# 7 Layer OSI Model

| | Layer | Functions |
|---|---|---|
| 7 | Application | How application uses network |
| 6 | Presentation | How to represent & display data |
| 5 | Session | How to establish communication |
| 4 | Transport | How to provide reliable delivery (error checking, sequencing, etc.) |
| 3 | Network | How addresses are assigned and packets are forwarded |
| 2 | Data Link | How to organize data into frames & transmit |
| 1 | Physical | How to transmit "bits" |

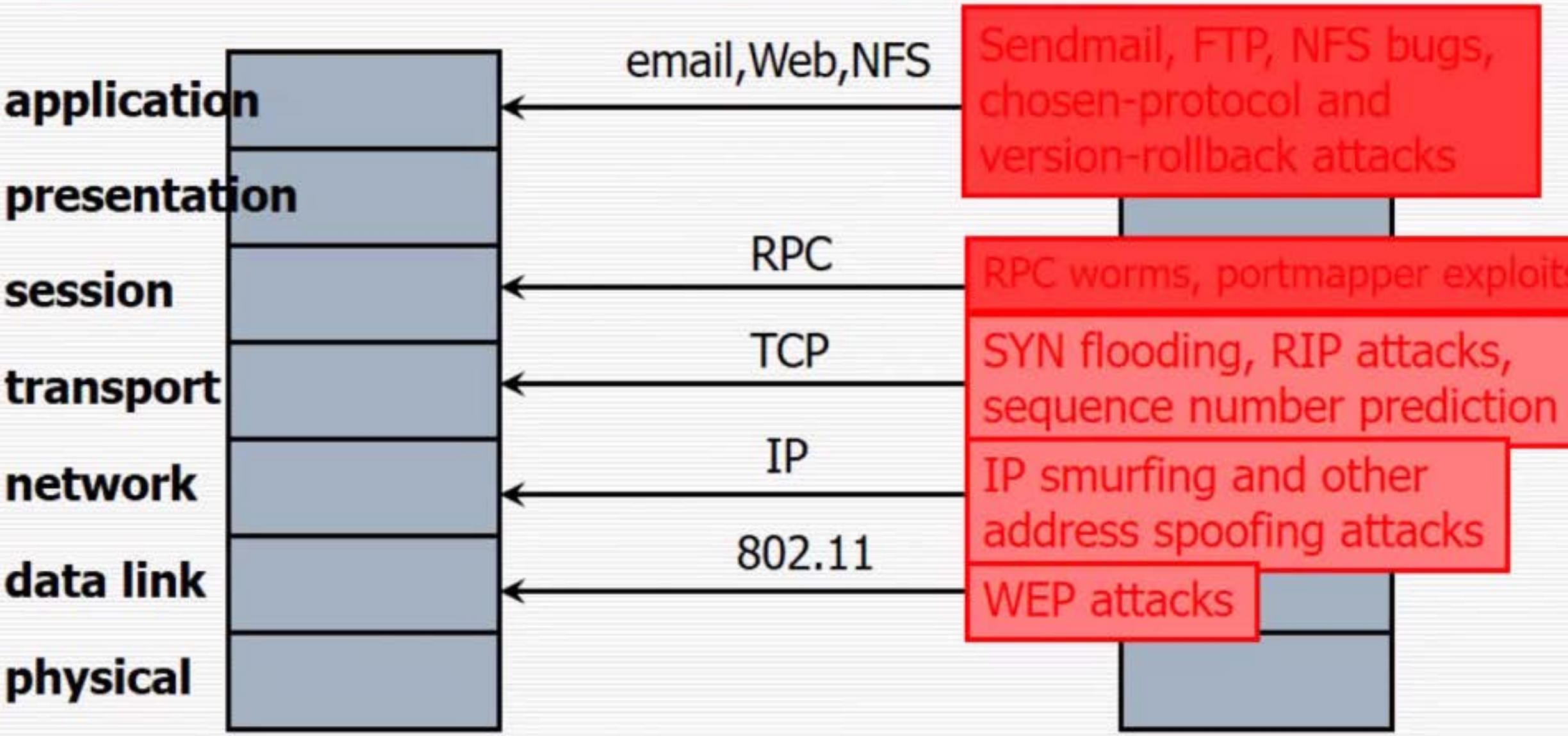
# OSI Security Architecture

- **ITU-T Recommendation X.800 Security Architecture for OSI** which defines a systematic approach to assessing and providing security
- International Telecommunications Union (ITU) is a United Nations sponsored agency that develops standards relating to telecommunications and to Open system Interconnection (**OSI**)

# 7 Layer OSI Model

| | Layer | Functions |
|---|---|---|
| 7 | Application | How application uses network |
| 6 | Presentation | How to represent & display data |
| 5 | Session | How to establish communication |
| 4 | Transport | How to provide reliable delivery (error checking, sequencing, etc.) |
| 3 | Network | How addresses are assigned and packets are forwarded |
| 2 | Data Link | How to organize data into frames & transmit |
| 1 | Physical | How to transmit "bits" |

# OSI Network Stack and Attacks (V. Shmatikov)




Only as secure as the single weakest layer...

# OSI Security Architecture

ITU-T X.800 "Security Architecture for OSI" defines a systematic way of defining and providing security requirements

- for us it provides a useful, if abstract, overview of concepts we will study
