## MSC-CS : MCS23022

# CRYPTOGRAPHY & NETWORK SECURITY

## UNIT - 1

## Unit-1: Computer and Network Security Concepts :

Computer Security Concepts- The OSI Security Architecture – Security Attacks - Security Services- Security Mechanisms - Fundamental Security Design Principles – Attack Surfaces and Attack Frees – A Model for Network Security Standards

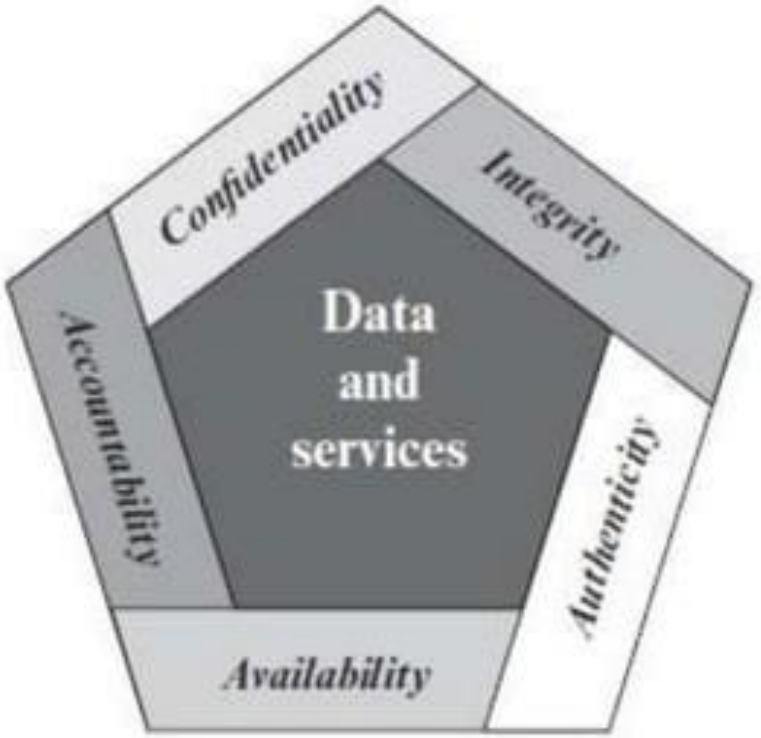
# Cryptography

- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- The term is derived from the **Greek word kryptos,** which means hidden.
- Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading **private messages**

**Cryptographic algorithms and protocols** can be grouped into **four main areas**:

- **Symmetric encryption:** Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.
- **Asymmetric encryption:** Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.
- **Data integrity algorithms:** Used to protect blocks of data, such as messages, from alteration.
- **Authentication protocols:** These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

# Essential Network and Computer Security Requirements



- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for **protecting personal privacy and proprietary information.**
- **Integrity:** Guarding against **improper information modification or destruction**, including ensuring information nonrepudiation and authenticity.
- **Availability:** Ensuring **timely and reliable access** to and use of information.
- **Authenticity:** The property of being **genuine and being able to be verified and trusted confidence** in the validity of a transmission, a message, or message originator.
- **Accountability:** The security goal that **generates the requirement for actions of an entity** to be traced uniquely to that entity.

# Legal, Ethical and Professional Aspects of Security

**Cybercrime And Computer Crime:**

- **Computer crime**, or **cybercrime**, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.
- The term **cybercrime** has a connotation of the use of networks specifically, whereas **computer crime** may or may not involve networks.

The U.S. Department of Justice [DOJ] **categorizes computer crime** based on the role that the computer plays in the criminal activity, as follows:

- Computers as targets
- Computers as storage devices
- Computers as communications tools

# Privacy Law and Regulation

A number of international organizations and national governments have introduced laws and regulations intended to protect individual privacy.

- Notice
- Consent
- Consistency
- Access
- Security
- Onward transfer
- Enforcement

# Law and Ethics in Information Security

**Laws:**

- Rules that mandate or prohibit certain behavior
- Drawn from ethics

**Ethics:**

- Define socially acceptable behaviors

**Key difference:**

- Laws carry the authority of a governing body
- Ethics do not carry the authority of a governing body
- Based on cultural mores
- Fixed moral attitudes or customs
- Some ethics standards are universal

# Policy Versus law

**Policies:**

- Guidelines that describe acceptable and unacceptable employee behaviors
- Functions as organizational laws
- Has penalties, judicial practices, and sanctions

**Difference between policy and law:**

- Ignorance of policy is acceptable
- Ignorance of law is unacceptable

**Keys for a policy to be enforceable:**

- Dissemination
- Review
- Comprehension
- Compliance
- Uniform enforcement

# Types of Law

- **Civil –** govern a nation or state
- **Criminal –** addresses activities and conduct harmful to public
- **Private –** encompasses family, commercial, labor, and regulates the relationship between individuals and organizations
- **Public –** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments

## United States Privacy Initiatives:

- Banking and financial records
- Credit reports
- Medical and health insurance records
- Children's privacy
- Electronic communications

**Ethical issues arise as the result of the roles of computers, such as the following:**

- **Repositories and processors of information:** Unauthorized use of otherwise unused computer services or of information stored in computers raises questions of appropriateness or fairness.
- **Producers of new forms and types of assets:** For example, computer programs are entirely new types of assets, possibly not subject to the same concepts of ownership as other assets.
- **Instruments of acts:** To what degree must computer services and users of computers, data, and programs be responsible for the integrity and appropriateness of computer output?
- **Symbols of intimidation and deception:** The images of computers as thinking machines, absolute truth producers, infallible, subject to blame, and as anthropomorphic replacements of humans who err should be carefully considered.

