Institute of Information Technology

Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (5th Batch)

Lecture: 06

Network Security Basic

Prepared by:

K M Akkas Ali

akkas_khan@yahoo.com, akkas@juniv.edu

Associate Professor

Institute of Information Technology (IIT)

Jahangirnagar University, Dhaka-1342

Objectives of this Lecture:

- To define computer security, network security and the challenges in them
- To define basic terminology related to security
- To define three security goals for network security
- To define security attacks that threaten security goals
- To define security services and mechanisms
- To illustrate a model for network security

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Network Security: An Introduction

During initial days of internet, its use was limited to military and universities for research and development purpose.

- Later when all networks merged together and formed the Internet, the data used to travel through public transit network.
- Common people may send the data that can be highly sensitive such as their bank credentials, username and passwords, personal documents, online shopping details, or confidential documents.
- With the rapid growth in the Internet, network security has become an integral part of computer and information security.
- In order to come up with measures that make networks more secure, it is important to learn about the vulnerabilities that could exist in a computer network and then have an understanding of the typical attacks that have been carried out in such networks.

Network Security: An Introduction

The requirements of security within an organization have undergone three major changes in the last several decades:

1. Before the advent of data processing equipment, the security of information of an organization was provided primarily by physical and administrative means.
   - An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is personnel screening procedures used during the hiring process.

2. With the introduction of the computer, the security of information stored on the computer was maintained by automated tools consisting of hardware and software.

3. With the introduction of network and communication facilities, the security for carrying data between hosts becomes more challenges.
   - Network security measures are needed to protect data during their transmission.

Importance of Security

Why Security?

- Computer security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated. These include:
  - Damage or destruction of computer systems.
  - Damage or destruction of internal data.
  - Loss of sensitive information to hostile parties.
  - Use of sensitive information to steal items of monetary value.
  - Use of sensitive information against the organization's customers which may result in legal action by customers against the organization and loss of customers.
  - Damage to the reputation of an organization.
  - Monetary damage due to loss of sensitive information, destruction of data, hostile use of sensitive data, or damage to the organization's reputation.

Importance of Security

Why Security?

- Therefore, no one can deny the importance of security in networking.
- Security in networking is based on cryptography, the science and art of transforming messages to make them secure and immune to attack.
- We are living in the information age. We need to keep information about every aspect of our lives.
- Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks.
- To be secured, information needs to be-
  - hidden from unauthorized access (confidentiality)
  - protected from unauthorized change (integrity).
  - available to an authorized entity when it is needed (availability).

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Importance of Security (cont…)

- Until a few decades ago, the information collected by an organization was stored on physical files.
  - The confidentiality of these files was achieved primarily by physical and administrative means. An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is restricting the access to a few authorized and trusted people in the organization.
  - In the same way, only a few authorized people were allowed to change the contents of the files.
  - Availability was achieved by designating at least one person who would have access to the files all the times.

Importance of Security (cont…)

- With the advent of computers, information storage became electronic. Instead of being stored on physical media, it was stored in computers.
- The three security requirements, however, did not change. The files stored in computers also require these security requirements, but their implementation is different and more challenging.
  - Computer networks created a revolution in the use of information.
  - Information is now distributed rather than centralized.
  - Authorized people can send and retrieve information from a distant place using computer networks.
- So, the security requirements mention before have some new dimensions.
- Not only should information be confidential when it is stored in a computer; there should also be a way to maintain its confidentiality when it is transmitted from one computer to another.

Examples of Security Violation

- Consider the following examples of security violations during transmission of information:

1. User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.
2. A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.
3. Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.
4. An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.
5. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

The Challenges of Computer Security

Computer and network security is both fascinating and complex. Some of the reasons include:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed].

The Challenges of Computer Security (cont…)

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users (and even security administrators) view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

Security Basic

What is security?

- Security means the prevention of and protection against assault, damage, fire, fraud, invasion of privacy, theft, unlawful entry, and other such occurrences caused by deliberate action.
- Therefore, the quality or state of being secure- to be free from danger, is called security.
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

Categorizing security in IT Arena:

In the field of information technology, security can be categorized into a number of ways:

- Computing security
- Application security
- Operating System security
- Network security
- Database security
- Information security

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is computer security?

Answer depends upon the perspective of the person you're asking-

- Network administrator has a different perspective than an end user or a security professional.
  - "A computer is secure if you can depend on it and its software to behave as you expect".
- Computer security means all the processes and mechanisms by which computer-based equipments, information stored in the computer and services provided by the computer are protected from unintended or unauthorized access, change or destruction.
- Computer security also refers to techniques in which a computer system is protected from data corruption, destruction, interception, loss, or unauthorized access.
- Computer security deals with computer-related assets that are subject to a variety of threats and for which various measures are taken to protect those assets.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

- Computer can be either a subject and/or an object of an attack.
  - When the subject of an attack, computer is used as an active tool to conduct attack.
  - When the object of an attack, computer is the entity being attacked.

Computer as the Subject and Object of an attack

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is Application Security?

- Application security encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system through flaws in the design, development, deployment, upgrade, or maintenance of the application.
- Applications only control the use of resources granted to them. They determine the use of these resources by users of the application through application security.
- Principle approach for application security includes:
  - Knowing your threats.
  - Securing the network, host and application.
  - Incorporating security into your software development process.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is Operating System Security?

- In a standalone computer system, all resources, data, application and users are OS-oriented.
- OS is responsible for communicating with the hardware and users.
- It safeguards data and applications stored in primary and secondary memory, properly manages various resources of the computer system, and establishes connection to other computer systems via the network. Therefore, OS is responsible for total operation of a computer system.
- As OS is responsible for the total operation of a computer system, so, it is the weak point for the information pirates.
- Flaws, commonly called 'bugs' or 'security holes', in the operating system on your computer (think Windows or Mac OS X) are being discovered almost daily.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is Network Security?

- Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data.
  - Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is Internet Security?

- Internet security is measures to protect data during their transmission over a collection of interconnected networks.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Basic

What is Database Security?

