Information Security

Prepared By

-Anooja Joy

Information Security

Infosec *is the set of* ***strategies*** *for managing the* ***processes, practices, policies*** *and* ***tools*** *for protecting* ***information assets*** *and* ***information systems*** *from* ***unauthorized access, use, disclosure, disruption, modification****, or* ***destruction*** *while being* ***stored*** *or* ***transmitted across****.*

Why Information Security?

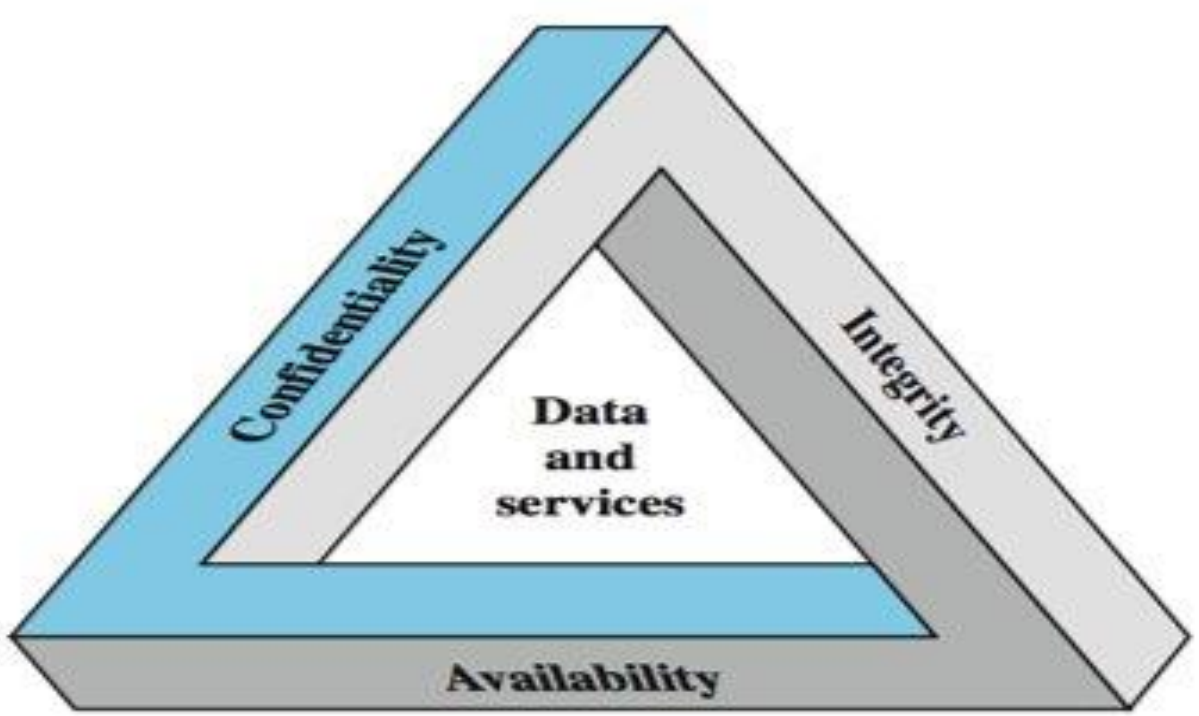
- Information is the greatest asset that must be protected.
- Information is processed or organized data.

  Eg: social media profiles , Data in mobile phone, biometrics information etc.

- Elements of Information Security Mechanism.
  - **Security Attack**
  - **Security Mechanism (control)**
  - **Security Service**

Goals of Information Security

- Known as **CIA triad** are the **Information Security Principles** or **fundamental security objectives**.
  - **Protect Confidentiality**
  - **Maintain Integrity**
  - **Ensure Availability**



Confidentiality (Secrecy)

- Only the **sender** and **intended receiver** should be able to understand the contents of the transmitted message ie, **preventing unauthorized person from reading the message.**
- Implies **personal privacy** and **protection of proprietary information** from Unauthorized access should be prevented while **Storage** and **Transmission.**
- Information about system or its users cannot be learned by an attacker.
- **EG:** Bank must prevent Trudy from learning Bob's account balance

How to ensure Confidentiality?

- **Passwords, encryption, authentication, and defense against penetration attacks**

Integrity

- **Integrity** means maintaining data in its correct state and preventing **content** of the **communication** or **message not being altered**, either maliciously or by accident, in transmission.
- Integrity assures information and programs are complete and accurate and are changed only in a **specific** and **authorized manner**.
- Changes should be by authorized entities and through authorized mechanisms.
- **EG:** Trudy must not be able to change Bob's account balance. Bob must not be able to improperly change his own account balance.

How to ensure Integrity?

