Network Attacks Overview

Segurança Informática em Redes e Sistemas
2024/25

David R. Matos, Ricardo Chaves
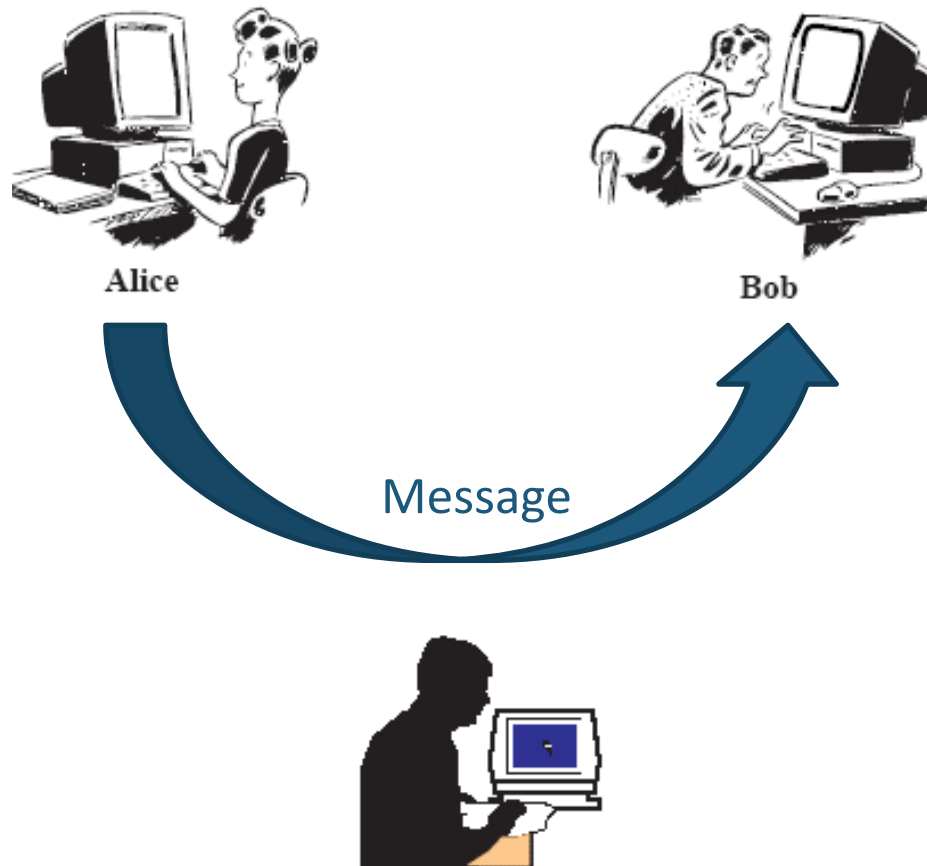
Roadmap
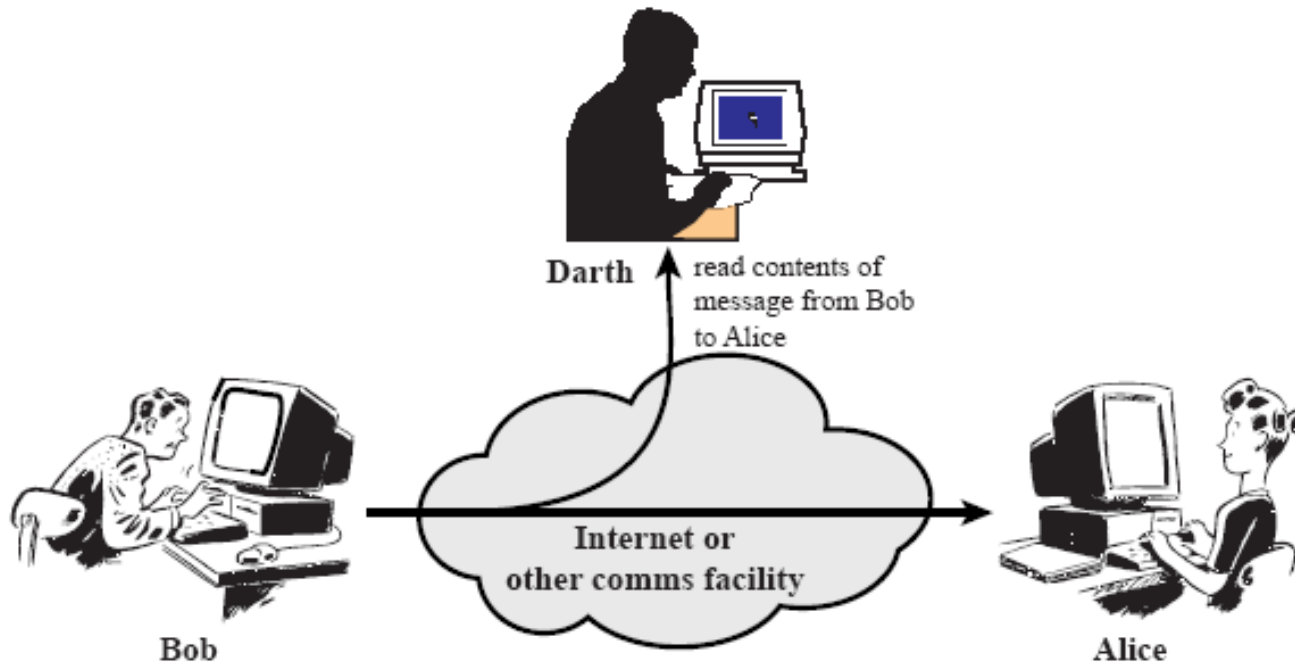
- Network attacks
- Security models

