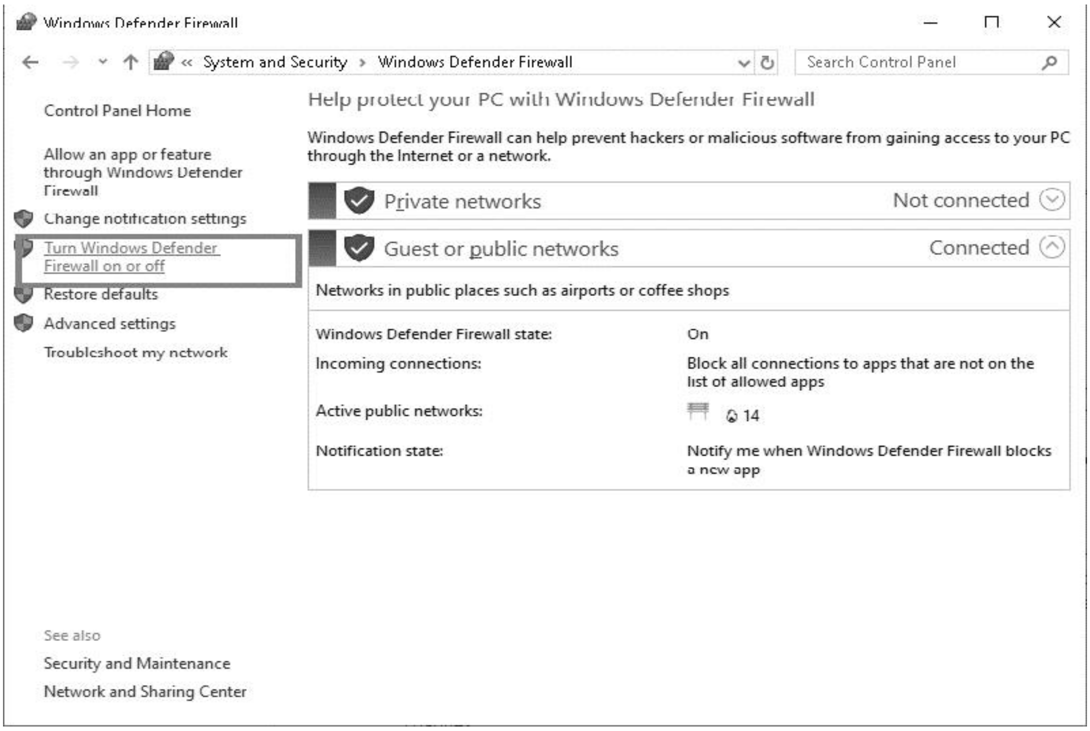
Step 3: Next, we need to click on 'Windows Defender Firewall', as shown below:


System and Security
Control Panel > System and Security >
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Windows Firewall
System
View amount of RAM and processo
Launch remote assistance
Power Options
Change battery settings
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Backup and Restore (Windows 7)
Backup and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimize your drives

Windows Defender Firewall
Set firewall security options to help protect your computer from hackers and malicious software.

Figure 5 Step 3 Select Windows Defender Firewall option

Step 4: We are then required to click on 'Turn Windows Defender Firewall on or off'. This option is shown in the left side panel of the screen:


Windows Defender Firewall
« System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