- The OSI security architecture focuses on security attacks, mechanisms and services

# Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- note terms:
  - ***threat*** – a potential for violation of security
  - ***attack*** – an assault on system security, a deliberate attempt to evade security services

# Threats and Attacks

- **Threat** - a potential for violation of security or a possible danger that might exploit a vulnerability
- **Attack** - an assault on system security- an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

# Attacks, Services and Mechanisms

- **Security Attack:** Any action (active or passive) that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms

# Security Attacks

- **Interruption:** This is an attack on availability
  - Disrupting traffic
  - Physically breaking communication line
- **Interception:** This is an attack on confidentiality
  - Overhearing, eavesdropping over a communication line

# Security Attacks (continued)

- **Modification:** This is an attack on integrity
  - Corrupting transmitted data or tampering with it before it reaches its destination
- **Fabrication:** This is an attack on authenticity
  - Faking data as if it were created by a legitimate and authentic party

# Threats

- Disclosure – unauthorized access to information
- Deception – acceptance of false data
- Disruption- interruption or prevention of correct operation
- Usurpation- unauthorized control of some part of a system

# Examples of Threats

- Snooping intercepting information ("passive" wiretapping)
- Modification or alteration of information by "active" wiretapping
- Masquerading or spoofing
- Repudiation of origin
- Delay or denial of service

