Network Security Attacks

ICT 3156

Four Potential Types Of Harm

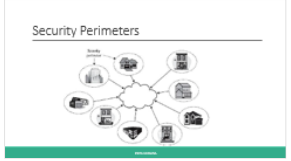
- Interception, or unauthorized viewing
- Modification, or unauthorized change
- Fabrication, or unauthorized creation
- Interruption, or preventing authorized access

Eavesdropping or wiretapping

Integrity failures

Denial of Service

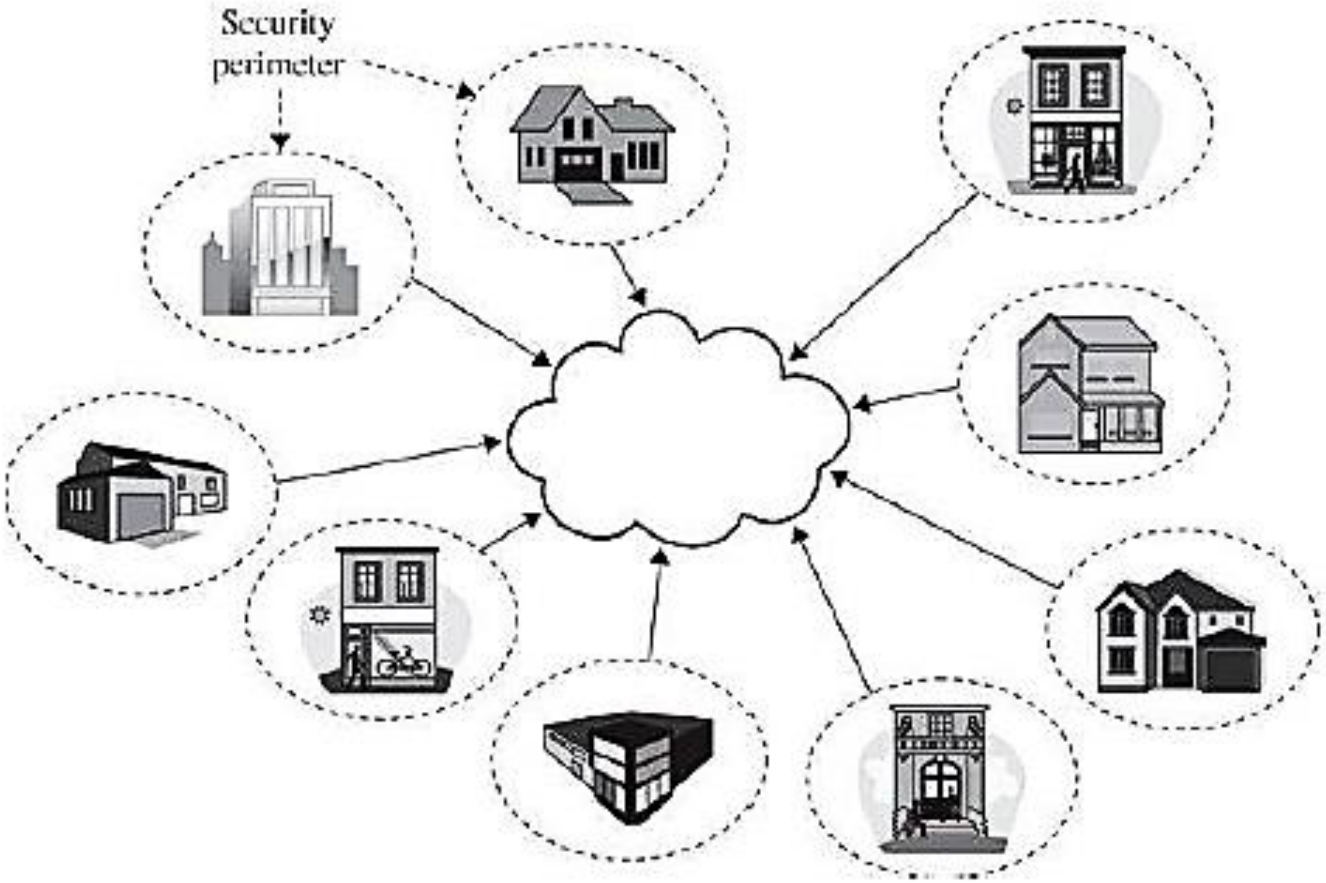
Interception: Eavesdropping and Wiretapping



