Cyber Security Concepts

Lecture-2

Department of CSE, IUT

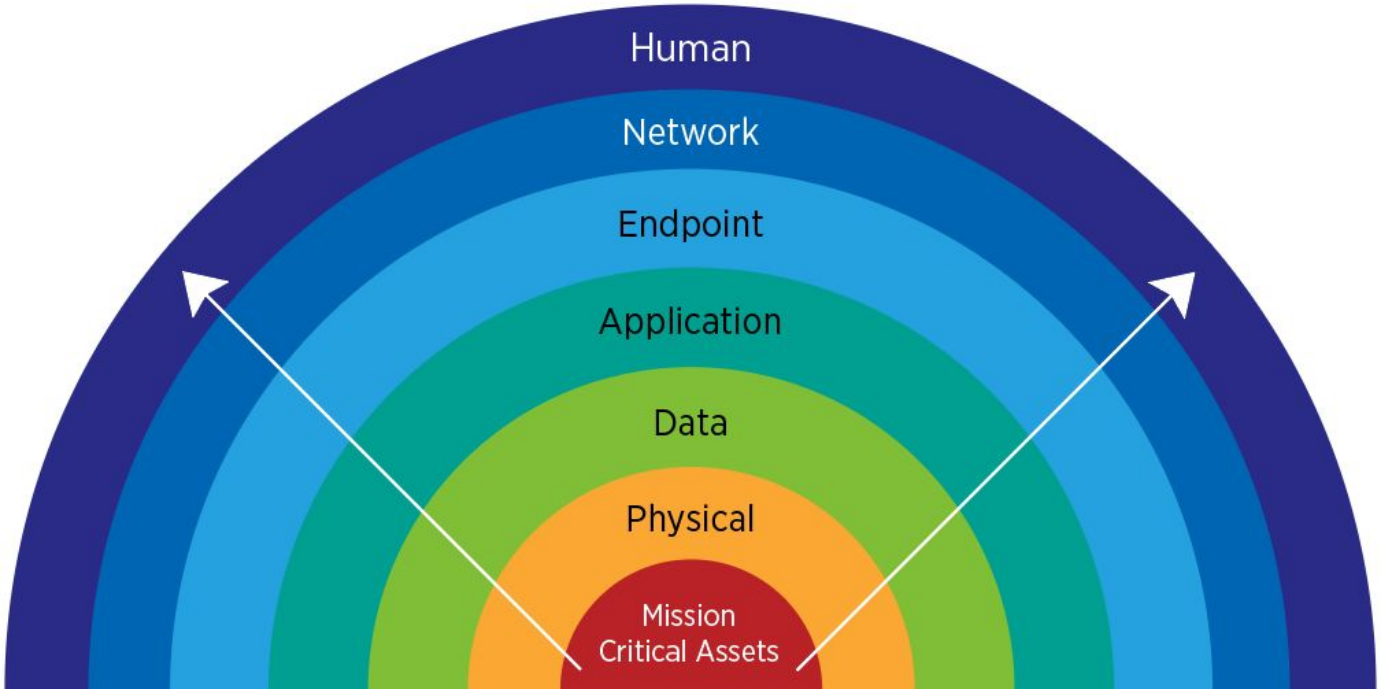
Cyber Security: Terminology

- **Cyber Space-** interconnected digital environment of networks, services, systems, and processes
- **Cyber incident-** cyber event that involves a loss of information security or impacts business operations
- **Cyber insurance:** insurance that covers or reduces financial loss to the insured caused by a cyber incident
- **Cyber-Physical Systems (CPS):** are systems composed of physical systems (hardware), software systems and potentially other types of systems (e.g., human systems). These are closely integrated and networked to deliver some global behaviour.

Cyber Security: Terminology

- **Cyber-Physical Systems (CPS):** are systems composed of physical systems (hardware), software systems and potentially other types of systems (e.g., human systems). These are closely integrated and networked to deliver some global behaviour.

Cyber Security: Concept



Cyber Security: Concept

What is Software Security?