# Need for Security at Multiple levels

- The field of ***Network and Internet security*** consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information
- Following are some examples for security violation
  - **User A** transmits a file to **user B**. The file contains **sensitive information** 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

# Need for Security at Multiple levels

- 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 **computer E**, which accepts the message as coming from manager D and updates its authorization file accordingly
- Rather than intercept a message, **user F** constructs its own message with the desired entries and transmits that message to **computer 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

# Security Policy

**P.1.** → A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information while ensuring compliance with statutory, regulatory and contractual requirements.

**P.2.** → Classified information shall only be taken for use away from the organization in an encrypted form unless its confidentiality can otherwise be assured.

# Security Policy

**P.3.** → Procedures shall be established to ensure that authorized staff may gain access, when needed, to any important business information being held in encrypted form.

**P.4.** → The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.

# Security Policy

**P.5.→** Encryption shall be used whenever appropriate on all remote access connections to the organization's network and resources.

**P.6.→** A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

# OSI Security Architecture

- It is a systematic way of defining the requirements for the security
- It characterize the approaches to satisfy the various security products and polices
- **X.800 security architecture** of OSI defines such a systematic approach
- OSI security architecture is useful for **organizing the task of providing security**

# OSI Security Architecture

- Since this architecture was developed as an **international standard**, Computer and Communications vendors have **developed security features for their products and services** that relate to **this structured definition of services and mechanisms**

# OSI Security Architecture

- The OSI security architecture focuses on
  - Security Attacks
  - Security Mechanism
  - Security Services

# Security Attacks

❖ **Security Attacks:**

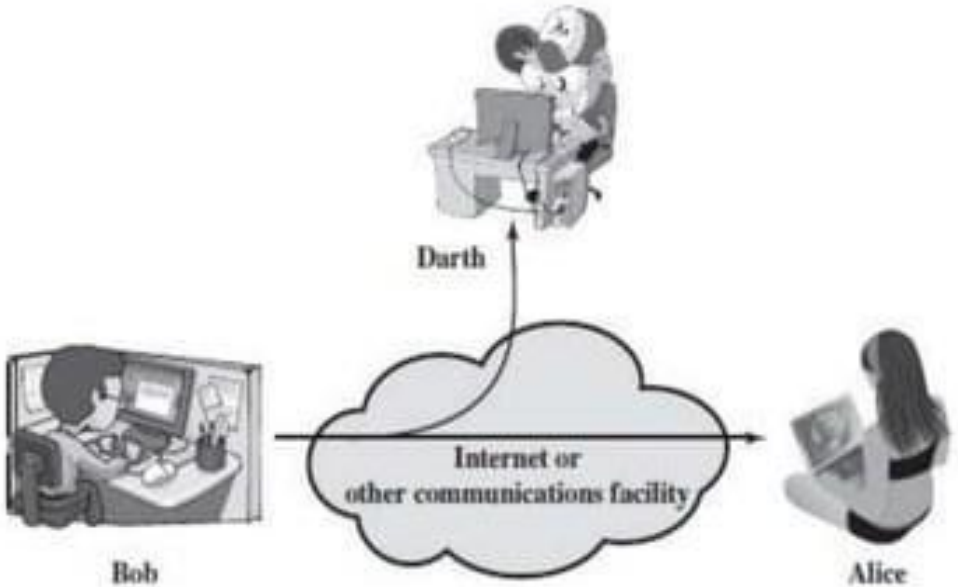
- Any action that **compromises the security** of information owned by an organization

❖ Classifications:

- *Passive attacks*
- *Active attacks*

# Passive Attacks

- Passive attacks are in the nature of **eavesdropping on**, or **monitoring of**, transmissions.



# Passive Attacks

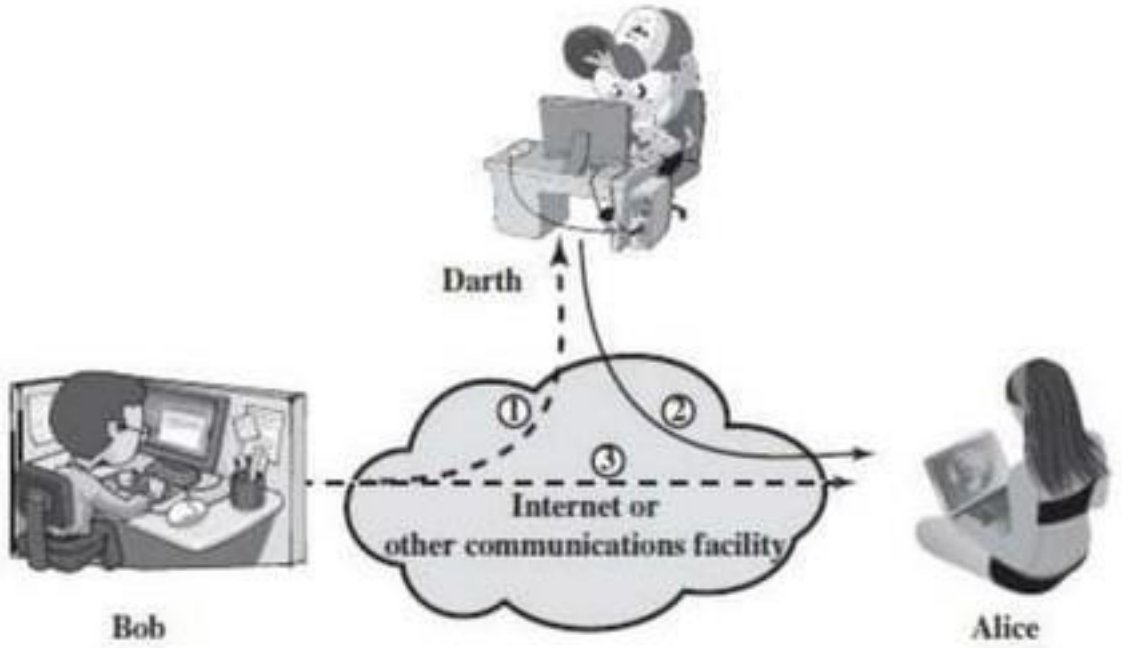
- The goal of the opponent is **to obtain information** that is being transmitted.
- Two types of passive attacks are
  - Release of message contents
  - Traffic analysis.

