Network Security
EE 5733 / CS 5713

Prof Dr Amir Qayyum

M. A. Jinnah University, Islamabad

Introduction (Chapter 1)

- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of defense
- A model for Internetwork security

The Art of War

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—***The Art of War,*** **Sun Tzu**

Background

- Information security requirements have changed in recent times
  - Security was traditionally provided by physical and administrative mechanisms
- Computer use requires automated tools to protect files and other stored information
- Use of networks and communication links requires measures to protect data during transmission

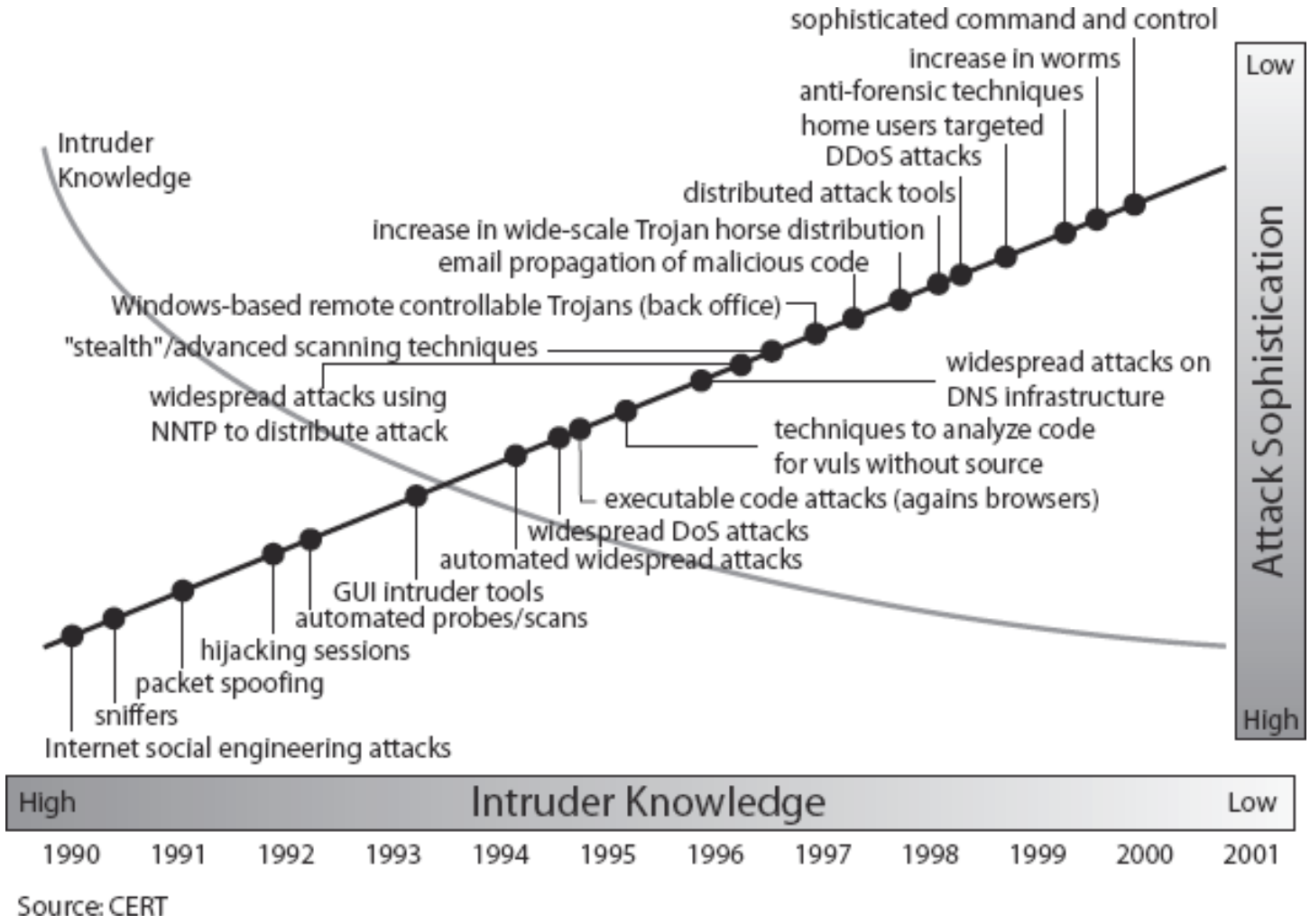
Definitions

- Computer Security
  - Generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - Measures to protect data during its transmission
- Internet Security
  - Measures to protect data during its transmission over a collection of interconnected networks