Network communication parties

- Alice
- Bob
- Charlie

- Darth
- Eve
- Mallory

Alice

Bob

Message

Passive attacks:
Listen (information disclosure)

Darth — read contents of message from Bob to Alice

Bob

Internet or other comms facility

Alice

Passive attacks:
Listen (traffic analysis)

Darth

observe pattern of
messages from Bob
to Alice

Internet or
other comms facility

Bob

Alice
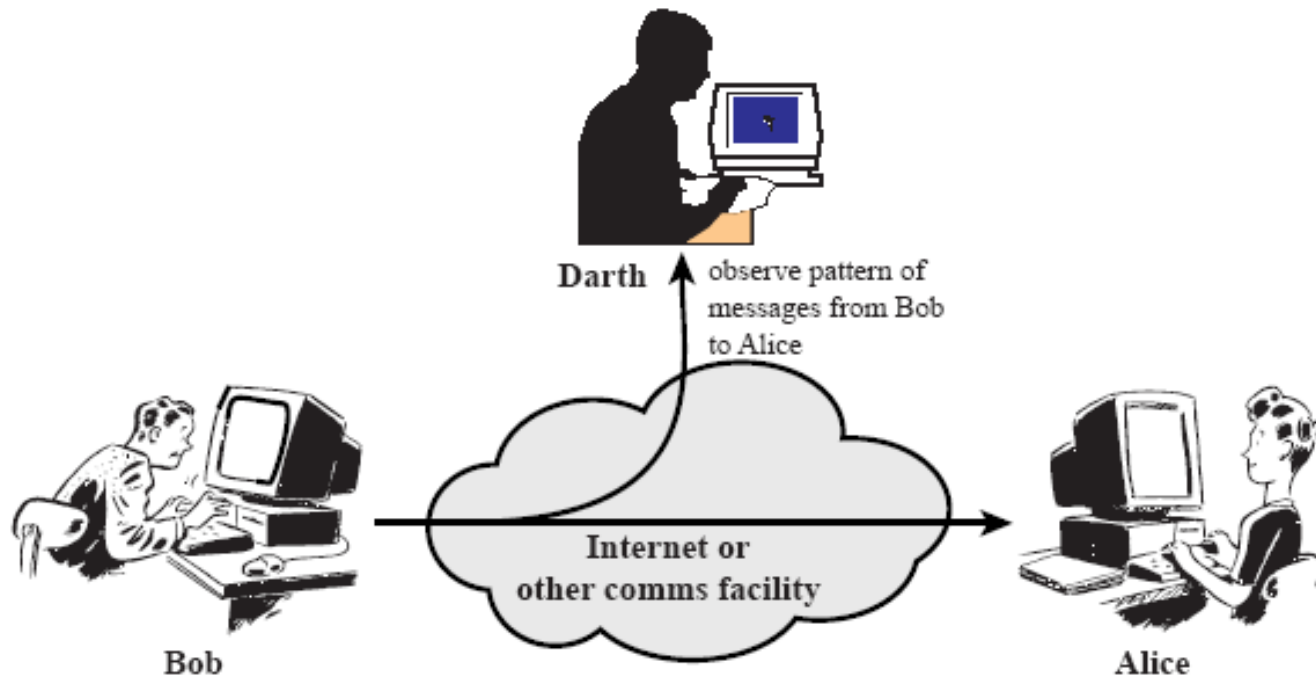
Active attacks: Impersonation

Darth

Message from Darth that appears to be from Bob

Bob

Internet or other comms facility

Alice
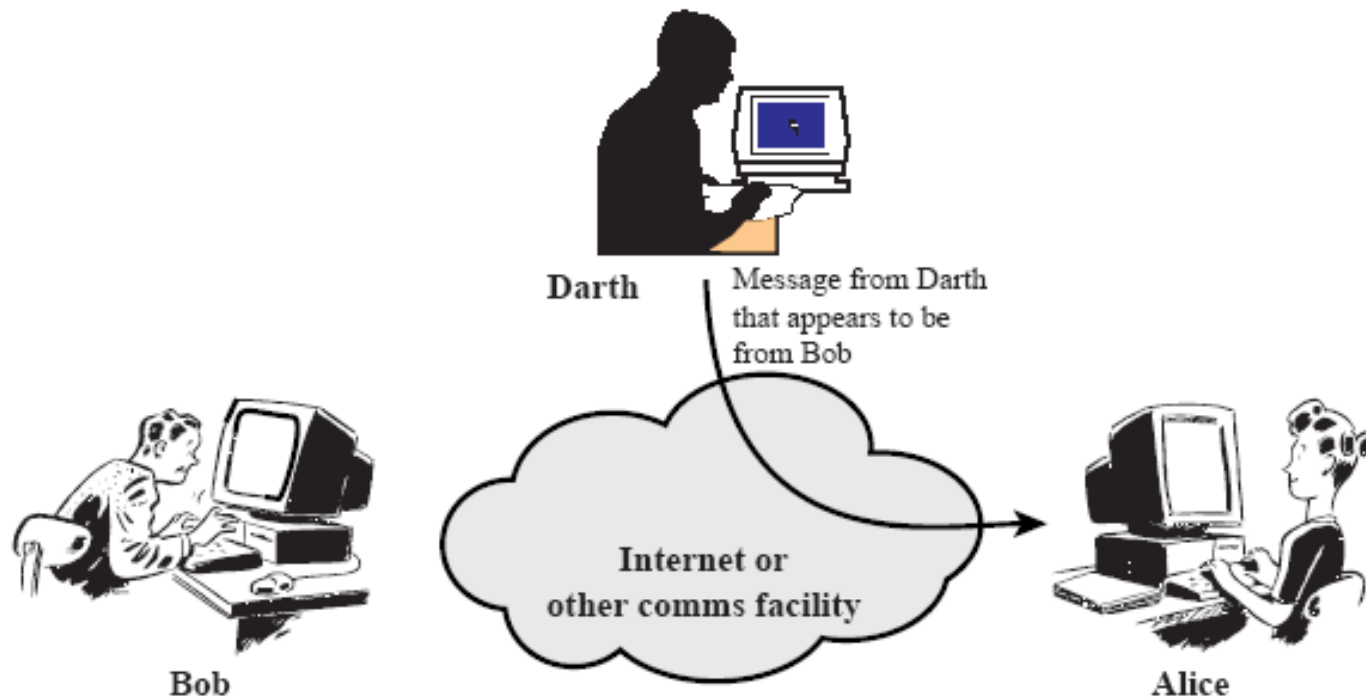
Active attacks: Tampering

Darth

Darth modifies message from Bob to Alice