# Passive Attacks

- **Release of message contents**
  - capture and read the content.
  - A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- **Traffic analysis**
  - Can't read the information, But observe the pattern
  - Determine the location and identity of communicating parties
  - Observe frequency and length of communication

# Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream



# Active Attacks

- It can be subdivided into four categories:
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

# Active Attacks

## ➢ Masquerade

- A **masquerade** takes place when one entity pretends to be a different entity
- Masquerade is a type of attack where the attacker **pretends to be an authorized user** of a system in order to gain access to it or to gain greater privileges than they are authorized for.

# Active Attacks

## ➢ Replay

- A replay attack also known as playback attack.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

# Active Attacks

## ➢ Modification of messages

- It simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect

## ➢ Denial of service

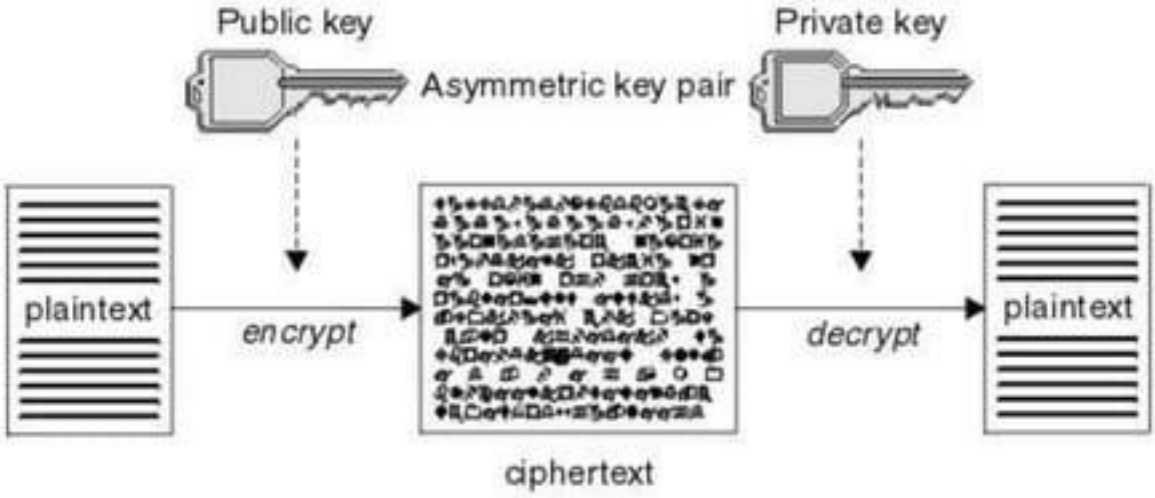
- A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service

# Security Mechanisms

- **Security mechanism:**
  - A process that is designed to detect, prevent, or recover from a security attack
- The following are some security mechanisms defined in X.800
  - *Encipherment*
  - *Access Control*
  - *Digital Signature*
  - *Data Integrity*
  - *Authentication Exchange*
  - *Traffic Padding*
  - *Routing Control*
  - *Notarization*

# Security Mechanisms

- **Encipherment**
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible.
  - The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.