Emphasis of this Course

- Emphasis is on **internet security**
- Consists of measures to deter, prevent, detect and correct security violations
  - That involve the transmission of information
- Requirements seem straightforward, but …
  - The mechanisms used to meet them can be quite complex …

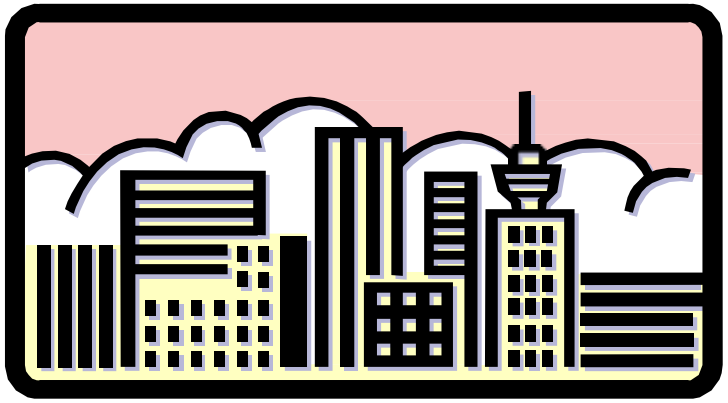
Security Trends



Source: CERT

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- Defines a systematic way of defining and providing security requirements
- Provides a useful, if abstract, overview of concepts we will study



Aspects of Security

- Need systematic way to define requirements
- Consider three aspects of information security:
  - Security attack
  - Security mechanism
  - Security service
- Consider in reverse order

Security Attack

- Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Have a wide range of attacks
-
- Note: often *threat* & *attack* mean same