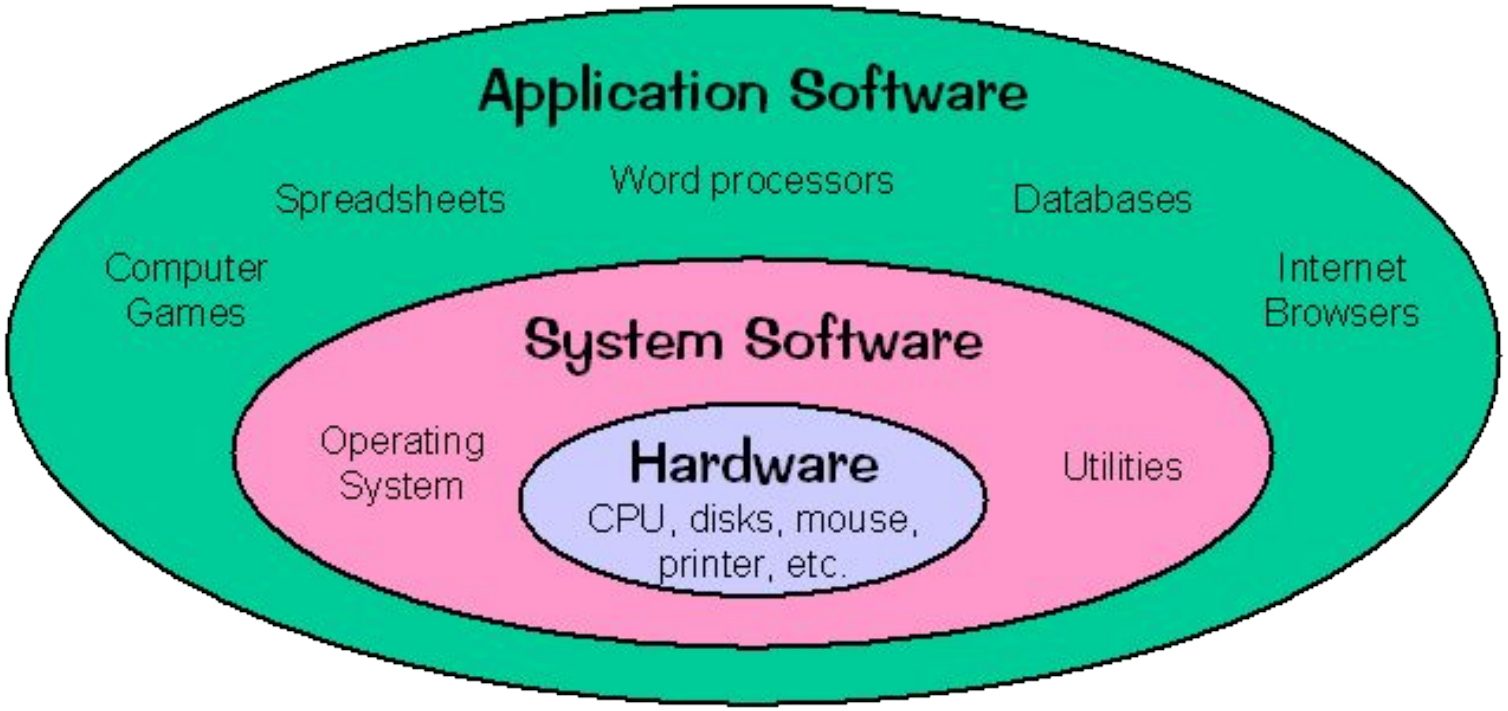
Software security is a kind of computer security that **focuses** on **the secure design and implementation of software.**

- Using the best language, tools, methods

- **Focus of study:**

  The Code

Software : Concepts



Software : Concepts

System Software	Application Software
• System software are mainly designed for managing system resources.	• Application software are designed to accomplish tasks for specific purposes.
• Programming of system software is complex.	• Programming of application software is comparatively easy.
• A computer cannot run without system software.	• A computer can easily run without application software.
• System software do not depend on application software.	• Application software depend on system software and cannot run without system software.

Software : Concepts

Software Security vs Application Security

Software Security	Application Security
Proactive Build security in Preventive costs	Reactive Build security around Corrective costs
• Design for security • Testing for security • Software security education	• Network centric approach • Protect software after development • Finding and fixing security issues

What is the most effective way to protect software?

What is Network Security?

- **Network security:**
  - Protection of the **underlying networking infrastructure** from unauthorized access and misuse.

What is Application Security?

- **Application security**
  - aims to protect **Software code, Software and hardware system, Data** against cyber threats.
  - introduce a secure software development life cycle to development teams.

What is Web Security?

- Process, technology or method for protecting
  - Web servers, web applications, and web services against different security threats that exploit vulnerabilities in an application's code.
  - Critical to the business continuity

The web and the use of DNS services specifically are part of 91% of all malware attacks

Email and web together are a key part for 99% of successful breaches.

- Commonly, prime target by the threat actors
  - Ease of execution

What is Mobile Application Security?

- Mobile app security is the practice of safeguarding **high-value mobile applications** and your digital identity from fraudulent attack in all its forms.

What is Information Security?

- Information security
  - Protecting information and information systems from unauthorized use, assess, modification or removal.
  - Two sub-categories
    - Physical environment by ensuring the premises is secure
    - No one can access information electronically
  - Concerned with making sure data in any form is kept secure and is a bit more broad than cybersecurity