# Safeguards and Vulnerabilit

- A **Safeguard** is a countermeasur protect against a threat

- A weakness in a safeguard is call **vulnerability**

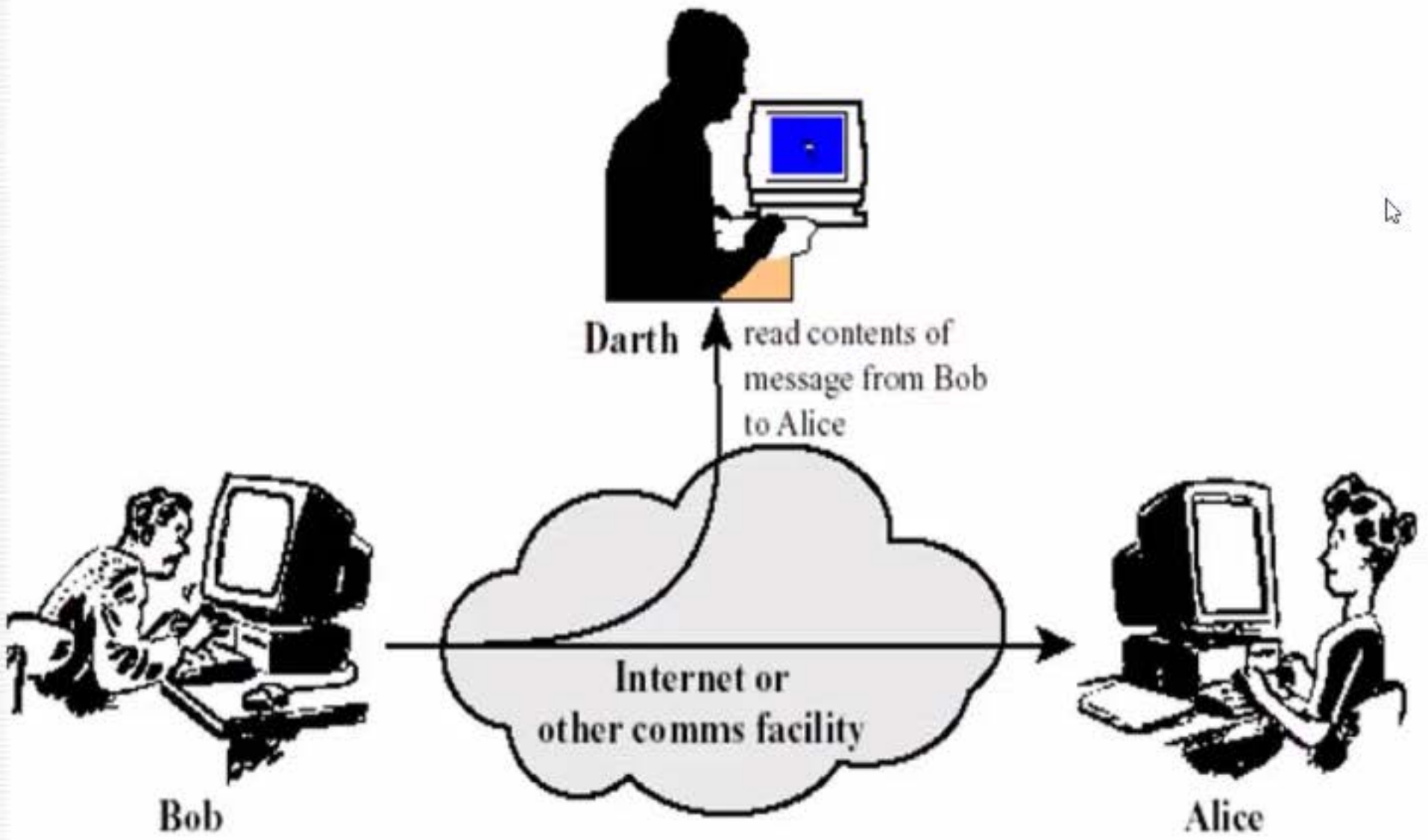
# Passive and Active Attacks

- Security attacks are usually classified as passive or active:
- **Passive**- attempts to learn or make use of information from the system, but does not affect system resources.
- **Active**- attempts to alter system resources or affect their operation.