Security Perimeters

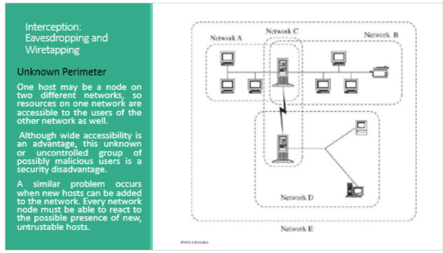
- Concept of a security perimeter.
- Outside your zone, your ability to secure your data is limited.
- Wiretapping is the name given to data interception, often covert and unauthorized.
- Even a backdoor intended only for court-authorized **wiretaps** can be misused.
- Why it happens?
- Users generally have little control over the routing of a signal.
- Encryption is the strongest and most commonly used countermeasure against interception, although physical security, dedicated lines, and controlled routing have their roles, as well.

Security Perimeters



Interception: Eavesdropping and Wiretapping

- What Makes a Network Vulnerable to Interception?
- Anonymity
- Many Points of Attack.
    - When a file is stored in a network host remote from the user, the data or the file itself may pass through many hosts to get to the user. The user must depend on the access control mechanisms in each of these systems.
- Sharing
- System Complexity
- Unknown Perimeter
- Unknown Path



Interception: Eavesdropping and Wiretapping

Unknown Perimeter

One host may be a node on two different networks, so resources on one network are accessible to the users of the other network as well.

Although wide accessibility is an advantage, this unknown or uncontrolled group of possibly malicious users is a security disadvantage.

A similar problem occurs when new hosts can be added to the network. Every network node must be able to react to the possible presence of new, untrustable hosts.

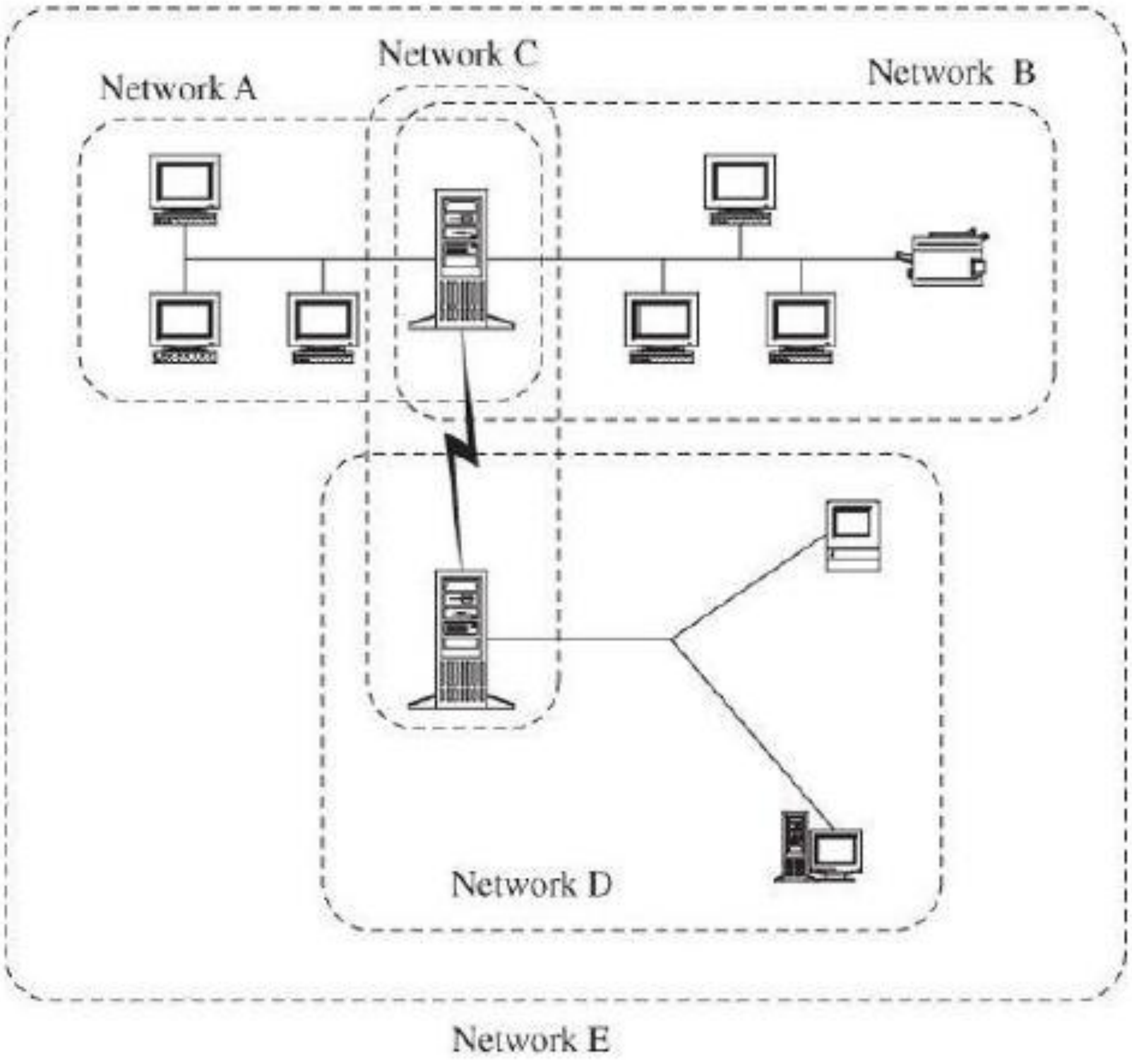
Interception: Eavesdropping and Wiretapping