Security Attacks

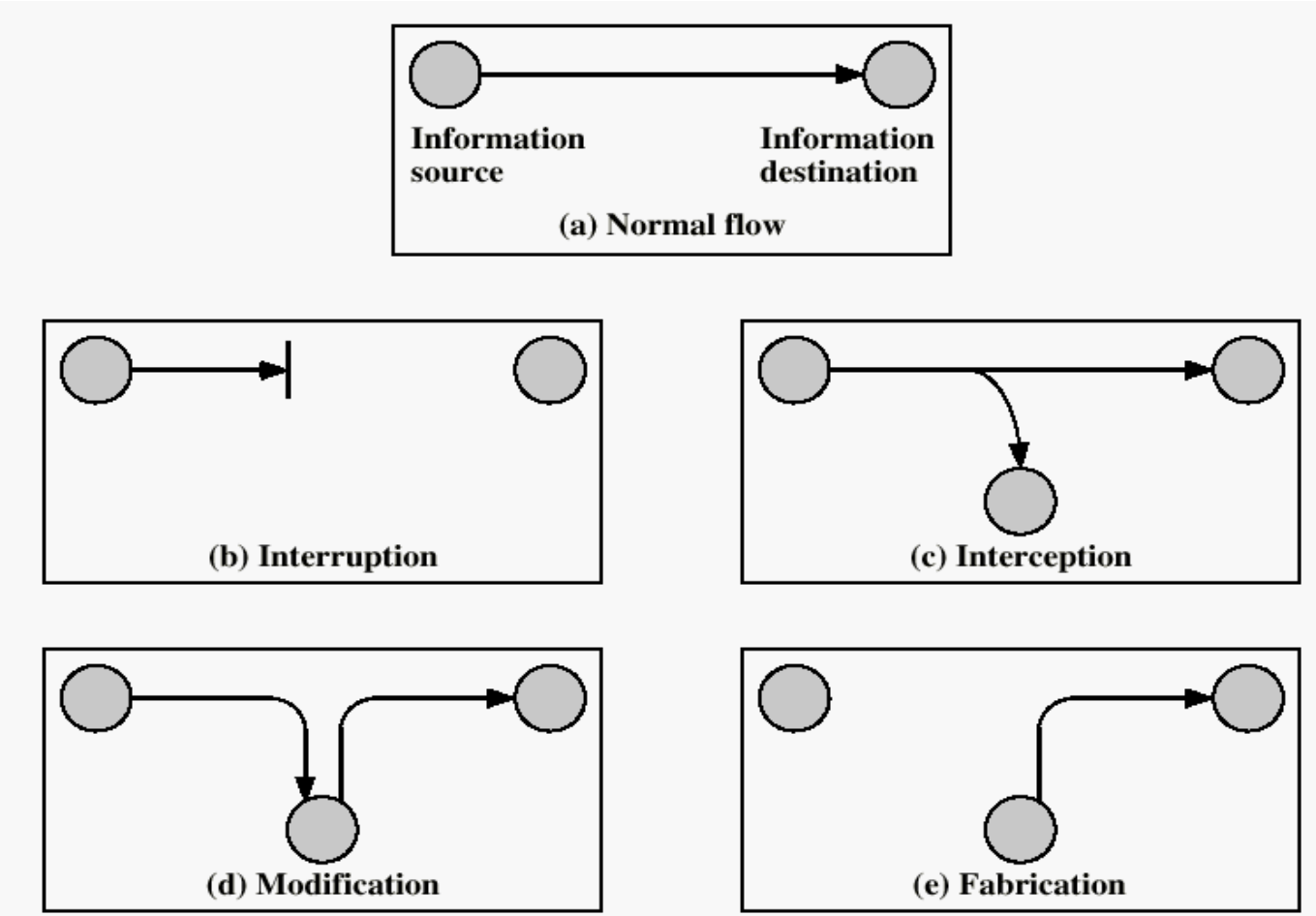


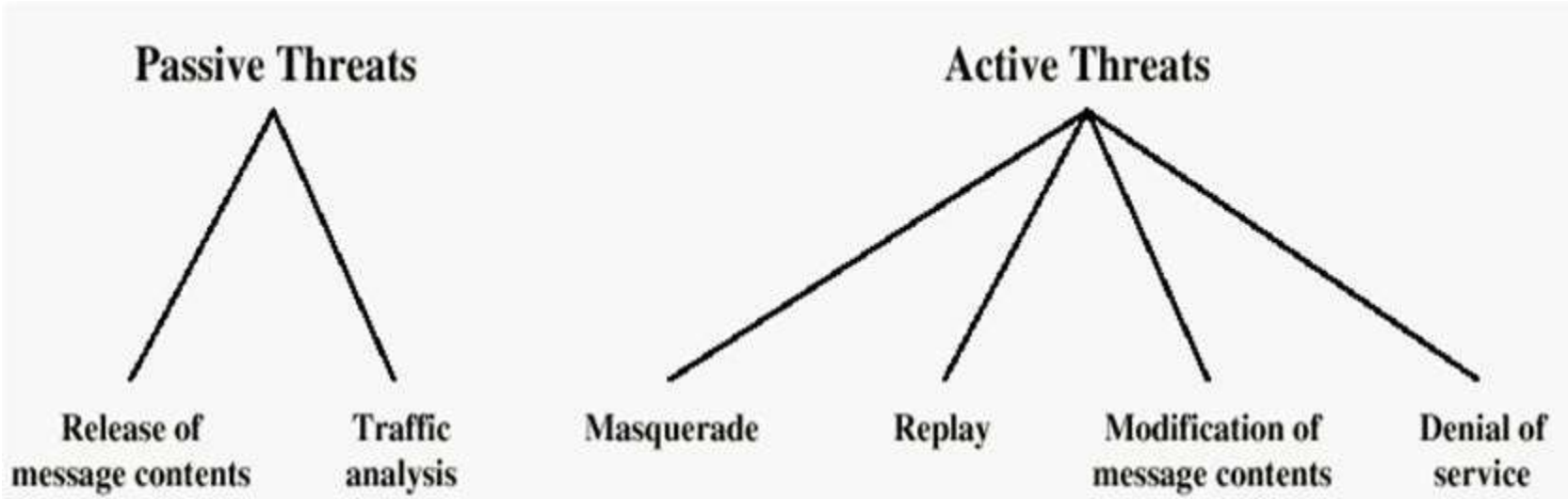
Figure 1.1 Security Threats

Security Attacks

- Interruption
  - Attack on availability
- Interception
  - Attack on confidentiality
- Modification
  - Attack on integrity
- Fabrication
  - Attack on authenticity