# Security Mechanisms

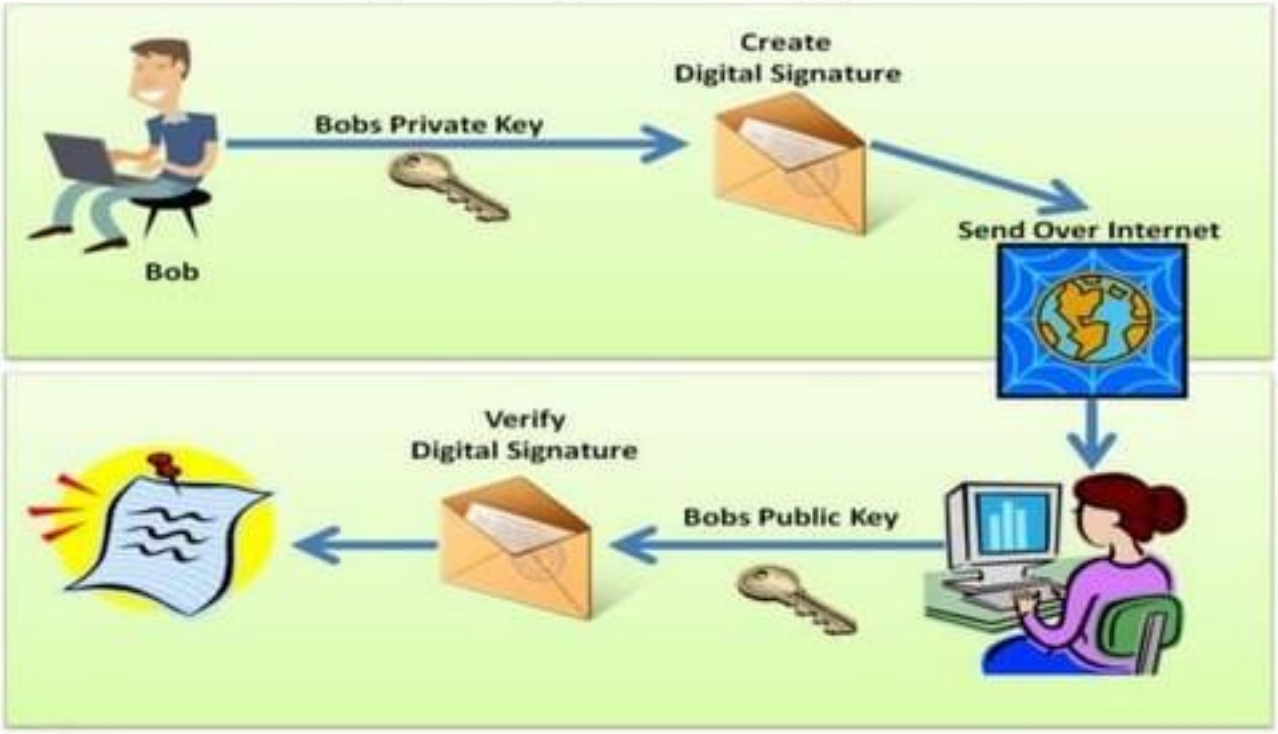
## ➢ Access Control

– A variety of mechanisms that enforce access rights to resources.

# Security Mechanisms

## ➢ Digital Signature

– Here the sender can electronically sign the data and the receiver can electronically verify the signature.

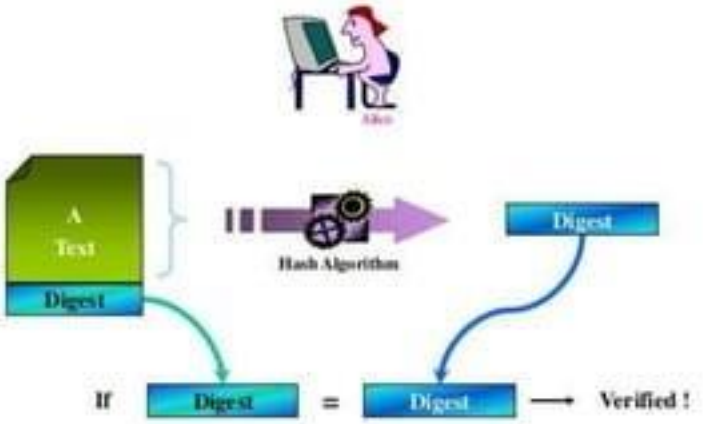


# Security Mechanisms

## ➢ Data Integrity

- The assurance that the data has not been altered in an unauthorised manner since the time that the data was last created, transmitted, or stored by an authorised user.
- A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