Unknown Perimeter

One host may be a node on two different networks, so resources on one network are accessible to the users of the other network as well.

Although wide accessibility is an advantage, this unknown or uncontrolled group of possibly malicious users is a security disadvantage.

A similar problem occurs when new hosts can be added to the network. Every network node must be able to react to the possible presence of new, untrustable hosts.



Modification, Fabrication: Data Corruption

- Threat: communication will be changed during transmission.
- Three attacks : Modification, Insertion, and Replay.
- Data corruption can be intentional or unintentional, from a malicious or non-malicious source, and directed or accidental.
- When can it occur?
- Data corruption can occur during data entry, in storage, during use and computation, in transit, and on output and retrieval.

Modification, Fabrication: Data Corruption

- Sequencing
- Substitution
- Insertion
- Replay

Modification, Fabrication: Data Corruption

- **Sequencing**
  - Sequencing attack or problem involves permuting the order of data.
  - Occurs when a later fragment of a data stream arrives before a previous one.
- **Insertion**
  - In an insertion attack, data values are inserted into a stream.
  - An attacker does not even need to break an encryption scheme in order to insert authentic-seeming data.??

Modification, Fabrication: Data Corruption

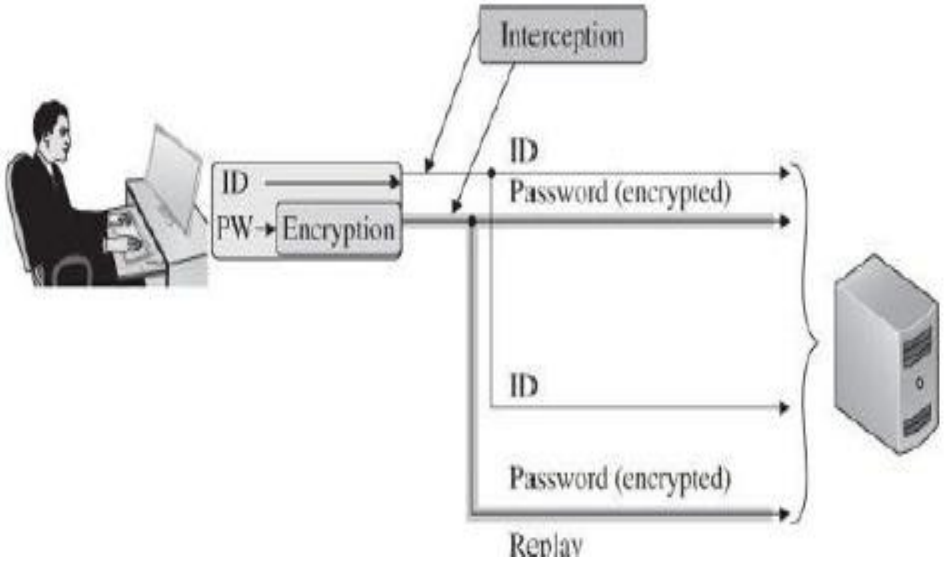
- **Substitution**
  - A substitution attack is the replacement of one piece of a data stream with another.
  - Substitution errors (non-malicious) can occur with adjacent cables or multiplexed parallel communications in a network; occasionally, interference, called crosstalk allows data to flow into an adjacent path.
  - A malicious attacker can perform a substitution attack by splicing a piece from one communication into another.
  - The obvious countermeasure against substitution attacks is encryption or creating an integrity check. How it benefits?
  - Not all substitution attacks are malicious.