# Passive and active attacks

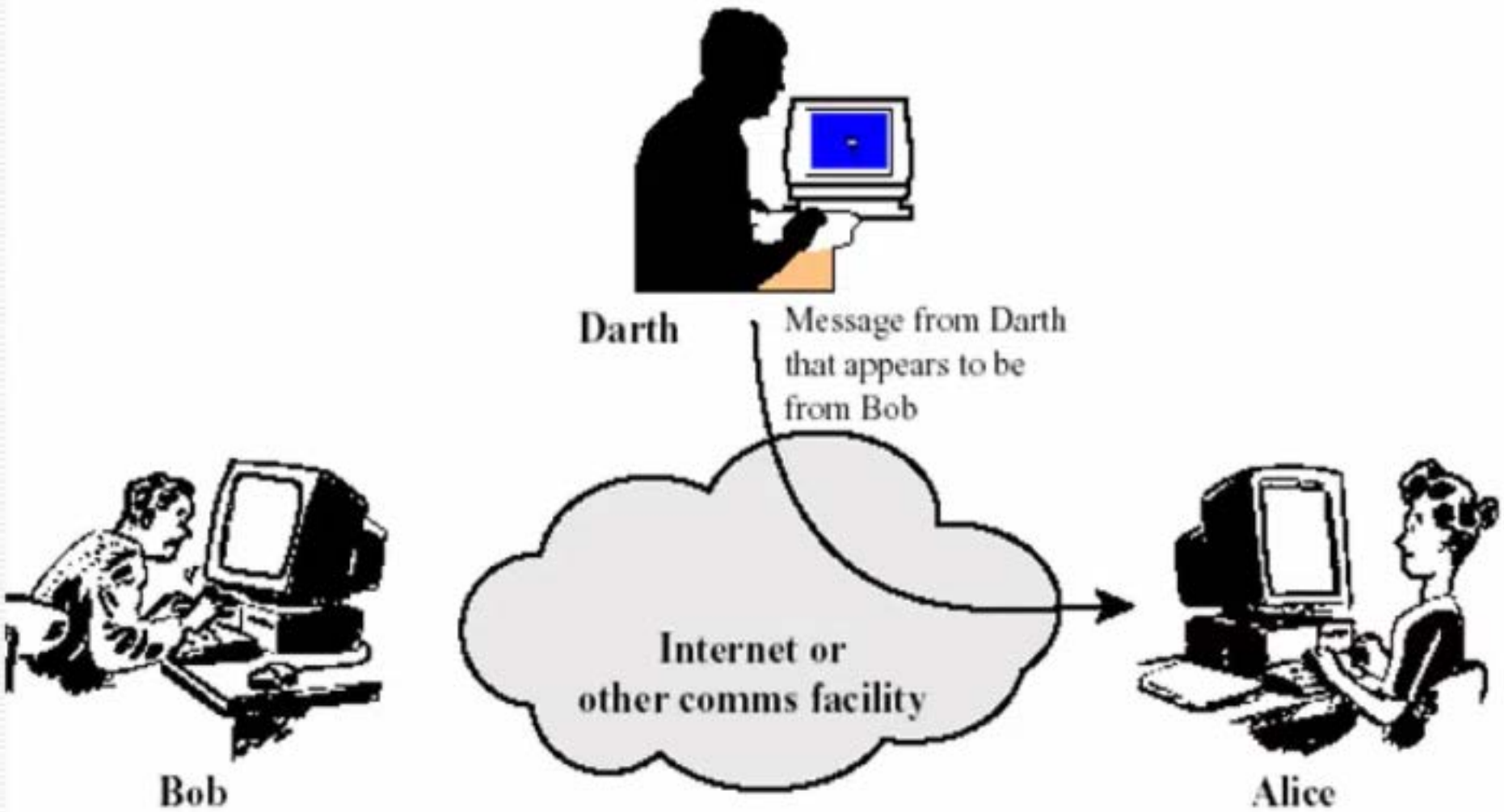
- **Passive attacks-** goal to obtain information
  - No modification of content or fabrication
  - Eavesdropping to learn contents or other information (transfer patterns, traffic flows etc.)
    - Release of message contents
    - Traffic analysis
- **Active attacks-** modification of content and/or participation in communication to
  - Impersonate legitimate parties (Masquerade)
  - Replay or retransmit
  - Modify the content in transit
  - Launch denial-of-service attacks

