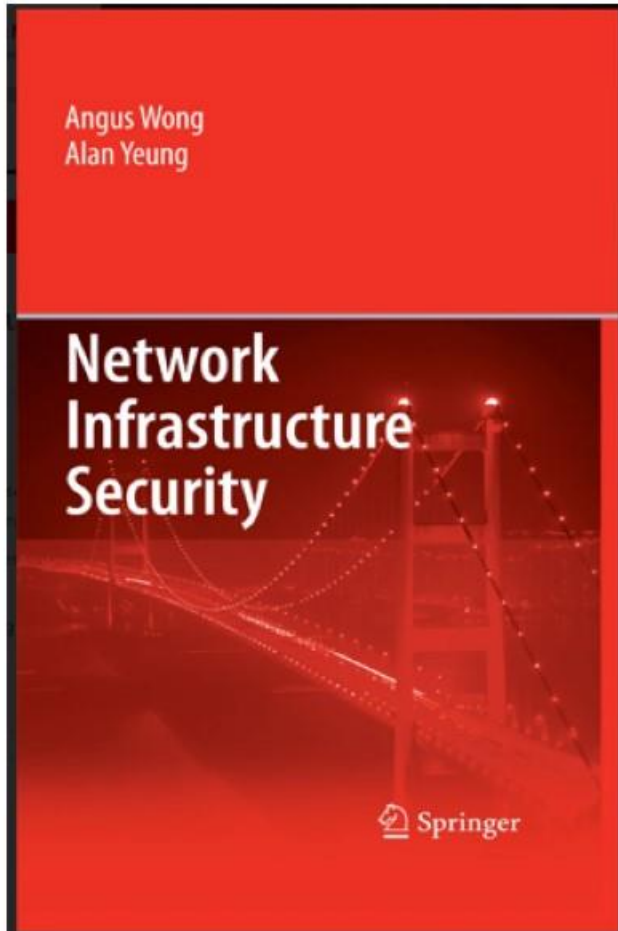


Prepared by Dr. Mohammed Anbar

Network Security (CYB 630)
Network Infrastructure Security (part one)

Lecture 1





Some of the contents in this presentation is adopted from the resources provided by the authors of the following book:

Wong, Angus, and Alan Yeung. *Network infrastructure security*. Springer Science & Business Media, 2009.

Chapter

01

Learning objectives

- Explain Network Infrastructure and its security,
- Differentiate between Information Security and Network Infrastructure security,
- Explain Network Infrastructure components ,
- Explain switch security,
- Explain Dynamic Host Configuration Protocol (DHCP) security ,
- Explain Domain Name System (DNS) security .

Network Infrastructure

- Network infrastructure refers to resources that enable network connectivity, communication, operation, and management.
- Typically, it includes networking hardware, software, and services.
- If your network is not secure, it presents a significant vulnerability to various attacks such as denial-of-service, malware, spam, and unauthorized access.

Information security vs Network Infrastructure security

Information security

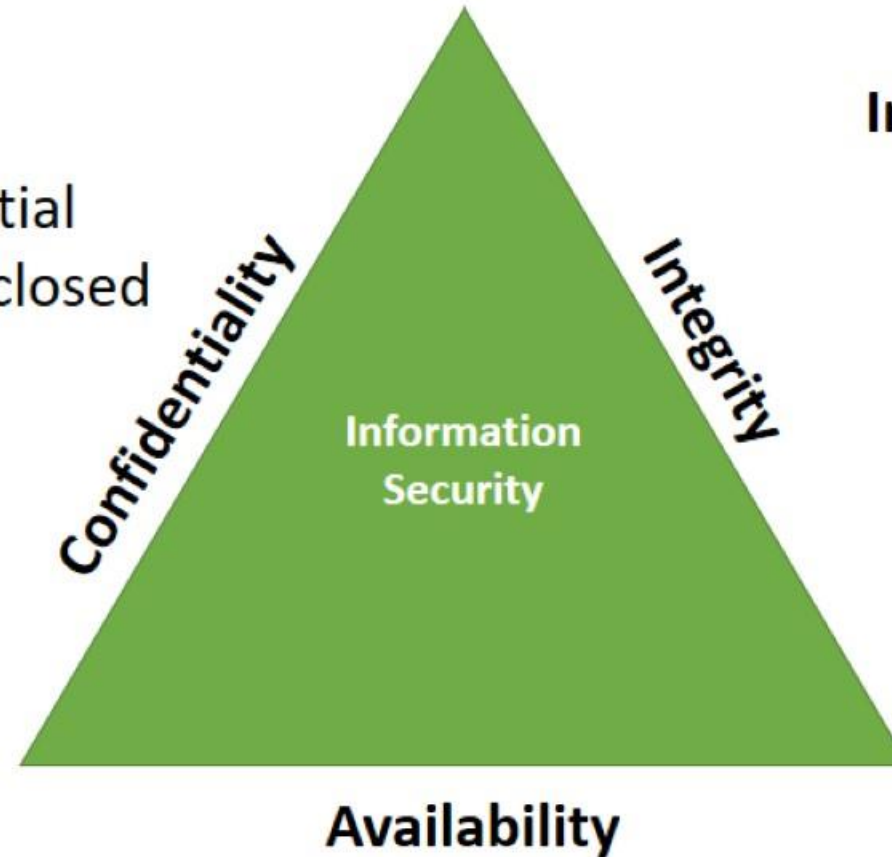
- Information security is a set of strategies or procedures which are designed and implemented to prevent and protect digital and non-digital information or any other sensitive information or data from unauthorized access.
- Confidentiality, integrity, and availability (CIA triad), is a model designed to guide policies for information security within an organization.
- CIA is usually present because these are typically viewed as the primary goals and objectives of a security infrastructure.