- Database security means protecting a database from destructive forces and the unwanted actions of unauthorized users.
- Some data security technologies include:
  - **Disk Encryption**
    - It refers to encryption technology that encrypts data on a hard disk drive.
  - **Hardware based Mechanisms for Protecting Data**
    - Software based security solutions encrypt the data to prevent them from being stolen. However, a malicious program or a hacker may corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access.
  - **Backups**
    - Backups are used to ensure data which is lost can be recovered.
  - **Data Masking**
    - It is the process of obscuring or masking specific data within a database to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel.
  - **Data Erasure**
    - It is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

Security Basic

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information.
- In information technology, security is the protection of information assets through the use of technology, processes, and training.

Necessary tools for Information Security:

- Policy
- Awareness
- Training
- Education
- Technology

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

A Model for Network Security

- A model for network security is shown in the figure.
- A message is to be transferred from one party to another across some sort of Internet service.

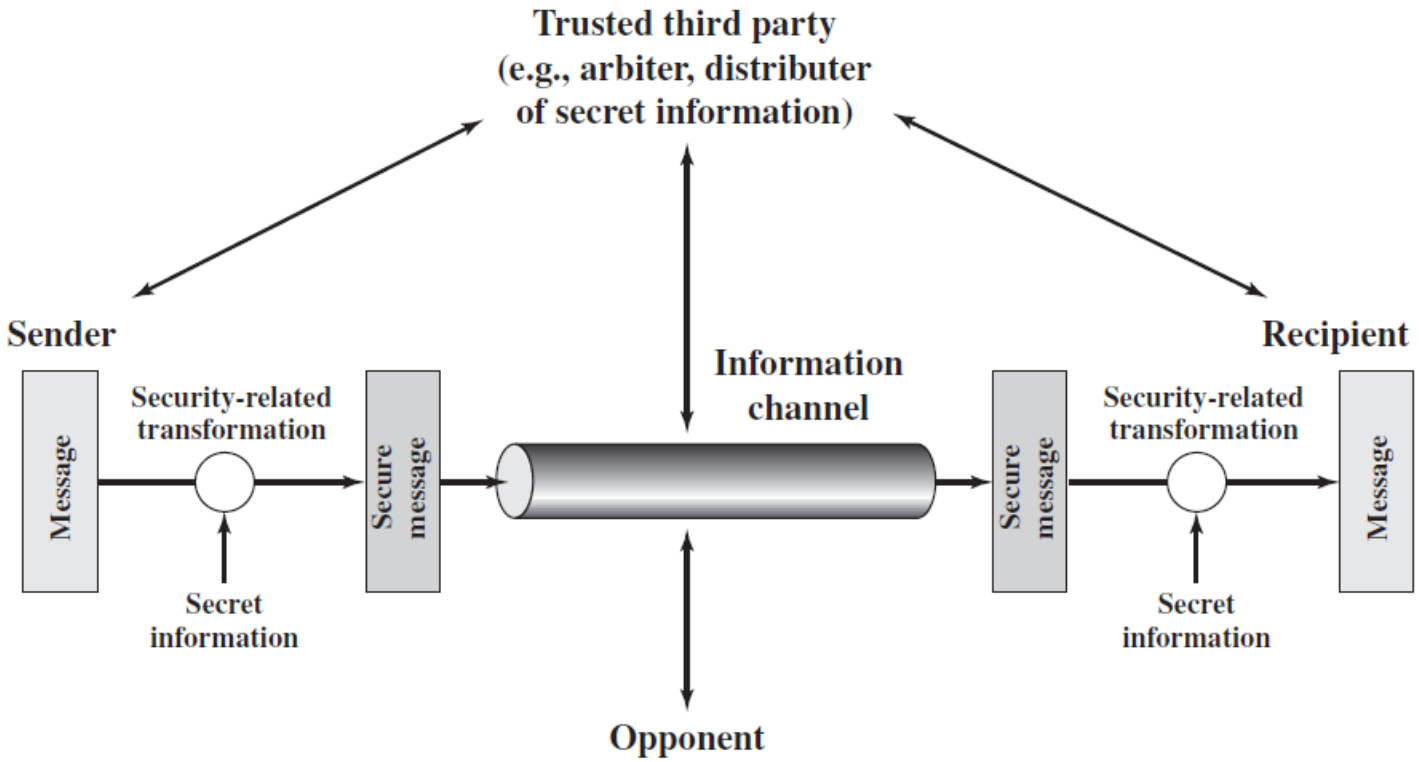


Figure: A model for network security

- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

A Model for Network Security

- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.
- All of the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.

   Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

   An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A Model for Network Security

- A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.
- This general model shows that there are four basic tasks in designing a particular security service:

    1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
    2. Generate the secret information to be used with the algorithm.
    3. Develop methods for the distribution and sharing of the secret information.
    4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Critical characteristics of information security

- Information is an asset that has a value like any other asset. The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

The CIA and DAD Triads of information security

CIA Triad:

The core concepts of information security are confidentiality, integrity, and availability. These principals are known as the CIA triad and are the foundation for combating the DAD triad.

CIA Triad or Triangle:

- **Confidentiality**:

  Confidential information should not be accessible to unauthorized users. That is, messages sent by Alice to Bob should not be readable by Eve.

- **Integrity**:

  Ensuring that data may only be modified through an authorized means. That is, Bob should be able to detect when data sent by Alice has been modified by Eve.

- **Availability**:

  Authorized users should be able to access data for legitimate purposes as necessary.