- **Checksums, version control software and frequent backups**

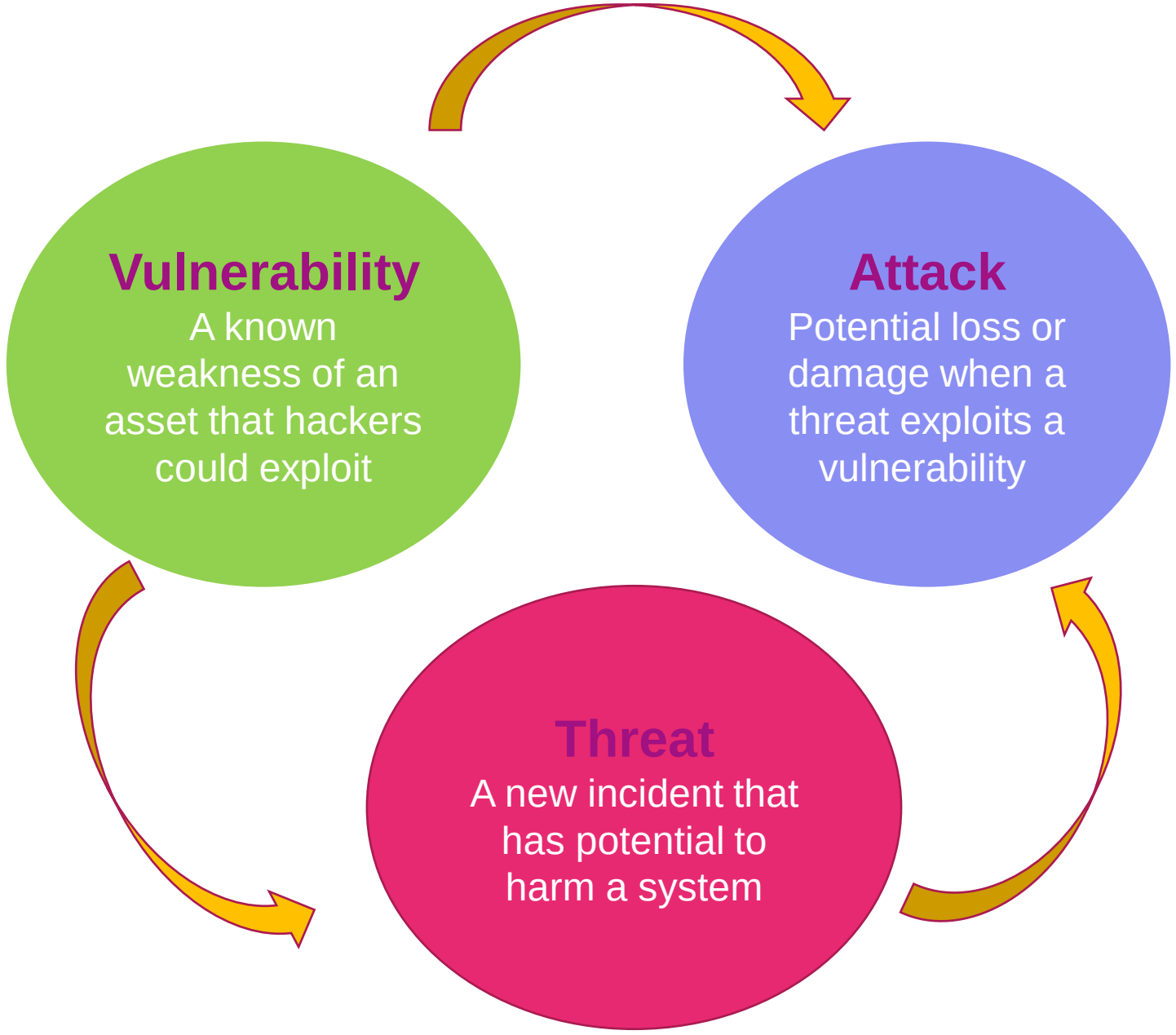
Availability

- Data is available or accessible in a ***timely*** *and* ***reliable manner*** to **authorized entities** **whenever needed**
- Data *can* be accessed by those who have the proper permissions.
- **EG:** Alice must be able to make transaction in Bank anytime whenever required.

How to ensure Availability?

- **matching network and computing resources, implementing a good backup policy for disaster recovery**

Threats, Vulnerabilities and Attacks



Vulnerability

- ***Vulnerability*** – A vulnerability is a **flaw** or **weakness** in a system's design, implementation, or operation and management because of poor design, configuration mistakes, or inappropriate and insecure coding techniques which **attackers can exploit** to cause loss or harm. Vulnerabilities can be summed up as the "soft spots" by which **threats can happen**.

Eg: server misconfigurations, sensitive data transmitted in plain text, Using non-validated input

Threat

➢ ***Threat*** – A threat to a computing system is a **set of circumstances that has potential** to cause loss or harm by breaching security**. A possible danger that exploit a vulnerability.** It may result in harm to a system or organization, disrupt the operation, functioning, integrity, or availability of a network or system. Threats can be deliberate or accidental. A threat can be blocked by control of vulnerability.

