VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Information & Systems Security

SWE3002

Dr. Malathi D.

Information & Systems Security

Course Objectives

- To learn principles of cryptography, network and information security.
- To comprehend mathematical foundations of cryptography
- To introduce the practices of cryptography and network security along with its applications
- To use the information sources

Expected Outcomes

On completion of this course, students will be able to

- Identify the challenges of security attacks
- Understand the elementary cryptography based on symmetric and public-key encryption techniques
- Understand public Key Crypto Systems models, RSA algorithm, Diffie-Hellman key exchange
- Apply Cryptographic hash functions SHA-512, MAC requirements, security, HMAC, Digital signatures
- To generate the key distributions using symmetric and asymmetric encryptions
- Enumerate malicious software, viruses and counter measures
- Understand Operating Systems & Data base Security issues and control methods
- Study Applications of Information & Systems Security in industry

Unit – 1

Fundamentals of Security

Fundamentals of Security

- **Definitions & challenges of Security**
    - Cybersecurity
        - Information security
        - Network security
    - CIA triad
    - Challenges
- **OSI security architecture**
    - Security Attacks
    - Security Services
    - Security Mechanisms
- **Security policies**
- **Access control structures**

Definitions & challenges of Security

Definition of Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of **preserving the integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Cybersecurity

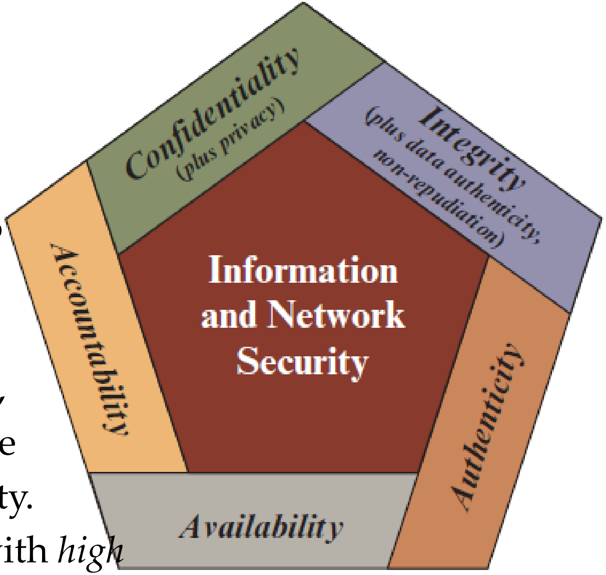
- ***Protection of information that is stored, transmitted, and processed in a networked system*** of computers, other digital devices, and network devices and transmission lines, including the Internet.
- Protection encompasses confidentiality, integrity, availability, authenticity, and accountability.
- ***Methods of protection*** include organizational policies and procedures, as well as technical means such as ***encryption and secure communications protocols***.
- It encompasses information security (electronic and physical information) and network security.
    - **Information security**: *Preservation* of confidentiality, integrity, and availability of information. In addition, authenticity, accountability, non-repudiation, and reliability can also be involved.
    - **Network security**: *Protection* of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

Definitions & challenges of Security

Security Objectives

- The cybersecurity definition introduces three key objectives i.e. confidentiality, integrity and availability.
- These three concepts form the **CIA triad**.
- **Confidentiality**
    - ***Data confidentiality***: Assures that ***private or confidential information*** is not made available or disclosed to unauthorized individuals.
    - ***Privacy***: Assures that individuals control or influence what information related to them may be collected and stored and ***by whom and to whom that information may be disclosed***.
- **Integrity**
    - ***Data integrity***: Information and programs ***can be changed*** only in a specified and authorized manner. **Data authenticity* is what it claims to be or what it is claimed to be. **Non-repudiation,* both the sender and recipient of information is provided with proof of delivery and proof of the sender's identity, respectively, so ***neither can later deny*** having processed the information.
    - ***System integrity***: Assures that a system ***performs its intended function in an unimpaired manner,*** free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability**: Assures that systems work promptly and service is ***not denied to authorized users***.

Definitions & challenges of Security



- In addition to CIA triad, two more concepts are needed. They are:
  - **Authenticity**: Verifying that users are who they say they are, each input arriving at the system came from a trusted source.
  - **Accountability**: Systems must ***keep records*** of their activities to permit later forensic analysis ***to trace security breaches*** or to aid in transaction disputes.
- Three levels of security breaches: **Low**, **Moderate**, **High**
  - **Confidentiality:** *Student grade information* – highly confidential, *Student enrollment information* - moderate, results in less damage if disclosed. *Directory information* - assigned a low confidentiality.
  - **Integrity:** *Patient's medical information* stored in db is an asset with *high requirement* for integrity. *Moderate level* of integrity requirement is a *Web site that offers a forum to registered users* to discuss specific topic, and *low integrity* requirement is an *anonymous online poll*.
  - **Availability:** *Authentication services* is highly important, inability to access resources if it fails. *Moderate availability requirement is a University Web site*, not important but its unavailability will cause some embarrassment. *An online telephone directory lookup app.* is a *low availability requirement*.