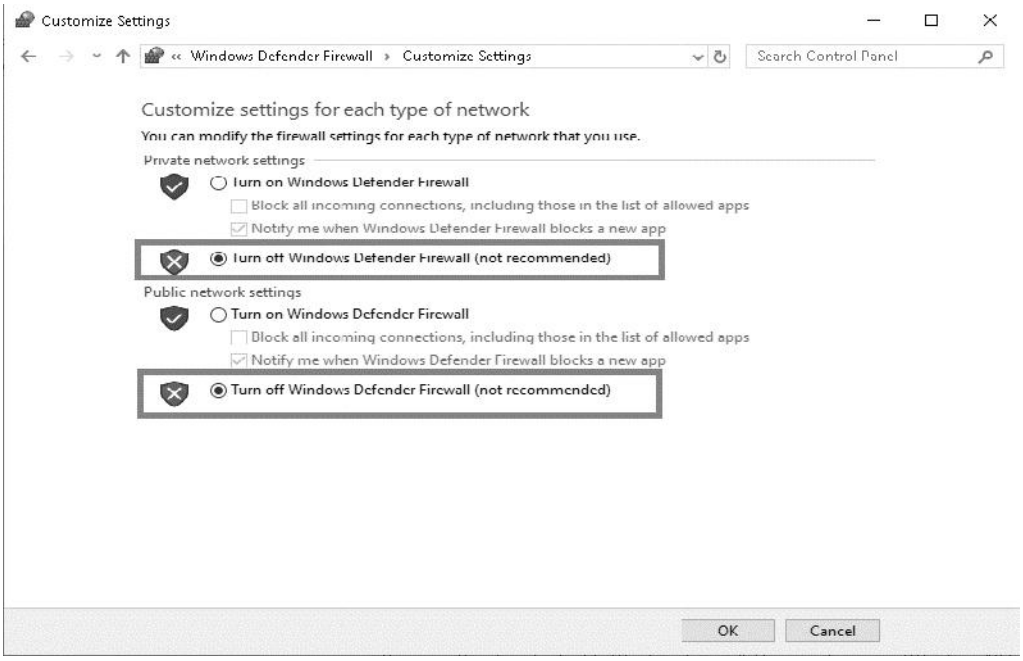
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	14
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Notes: In some computers, the option of 'Windows Defender Firewall' might instead be displayed as 'Windows Firewall'.

Step 5: On the next screen, we need to click on the circle radio button next to 'Turn off Windows Defender Firewall (not recommended)'.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

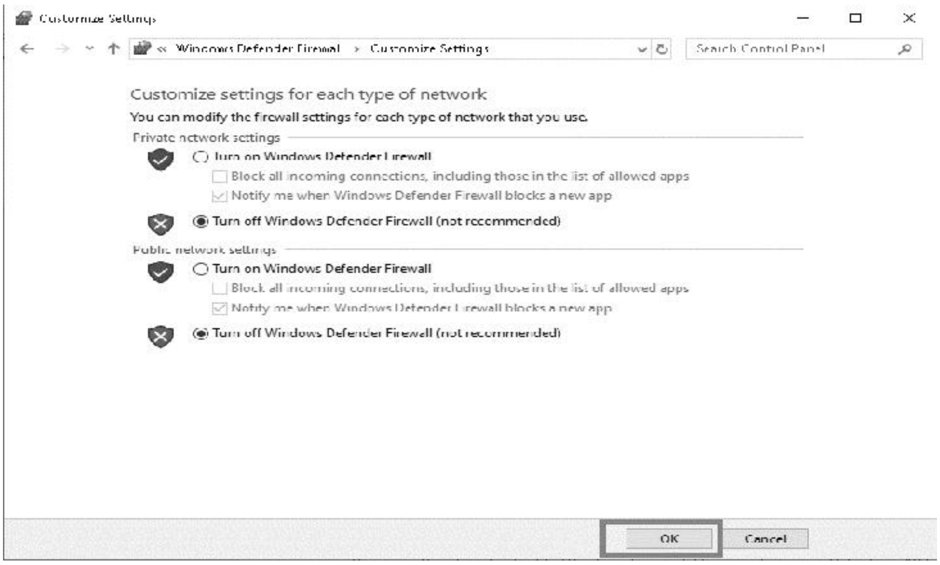
☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Figure 6 Warning of turning off windows defender

Here, we can select the firewall settings for different types of networks. Using this screen, we can turn off or disable the firewall for private networks, public networks, or both. We need to select the circle radio button next to 'Turn off Windows Defender Firewall (not recommended)' under both the private and the public network settings.