Bob

Internet or other comms facility

Alice

Active attacks: Replay

Darth — Capture message from Bob to Alice; later replay message to Alice

Internet or other comms facility

Bob

Alice
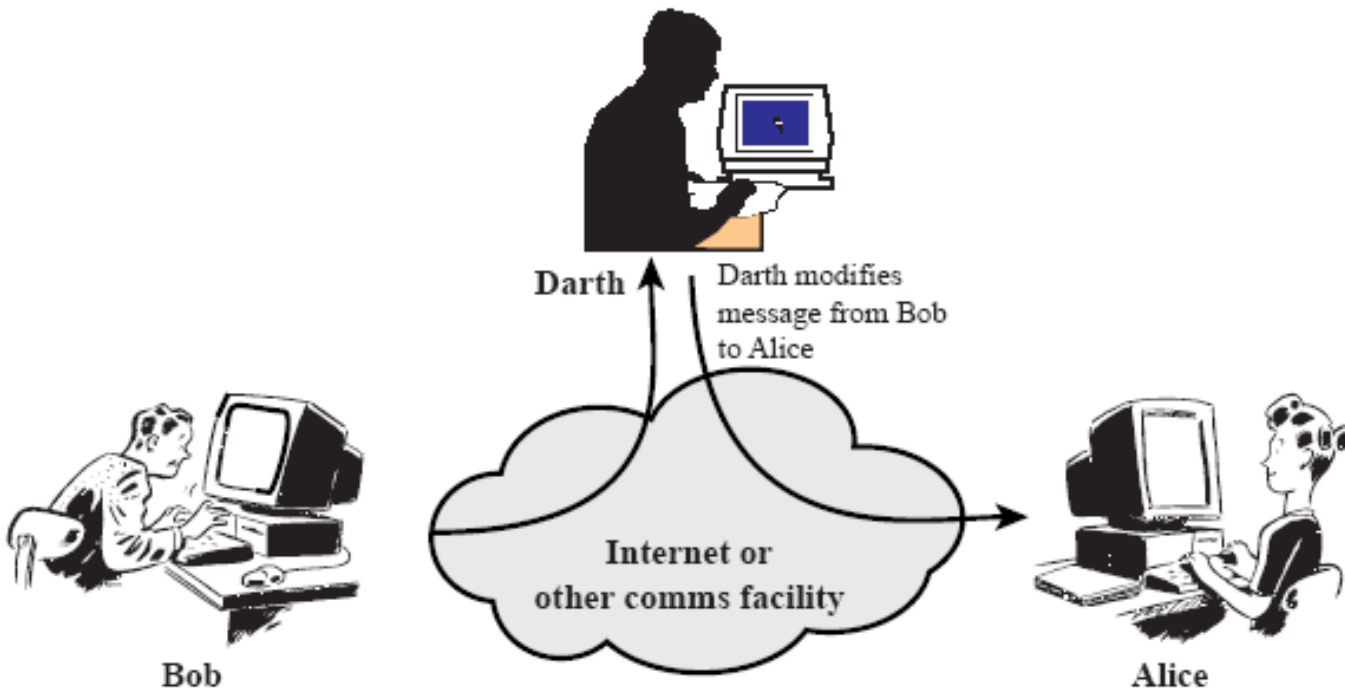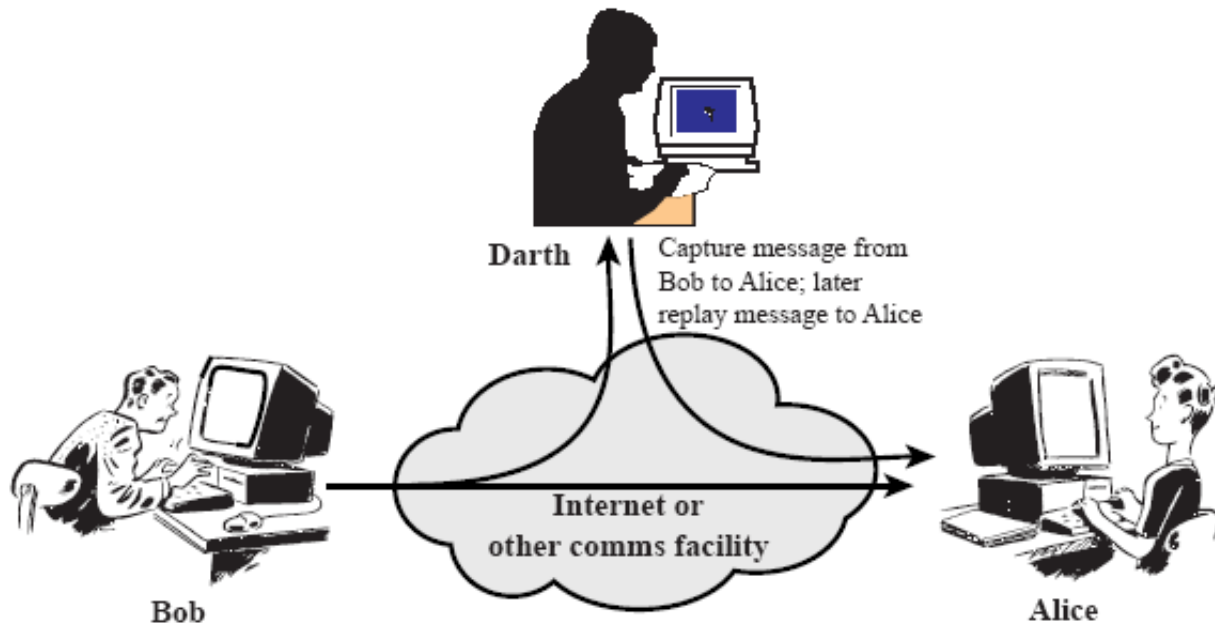
Active attacks:
Denial of Service (DoS)