Definitions & challenges of Security

Challenges of Computer Security

- Major security requirements are confidentiality, authentication, non-repudiation, or integrity. But the ***mechanisms*** used to meet those requirements are ***quite complex***.
- In developing a security mechanism, 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.
- 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. ***Only when the various aspects of the threat are considered that elaborate security mechanisms make sense***.
- Having designed various security mechanisms, it is ***necessary to decide where to use them***. ***At what points in a network*** (physical placement) and ***at what layer*** or layers of TCP/IP (logical sense) such security mechanisms are needed.
- Security mechanisms typically ***involve more than a particular algorithm or protocol***. They also require that participants be in possession of some secret information (encryption key), which raises questions about the creation, distribution, and protection of that secret information.

Definitions & challenges of Security

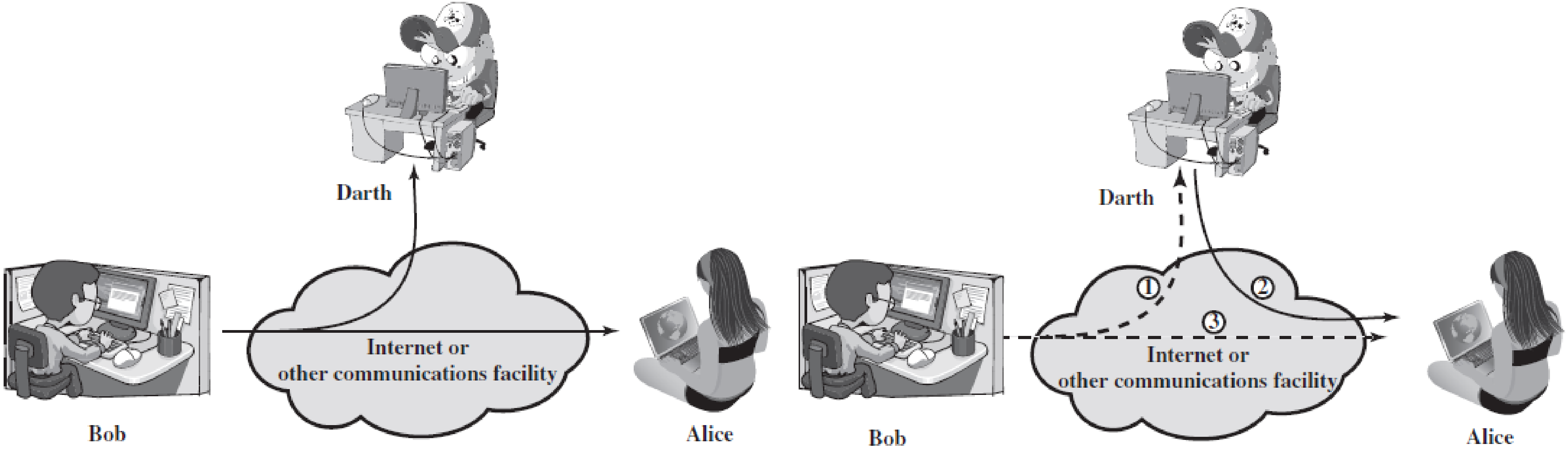
  - **Example**: If the proper functioning of the ***security mechanism requires setting time limits*** on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
- Information and network security is essentially a ***battle of intelligence 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.
- 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.
- Security ***requires regular, even constant, monitoring***, and this is ***difficult in today's short-term,*** overloaded environment.
- 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.
- Many users and even security administrators view ***strong security as an obstruction to efficient and user-friendly operation*** of an information system or use of information.

The OSI Security Architecture

- Some systematic way is needed to define security requirements of an organization and approaches to satisfying those requirements.
- ***ITU-T^3 Recommendation X.800, Security Architecture for OSI*** (Open Systems Interconnection), defines a systematic approach to providing security at each layer.
- The OSI Security Architecture defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network.
- The OSI security architecture focuses on:
  - **Security attack**: Any action that compromises the security of information owned by an organization.
  - **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
  - **Security service**: A processing or communication 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.