# Passive Attacks



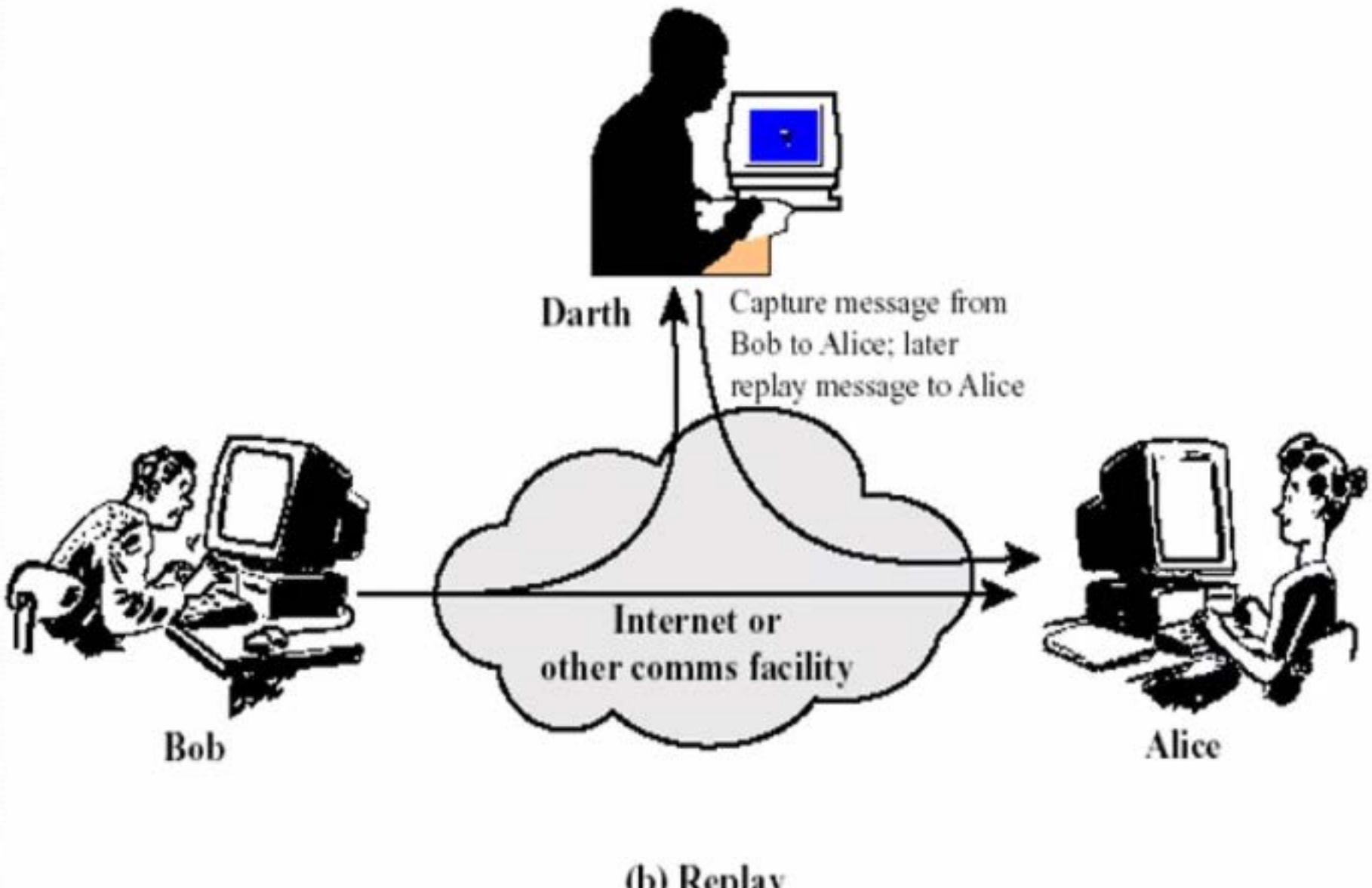

(a) Release of message contents

# Active Attacks




(a) Masquerade

# Active Attacks




(b) Replay

# Summary of Passive and Active Threats

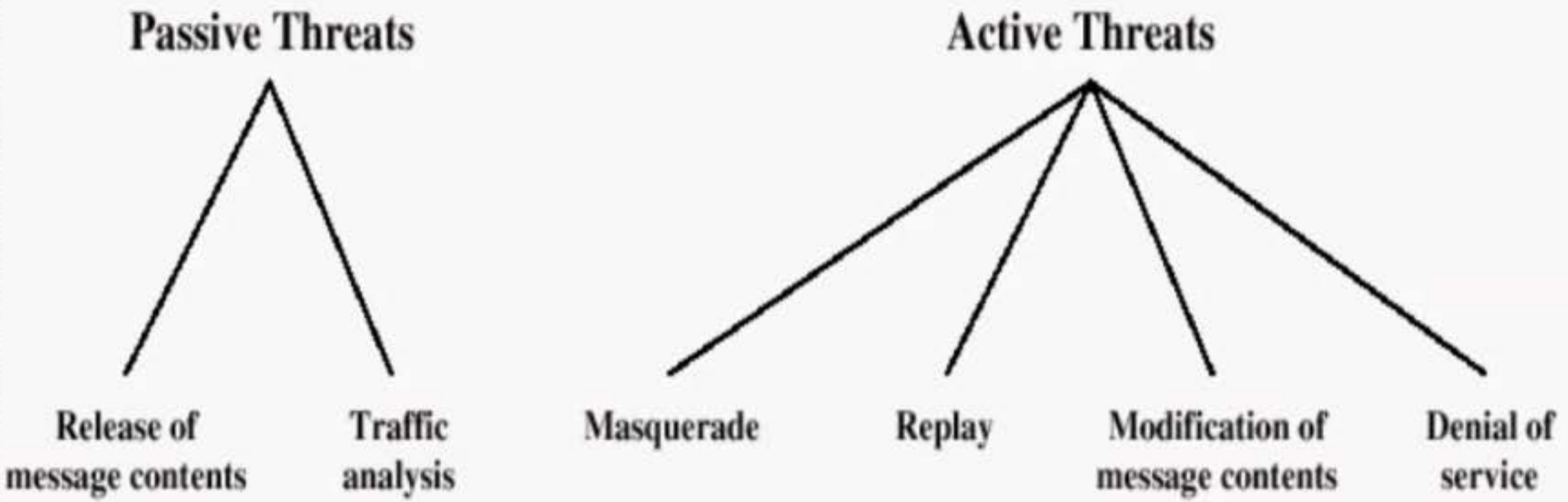



**Figure 1.2 Active and Passive Security Threats**

# Services and Mechanisms

- A **security** policy is a statement of what is and what is not allowed.
- A **security** service is a measure to address a threat
  - E.g. authenticate individuals to prevent unauthorized access
- A **security** mechanism is a means to provide a service
  - E.g. encryption, cryptographic protocols

# Security Services

- (X.800) defines a security service as a service provided by the protocol layer of a communicating system, that ensures adequate security of the systems or data transfers
- 5 Categories
  - Authentication
  - Access Control
  - Data confidentiality
  - Data Integrity
  - Nonrepudiation (and Availability)

# Security services

- RFC 2828 defines a security service as "a processing or communication service provided by a system to give a specific kind of protection to system resources"
- Security services implement security policies and are implemented by security mechanisms.

# Security Services

- Authentication (who created or sent the data)
- Access control (prevent misuse of resources)
- Confidentiality (privacy)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

# Security Services

## Examples

- **Authentication**
  - Ensuring the proper identification of entities and origins of data before communication
    - have both peer-entity & data origin authentication
- **Access control**
  - Preventing unauthorized access to system resources
- **Data confidentiality**
  - Preventing disclosure to unauthorized parties
- **Data integrity**
  - Preventing corruption of data
- **Non-repudiation**
  - Collecting proof to prevent denial of participation in transaction or communication
- **Availability**
  - Protection against denial-of-service

# Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques
- hence our focus on this topic