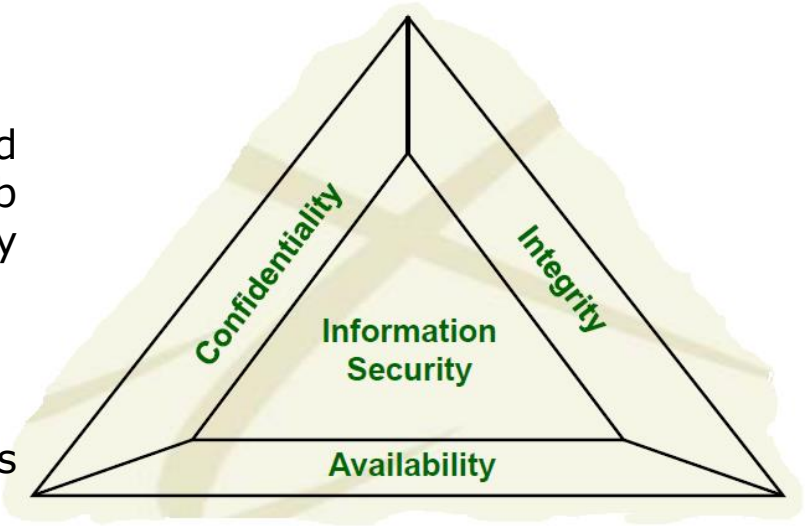


Figure: ***CIA Triad***

The CIA and DAD Triads of information security

DAD Triad or Triangle:

- DAD triad provides means for defeating the security of an organization.
- Malicious hackers have developed their own triad, the DAD triad, to counter the CIA triad of security professionals.
- Each leg of the DAD triad is targeted at defeating the mechanisms associated with one leg of the CIA triad.
- Having a good understanding of the CIA triad also means understanding the DAD triad that opposes the CIA triad.

- **Disclosure**:
  - Unauthorized individuals gain access to confidential information.
- **Alteration:**
  - Data is modified through some unauthorized mechanism.
- **Denial**:
  - Authorized users cannot gain access to a system for legitimate purposes.

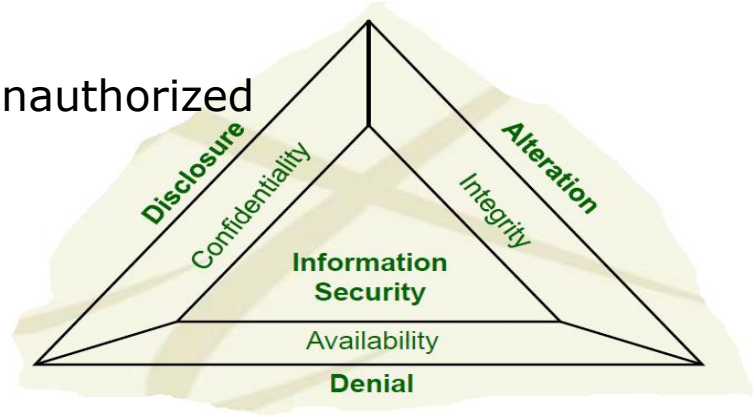
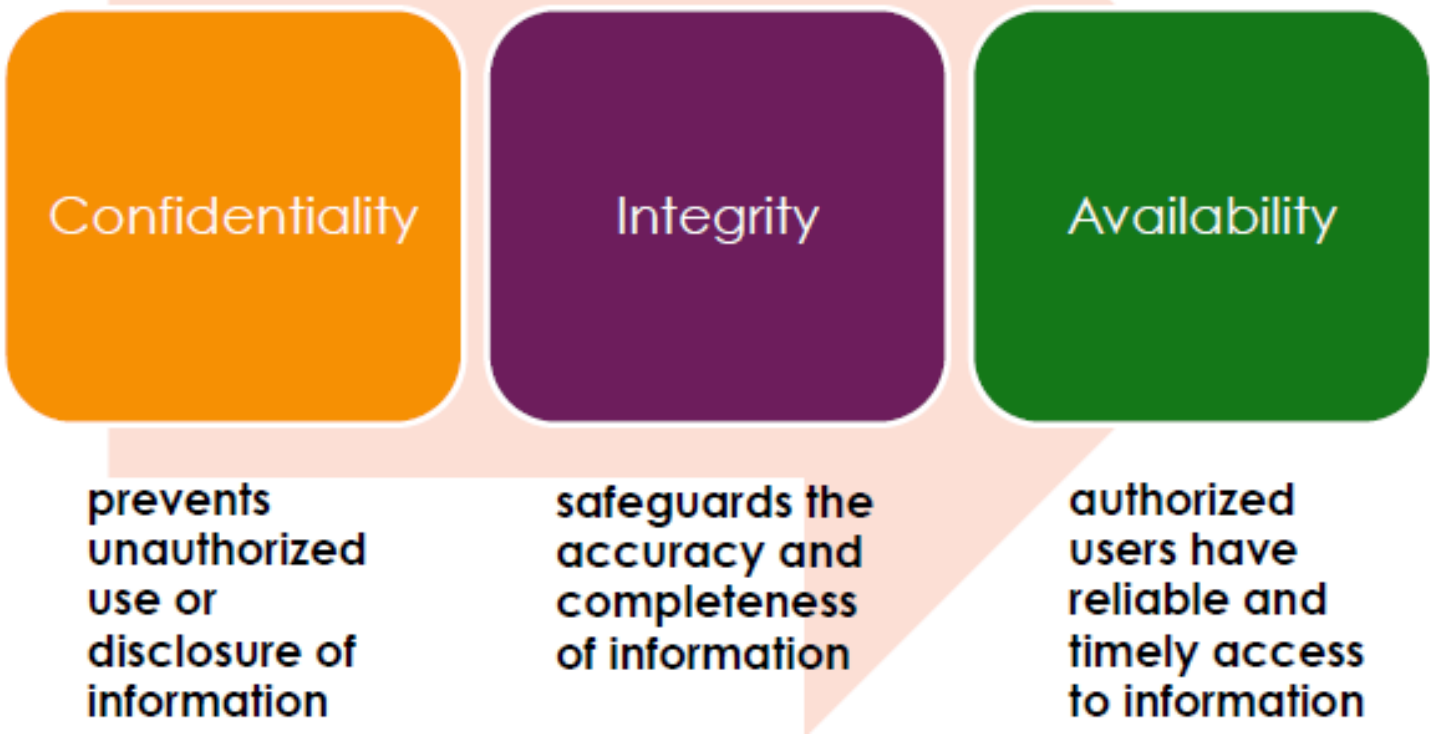


Figure: *DAD Triad*

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Goals of Information Security

- **Three main goals of information security are:**



- **Other goals are: authentication, non-repudiation, anonymity etc.**

Security Goals of Information

Confidentiality:

- Confidentiality is probably the most common aspect of information security.
- It means keeping data secret from all but those authorized to see it—messages sent by Alice to Bob should not be readable by Eve.
  - We need to protect our confidential information. For example, an organization needs to guard against those malicious actions that endanger the confidentiality of its information.
  - Confidentiality is applicable to stored information as well as information that is to be transmitted. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer , we need to conceal it during transmission.