Security Attacks

- Security attacks is of two types:
  - i) **Passive attack** attempts to ***learn or make use of information*** from the system but does not affect system resources,
  - ii) **Active attack** attempts to ***alter*** system resources or affect their operation.



(a) Passive attacks

(b) Active attacks

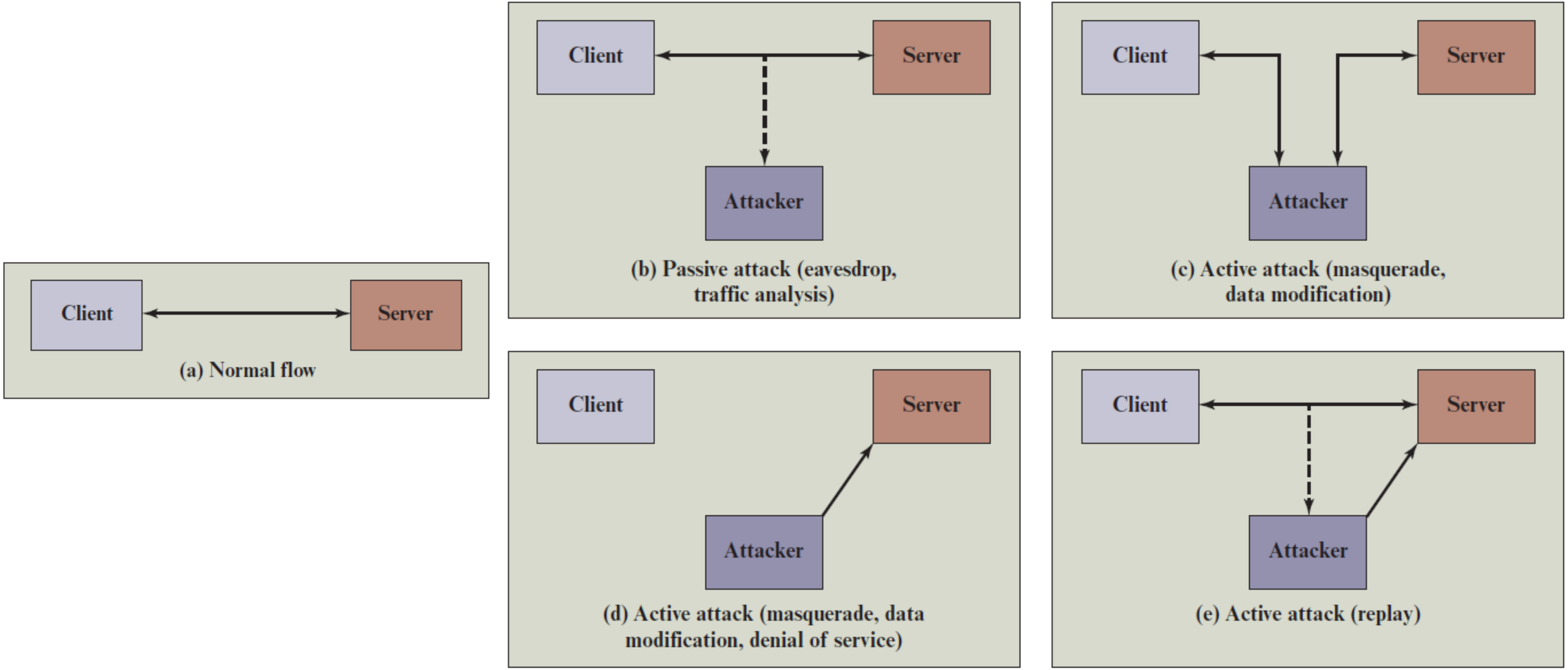
Security Attacks: Passive attacks

- The goal of the opponent is to obtain information that is being transmitted. Eavesdropping on, or monitoring of, transmissions.
- Two types of passive attacks are the ***release of message contents*** and ***traffic analysis***.
- **Release of message contents**:
  - A telephone conversation, an e-mail message, and a transferred file may contain sensitive or confidential information, ***prevent an opponent from learning the contents of these transmissions***.
- **Traffic analysis**:
  - Masking the contents of messages or other information traffic so that opponents, ***even if they captured the message, could not extract the information from the message***.
  - The common technique for masking contents is ***encryption***. Still, an opponent might be able to ***observe the pattern*** of these messages.
  - The opponent could determine the location and identity of communicating hosts and could ***observe the frequency and length of messages*** being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
- Passive attacks are very ***difficult to detect***, because they do not involve any alteration of the data.
- However, it is ***feasible to prevent*** the success of these attacks, usually by means of encryption.