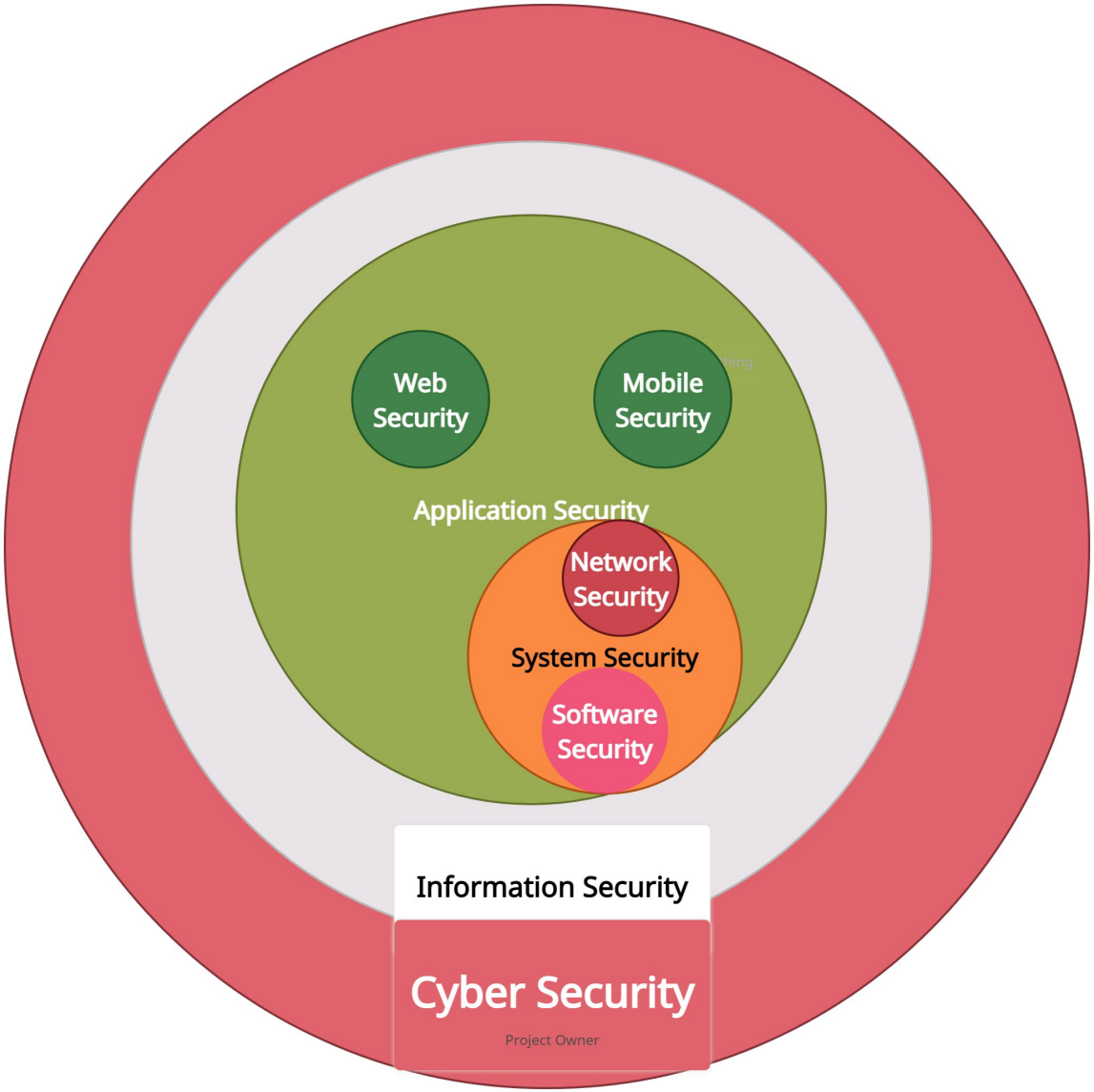
What is Cyber Security?

Cybersecurity = security of information systems, applications and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

availability, integrity and secrecy

- Protection of **internet-connected systems** such as hardware, software and data from cyberthreats

Cyber Security: Concept



Cyber Security: ?