Ø**Eg: Interception**(unautorised party gaining access to asset), **Interruption**(an asset is unavailable, lost or damaged), **modification**(after accessing unauthorized datat it is tampered) **and fabrication**(unauthorized person creates a fabrication of counterfeit objects on a system)

Attack

➢ ***Attack*** – An attack is an **assault on system security** that derives from an intelligent threat, ie a **deliberate attempt** to evade security services and security policies of a system.

- **Eg: Trojan, DDOS**

Threat VS Attack

- **Threat** can be either **intentional** or **unintentional** whereas an **attack** is **intentional.**
- **Threat** is a circumstance that has **potential to cause loss or damage** whereas **attack** is **attempted to cause damage**.
- **Threat** to the information system **doesn’t mean information was altered or damaged** but **attack** on the information system means there **might be chance to alter, damage, or obtain information when attack was successful.**

Vulnerability Types

Vulnerabilities are broadly classified as **Hardware, Software & Data Vulnerabilities.**

Hardware Vulnerabilities

These are attacks on computer systems and networks based on exploiting hardware design or manufacturing bugs, or "not playing by the rules" in dealing with the hardware.

1. **Computers with conventional BIOS:** Older PCs, as well as laptops and notebooks, with conventional BIOS cannot run **Secure Boot**, a feature of UEFI that was first added in Microsoft Windows 8 and now appears in newer editions, as well as Windows Server. Secure Boot helps to prevent malware from loading onto a computer during the boot process.
2. **Old routers:** Aimed mainly at small offices/home offices (SOHOs), old routers — especially those manufactured in 2011 and earlier — can have serious vulnerabilities.
3. **Solid-State Drives Failing to Encrypt:** SSD requires a password in addition to the OS login password, and the technology automatically encrypts and decrypts data on the drive.

Software Vulnerabilities

Software flaws that arises frommodification, deletion or misplacement of software architecture

- **Backdoors : A program that has a secret entry point to** bypass normal means of authentication . Hidden from casual inspection . Installed separately or integrated into software
- **Code Exploits:** Use of poor coding practices left uncaught by testing. **Defense:** In depth unit testing and integration testing
- **Information Leaks:** code that makes information accessible to unauthorized people or programs.
- **Social Engineering :** Misleading a user into giving up secrets or into giving access to a computer to an attacker is known as *social engineering*. Manipulate the weakest link of cyber security – the user – to gain access to otherwise prohibited resources **Defense:** Train personnel
- **Buffer Overflows:** A buffer overflow occurs when an application attempts to write data past the end of a buffer. Buffer overflows can cause applications to crash, can compromise data, and can provide an attack vector for further privilege escalation to compromise the system on which the application is running.

Data Vulnerabilities

- **Unvalidated Inputs: input received by the program from an untrusted source is a potential target for attack u**nless input data is checked carefully. This process is commonly known as input validation or sanity checking.
- Examples of input from an untrusted source that should be verified include:
  - text input fields
  - commands passed through a URL used to launch the program
  - audio, video, or graphics files provided by users or other processes and read by the program
  - command line input
  - any data read from an untrusted server over a network
  - any untrusted data read from a trusted server over a network (user-submitted HTML or photos, for example)
- **Data Leakage**: Unauthorized electronic or physical transmission of data or information from within a company to an external destination or recipient could leave data in the wrong hands
- Eg: **Eavesdropping:** Data transmitted without encryption can captured and read by parties other than the sender and receiver **Defense:** Use of strong cryptography to minimize clear text on the network .

Examples of Vulnerabilities

- **Unpatched Software** – Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.
- **Misconfiguration** – System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.
- **Weak Credentials** – An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.
- **Phishing, Web & Ransomware** – Phishing is used by attackers to get users to inadvertently execute some malicious code, and thereby compromise a system, account or session. The adversary will send your users a link or malicious attachment over email (or other messaging system), often alongside some text/image that entices them to click.
- **Trust Relationship** – Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.

Examples of Vulnerabilities

- **Compromised Credentials** – An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.
- **Malicious Insider –** An employee or a vendor who might have access to your critical systems can decide to exploit their access to steal or destroy information or impair them. This is particularly important for privileged users and critical systems.
- **Missing/Poor Encryption** – With attacks on Missing/Poor Encryption, an attacker can intercept communication between systems in your network and steal information. The attacker can intercept unencrypted or poorly encrypted information and can then extract critical information, impersonate either side and possibly inject false information into the communication between systems.
- **Zero-days & Unknown Methods** – Zero days are specific software vulnerabilities known to the adversary but for which no fix is available, often because the bug has not been reported to the vendor of the vulnerable system. The adversary will try to probe your environment looking for systems that can be compromised by the zero day exploit they have, and then attack them directly or indirectly.