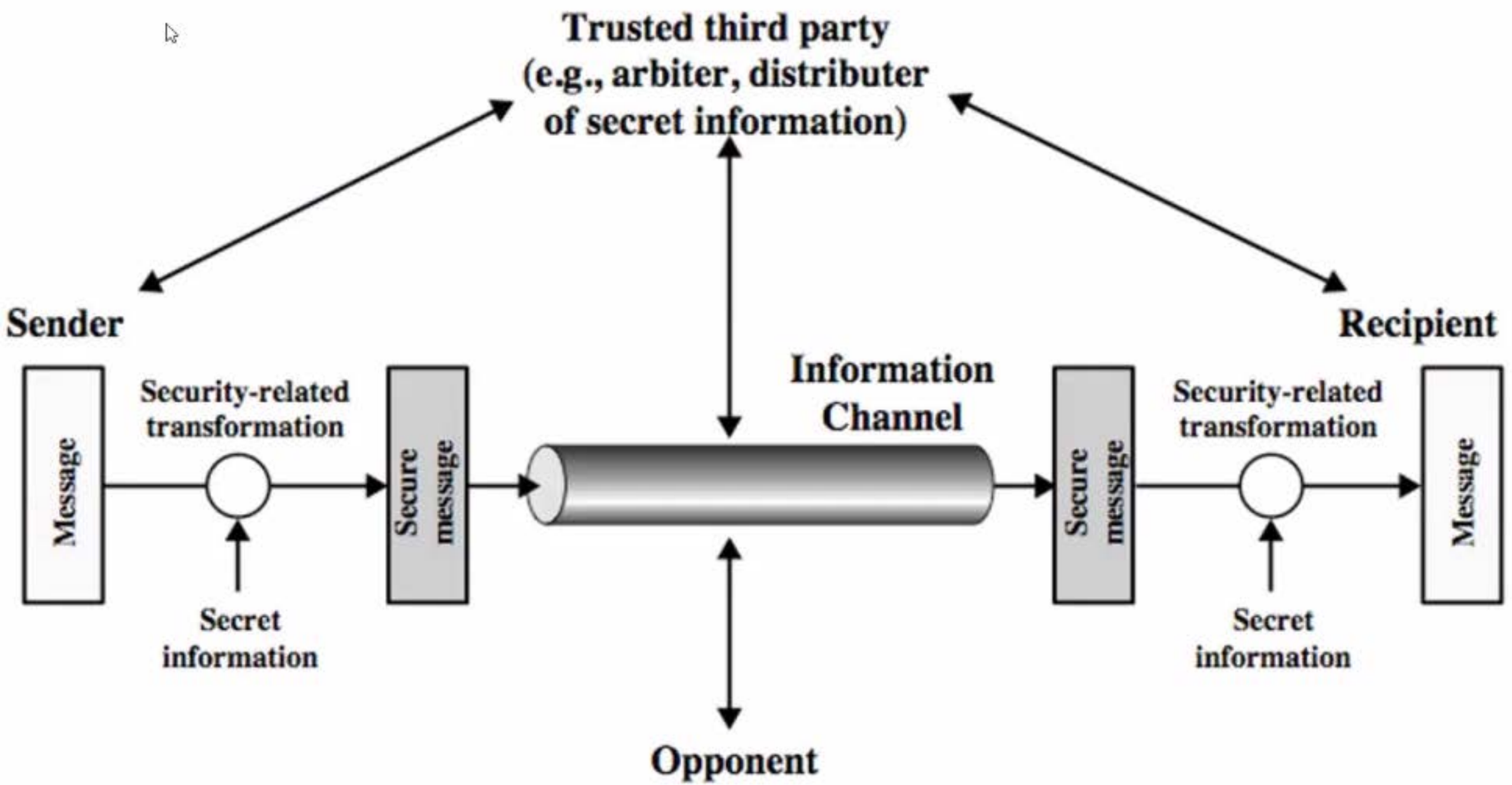
# Security Mechanisms Examples

- Two types
  - **Specific** mechanisms existing to provide certain security services
    - E.g. encryption used for authentication
    - Other examples: encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
  - **Pervasive** mechanisms which are general mechanisms incorporated into the system and not specific to a service
    - E.g. security audit trail
    - Other examples: trusted functionality, security labels, event detection, security audit trails, security

# Model for Network Security

- Basic tasks
  - Design an algorithm that opponent cannot defeat
  - Generate the secret information to be used with the algorithm
  - Develop methods for distributing secret information
  - Specify a protocol to be used
- May need a trusted third party to assist

# Model for Network Security



# Security Models

- Part 1 and 2 of this book concentrate on the model for Network Security
- There are other security related situations that do not fit into this model and are covered in Part 3.
- A Network Access Security Model reflects the concern for protecting an information system from unwanted access, for example by hackers or malware (malicious programs).