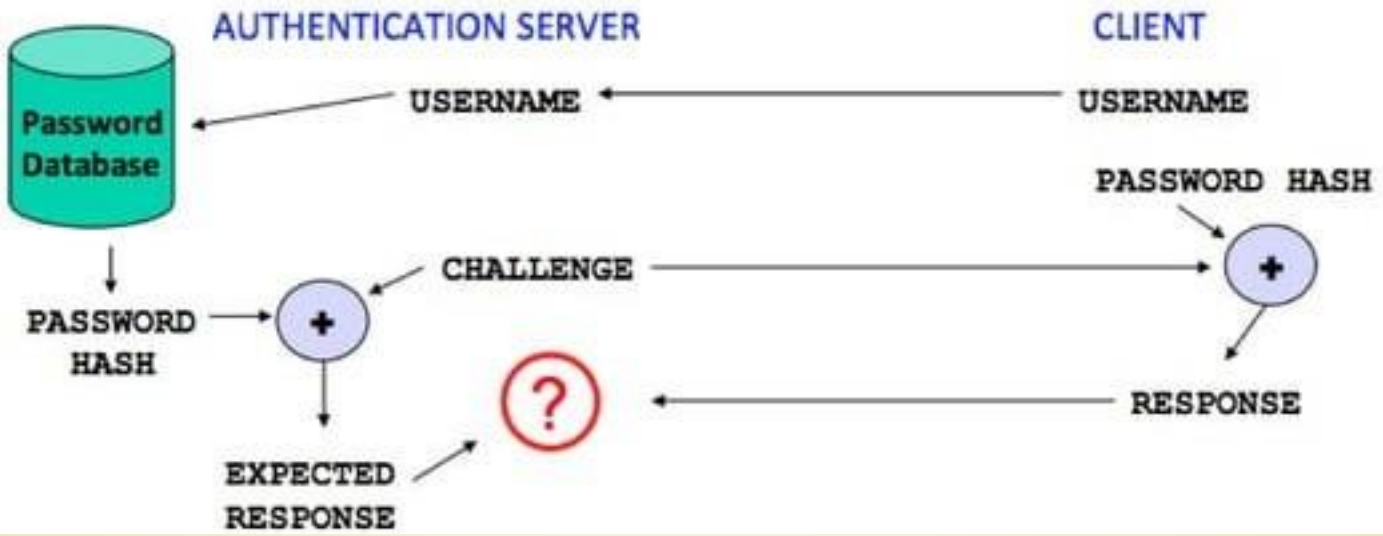
**Data Integrity – Verifying a Hash**



# Security Mechanisms

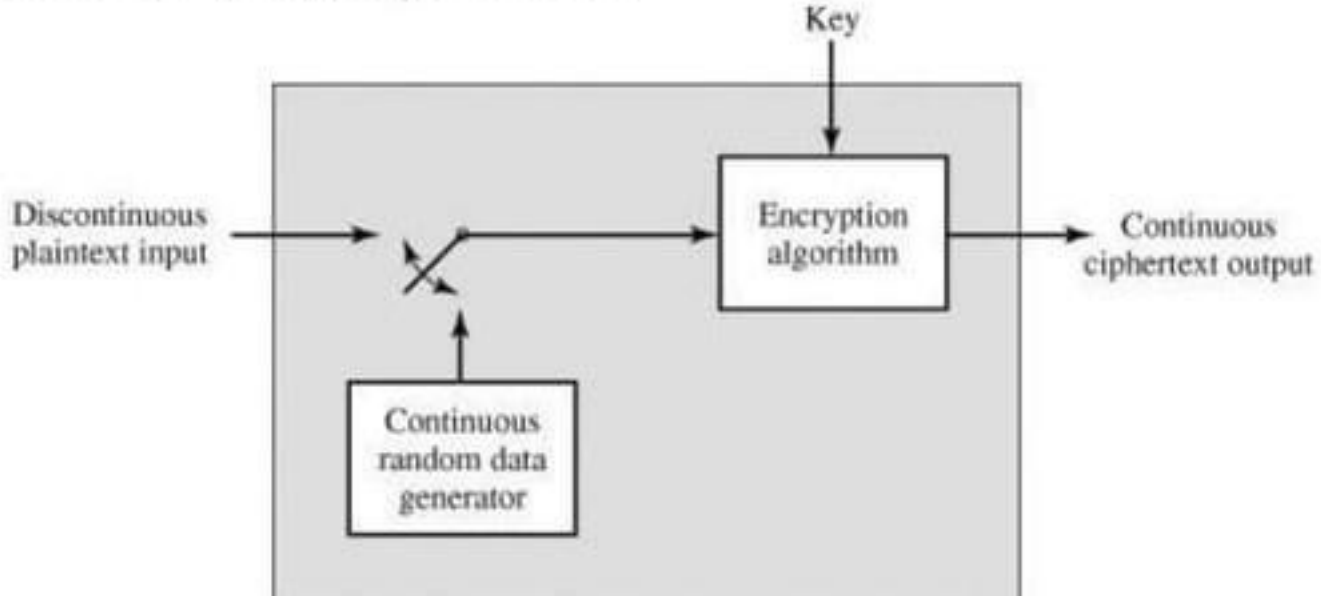
## ➢ Authentication Exchange

– A mechanism intended to ensure the identity of an entity by means of information exchange.



# Security Mechanisms

- **Traffic Padding**
  - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts
  - Traffic padding may be used to hide the traffic pattern, which means to insert **dummy traffic into the network** and present to the intruder a different traffic pattern.



# Security Mechanisms

- **Routing Control**
  - Enables selection of particular physically 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.

# Security Mechanisms

## ➢ Notarization

– The use of a trusted third party to assure certain properties of a data exchange.

# Security Services

- It is a processing or communication service that is provided by a system to give a **specific kind of protection to system resources.**
- Security services implement ***security policies*** and are implemented by ***security mechanisms***.
- X.800 divides these services into **five categories and fourteen specific services**

# Security Services

- The five categories are
  - **Authentication**
  - **Access Control**
  - **Data Confidentiality**
  - **Data Integrity**
  - **Nonrepudiation**

# Authentication

- The authentication service is concerned with **assuring that a communication is authentic**
- Two specific authentication services are defined in X.800:
  - Peer entity authentication
  - Data origin authentication

# Authentication

- **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

- Confidentiality is the protection of transmitted data from passive attacks
  - ❖Connection Confidentiality
  - ❖Connectionless Confidentiality
  - ❖Selective-Field Confidentiality
  - ❖Traffic-Flow Confidentiality

# Data Confidentiality

- 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**

# 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
  - Connection Integrity without Recovery
  - Selective-Field Connection Integrity
  - Connectionless Integrity
  - Selective-Field Connectionless Integrity

# Data Integrity

- 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.

# Data Integrity

- 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

# 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.**

# Relationship Between Security Services and Mechanisms

| SERVICE \ MECHANISM | Enciphherment | Digital signature | Access control | Data integrity | Authentication exchange | Traffic padding | Routing control | Notarization |
|---|---|---|---|---|---|---|---|---|
| Peer entity authentication | Y | Y | | | Y | | | |
| Data origin authentication | Y | Y | | | | | | |
| Access control | | | Y | | | | | |
| Confidentiality | Y | | | | | | Y | |
| Traffic flow confidentiality | Y | | | | | Y | Y | |
| Data integrity | Y | Y | | Y | | | | |
| Nonrepudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

# Fundamental Security Design Principles

- The National Centers of Academic Excellence (NCAE) in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security listed the following as fundamental security design principles:
  - Economy of mechanism
  - Fail-safe defaults
  - Complete mediation
  - Open design
  - Separation of privilege
  - Least privilege

## Fundamental Security Design Principles

- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

## Fundamental Security Design Principles

### Economy of Mechanism

- Economy of mechanism means that the design of security measures embodied in both hardware and software should be **as simple and small as possible**.
- The motivation for this principle is that relatively simple, small design is easier to test and verify thoroughly.
- The more complex the mechanism, the more likely it is to possess exploitable flaws.
- Simple mechanisms tend to have fewer exploitable flaws and require less maintenance.