Three key principles (the CIA triad)

Confidentiality

Assures that confidential information is not disclosed to unauthorized individuals

Overall, an information security mechanism should precisely address each of these **CIA triad principles**.

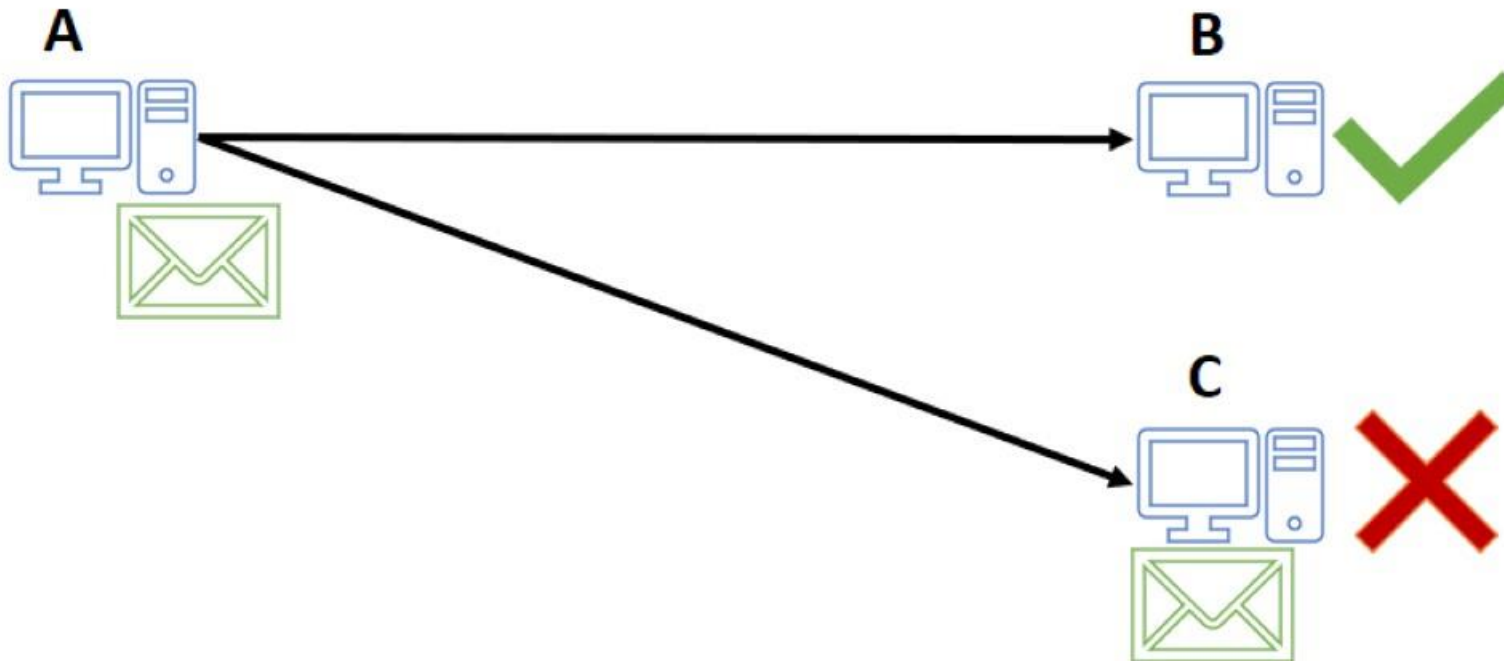


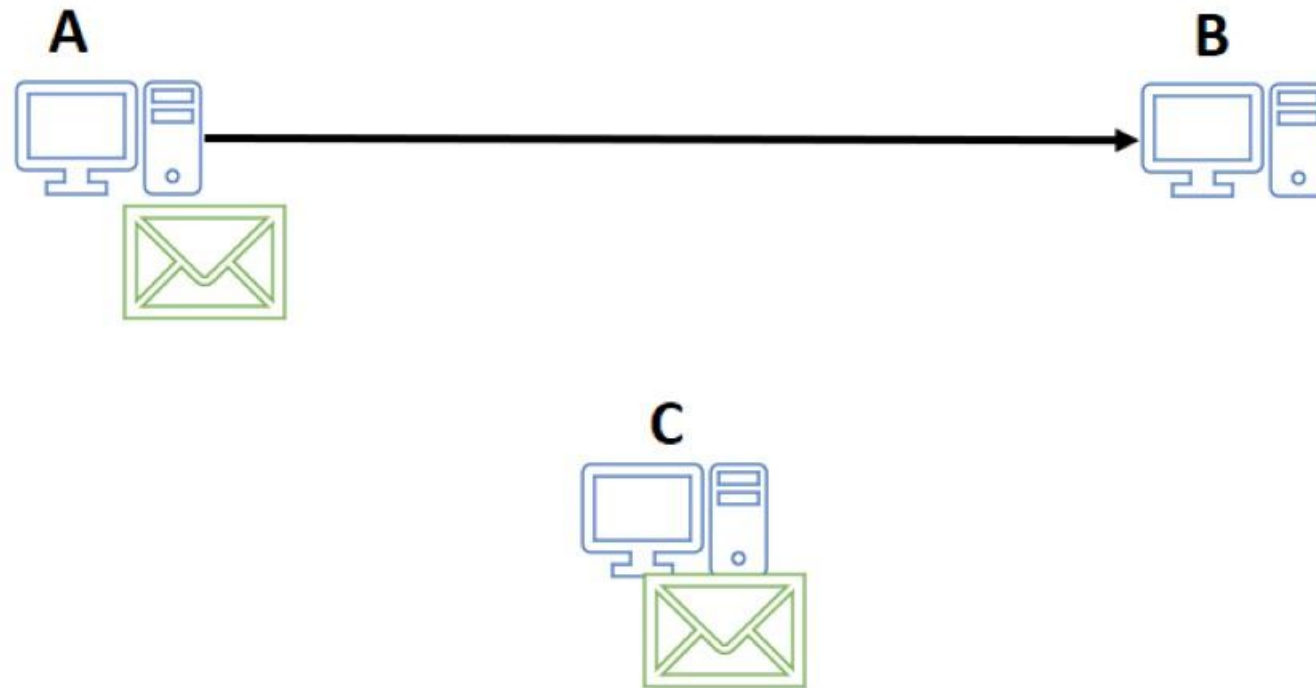
Integrity

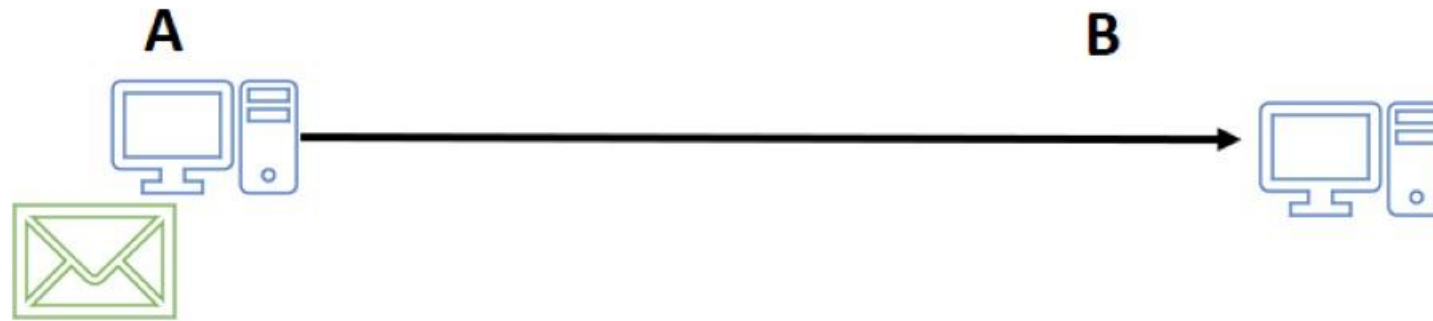
Assures that information and programs are changed only in a specified and authorized manner