Let's clarify the Network security in brief …

Network Security: Overview

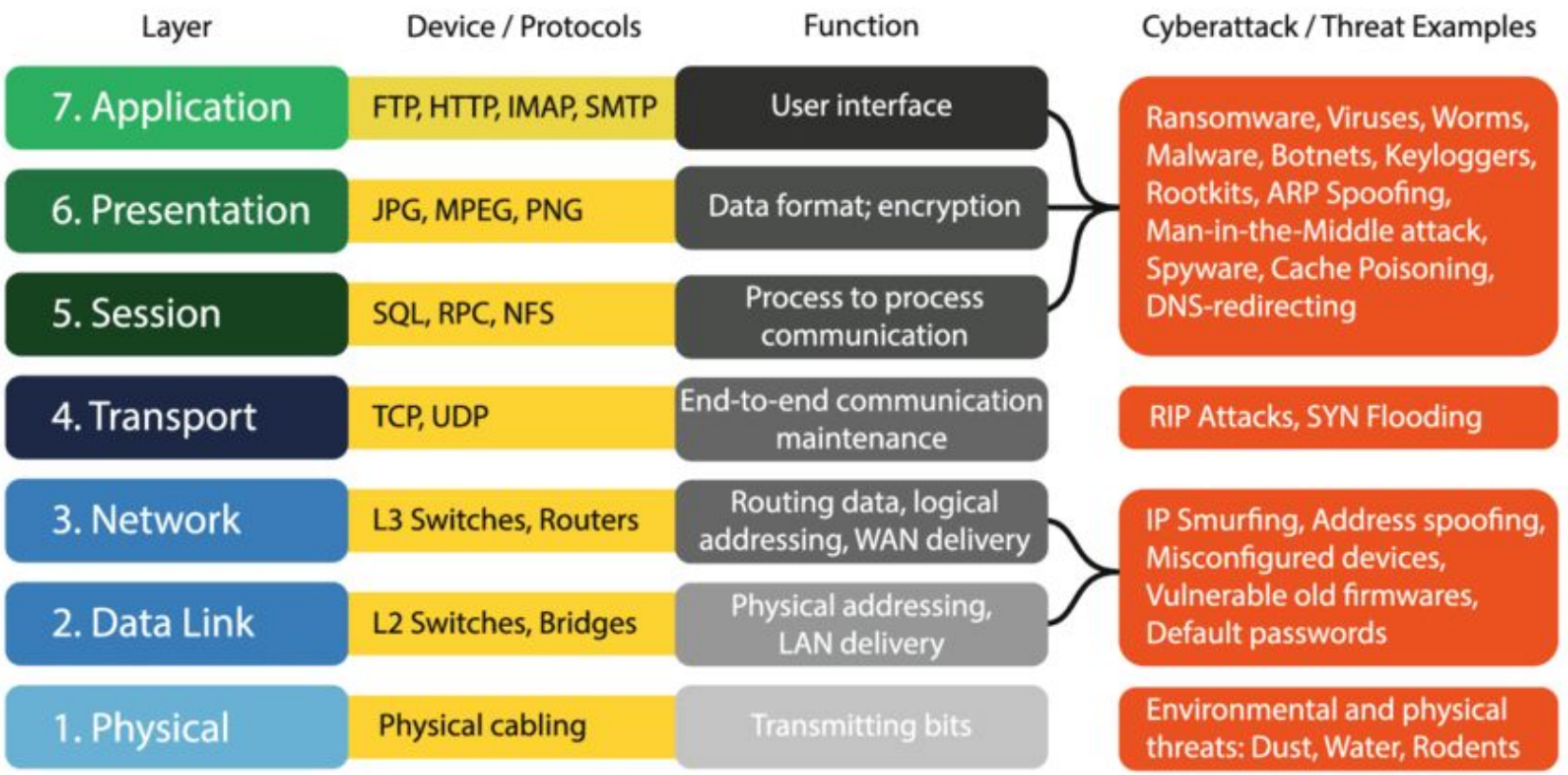
- **Network security:**
  - Protection of the **underlying networking infrastructure** from unauthorized access and misuse.

The web and the use of DNS services specifically are part of 91% of all malware attacks

Email and web together are a key part for 99% of successful breaches.