## Fundamental Security Design Principles

### Fail-Safe Defaults

- Fail-safe default means that access decisions should be based on permission rather than exclusion.
- The default situation is **lack of access**, and the protection scheme identifies conditions under which access is permitted.
- A mechanism that explicitly excludes access tends to fail by allowing access, a failure that may long go unnoticed in normal use.

## Fundamental Security Design Principles

### Complete Mediation

- Complete mediation means that every access must be checked against the access control mechanism.
- Systems should not rely on access decisions retrieved from a cache.
- In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories.
- File access systems appear to provide an example of a system that complies with this principle. However, typically, once a user has opened a file, no check is made to see of permissions change.

## Fundamental Security Design Principles

### Open Design

- Open design means that the design of a security mechanism should be open rather than secret.
- For example, encryption keys must be secret, encryption algorithms should be open to public scrutiny.
- The algorithms can then be reviewed by many experts, and users can therefore have high confidence in them. This is the philosophy behind the NIST program of standardizing encryption and hash algorithms, and has led to the widespread adoption of NIST-approved algorithms.

## Fundamental Security Design Principles

### Separation of Privilege

- Separation of privilege is defined in [SALT75] as a practice in which multiple privilege attributes are required to achieve access to a restricted resource.
- A good example of this is multifactor user authentication, which requires the use of multiple techniques, such as a password and a smart card, to authorize a user.
- The term is also now applied to any technique in which a program is divided into parts that are limited to the specific privileges they require in order to perform a specific task. This is used to mitigate the potential damage of a computer security attack.

## Fundamental Security Design Principles

### Least Privilege

- Least privilege means that every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- The system security policy can identify and define the various roles of users or processes.
- Each role is assigned only those permissions needed to perform its functions.
- Each permission specifies a permitted access to a particular resource (such as read and write access to a specified file or directory, and connect access to a given host and port).

## Fundamental Security Design Principles

### Least Common Mechanism

- Means that the design should minimize the functions shared by different users, providing mutual security.
- This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

## Fundamental Security Design Principles

### Psychological Acceptability

- Implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.
- If security mechanisms hinder the usability or accessibility of resources, users may opt to turn off those mechanisms.

## Fundamental Security Design Principles

### Psychological Acceptability

- Where possible, security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction.
- In addition to not being intrusive or burdensome, security procedures must reflect the user's mental model of protection.
- If the protection procedures do not make sense to the user or if the user must translate his image of protection into a substantially different protocol, the user is likely to make errors.

## Fundamental Security Design Principles

### Isolation

- Is a principle that applies in three contexts:
  - **Public Access Systems**: Should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering.
    - ✓ In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data are stored and isolate them, either **physically** or **logically**.

## Fundamental Security Design Principles

- **The Processes and Files of Individual Users Should be Isolated From One another Except Where it is Explicitly Desired:** All modern operating systems provide facilities for such isolation, so that individual users have separate, isolated process space, memory space, and file space, with protections for preventing unauthorized access.
- **Security Mechanisms Should be Isolated in the Sense of Preventing Access to those Mechanisms:** For example, logical access control may provide a means of isolating cryptographic software from other parts of the host system and for protecting cryptographic software from tampering and the keys from replacement or disclosure.

## Fundamental Security Design Principles

### Encapsulation

- Can be viewed as a specific form of isolation based on object-oriented functionality.
- Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points.




- Stallings, W. (2016). *Network security essentials: applications and standards*. Hoboken, NJ: Pearson Education, Inc.

## Fundamental Security Design Principles

### Modularity

- In the context of security, modularity refers to both the *development of security functions* as separate, protected modules and to the *use of a modular architecture for mechanism design and implementation*.
- With respect to the use of separate security modules, the design goal here is to **provide common security functions and services**, such as cryptographic functions, as common modules.
- For example, numerous protocols and applications make use of cryptographic functions.

## Fundamental Security Design Principles

### Modularity

- Rather than implementing such functions in each protocol or application, a more secure design is provided by developing a common cryptographic module that can be invoked by numerous protocols and applications.
- The design and implementation effort can then focus on the secure design and implementation of a single cryptographic module, including mechanisms to protect the module from tampering.
- With respect to the use of **a modular architecture**, each security mechanism should be able to support migration to new technology or upgrade of new features without requiring an entire system redesign.




- Stallings, W. (2016). *Network security essentials: applications and standards*. Hoboken, NJ: Pearson Education, Inc.

## Fundamental Security Design Principles

### Layering

- Layering refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
- By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected.
- This technique is often referred to as **defense in depth**.

## Fundamental Security Design Principles

### Least Astonishment

- Least astonishment means that a program or user interface should always respond in the way that is least likely to astonish the user.
- For example, the mechanism for authorization should be transparent enough to a user that the user has a good intuitive understanding of how the security goals map to the provided security mechanism.

## Attack Surfaces and Attack Trees

### Attack Surfaces

- An attack surface consists of the reachable and exploitable vulnerabilities in a system [MANA11, HOWA03]. Examples of attack surfaces are the following:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available on the inside of a firewall
  - Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats.
  - Interfaces, SQL, and Web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack.