Security Attacks: Active attacks

- Active attacks involve some ***modification of the data stream*** or the ***creation of a false stream***
- **Masquerade attack**: O*ne entity pretends to be other entity*.
  - It usually includes one of the other forms of active attack. For example: authentication sequences can be captured and replayed after a valid authentication sequence has taken place.
- **Replay attack**: Involves the ***passive capture of a data unit and its subsequent retransmission*** to produce an unauthorized effect.
- **Modification of messages**: ***Some portion of a legitimate message is altered***, or that messages are ***delayed or reordered***, to produce an unauthorized effect.
  - *Example*: Message "Allow A to read confidential file accounts" is modified to mean "Allow B to read confidential file accounts."
- **Denial of service attack**: ***Prevents or inhibits the normal use or management of communications facilities***.
  - *Example*: An entity may suppress all messages directed to a particular destination, disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.
- Difficult to prevent but detection & recovery from any disruption or delays caused by them are possible.

Security Attacks: Types of attacks



(a) Normal flow

(b) Passive attack (eavesdrop, traffic analysis)

(c) Active attack (masquerade, data modification)

(d) Active attack (masquerade, data modification, denial of service)

(e) Active attack (replay)

Security Services

- X.800 divides these security services into ***five categories*** and ***fourteen specific services***.
- **Authentication**
  - The authentication service is concerned with ***assuring that a communication is authentic***.
  - In the case of a ***single message***, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
  - In the case of an ***ongoing interaction***, such as the connection of a terminal to a host, two aspects are involved. At the time of connection initiation, the ***service assures that***
    - ***the two entities are authentic***,
    - the ***connection is not interfered*** with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of ***unauthorized transmission or reception***.
  - **Peer entity authentication**
    - Peer entity authentication is provided for use ***at the establishment*** of, or ***at times during the data transfer*** phase of, a connection. It attempts to provide confidence that an entity is not performing either ***a masquerade or an unauthorized replay of a previous connection***.
  - **Data origin authentication**
    - Provides for the validation of the ***source of a data unit***. It ***does not provide protection against the duplication or modification of data units***. Example: E-mail, where there are no prior interactions between the communicating entities.

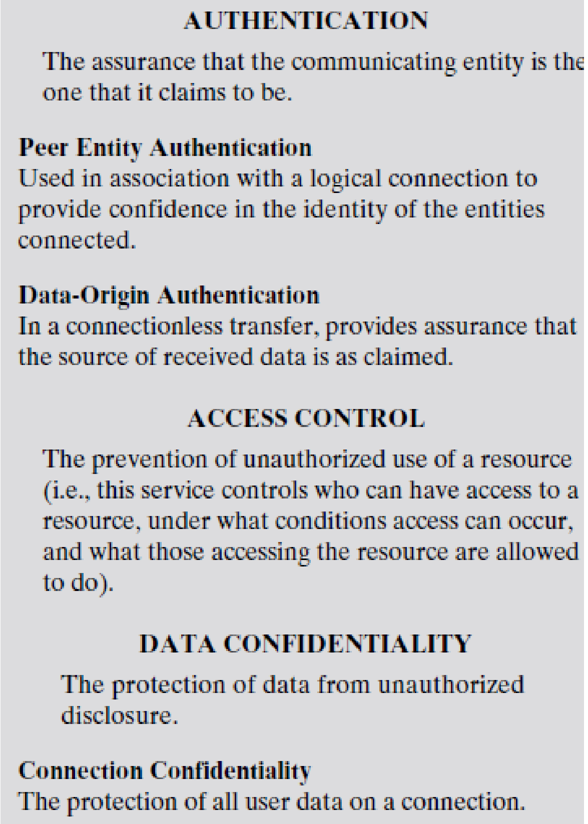
Security Services

- **Access Control**
  - ***Ability to limit and control the access*** to host systems and applications via communications links.
  - To achieve this, each entity trying to gain access must ***first be identified, or authenticated***, so that access rights can be tailored to the individual.
- **Data Confidentiality**
  - Confidentiality is the ***protection*** of transmitted data ***from passive attacks***.
  - Several levels of protection:
    - The broadest service ***protects all user data transmitted between two users over a period of time***. **Example**: when a TCP connection is set up between two systems, this broad protection ***prevents the release of any user data transmitted over the TCP connection***.
    - Narrower forms of this service, including the protection of a ***single message or even specific fields*** within a message. These refinements are less useful than the broad approach and may even be ***more complex and expensive to implement***.
    - P***rotection of traffic flow from analysis***. An attacker unable to observe the ***source and destination, frequency, length, or other characteristics*** of the traffic on a communications facility.
- **Data Integrity**
  - Integrity can apply to a ***stream of messages, a single message, or selected fields within a message***.
  - Integrity service relates to ***active attacks***, so concerned with ***detection rather than prevention***.