Threats

- Why Threats arises?
  - Misconfigured hardware or software
  - Poor network design
  - Inherent technology weaknesses
  - End-user carelessness
  - Intentional end-user acts

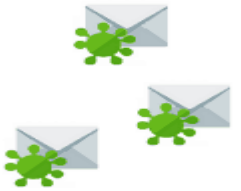
Threat Types

1. **Unstructured threats:** Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. usually the result of an attacker identifying the vulnerability by scanning the network looking for "targets of opportunity." Unstructured threats often involve unfocused assaults on one or more network systems, often by individuals with limited or developing skills.
2. **Structured threats:** *Structured threats* are more focused by one or more individuals with higher-level skills actively working to compromise a system of target. A structured threat is an organized effort to breach a specific network or organization. These threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts
3. **External threats:** can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers
4. **Internal threats:** Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network

Cyber Threat Evolution

Some common threats

Virus	**A program capable of replicating with little or no user intervention, and the replicated programs also replicate.**
Worm	A form of virus that spreads by creating duplicates of itself on other drives, systems, or networks. A worm working with an e-mail system can mail copies of itself to every address in the e-mail system address book. Code Red and Nimda are examples of high-profile worms that have caused significant damage in recent years.
Trojan horse	An apparently useful or amusing program, possibly a game or screensaver, but in the background it could be performing other tasks, such as deleting or changing data, or capturing passwords or keystrokes. A true Trojan horse isn't technically a virus because it doesn't replicate itself.



Top Network Threats

- **Information Gathering**
  - Network devices can be discovered and profiled in much the same way as other types of systems.
  - Attackers usually start with **port scanning**. After they identify open ports, they use banner grabbing and enumeration to **detect device types** and to **determine operating system** and **application versions**
  - Armed with this information, an attacker can attack known vulnerabilities that may not be updated with security patches.
- **Sniffing/Evesdropping**
  - *Sniffing* or *eavesdropping* is the act of monitoring traffic on the network for data such as plaintext passwords or configuration information
  - attackers can crack packets encrypted by lightweight hashing algorithms and can decipher the payload that you considered to be safe

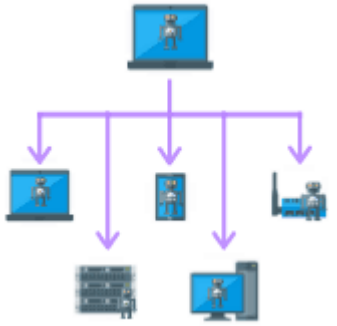
Top Network Threats

- **Spoofing**
  - Spoofing is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet.
  - Spoofing may be used to hide the original source of an attack or to work around network access control lists (ACLs) that are in place to limit host access based on source address rules.
- **Session Hijacking**
  - **Session hijacking** is an attack where a user **session** is taken over by an attacker. Also known as man in the middle attacks, session hijacking deceives a server or a client into accepting the upstream host as the actual legitimate host
  - Instead the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination.
- **Denial of Service**
  - Denial of service denies legitimate users access to a server or services. The aim of the attack is to send more requests to a server than it can handle.
  - The attack exploits a potential vulnerability in the TCP/IP connection establishment mechanism and floods the server's pending connection queue

Network Threat Counter Measures

Threat	Countermeasures
Information Gathering	• Configure routers to restrict their responses to footprinting requests. • Configure operating systems that host network software (for example, software firewalls) to prevent footprinting by disabling unused protocols and unnecessary ports
Sniffing	• Use strong physical security and proper segmenting of the network. This is the first step in preventing traffic from being collected locally. • Encrypt communication fully, including authentication credentials. This prevents sniffed packets from being usable to an attacker. • SSL and IPSec (Internet Protocol Security) are examples of encryption solutions
Spoofing	• Filter incoming packets that appear to come from an internal IP address at your perimeter • Filter outgoing packets that appear to originate from an invalid local IP address
Session Hijacking	• Use encrypted session negotiation. • Use encrypted communication channels. • Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences
Denial of service	• Apply the latest service packs • Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

Top Host Threats



- **Botnet:** A botnet is a network of Internet-connected and malware-infected devices, which have been co-opted by cybercriminals. It is used to distribute spam and malware, or launch distributed denial-of-service attacks.
- **Adware:** A type of malicious software that installs or renders advertising on a computing system to generate revenue. Advertisements are often appear as pop-ups in windows that the user is unable to close. Sometimes adware is designed with multiple objectives.
- **Distributed Denial-of-Service (DDoS) Attacks:**Using the computers attached to a botnet, cybercriminals shut down—or deny service—to a victim's system users by overloading the computational resources of the website or system with data.
- **Keyloggers:** With keylogging software, bots collect information related to specific type of keyboard strokes, such as alpha-numeric/special character sequences associated with certain keywords, such as "bankofamerica.com" or "paypal.com".