Examples:

- In military, concealment of sensitive information is the major concern.
- In industry, hiding some information from competitors is crucial to operation of the organization.
- In banking, customers' accounts need to be kept secret.

Security Goals of Information

Integrity:

- It means ensuring that data has not been altered by unauthorized means— Bob should be able to detect when data sent by Alice has been modified by Eve.
- Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission.
  - Information needs to be changed constantly. For example, in a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.
  - Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power failure, may also create unwanted changes in some information.

Security Goals of Information

Authentication:

- Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.
- Two types of authentication are:

1. Entity authentication:
   - Entity authentication is a technique designed to let one party prove the identity of another party prior to access to the system resources (files, for example). For example, a student who needs to access her university resources needs to be authenticated during the logging process.
   - An entity can be a person, a process, a client, or a server.
2. Data origin authentication:
   - In data origin authentication, the receiver needs to be sure of the sender's identity and that an imposter has not sent the message. For example, Bob should be able to verify that data purportedly sent by Alice indeed originated with Alice.
   - This type of authentication is sometimes called message authentication.

Goals of Information Security

Availability:

- Information is useless if it is not available. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity. Imagine, what would happen to a bank if the customers could not access their accounts for transactions.
- Therefore, the information created and stored by an organization needs to be available to authorized entities.
- Information needs to be changed constantly, which means it must be accessible to authorized entities.

Security Goals of Information

Non-repudiation:

- Non-repudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send.
  - For example, when Bob receives a message purportedly from Alice, not only is Bob convinced that the message originated with Alice, but Bob can convince a neutral third party of this; thus Alice cannot deny having sent the message to Bob.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Goals of Information

Anonymity:

- Anonymity means "without a name" or "namelessness". It typically refer to the state of an individual's personal identity (or personally identifiable information) being publicly unknown.
- Encryption only hides what is being said. It can satisfy the confidentiality requirements, but it does not hide who is talking to whom. Anonymity hides who is saying it.
  - With the widespread acceptance of the Internet as a public medium for communication and information retrieval, there has been rising concern that the personal privacy of users can be eroded by cooperating network entities.
  - This is due to the fundamental nature of the Internet Protocol (IP) that is used to communicate across the network. Each packet carries the IP address of the machine that sent the packet as well as the IP address of the intended recipient of the packet. Under normal communication, any eavesdropper (e.g., a machine that sits on the network along the path a packet travels) can easily determine what entities are communicating, and any recipient of a packet is able to determine the source directly from received packets. Such monitoring and information gathering activities by eavesdroppers can adversely affect persons communicating over the Internet.

Security Goals of Information

Anonymity (cont...):

- A technical solution to maintaining privacy is to provide anonymity. Anonymous communication hides who is communicating with whom. For example, on the internet anonymous communication would hide a sender's (or recipient's) network address (IP address, email address, etc.) from unwanted observation.

- Anonymity is very useful when a person desires to protect their identity from discovery.
- Anonymous communication can encourage a number of beneficial activities such as-
  - anonymous tips for investigative journalists and law enforcement officials,
  - self-help discussion groups without fear of embarrassment,
  - personal privacy protection in general during web browsing,
  - Acts of charity have been performed anonymously when benefactors do not wish to be acknowledged.
  - A person who feels threatened might attempt to mitigate that threat through anonymity.
  - A citizen trying to report a crime would fear personal injury if their privacy was compromised to the perpetrators.
  - In universities for course and faculty evaluation by students;

Aspect of Security

Consider three aspects of information security:

1. Security attack:
   Any action that compromises the security of information owned by an organization is termed as security attack.
2. Security service:
   Security service enhances the security of data processing systems and information transfers of an organization. It is intended to counter security attacks using one or more security mechanisms
3. Security mechanism:
   To detect, prevent, or recover the information and information system from various security threats, security mechanisms are used.

Security Attack

What is Security Attack?

- Any action that compromises the security of information owned by an organization is termed as security attack.
  - Threat and attack are often used to mean the same thing.
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Kinds of Security Attacks

- The three goals of information security- confidentiality, integrity, and availability - can be threatened by security attacks.
- They can be classified using different approaches. Two approaches are mentioned here.

Category of attacks based on the security goals:

There are three groups of attacks based on the security goals. These are:

- 1. Attacks threatening confidentiality
- 2. Attacks threatening integrity
- 3. Attacks threatening availability

Category of attacks based on their effects on the system:

There are two groups of attacks based on their effects on the system. These are:

- 1. Passive attacks
- 2. Active attacks

Attacks Based on the Security Goals

Figure below shows the taxonomy of attacks based on the security goals:

1. Attacks Threatening Confidentiality

- Snooping
- Traffic analysis

2. Attacks Threatening Integrity

- Modification
- Masquerading
- Replaying
- Repudiation

3. Attacks Threatening Availability

- Denial of service

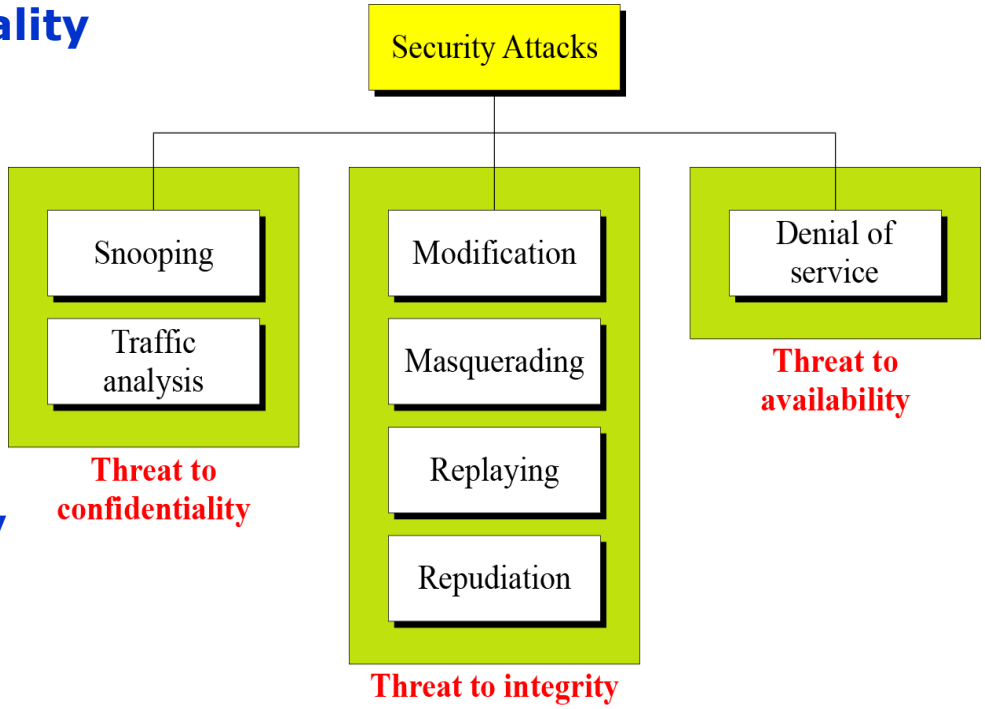


Figure: ***Taxonomy of attacks with relation to security goals***

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Confidentiality:

In general, there are two types of attacks threaten the confidentiality of information:

1. Snooping
2. Traffic analysis

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Confidentiality:

Snooping:

- It refers to unauthorized access to data or interception of data.
- For example, a file transferred through the internet may contain confidential information. An unauthorized entity (say, Eve) may intercept the transmission and use the contents for her own benefit.
- To prevent snooping, the data can be made nonintelligible to the interceptor by using cryptography.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Confidentiality:

Traffic Analysis:

- It refers to refers to obtaining some other type of information by monitoring online traffic.
- Although encipherment of data may make it nonintelligible for interceptor (say, Eve), she can find the electronic address (such as the e-mail address) of the sender or the receiver. She can collect pairs of requests and responses to help her guess the nature of transaction.

Attacks Based on the Security Goals

Attacks Threatening Integrity:

The integrity of data can be threatened by several kinds of attacks:

-Modification

- Masquerading

- Replaying

- Repudiation

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Integrity:

Modification:

- After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.
- Sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.
- For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit herself. It means that the attacker intercepts the message and changes it.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Integrity:

Masquerading :

- Masquerading or spoofing happens when the attacker impersonates somebody else. For example, an attacker might steal the bank card and PIN of a customer and pretend that she is that customer.
- Sometimes the attacker pretends instead to be the receiver entity. For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

- A hacker can concoct a fake website. Through a security hole in the genuine website, he may allow his IP address to substitute for that of the real one. The innocent traffic going to the legitimate website is funneled to the fake website. When orders or queries arrive, the hacker can make all kinds of alterations—direct the traffic to a third website, change the nature of the orders, and so on. An imposter who sends a false message is spoofing. That is, spoofing is the act of sending a message while pretending to be the authorized user.

Attacks Based on the Security Goals

Attacks Threatening Integrity:

Replaying:

- Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.
- For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to the bank to receive another payment from the bank.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Integrity:

Repudiation:

- It means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.
- This type of attack is different from other attacks because it is performed by one of the two parties involved in the communication: the sender or the receiver.
- An example of denial by the sender could occur when a customer asking her bank to send some money to a third party but later denying that she has made such a request.
- An example of denial by the receiver could occur when a person buy a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Attacks Based on the Security Goals

Attacks Threatening Availability:

Denial of Service:

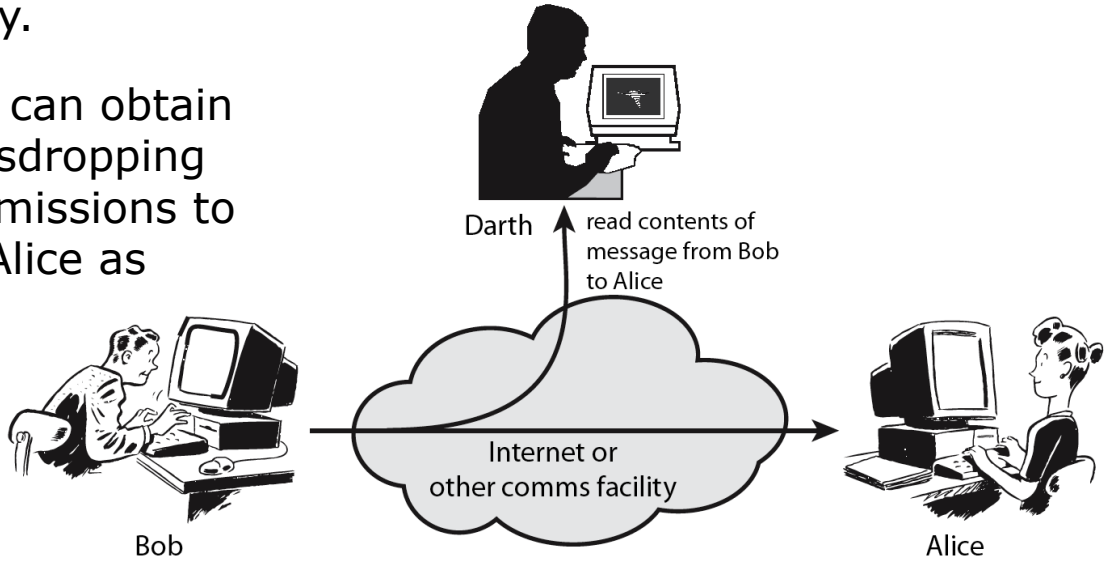
- Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.
- The attacker can use several strategies to achieve this. For example,
  - The attacker might send so many bogus requests to a server that it crashes because of the heavy load.
  - The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding.
  - The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Passive Attacks:

Passive Attacks:

- In a passive attack, the attacker goal is just to obtain information. This means that the attack does not modify or harm the system. The system continues with its normal operation.
- The attack may harm the sender or receiver of the message, but the system is not affected. They do not involve any alteration of data. For this reason, it is difficult to detect this type of attack until the sender or the receiver finds out about the leaking of confidential information.
- Passive attacks can be prevented by encipherment of the data.
- Example: Snooping and traffic analysis are the example of passive attacks that threaten confidentiality.
- Eve, as a passive attacker, can obtain message contents by eavesdropping on, or monitoring of, transmissions to the message from Bob to Alice as shown in the figure.