## Attack Surfaces and Attack Trees

### Attack Surfaces

- Attack surfaces can be categorized in the following way:
  - *Network attack surface*: This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet.
  - Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
  - *Software attack surface*: This refers to vulnerabilities in application, utility, or operating system code. A particular focus in this category is Web server software.
  - *Human attack surface*: This category refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

## Attack Surfaces and Attack Trees

### Attack Trees

- An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities [MAUW05, MOOR01, SCHN99].
- The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and sub-nodes of the tree.
- Each sub-node defines a sub-goal, and each sub-goal may have its own set of further sub-goals, etc.
- The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack.

## Attack Surfaces and Attack Trees

### Attack Trees

- The motivation for the use of attack trees is to effectively exploit the information available on attack patterns.
- Organizations such as CERT publish security advisories that have enabled the development of a body of knowledge about both general attack strategies and specific attack patterns.
- Security analysts can use the attack tree to document security attacks in a structured form that reveals key vulnerabilities.
- The attack tree can guide both the design of systems and applications, and the choice and strength of countermeasures.
- The analysis used to generate the following tree considered the **three components** involved in authentication:

## Attack Surfaces and Attack Trees

### Attack Trees

- *User terminal and user (UT/U)*: These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user.
- *Communications channel (CC)*: This type of attack focuses on communication links.
- *Internet banking server (IBS)*: These types of attacks are offline attack against the servers that ***host the Internet banking application***.

## Attack Surfaces and Attack Trees

### Attack Trees

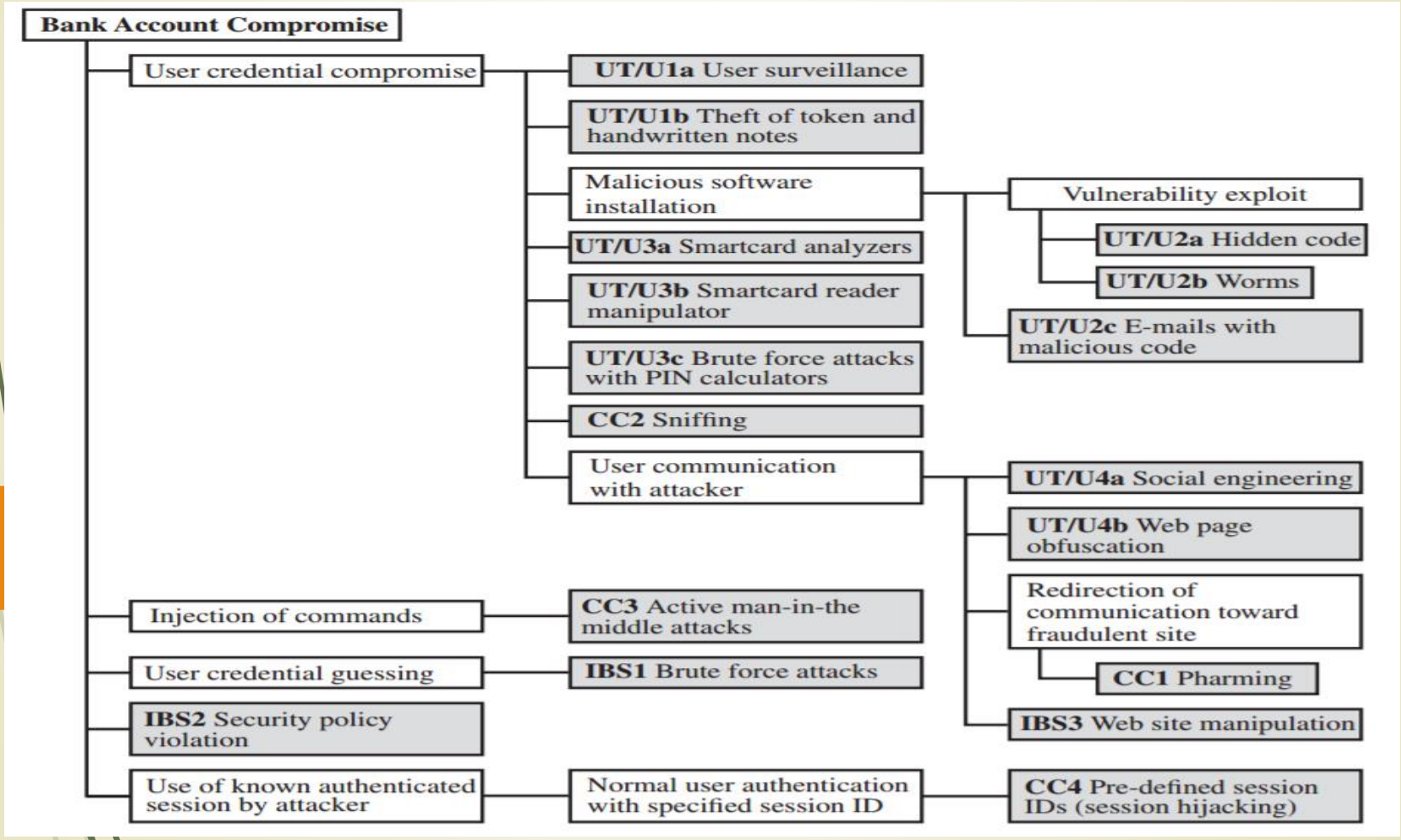
- Five overall attack strategies can be identified, each of which exploits one or more of the *three components*. *The five strategies* are as follows:
  - ***User credential compromise***: This strategy can be used against many elements of the attack surface. There are procedural attacks, such as monitoring a user's action to observe a PIN or other credential, or theft of the user's token or handwritten notes. An adversary may also compromise token information using
  - ***Injection of commands***: In this type of attack, the attacker is able to intercept communication between the UT and the IBS. Various schemes can be used to be able to impersonate the valid user and so gain access to the banking system.