Availability

Assures that systems and services are not denied to authorized users



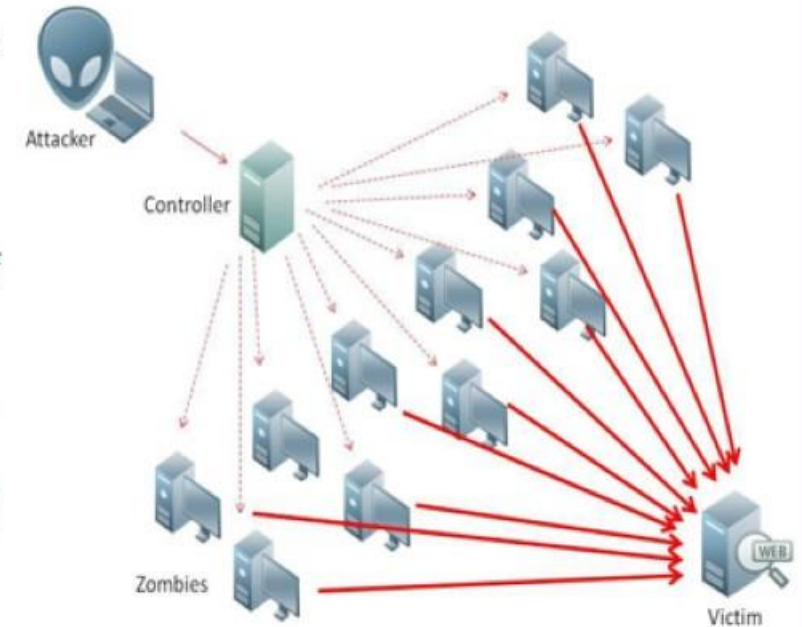




- While the provision of information is important, it becomes meaningless if the data, no matter how secure its content, cannot be correctly delivered through the infrastructure of the Internet to its intended destination.
- On the other hand, if the infrastructure is attacked, a large area (or even the entire) Internet will be affected, causing economic damages. Therefore, in recent years, much concern has been drawn to how securing the Internet infrastructure is.

- Unlike network information security which focuses on information protection, infrastructure security focuses on the protection of the network infrastructure itself.
- The protection of the network infrastructure focuses on how to detect network attacks and how to prevent routers or other network devices from being compromised.
- The approach to infrastructure security includes the use of secure Internet protocols, traffic monitoring, and firewalls.

- The attack on Network Infrastructure would affect a large portion of the Internet and create a large amount of service disruption.
- Since our daily operations highly depend on the availability and reliability of the Internet, the security of its infrastructure has become a high-priority issue.
- An example of Network Infrastructure is Distributed Denial of Service (DDoS) attacks.



➤ Internet infrastructure is vulnerable

- Many network devices and protocols were designed without security concerns in mind at the beginning. Unfortunately, those protocols now form part of the Internet infrastructure, making it vulnerable to various kinds of attacks.

➤ Security and performance trade-off

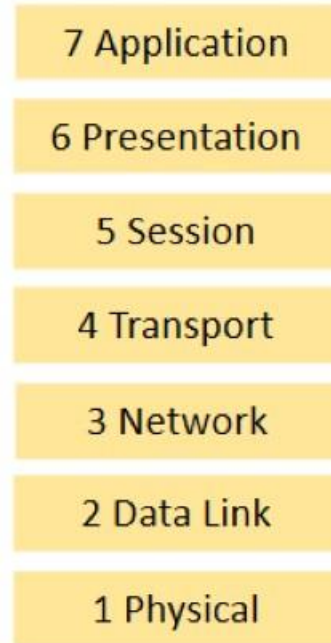
- Security usually requires extra processes to run or more CPU cycles to execute the security process. It certainly reduces the performance of current devices.