Modification, Fabrication: Data Corruption

- **Replay**
  - In a replay attack, legitimate data are intercepted and reused, generally without modification.
  - A replay attack differs from both a wiretapping attack and a man-in-the-middle attack.
  - The interceptor need not know the content or format of a transmission.
  - Can succeed on encrypted data without altering or breaking the encryption.

Modification, Fabrication: Data Corruption

- **Replay**
  - Can also be used with authentication credentials.
  - If the attacker can interject the encrypted password into the communications line, then the attacker can impersonate a valid user without knowing the password.
  - Cookies.
  - Physical Replay. CCTV, Biometrics, and so on.
  - Replay attacks can circumvent ordinary identification, authentication, and confidentiality defenses.
  - Thus they allow the attacker to initiate and carry on an interchange under the guise of the victim.
  - Sequence numbers help counter replay attacks.



Interruption: Loss of Service

- Can be malicious or non-malicious, intentional or accidental.
- Unlike confidentiality and integrity failures, however, denial of service is not binary.
- In mesh architecture of the Internet, redundancy and fault tolerance were important characteristics, and the robustness remains.
- However, the final connection between a host and the larger network infrastructure, is a unique pathway, so any failure there isolates the host.
- Network design incorporates redundancy to counter hardware failures.
- What are some of the factors that leads to loss of service?
- Routing, excessive demand, component failure and so on.

Interruption: Loss of Service

- **Routing**
  - One piece of bad information can poison the data pool of many routers, thus disrupting flow for many paths.
  - Routing supports efficient resource use and quality of service. Misused, it can cause denial of service.
- **Excessive Demand**
  - Motivation: Network capacity is enormous but finite, and capacity of any particular link or component is much smaller.
  - Denial-of-service attacks usually try to flood a victim with excessive demand.
- **Component Failure**
  - Being hardware devices, components fail; these failures tend to be sporadic, individual, unpredictable, and non-malicious.

Port Scanning

- Scanning is often used as a first step in an attack, a probe, to determine what further attacks might succeed.
- Why is it essential before an attack?
  - The problem for the attacker is to know which attacks to address to which machines.
  - Sending an attack against a machine that is not vulnerable is time consuming.
  - Can make the attacker stand out or become visible and identifiable.
- A port scan maps the topology and hardware and software components of a network segment.
- Port Scanning Tools. Secure Scanner by Cisco, Nmap, and so on.

Port Scanning

- Port scanning tells an attacker three things:
  - which standard ports or services are running and responding on the target system,
  - what operating system is installed on the target system, and
  - what applications and versions of applications are present.
- It can be obtained quietly, anonymously, without identification or authentication, drawing little or no attention to the scan.
- Knowing that a particular host runs a given version of an OS may make the attacker aware about the vulnerabilities associated with that version.
- Thus, a port scan can be a first step in a more serious attack.
- Another thing an attacker can learn is **connectivity**.

Port Scanning

- A glimpse of the plethora of information that can be learnt:
    - How many hosts there are?
    - What their IP addresses are?
    - What their physical (MAC) addresses are?
    - What brand each is?
    - What operating system each runs, and what version?
    - What ports respond to service requests?
    - What service applications respond, and what program and version they are running?
    - How long responses took (which reveals speed of various network connections and thus may indicate the design of the network)?

Book

- Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015, Chapter 6.