Security Services

  - A ***connection-oriented integrity service*** that deals with ***stream of messages***, assures that ***messages are received as sent with no duplication, insertion, modification, reordering, or replays***. It addresses both message stream ***modification and denial of service***.
  - A ***connectionless integrity service***, that deals with ***individual messages*** without regard to any larger context, generally provides ***protection against message modification only***.
  - If a ***violation of integrity is detected***, then the service may simply ***report this violation***, and some other portion of software or human ***intervention is required to recover from the violation***.
- **Non-repudiation**
  - Non-repudiation ***prevents either sender or receiver from denying a transmitted message***.
  - When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
  - Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.
- **Availability services**
  - Availability is the ***property of a system, or a system resource being accessible and usable upon demand*** by an authorized system entity, according to performance specifications for the system.
  - A ***variety of attacks can result*** in the loss of or reduction in availability. Some are amenable to ***automated countermeasures like authentication and encryption,*** whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

Security Services



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

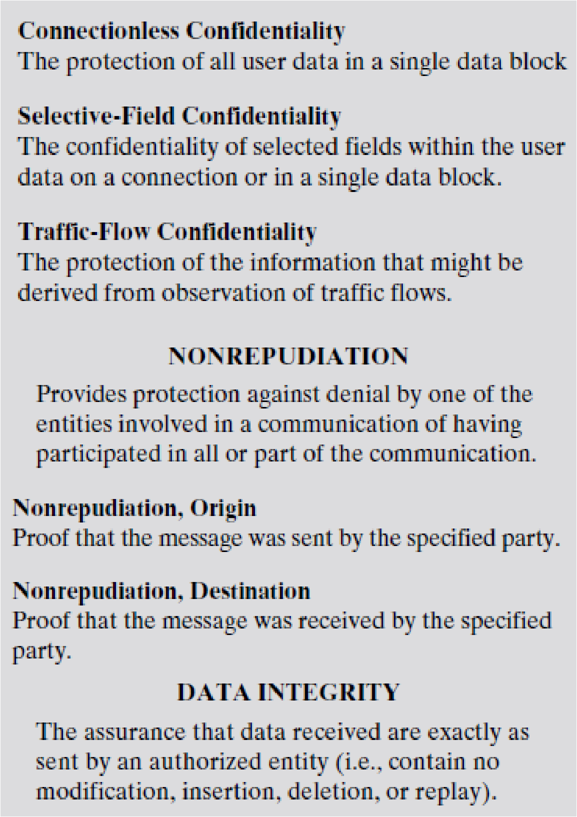
ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.



Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

NONREPUDIATION

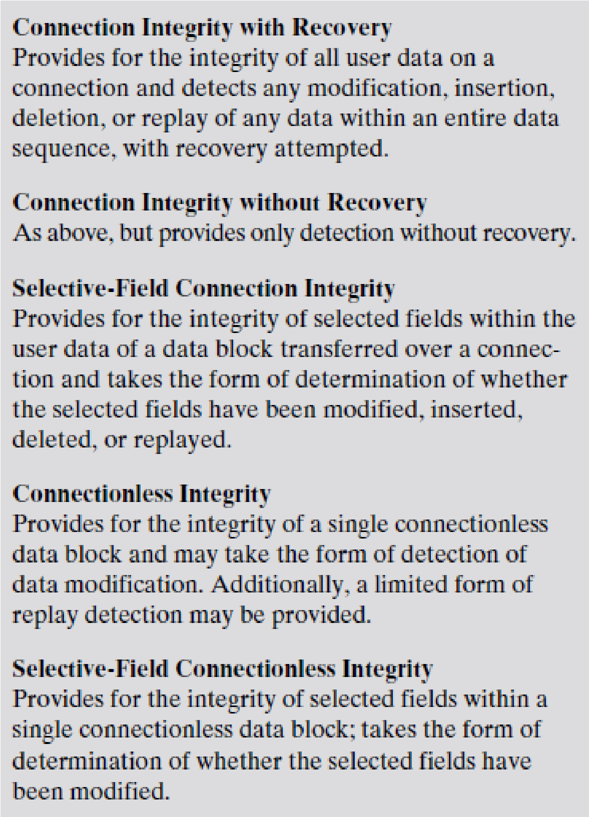
Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).



Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Security Mechanisms

- **Cryptographic algorithms**
  - A ***reversible cryptographic mechanism*** is simply an ***encryption algorithm*** that allows data to be encrypted and subsequently decrypted.
  - ***Irreversible cryptographic mechanisms*** include ***hash algorithms and message authentication codes***, which are used in digital signature and message authentication applications.
- **Data integrity:** Covers a variety of mechanisms ***used to assure the integrity of a data unit*** or stream of data units.
- **Digital signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
- **Authentication exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic padding:** The ***insertion of bits into gaps in a data stream*** to frustrate traffic analysis attempts.
- **Routing control:** Enables selection of particular physically or logically secure routes for certain data and ***allows routing changes***, especially ***when a breach of security is suspected***.
- **Notarization:** The use of a ***trusted third party to assure certain properties*** of a data exchange.
- **Access control:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

CRYPTOGRAPHY

- Cryptography is a branch of mathematics that deals with the ***transformation of data***.
- Cryptography is an essential component in the ***secure storage and transmission of data***, and in the ***secure interaction between parties***.
- Cryptographic algorithms are divided into three categories :
  - **Keyless**: Do not use any keys during cryptographic transformations.
  - **Single-key**: The result of a transformation is a function of the input data and a single key, known as a secret key.
  - **Two-key**: At various stages of the calculation, two different but related keys are used, referred to as a private key and a public key.
- **Keyless Algorithms**
  - This algorithms are ***deterministic functions*** that have certain properties useful for cryptography.
  - **Cryptographic hash function**: A hash function turns a variable amount of text into a small, fixed-length value called a hash value, hash code, or digest.
  - A **pseudorandom number generator** produces a deterministic ***sequence of numbers or bits*** that has the appearance of being a truly random sequence. Although the sequence ***appears to lack any definite pattern***, it will ***repeat after a certain sequence length***. Nevertheless, for some cryptographic purposes this apparently ***random sequence is sufficient***.