Top Host Threats

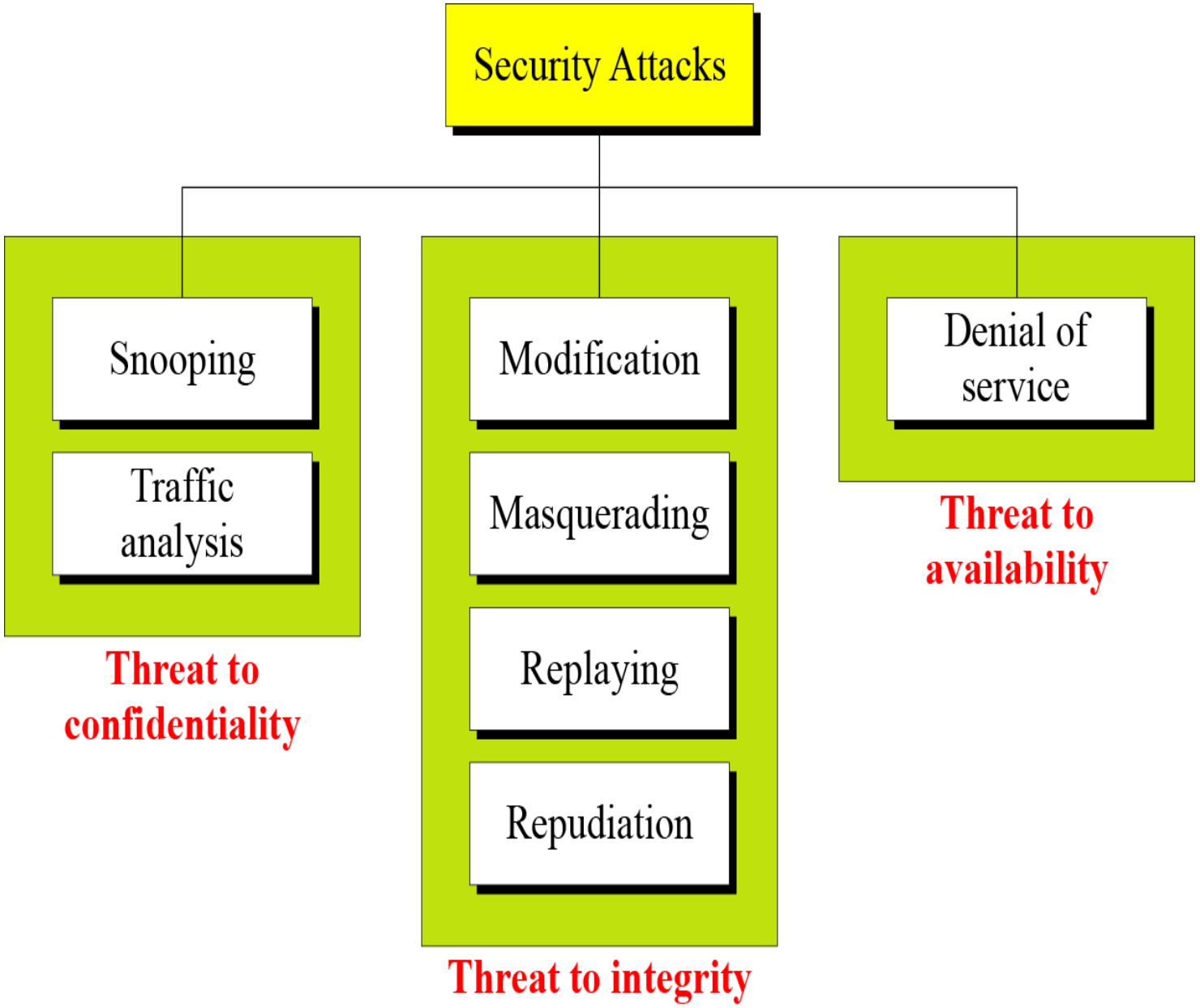
- **Rootkit:** Malicious software that enables access to sections of the computer, software, or system that would normally not be accessible. Malware often contains rootkits to allow concealment by modifying the operating system so that the malware remains hidden from the user.
- **Spyware:** Malicious software that spies on the computer user, capturing keystrokes, emails, documents, or even turning on the video camera. Sometimes embedded in adware.
- **Vishing:** A combination of the words 'voice' and 'phishing'. Vishing uses social engineering via a phone call to obtain personally sensitive information, such as bank account numbers, pins, or credit card numbers. Typically, the victim receives a call with an automated message from someone claiming to represent a financial institution, internet provider, or technology company. The message may ask the victim to enter an account number or pin. Once entered, the call redirects to an attacker via a voice-over-IP service, who then requests additional personally sensitive information.
- **Zero-day Attack:** A type of attack in which a cybercriminal leverages a system, software, or network vulnerability that is otherwise unknown to the public, cybersecurity professionals, and sometimes to the software or system developers.