➤ Attacks can be easily launched and difficult to be traced

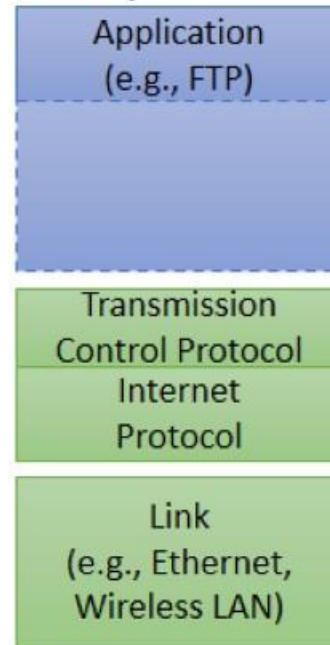
Anyone with a computer and an Internet connection can reach any point on the Internet, making it possible to launch an attack from anywhere in the world. Compounding the problem, a general computer can easily pretend itself as a switch or router (by running a special software package) and broadcast malicious information to mislead the real network devices to perform abnormally.

- The Open Systems Interconnection (OSI) model demonstrates how networks operate in terms of hardware and software.
- Each layer in the model performs different tasks for network communication and is useful to analyse the security properties of protocols and devices.
- More importantly, this type of model helps build a multi-layered “defense-in-depth” to provide maximum network security.

OSI 7-layer stack



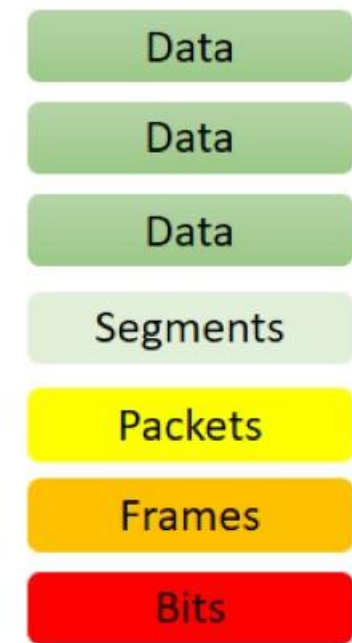
TCP/IP stack



OSI 7-layer stack



Data



Examples of Protocols at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPv4, IPv6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

Here are the different layers of this model and how it can best be implemented:

Physical layer: Defines physical and electrical characteristics of the network, such as cable types and signals used to transmit data.

- **Devices:** Repeater, hub, and network interface controller (NIC).
- **Vulnerabilities:** Loss of power, physical theft, damage, and modification of data and hardware.
- **Prevention controls:** Employ video/audio surveillance, lock your perimeter, use biometric/PIN and password authentication systems.

Data link layer: Defines how shared communication channels can be accessed, and data frames can be reliably transmitted.

- **Devices:** switches and bridges.
- **Vulnerabilities:** Media Access Control (MAC) addresses spoofing and flooding, unauthorized access due to weak authentication, and encryption in the wireless environment.
- **Prevention controls** MAC address filtering, strong wireless security, physical separation of layers with firewalls, and other IDS (Intrusion Detection Systems).

Network layer: Handles the task of routing network messages from one node to another and determines which path it needs to take to reach its destination.

- **Devices:** Router.
- **Vulnerabilities:** Route and IP address spoofing.
- **Prevention controls:** Anti-spoofing and filter policy, firewalls, broadcast monitoring.

Transport layer: Ensures that packets are transported reliably and without errors.

- **Vulnerabilities:** Spoofing of transmission mechanisms, overloading of transport layer mechanisms, fingerprinting.
- **Prevention controls:** Limit specific transmission protocols, implement stateful inspection on the firewall.

Session layer: Establishes conversations (sessions) between networked devices.

- **Vulnerabilities:** weak authentication mechanisms, passing Personally Identifiable Information (PII) in clear text, spoofed session identification information, brute force attacks.
- **Prevention controls** encryption when passing personal information, adequate account policy with expiration and authorization, limited failed timing and session attempts.

Presentation layer: Responsible for how data is presented to applications.

- **Vulnerabilities:** Crashed applications, remote manipulation, and execution, information leakage.
- **Prevention controls:** Employ cryptography and input validation.

Application layer: Deals with the techniques that applications use to communicate with the network.

- **Vulnerabilities:** Program flaws causing crashing and abnormal behavior, inadequate and complex security controls, and application design flaws.
- **Prevention controls:** Access control for applications should be detailed, flexible, and straightforward; review application code, implement a firewall, and IDS to monitor applications.

Networking Hardware:

- Routers
- Switches
- LAN cards
- Wireless routers
- Cables

Network Services:

- DSL
- Satellite
- Wireless protocols
- IP addressing

Networking Software:

- Network operations and management
- Operating systems
- Firewall
- Network security applications



Thank You