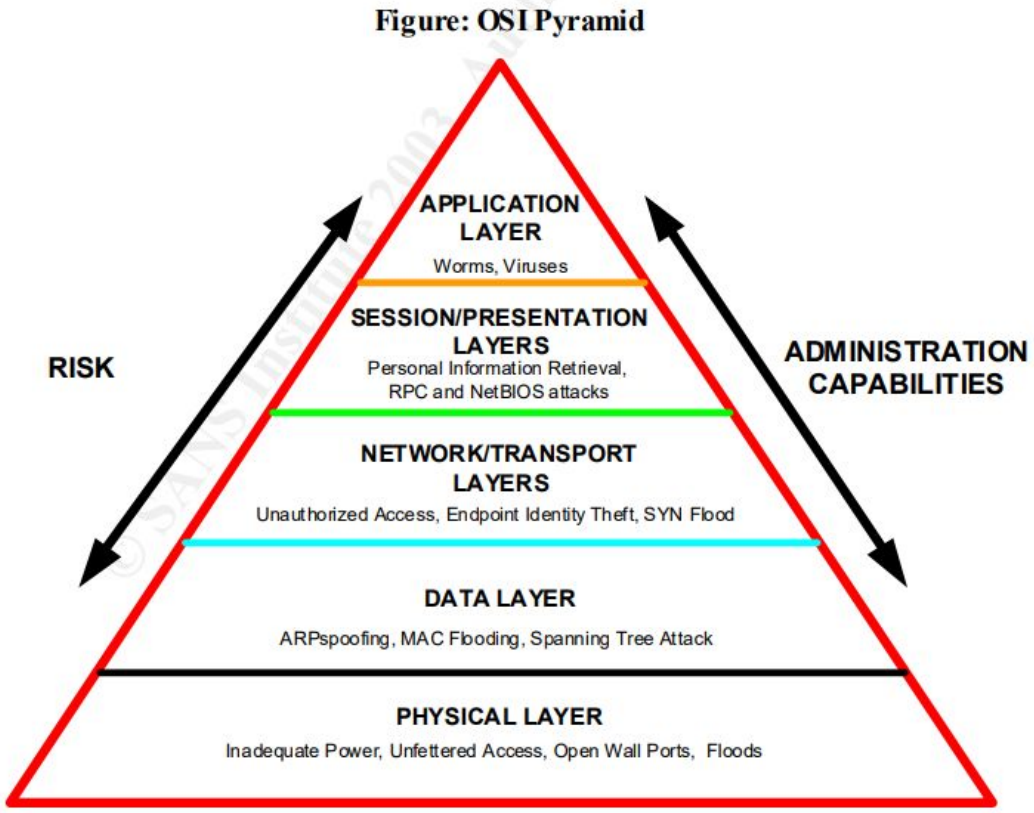
Network Security: Overview

in Network Protocol layers



Network Security: Overview

in Network Protocol layers

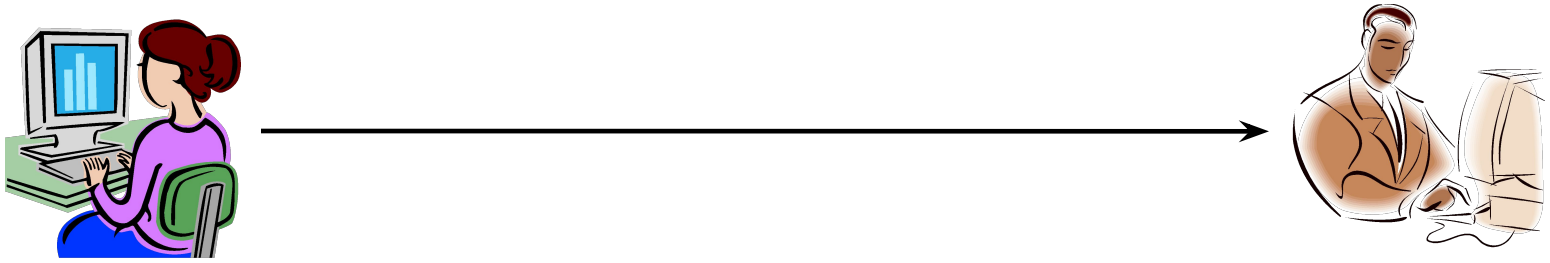


Network Security:
Commonly used placeholders in Security

- **Alice and Bob**: Alice wants to send a message to Bob

Alice

Bob



- **Eve:** an *eavesdropper*, is usually a passive attacker
- **Mallory:** a *malicious attacker;* unlike Eve, Mallory can modify messages, substitute her own messages, replay old messages, and so on

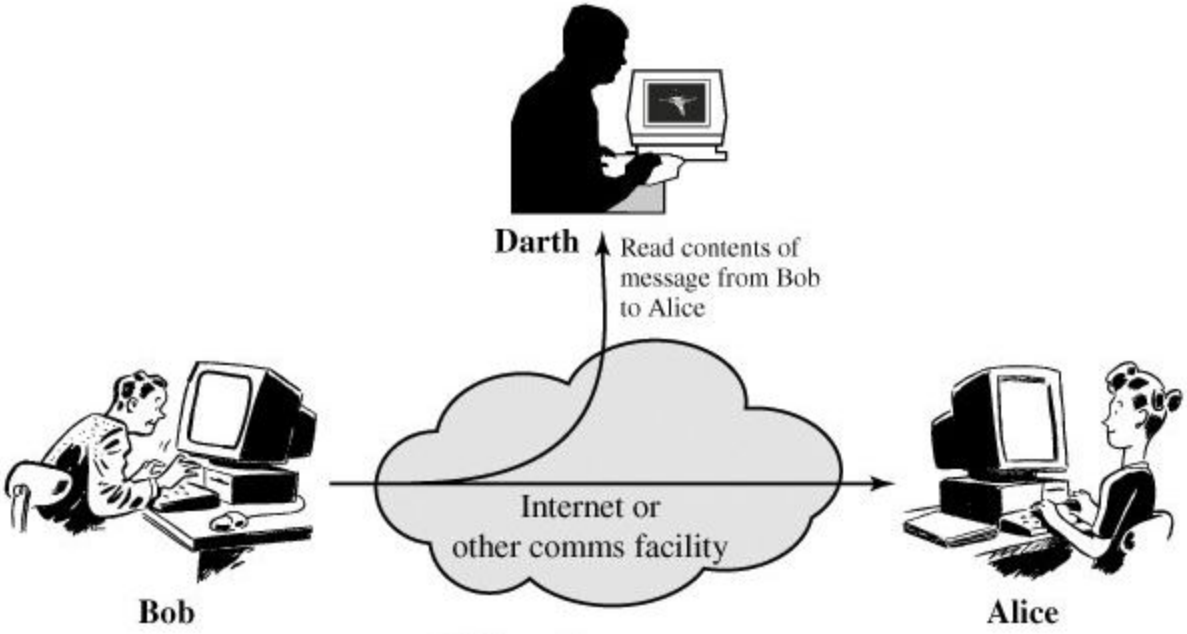
Network Security: Overview

Issues

- A sends a file to B: E intercepts it and reads it
  - How to send a file that looks gibberish to all but the intended receiver?
- A send a file to B: M intercepts it, modifies it, and then forwards it to B
  - How to make sure that the document has been received in exactly the form it has been sent
- M sends a file to B pretending it is from A
  - How to make sure your communication partner is really who (s)he claims to be
- A sends a message to B: M is able to delay the message for a while
  - How to detect old messages
- A sends a message to B. Later A (or B) denies having sent (received) the message
  - How to deal with electronic contracts
- E learns which user accesses which information although the information itself remains secure
- M prevents communication between A and B: B will reject any message from A because they look unauthentic