Darth

Darth disrupts service
provided by server

Bob

Internet or
other comms facility

Server
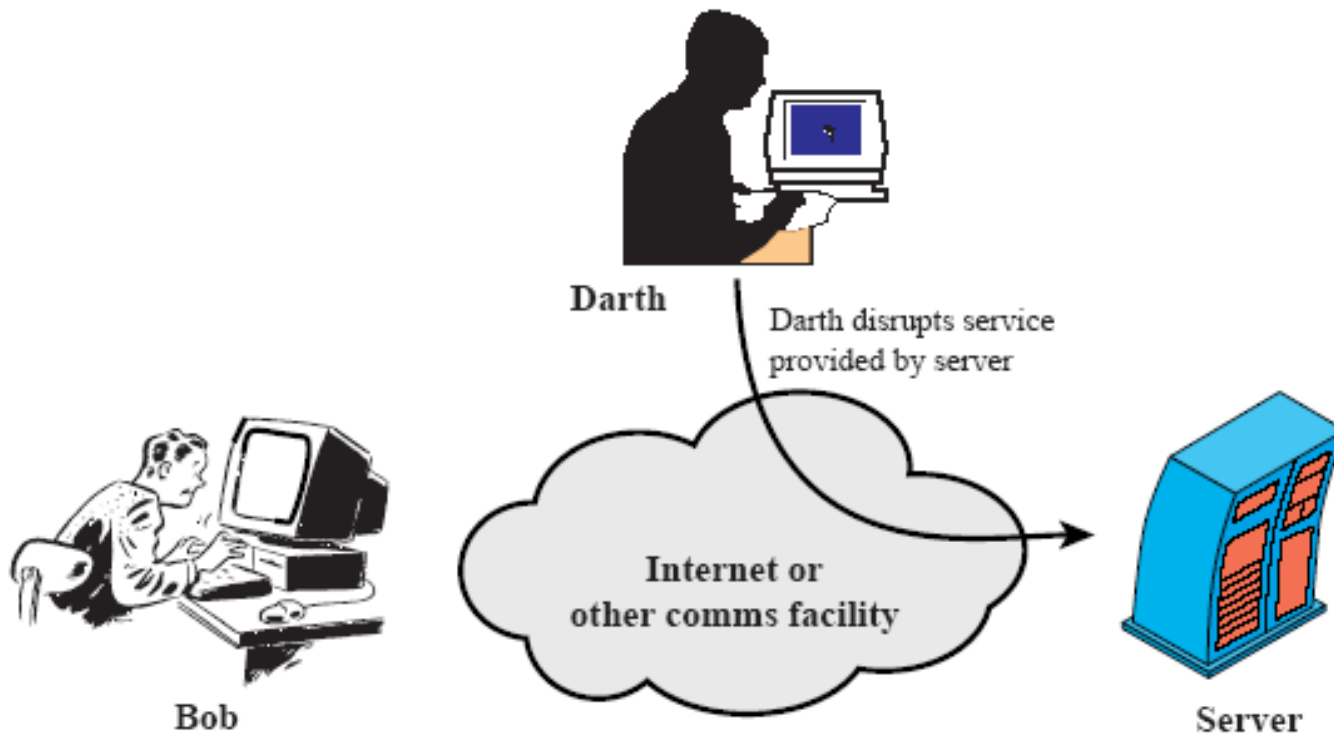
NETWORK SECURITY MODELS

Network Security Model I: Gatekeeper for access control

Information System

- Opponent
  - human (e.g., hacker)
  - software (e.g., virus, worm)