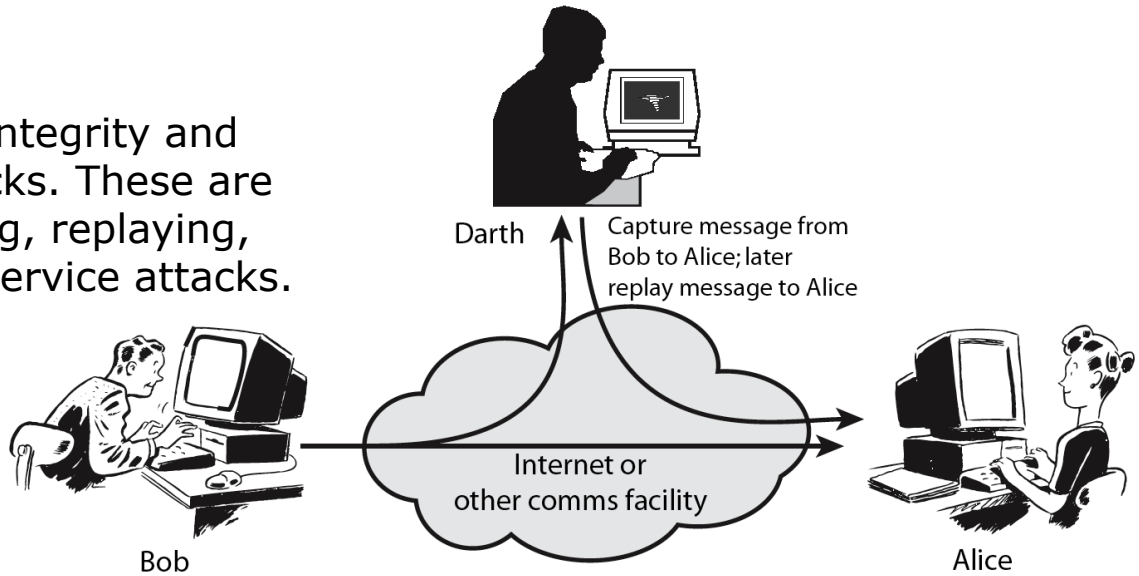
Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Active Attacks:

- An active attack may change the data or harm the system and system resources or affect their operation.
- Active attacks are normally easier to detect than to prevent.
- Active attacks present the opposite characteristics of passive attacks.
  - Whereas passive attacks are difficult to detect, measures are available to prevent their success.
  - On the other hand, active attacks are normally easier to detect than to prevent absolutely, because of the wide variety of potential physical, software , and network vulnerabilities.

Example:

- Attacks that threaten the integrity and availability are active attacks. These are modification, masquerading, replaying, repudiation and denial of service attacks.



Relationship Between Categories of Attacks

Table below shows the relationship between two categories of security attacks:

1. Attacks Threatening Confidentiality
- Snooping
- Traffic analysis

2. Attacks Threatening Integrity
- Modification
- Masquerading
- Replaying
- Repudiation

3. Attacks Threatening Availability
- Denial of service

1. Active Attacks:
- Modification
- Masquerading
- Replaying
- Repudiation
- Denial of service

2. Passive Attacks:
- Snooping
- Traffic analysis

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Table: Categorization of passive and active attacks

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

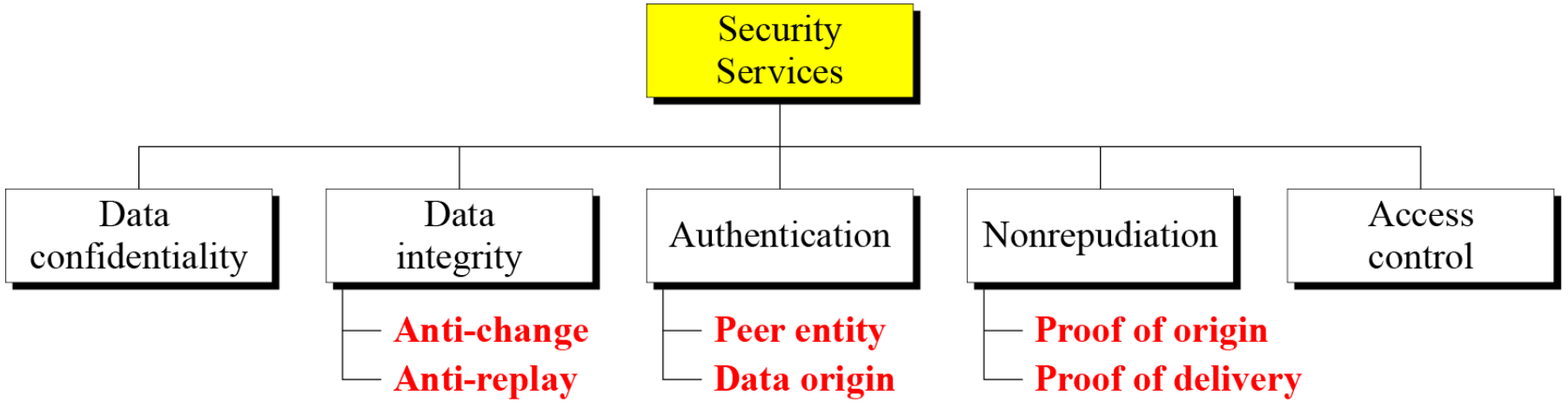
Security Services and Mechanism

- The International Telecommunication Union- Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services.
- Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service. Also, a mechanism can be used in one or more services.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Services Provided by Network Security

- Network security can provide one of the five services defined by ITU-T which are related to the security goals and security attacks. Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation. The fifth service provides entity authentication or identification.
- Figure below shows the taxonomy of five common services.