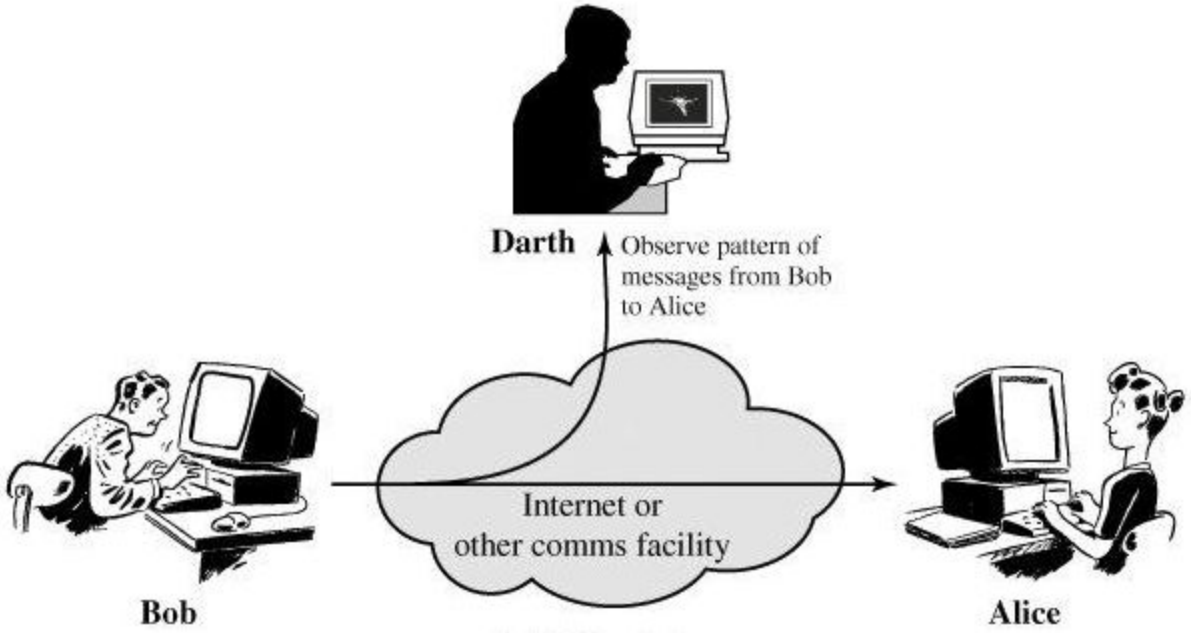
Network Security: Security Attacks

- Snooping or Eavesdropping:
  - Threat against confidentiality



Network Security: Security Attacks

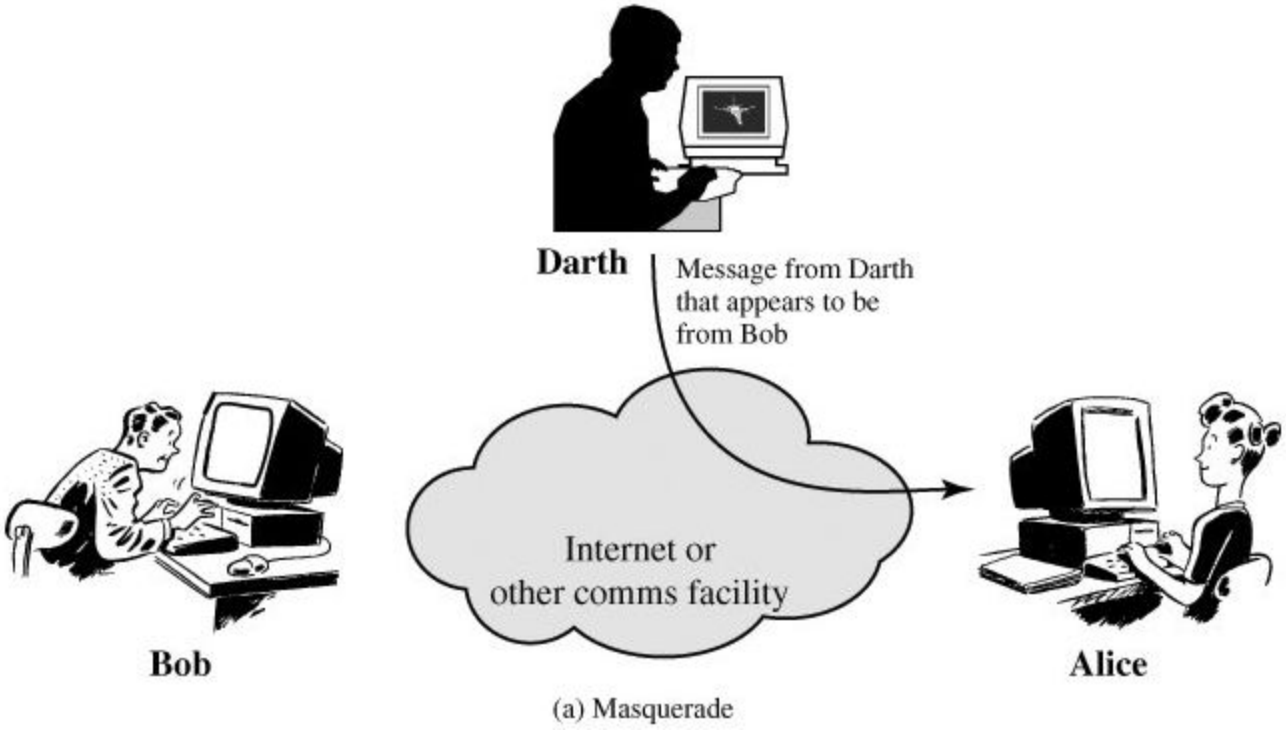
- Traffic analysis:
  - Threat against confidentiality