# Attack Surfaces and Attack Trees

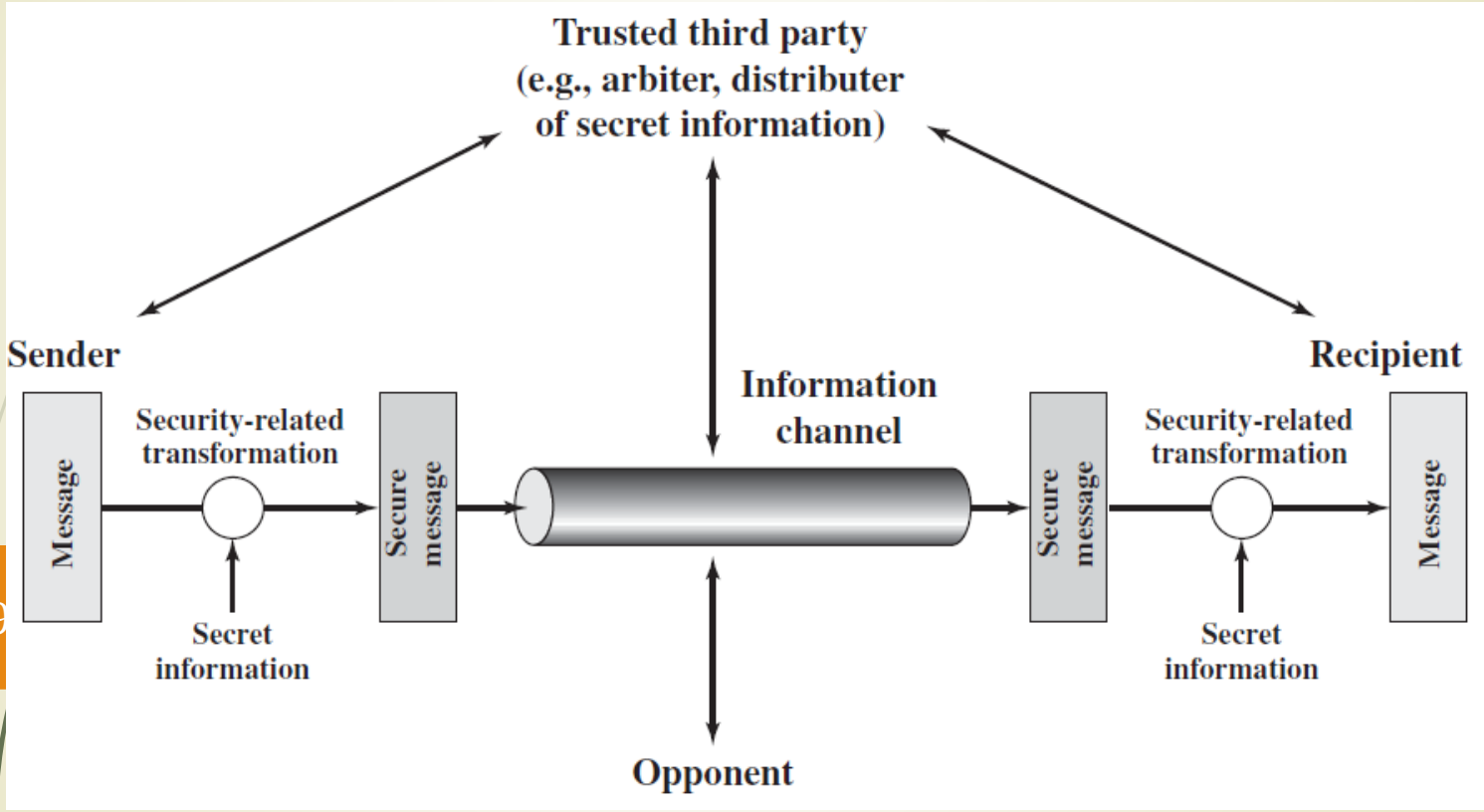
## Attack Trees

- ***User credential guessing***: It is reported in [HILT06] that brute force attacks against some banking authentication schemes are feasible by sending random usernames and passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based calculation.
- ***Security policy violation***: For example, violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.
- ***Use of known authenticated session***: This type of attack persuades or forces the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity.

# Attack Surfaces and Attack Trees



# A Model for Network Security



## A Model for Network Security

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.

# A Model for Network Security

- Many of us are familiar with the concerns caused by the existence of ***hackers*** who attempt to penetrate systems that can be accessed over a network.
- The *hacker* can be *someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system*.
- The intruder can be *a disgruntled employee* who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

## A Model for Network Security

- Another type of unwanted access is *the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers*.
- Programs can present two kinds of threats:

1. **Information access threats**: Intercept or modify data on behalf of users who should not have access to that data.
2. **Service threats**: Exploit service flaws in computers to inhibit use by legitimate users.

# Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services.
- Various organizations have been involved in the development or promotion of these standards.
- The most important of these organizations are as follows.
  - ***National Institute of Standards and Technology***: NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation.
  - Despite its national scope, NIST, Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

# Standards

- ***Internet Society***: ISOC is a professional membership society with worldwide organizational and individual membership.
- It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).
- These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).