Step 6: After selecting the radio buttons, we are required to click on the 'OK' button to keep the changes.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

These are the steps to disable Windows Firewall. Here, we have used Windows 10 to describe the complete step by step tutorial. The processes will be the same on Windows 7/8/8.1; however, the user interface may be slightly different.

Task: Write down the steps to Turn on Windows defender.

Summary

- The message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- Firewalls have been a first line of defense in network security for over 25 years
- Firewalls establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- Software Firewalls provide more granular control, in that they can allow access for one application or feature while blocking others
- Hardware firewalls, on the other hand, are physical devices, each with its own computing resources

Keywords

Encryption – Process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except the authorized parties. This assures data security.

Public key– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.

Private key– Key which is only known to the person who's private key it is.

Authentication-Authentication is any process by which a system verifies the identity of a user who wishes to access it.

Digital Signature: A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

Digital Certificate: Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

Firewalls: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Self Assessment

1. ________________ is the kind of firewall is connected between the device and the network connecting to internet.

A. Hardware Firewall

B. Software Firewall

C. Stateful Inspection Firewall

D. Microsoft Firewall

2. Network layer firewall works as a __________

A. Frame filter

B. Packet filter

C. Content filter

D. Virus filter

3. A digital signature is a mathematical technique which validates?

A. authenticity

B. integrity

C. Non-repudiation

D. All of the above

4. _____________ is a process which verifies the identity of a user who wants to access the system.

A. Authentication

B. Non-repudiation

C. Integrity

D. None of the above

5. _____________ ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

A. Authentication

B. Non-repudiation

C. Integrity

D. None of the above

6. digital Signature is

A. a bit string giving identity of a correspondent

B. a unique identification of a sender

C. an authentication of an electronic record by trying it uniquely to a key only a sender knows

D. an encrypted signature of sender

7. digital signature needs a

A. private-key system

B. shared-key system

C. public-key system

D. all of them

8. Packet filtering firewalls are deployed on ________

A. routers

B. switches

C. hubs

D. repeaters

9. _____ perform on network levels and filter all the traffic coming and going across a network.

A. Network firewall

B. Web application firewall

C. Hardware-based

D. Software-based

10. They are installed on different network nodes, controlling each outgoing and incoming packet or byte__________

A. Web application firewall

B. Hardware-based

C. Software-based

D. Host-based Firewall

11. A dedicated firewall that is installed within your network and all the traffic traverse through this device____

A. Web application firewall

B. Hardware-based

C. Software-based

D. Host-based Firewall

12. Firewalls leveraging cloud solutions are called _________

A. Web application firewall

B. Hardware-based

C. Cloud-based Firewall

D. Host-based Firewall

13. A firewall needs to be __________ so that it can grow proportionally with the network that it protects.

A. Robust

B. Expansive

C. Fast

D. Scalable

14. Digital signature is a.

A. Digital id,send as an attachment to a web page/e- mail/message

B. Is used for verifying the attachments send using web

C. Both a and b

D. None of these

15. What is not a role of encryption?

A. It is used to protect data from unauthorized access during transmission

B. It is used to ensure user authentication

C. It is used to ensure data integrity

D. It is used to ensure data corruption doesn't happen

Answers for Self Assessment

1.	A	2.	B	3.	D	4.	A	5.	C
6.	C	7.	C	8.	A	9.	A	10.	D
11.	B	12.	C	13.	C	14.	C	15.	D

Review Questions

1. Explain the concept of Digital Signature with the help of diagram.
2. Discuss Firewalls
3. Explain different types of Firewalls with diagram.
4. Define Host-based Firewalls
5. How does firewallwork?
6. What are the advantages and Limitations of Firewalls?

Further Readings

http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf

Web Links

https://www.signinghub.com/wp-content/uploads/2017/05/Basics-of-Digital-Signatures-and-PKI-s.pdf

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in