- It is easy to relate one or more of these services to one or more of the security goals.
- These services are designed to prevent the security attacks that we have mentioned earlier.

Services Provided by Network Security

- Network security can provide one of the five services defined by ITU-T which are related to the security goals and security attacks.
  - Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation.
  - The fifth service provides entity authentication or identification.
- Figure below shows the taxonomy of five common services.

- It is easy to relate one or more of these services to one or more of the security goals.
- These services are designed to prevent the security attacks that we have mentioned earlier.

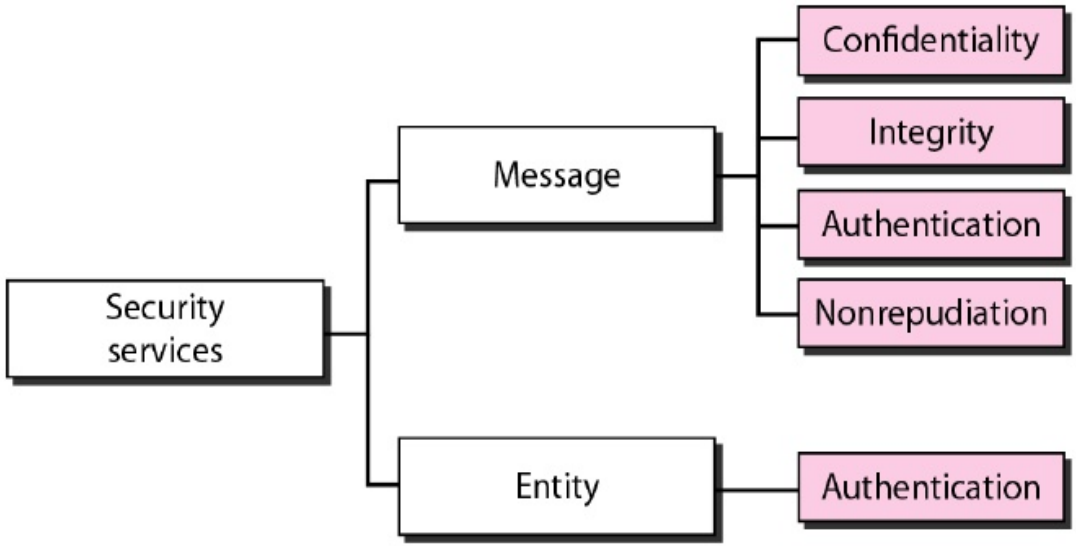


Figure: Taxonomy of Security Services

Security Services

Message Confidentiality:

- Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- This security service is designed to protect data from disclosure attack.
- The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. For example, when a customer communicates with her bank, she expects that the communication is totally confidential.

Security Services

Message Integrity:

- Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously.
- This service is designed to protect data from modification, insertion, deletion, and replaying by an adversary.
- As more and more monetary exchanges occur everyday over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Services

Message Authentication:

- In message authentication, the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.
  - Both the sender and receiver need to confirm the identity of other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. Face-to-face human communication solves this problem easily by visual recognition.
  - But when communicating entities exchange messages over a medium where they can not "see" the other party, authentication is not so simple. Why, for instance, should you believe that a received email containing a text string saying that the email came from a friend of yours indeed came from that friend? If someone calls on the phone claiming to be your bank and asking for your account number, secret PIN, and account balances for verification purposes, would you give that information out over the phone? Hopefully not.
- In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication).
- In connectionless communication, it authenticates the source of the data (data origin authentication).

Security Services

Message Nonrepudiation:

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.
- This service protects against repudiation by either the sender or the receiver of the data.
- In nonrepudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.

Security Services

Entity Authentication:

- An entity can be a person, a process, a client, or a server.
- Entity authentication is a technique designed to let one party prove the identity of another party prior to access to the system resources (files, for example). For example, a student who needs to access her university resources needs to be authenticated during the logging process.
- The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.

Security Services

Access Control:

- Access to protected information must be restricted to people who are authorized to access the information.
  - Access control is the ability to permit or deny the use of an object by a subject. It provides protection against unauthorized access to data. It limits and regulates the access to critical resources.
- This is done by identifying or authenticating the party that requests a resource and checking its permissions against the rights specified for the demanded object.
- It is assumed that an attacker is not legitimately permitted to use the target object and is therefore denied access to the resource. As access is a prerequisite for an attack, any possible interference is prevented.
- The foundation on which access control mechanisms are built start with identification and authentication.
- A firewall is an important access control system.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Services

Access Control (cont...):

- The most common form of access control used in multi-user computer systems are access control lists for resources that are based on the user and group identity of the process that attempts to use them.
  - The identity of a user is determined by an initial authentication process that usually requires a name and a password.
  - The login process retrieves the stored copy of the password corresponding to the user name and compares it with the presented one.
  - When both match, the system grants the user the appropriate user and group credentials.
  - When a resource should be accessed, the system looks up the user and group in the access control list and grants or denies access as appropriate.
- An example of this kind of access control can be found in the UNIX file system, which provides read, write and execute permissions based on the user and group membership. In this example, attacks against files that a user is not authorized to use are prevented by the access control part of the file system code in the operating system.

Security Services

Access Control (cont...):

- Access control is generally considered in four steps:
  1. Identification (who someone is)
  2. Authentication (who can login)
  3. Authorization (what authorized users can do)
  4. Accountability (identifies what a user did)

Identification:

- Identification is an assertion of who someone is or what something is. It provide username to establish a user's identity.
  - If a person makes the statement "Hello, my name is Asif" they are making a claim of who they are. However, their claim may or may not be true. Before Asif can be granted access to protected information it will be necessary to verify that the person claiming to be Asif really is Asif. Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to".