Access Channel

Gatekeeper function

- Computing resources (processor, memory, I/O)
- Data
- Processes
- Software
- Internal security controls

Example: **Firewall**
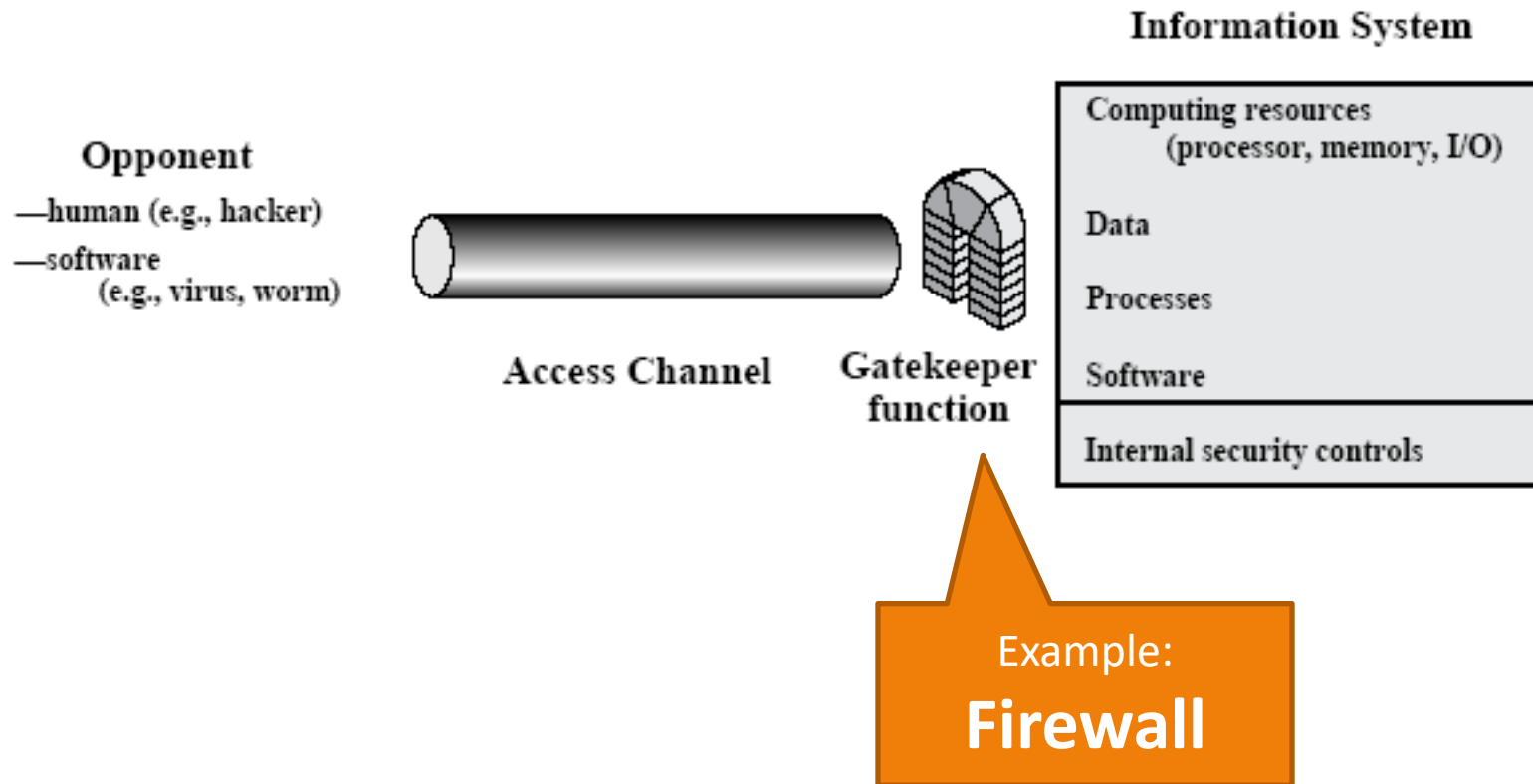
Network Security Model II: Secure communication channel

Example:
TLS