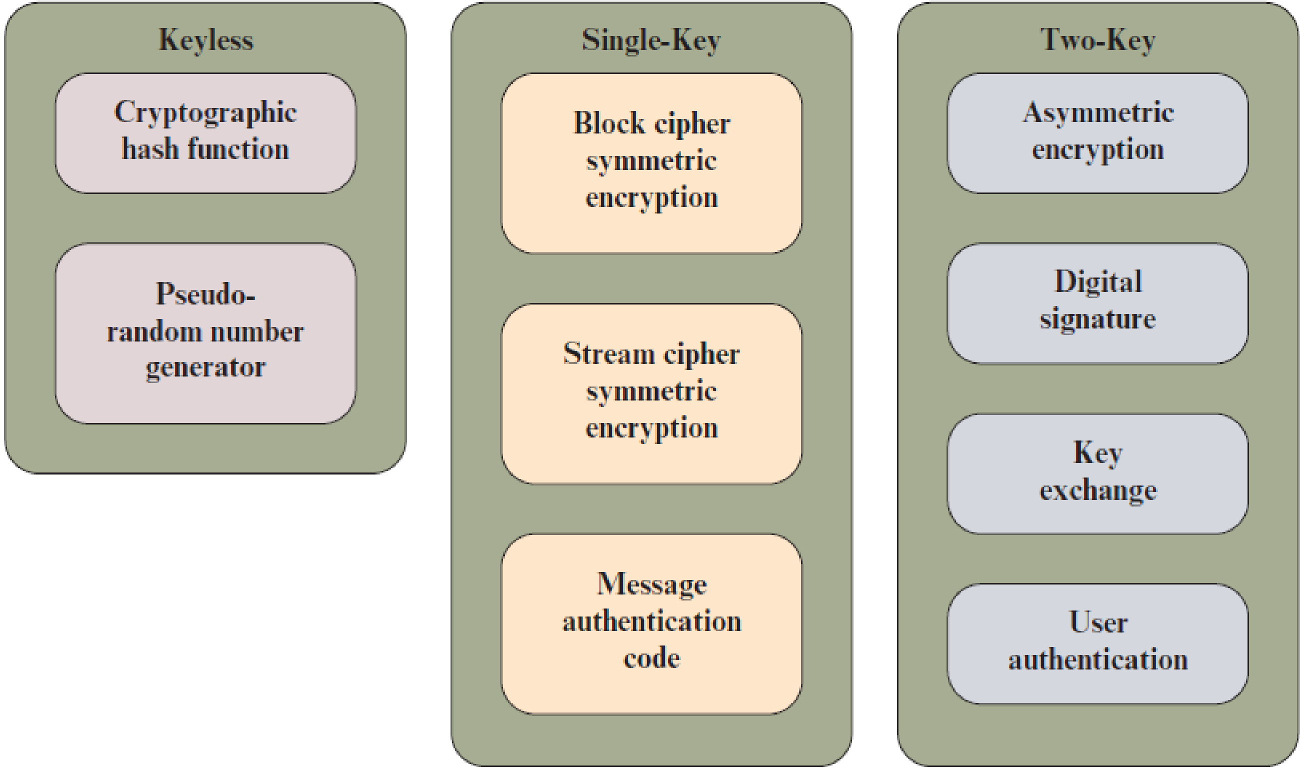
CRYPTOGRAPHY

- **Single-Key Algorithms**
  - Single-key cryptographic algorithms depend on the ***use of a secret key***. This key may be ***known to a single user*** for protecting stored data that is only going to be ***accessed by the data creator***.
  - ***Two parties share the secret key*** so that communication between the two parties is protected.
  - For certain applications, ***more than two users may share the same secret key***, the algorithm protects data from those outside the group who share the key.
  - Encryption algorithms that use a single key are referred to as ***symmetric encryption algorithms***.
  - With symmetric encryption, an ***encryption algorithm*** takes as input some data to be protected and a secret key and produces an unintelligible transformation on that data.
  - A corresponding ***decryption algorithm*** takes the transformed data and the same secret key and recovers the original data.
  - Symmetric encryption takes the following forms:
    - **Block cipher**: A block cipher operates on data as a ***sequence of blocks*** of size ***128 bits***. The transformation depends not only on the current data block and the secret key but also on the content of preceding blocks.
    - **Stream cipher**: A stream cipher ***operates on data as a sequence of bits***. An exclusive-OR operation is used to produce a bit-by-bit transformation.
  - Another form of single-key cryptographic algorithm is the ***message authentication code (MAC).***

CRYPTOGRAPHY

- **Message authentication code (MAC):**
  - The MAC is generated by a cryptographic transformation involving a ***secret key and a cryptographic hash function of the message***.
  - It is designed so that someone in control of the secret key ***can verify the integrity of the message***.
  - The MAC algorithm takes as ***input a message and secret key*** and ***produces the MAC***.
  - The recipient of the message plus the MAC can perform the same calculation on the message; if the calculated MAC matches the MAC accompanying the message, this provides assurance that the message has not been altered.
- **Two-Key Algorithms**
  - Two-key algorithms involve the use of two related keys. A ***private key*** is known only to a single user or entity, whereas the corresponding ***public key*** is made available to a number of users.
  - Encryption algorithms that use two keys are called as ***asymmetric encryption algorithms***.
    - An encryption algorithm ***takes data & private key as input*** and produces ciphertext. A decryption algorithm ***takes the ciphertext & public key and recovers the original data***.
    - An encryption algorithm ***takes data & public key as input*** and produces ciphertext. A decryption algorithm takes the ***ciphertext & private key and recovers the original data***.
  - Asymmetric encryption has a variety of applications: ***Digital signature algorithm, Key exchange, User authentication***.

CRYPTOGRAPHY



Keyless

- Cryptographic hash function
- Pseudo-random number generator

Single-Key

- Block cipher symmetric encryption
- Stream cipher symmetric encryption
- Message authentication code

Two-Key

- Asymmetric encryption
- Digital signature
- Key exchange
- User authentication

Security policies

- A security policy is a living document that states in writing how a company plans to protect its physical, digital and IT assets. They identify all company assets and all threats to those assets.
- Continuously updated and changing as technologies, vulnerabilities and security requirements change.
- ***Physical security policies*** protects company's physical assets like buildings and equipment which includes computers and other IT equipment.
- ***Data security policies*** protect intellectual property from data breaches and data leaks.
- Based on the scope and purpose, Security policies are divided into three types:
    - **Organizational**: These are a master blueprint of the entire organization's security program.
    - **System-specific**: It covers security procedures for an information system or network.
    - **Issue-specific**: These policies target certain aspects of the larger organizational policy. E.g. are:
        - ***Acceptable use policies*** define the rules and regulations for employee use of company assets.
        - ***Access control policies*** say which employees can access which resources.
        - ***Change management policies*** provide procedures for changing IT assets.
        - ***Disaster recovery policies*** ensure business continuity after a service disruption.
        - ***Incident response policies*** define procedures for responding to a security breach or incident as it is happening.