# General Security Access Model

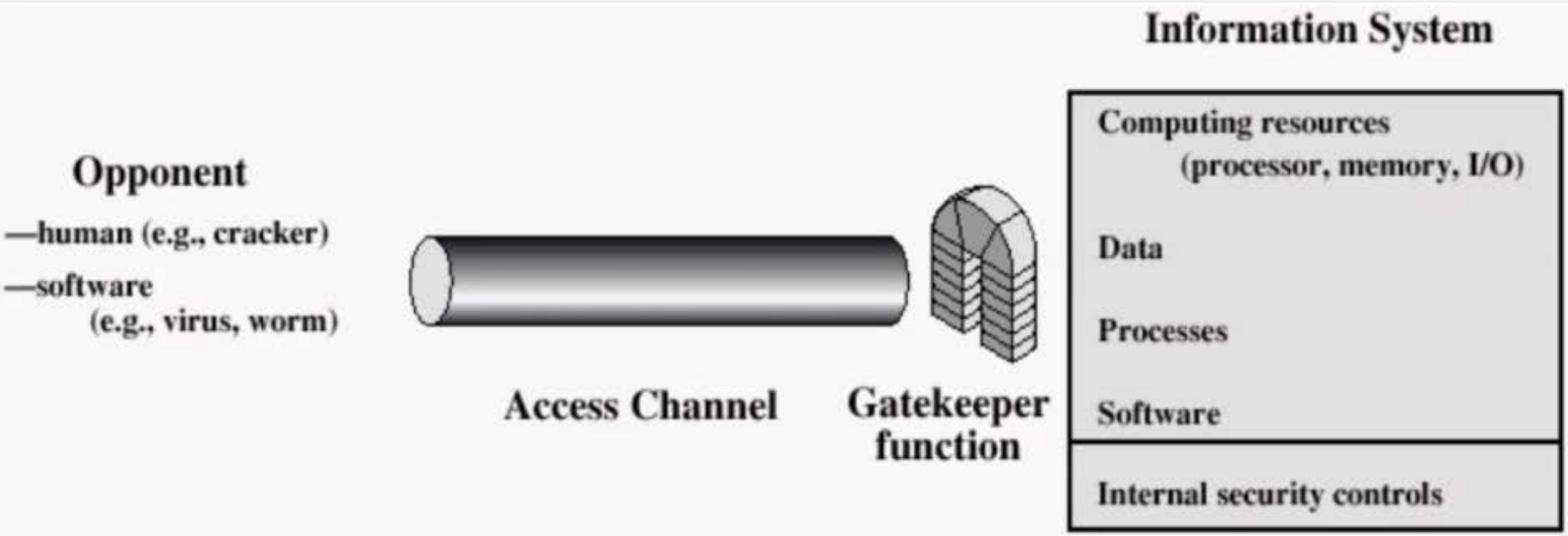



**Figure 1.4 Network Access Security Model**

# Model for Network Access Security

- Security mechanisms for controlling unwanted access fall into two categories.
- Using this model requires us to:
  1. select appropriate gatekeeper functions to identify users (for example, password-based login procedures)
  2. implement security controls to ensure only authorised users access designated information or resources (for example, monitor activities and analyze stored information to detect the presence of intruders

？ 如何设计osi安全体系结构
？？ 考虑的要素及其逻辑关系
？？？ 安全威胁/风险
？？？？ 安全策略
？？？？？ 安全机制
？？？？？？ 安全服务