General Application Threat Categories and Threats

Category	Threats
Input validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Authentication	Network eavesdropping; brute force attacks; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive data	Access sensitive data in storage; network eavesdropping; data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

Taxonomy of attacks with relation to security goals

Security Attack is any action that compromises the security of information owned by an organization.

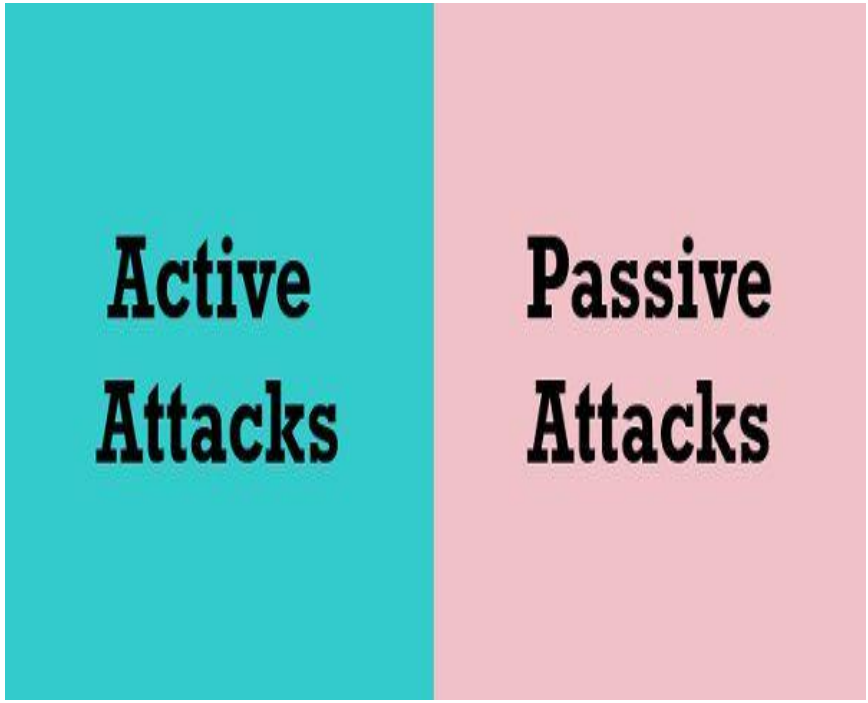


Security Attacks

- **Snooping** refers to unauthorized access to or interception of person's data or company's data .
- **Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.
- **Modification** means that the attacker intercepts the message and changes it.
- **Masquerading or spoofing** happens when the attacker impersonates somebody else.
- **Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation** 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.
- **Denial of service (DoS)** is a very common attack. It may slow down or totally interrupt the service of a system.

Attack categorization

- **Active Attacks:** An active attack attempts to **alter system resources** or **effect their operations**. Active attack involve some **modification of the data stream** or **creation** of false statement
- **Passive Attacks:** A Passive attack **attempts to learn or make use of information from the system** but **does not affect system resources.** The goal of the opponent is to obtain information that is being transmitted by observing the characteristics of communications that carry the data.
- Even **if message contents is encrypted**, an attacker can still determine **the identity and the location of the communicating parties**. Observe the **frequency and length of the messages** being exchanged and **guess the nature of the communication.**



Passive Attack Types

1. **The release of message content:**

   Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information can be revealed publicly using sniffing.

2. **Traffic analysis:**

   The data that is sniffed can be encrypted but still be used to determine the location and identity of communicating host 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.

Active Attack: Types

- **Masquerade:** Masquerade attack takes place when one entity pretends to be different entity.
- **Denial of Service:** It prevents normal use of communication facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.
- **Modification:** Modification means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect.
- **Repudiation:** This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message.
- **Replay:** It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect

Passive vs Active

- Attempts to learn or make use of information from the system but does not affect system resources.
- It poses a danger to the confidentiality of the data.
- Victims are not informed about the attack.
- Passive attacks – focus on Prevention
- Easy to stop
- Hard to detect
- Examples
  - Sniffing
  - Traffic Analysis

- Attempts to alter system resources or affect their operation
- It imposes a threat to the availability and integrity of the original piece of information.
- Victims get informed about the attack
- Active attacks – focus on Detection and Recovery
- Hard to stop
- Easy to detect
- Examples:
  - masquerade (spoofing)
  - replay