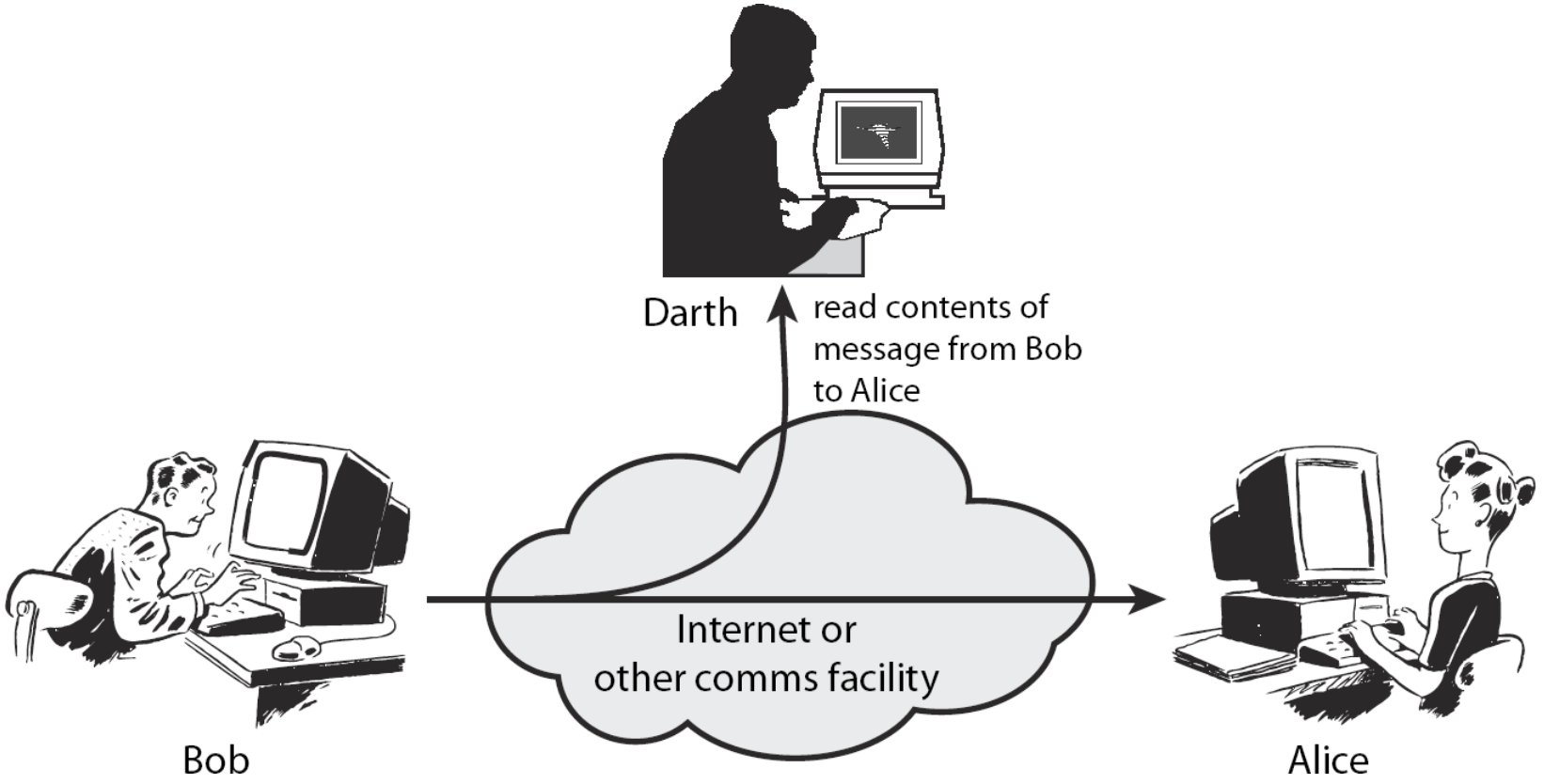
Classify Security Attacks

- **Passive attacks** – eavesdropping on, or monitoring of, transmissions
  - obtaining message contents, or
  - monitoring traffic flows
- **Active attacks** – modification of data stream
  - masquerading of one entity as some other
  - replaying previous messages
  - modifying messages in transit
  - denial of service