Security policies

Physical security policies

- Protects all physical assets including buildings, vehicles, inventory and machines.
- These assets include IT equipment, such as servers, computers and hard drives.
- Protecting IT physical assets is particularly important as it contain company data. If it is compromised, the information it contains and handles is at risk.
- Thus, information security policies are dependent on physical security policies to keep company data safe. Physical security policies include the following information:
    - sensitive buildings, rooms and other areas of an organization;
    - who is authorized to access, handle and move physical assets;
    - procedures and other rules for accessing, monitoring and handling these assets; and
    - responsibilities of individuals for the physical assets they access and handle.
- Security guards, entry gates, door and window locks and high-tech methods are all used to keep physical assets safe.
- **Example**: Biometric verification system can limit access to a server room.

Security policies

Information security policies

- These policies provide the following advantages.
  - **Protect valuable assets**: Ensure the confidentiality, integrity and availability of data. Often used to protect user sensitive data and personally identifiable information.
  - **Guard reputations**: Data breaches and other information security incidents can negatively affect an organization's reputation.
  - **Ensure compliance with legal and regulatory requirements**: Many legal requirements and regulations are aimed at security sensitive information. For example, ***Health Insurance Portability and Accountability Act*** details how companies handle protected health information.
  - **Dictate the role of employees**: Every employee generates information that may pose a security risk. Security policies provide guidance on the conduct required to protect these data.
  - **Identify third-party vulnerabilities**: Some vulnerabilities stem from interactions with other organizations that may have different security standards. Security policies help identify these potential security gaps.

Security policies

Key elements in a security policy

- statement of the purpose;
- statement that defines who the policy applies;
- statement of objectives, which usually encompasses the CIA triad;
- authority and access control policy that delineates who has access to which resources;
- data classification statement that divides data into categories of sensitivity (range from public information to information that could cause harm to the business if disclosed);
- data use statement that lays out how data at any level should be handled (includes data protection regulations, data backup requirements and network security standards);
- statement of the responsibilities and duties of employees and who will be responsible for overseeing and enforcing policy;
- security awareness training that instructs employees on security best practices; and
- effectiveness measurements that will be used to assess how well security policies are working and how improvements will be made.

Access Control

- A security process that enables organizations to manage ***who is authorized to access corporate data &resources***.
- Secure access control uses policies that ***verify users are who they claim to be*** and ensures appropriate control access levels are granted to users.
- Helping organizations to avoid data breaches and fighting attack vectors, such as a buffer overflow attack, KRACK attack, on-path attack, or phishing attack.
- **Components of Access Control**
  - **Authentication**: Initial process of establishing the identity of a user. Example: email service or online banking account with a username and password.
  - **Authorization:** Authorization adds an extra layer of security to the authentication process. It specifies access rights and privileges to resources to determine whether the user should be granted access to data or make a specific transaction.
    - Example: Requires user to provide two-factor authentication. It is the combination of something they know (password), something they possess (token), or something they are (biometric).
  - **Access**: Once a user's identity is verified, then permission is granted to access the resource.
  - **Manage**: Organizations can manage their access control system by adding and removing the authentication and authorization of their users and systems.
  - **Audit:** Organizations can enforce the principle of least privilege through the access control audit process. This enables them to gather data around user activity and analyze that information to discover potential access violations.

Access Control

- **Different Types of Access Controls**
  - Attribute-based Access Control (ABAC): It is a dynamic and context-based policy that defines access based on policies granted to users. The system is used in identity and access management (IAM) frameworks.
  - Discretionary Access Control (DAC): It allow the data owner to decide access control by assigning access rights to rules that users specify. When a user is granted access to a system, they can then provide access to other users as they see fit.
  - Mandatory Access Control (MAC): It places strict policies on individual users and the data, resources, and systems they want to access. The policies are managed by an organization's administrator. Users are not able to alter, revoke, or set permissions.
  - Role-Based Access Control (RBAC): RBAC creates permissions based on groups of users, roles that users hold, and actions that users take. Users are able to perform any action enabled to their role and cannot change the access control level they are assigned.
  - Break-glass Access Control: It involves the creation of an emergency account that bypasses regular permissions. In the event of a critical emergency, the user is given immediate access to a system or account they would not usually be authorized to use.
  - Rule-based Access Control: A rule-based approach sees a system admin define rules that govern access to corporate resources. These rules are typically built around conditions, such as the location or time of day that users access resources.

Text Book and Reference Books

Text Book

- Willian Stallings, Cryptography & Network Security – Principles and Practices, 6th Edition by Pearson Publishers, 2014.

Reference Books

- William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd Edition, 2014.
- Christof Paar & Jan Pelzl, Understanding cryptography, Springer, 2010.
- Charles P. Pfleeger, Security in Computing, 4th Edition, Pearson, 2009.