Active Attack Types

- **Viruses, Trojan Horses, and Worms**
  - A virus is a program that is designed to perform malicious acts and cause disruption to your operating system or applications.
  - A Trojan horse resembles a virus except that the malicious code is contained inside what appears to be a harmless data file or executable program. a Trojan is a form of non-replicating malicious software that contains hidden functionality. A Trojan typically does not attempt to propagate or inject itself into other files.
  - A worm is similar to a Trojan horse except that it self-replicates from one server to another. Worms are difficult to detect because they do not regularly create files that can be seen
  - Although these three threats are actually attacks, together they pose a significant threat to Web applications, the hosts these applications live on, and the network used to deliver these applications
- **Footprinting**
  - Examples of footprinting are port scans, ping sweeps, and NetBIOS enumeration that can be used by attackers to glean valuable system-level information to help prepare for more significant attacks.
  - The type of information potentially revealed by footprinting includes account details, operating system and other software versions, server names, and database schema details
- **Password Cracking**
  - If the attacker cannot establish an anonymous connection with the server, he will try to establish an authenticated connection.
  - The use of blank or weak passwords makes the attacker's job even easier
- **Denial of Service**
- **Arbitrary Code Execution**
  - If an attacker can execute malicious code on your server, the attacker can either compromise server resources or mount further attacks against downstream systems
- **Unauthorized Access**
  - Inadequate access controls could allow an unauthorized user to access restricted information or perform restricted operations

Host Attacks Counter Measures

Threat	Countermeasures
Viruses, Trojan Horses and Worms	• Stay current with the latest operating system service packs and software patches. • Block all unnecessary ports at the firewall and host. • Disable unused functionality including protocols and services. •Harden weak, default configuration settings
Foot Printing	• Disable unnecessary protocols. • Lock down ports with the appropriate firewall configuration. • Use TCP/IP and IPSec filters for defense in depth. • Configure IIS to prevent information disclosure through banner grabbing. • Use an IDS that can be configured to pick up footprinting patterns and reject suspicious traffic
Password Cracking	• Use strong passwords for all account types. • Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password. • Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications. • Audit failed logins for patterns of password hacking attempts
Arbitrary Code Execution	• Configure IIS to reject URLs with "../" to prevent path traversal. • Lock down system commands and utilities with restricted ACLs. • Stay current with patches and updates to ensure that newly discovered buffer overflows are speedily patched
Unauthorized Access	• Configure secure Web permissions. • Lock down files and folders with restricted NTFS permissions. • Use .NET Framework access control mechanisms within your ASP.NET applications, including URL authorization and principal permission demands

Security Services & Mechanisms

OSI Security Architecture

- **ITU-T(X.800)[International Telecommunication Union-Telecommunication Standardization Sector]** is a security architecture for OSI that systematically define some security services and some mechanisms to implement those services.
- It defines 3 aspects of information security.
  - **Security Services:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms and is a service provided by the protocol layer of a communicating system
  - **Security Mechanism:** A mechanism that is designed to detect, prevent or recover from a security attack.
  - **Security Attack:** Any action that compromises the security of information

Security Services

- **Data Confidentiality:** Data confidentiality is designed to protect data from disclosure attack. It is designed to prevent snooping and traffic analysis attack
- **Data Integrity:** It is designed to protect data from modification, insertion, deletion and replaying by an adversary.
- **Authentication:** Both the sender and receiver need to confirm the identity of other party involved in the communication. Property of being genuine and to be verified as trusted one. Verifying users and ensuring data is coming from trusted source.
  - **Passwords**
  - **Biometrics**
- **Non-repudiation/Accountability:** An entity is prevented from denying its previous commitments or actions. Property by which an action can be traced back uniquely to the entity associated with it. Systems must trace security breaches with help of activity records.
    - **Logs**

Security Services/Objectives of Information Security

- **Access control/ Authorization:** *Access control* is the process of controlling who is allowed to do what. This ranges from controlling physical access to a computer—keeping your servers in a locked room, for example—to specifying who has access to a resource (a file, for example) and what they are allowed to do with that resource (such as read only). Some access control mechanisms are enforced by the operating system, some by the individual application or server, some by a service (such as a networking protocol) in use.
- An entity cannot access any entity that it is not authorized to. The process of granting or denying access rights to a network resource.
- access control refers **to the prevention of unauthorized use of a resource** (this service controls who can have access to certain resources, under what conditions access can occur, and what those accessing the resources are allowed to do.
    - **Access Control Lists and Capabilities**
    - **Multilevel security (MLS), security modeling, covert channel, inference control**
    - **Firewalls, intrusion detection (IDS)**

Security Services/Objectives of Information Security

- **Anonymity/ Privacy**

  The identity of an entity if protected from others.