(b) Traffic analysis

Network Security: Security Attacks

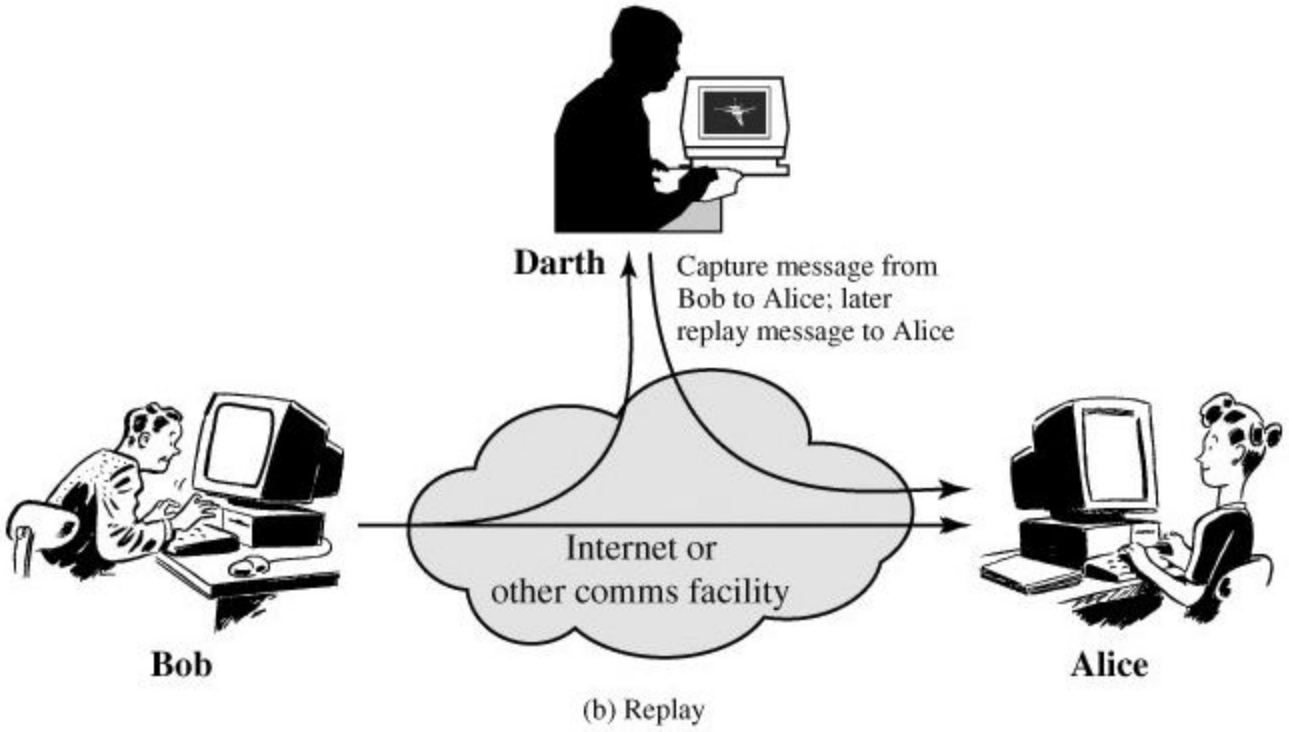
- Masquerade:
  - Threat against Integrity