Security Services

Access Control (cont...):

Authentication:

- Authentication is the act of verifying a claim of a user's identity.
  - The term "user" may refer to a person, an application or process, a machine or a device.
- When Asif goes into a bank to make a withdrawal, he tells the bank teller he is Asif —a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has Asif printed on it and compares the photograph on the license against the person claiming to be Asif. If the photo and name match the person, then the teller has authenticated that Asif is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that they are the person they username belongs to.
- There are three different types of information that can be used for authentication:
  - ***Something you know:*** things such as a PIN, a password, passphrase or your mother's maiden name.
  - ***Something you have:*** a driver's license, token, passport or a smart card, RFID.
  - ***Something inherent:*** This is an inherent characteristics of the claimant. e.g. conventional signature, fingerprints, voice, facial characteristics, retinal pattern, and handwriting.

Security Services

Access Control (cont…):

Example of Tokens:

eToken

RFID cards

Smart Cards

Fingerprint scanner

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Services

Access Control (cont…):

Authorization:

- Authorization defines the user's rights and permissions on a system. It grants a user access to a particular resource and what actions he is permitted to perform on that resource.
- After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.
- Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions.
- The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms—some may even offer a choice of different access control mechanisms.
- Access criteria is done based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type
- Authentication simply identifies a party, but authorization defines whether they can perform certain action.

Security Services

Access Control (cont…):

Accountability:

- It is a security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Accountability supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action.

Security Mechanisms

- To detect, prevent, or recover the information and information system from various security threats, security mechanisms are used.
- Some widely used security mechanisms used to implement the security services recommended by ITU-T is illustrated below.
- To implement security goals of information, two techniques are widely used:
  - Cryptography
  - Steganography

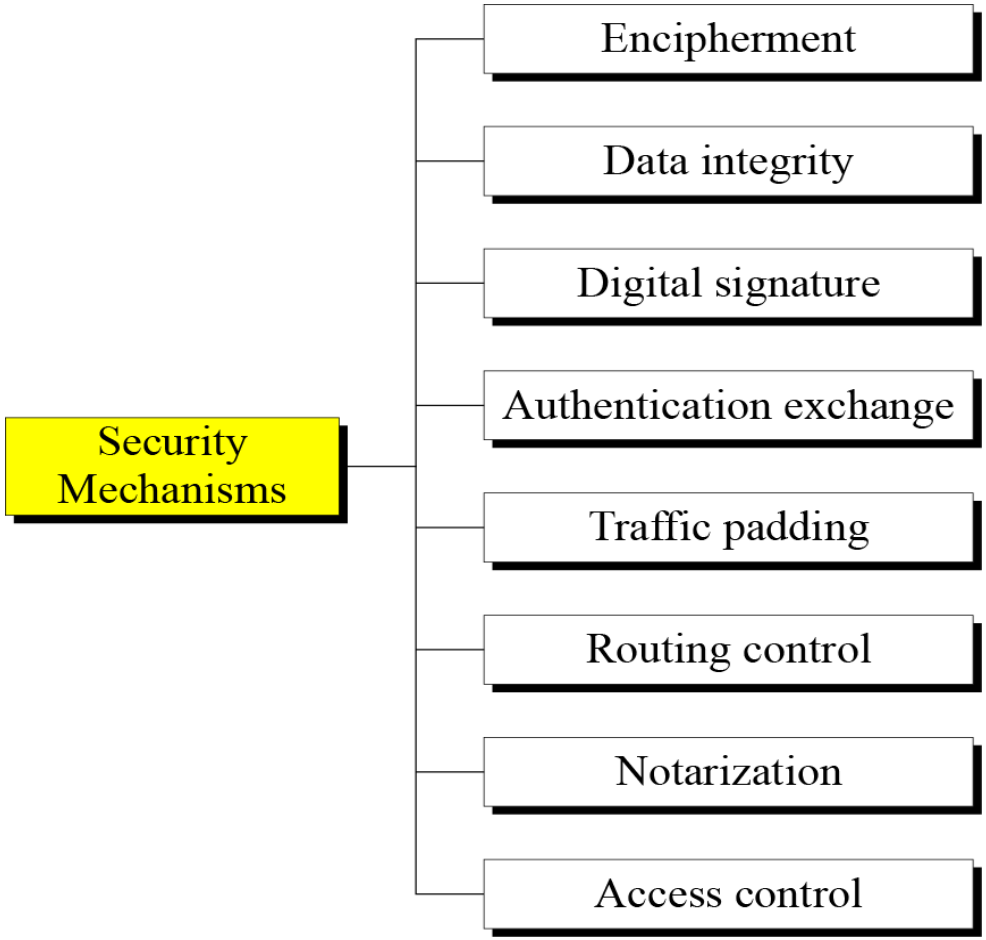


Figure: Taxonomy of Security Mechanisms

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Mechanisms

Encipherment:

- It means hiding or covering data.
- Encipherment can provide confidentiality.
- It can also be used to complement other mechanisms to provide other services.
- Two techniques are widely used for enciphering: cryptography and steganography.

Data Integrity:

- This mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.
- The receiver receives the data and checkvalue.
- He then creates a new checkvalue from the received data and compares the newly created checkvalue with the one received.
- If the two checkvalues are the same, the integrity of data has been preserved.

Security Mechanisms

Digital Signature:

- A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.
- The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Authentication Exchange:

- In authentication exchange, two entities exchange some messages to prove their identity to each other.
- For example, one entity can prove that she knows a secret that only she is supposed to know.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka

Security Mechanisms

Traffic Padding:

- Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

Routing Control:

- It means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Security Mechanisms

Notarization:

- Notarization means selecting a third trusted party to control the communication between two entities.
- This can be done, for example, to prevent repudiation.
- The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

Access Control:

- Access control uses methods to prove that a user has access right to the data or resources owned by a system.
- Examples of proofs are passwords and PINs.

Prepared by: K M Akkas Ali, Associate Professor, IIT, Jahangirnagar University, Dhaka