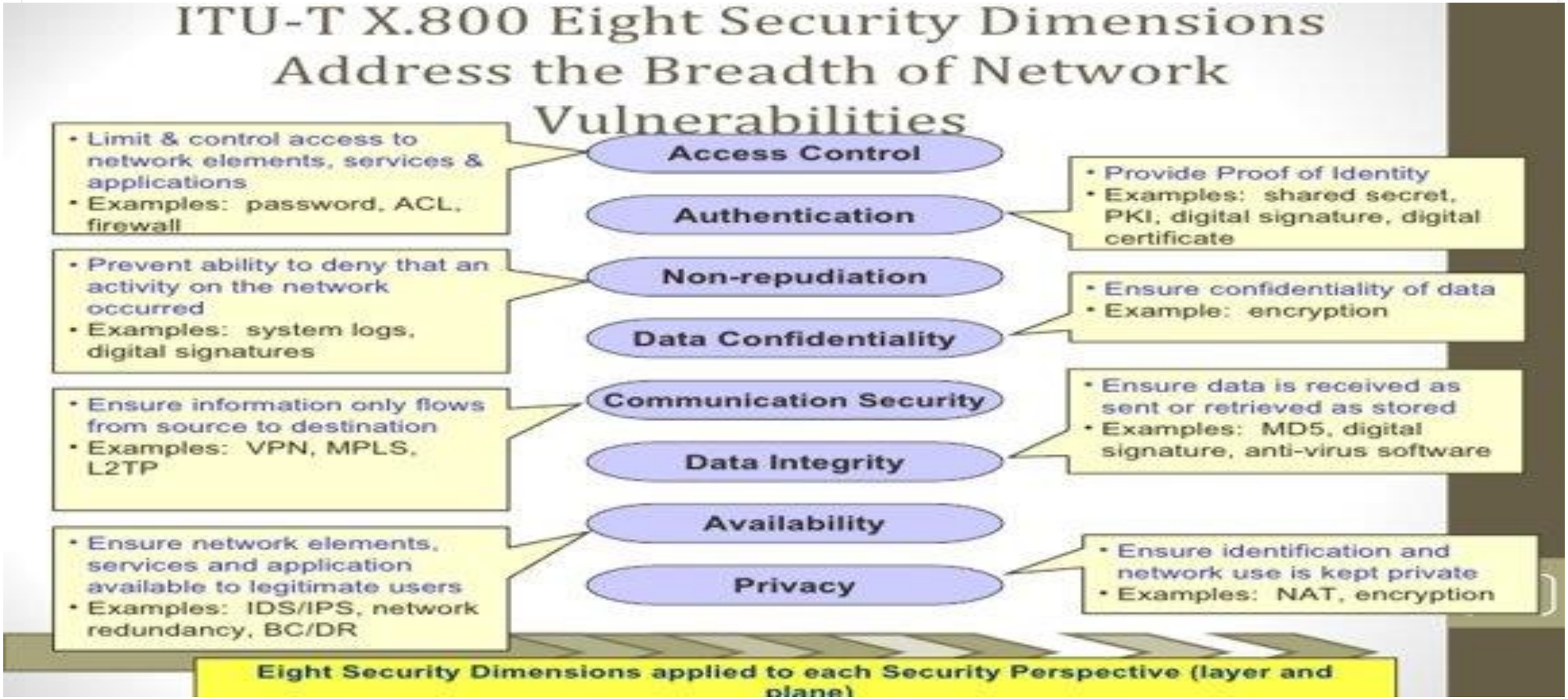
- **Communication Security**

  Ensures information flow only from source to destination

- **Availability**

  Ensures service and information are available to legitimate users whenever available

ITU-T Security Services



Security Mechanism to implement Security Services

- Security mechanisms are used to implement security services. They include (X.800):
  1. **Encipherment:** Hiding/covering of data using cryptographic or steganographic mechanism
  2. **Digital signature:** It is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. Sender uses a process to show she owns a private key for a public key which is been announced publicly. Receiver uses sender's public key to prove that message is signed by sender.
  3. **Access Control mechanisms:** Methods to prove the user has access rights to data or resources owned by a system. Examples of proofs are passwords and PIN.
  4. **Data Integrity mechanisms:** Appends a check value in message that is sent. Receiver calculates the check value from data and compares both so integrity of data is preserved.

Security Mechanism to implement Security Services

5. **Authentication Exchange:** 2 entities exchange some message to prove their identities to each other. Eg: a commonly shared secret
6. **Traffic Padding:** Inserting some bogus data to prevent attackers attempt for traffic analysis. Traffic padding means insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
7. **Routing Control:** Routing control means selecting and continuously changing different available routes between the sender and the receiver to avoid eavesdropping.
8. **Notarization:** The use of a trusted third party to assure certain properties of a data exchange and control communication. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that he has made such a request.

Mapping of goals to security services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Thank You

Ref:
1.Security in Computing: Charles P Pfleeger, Shari Lawrence Pfleeger
2. Cryptography and Network Security: Behrouz Ferouzan, Debdeep Mukhopadhyay

anooja@somaiya.edu