(a) Masquerade

Network Security: Security Attacks

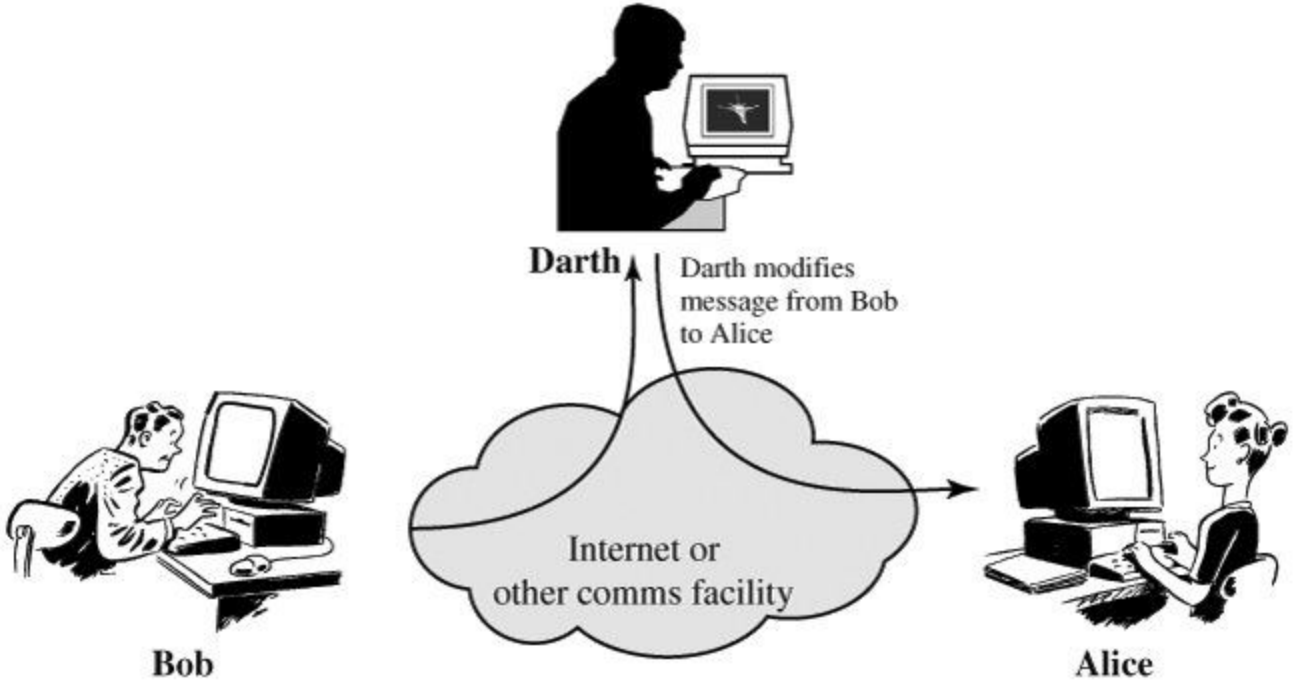
- Replay:
  - Threat against Integrity



(b) Replay

Network Security: Security Attacks

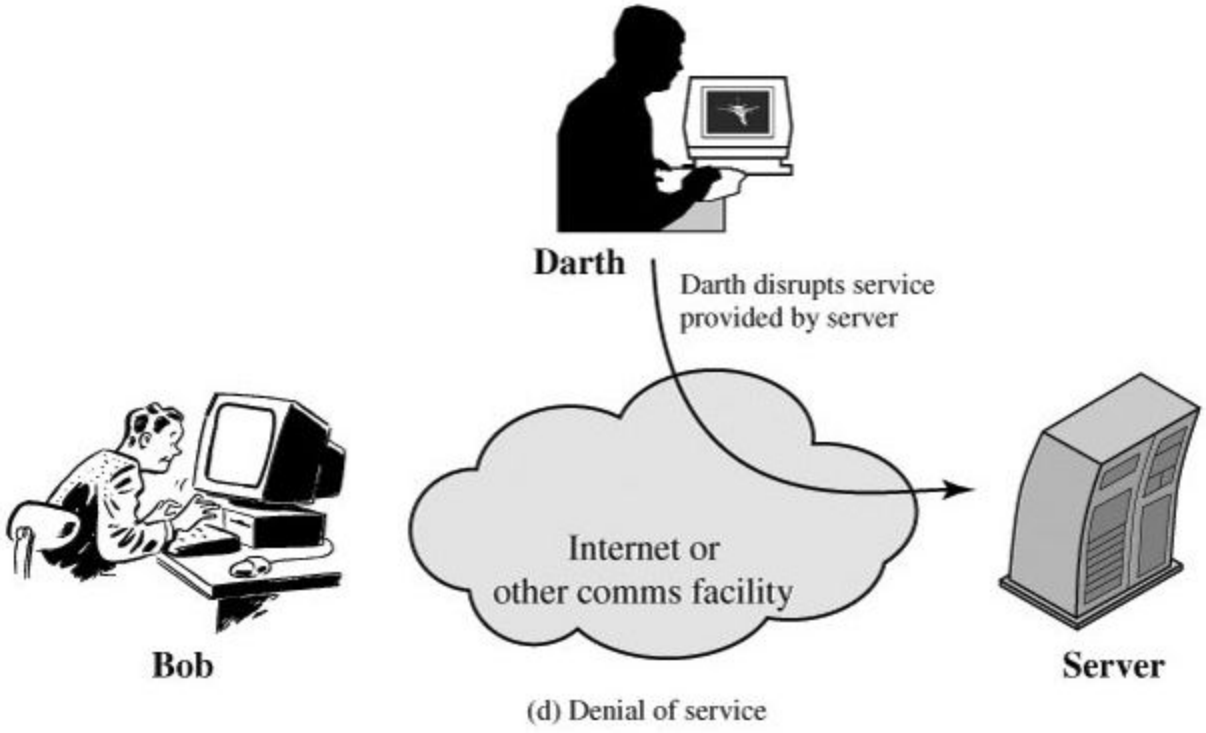
- Modification of message:
  - Threat against Integrity



(c) Modification of messages

Network Security: Security Attacks

- Denial of service (DoS):
  - Threat against Availability



(d) Denial of service

References

- Chapter -1: Cryptography and Network Security Principles and Practices, Fourth Edition. By William Stallings.