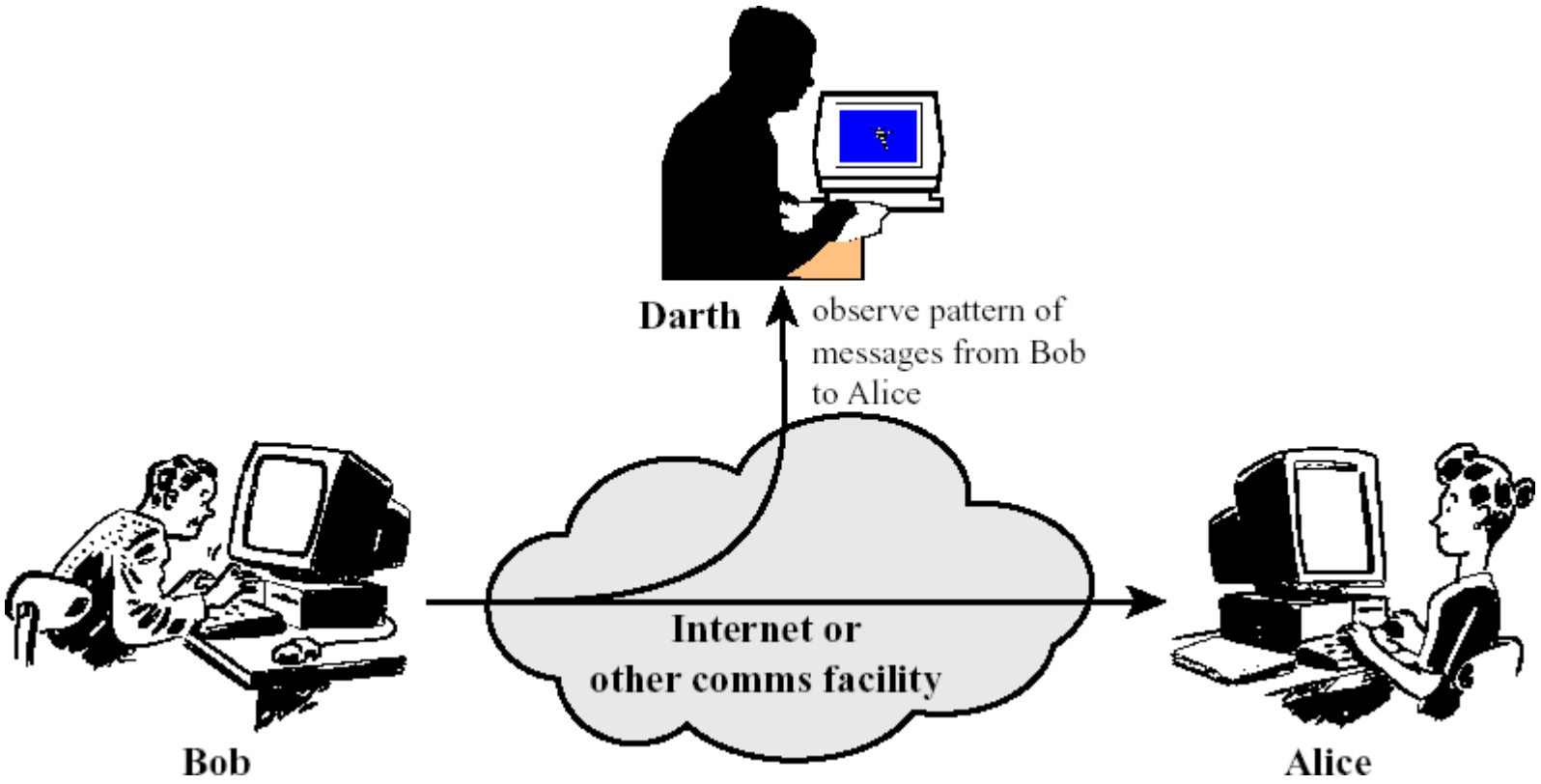


Active and Passive Security Threats

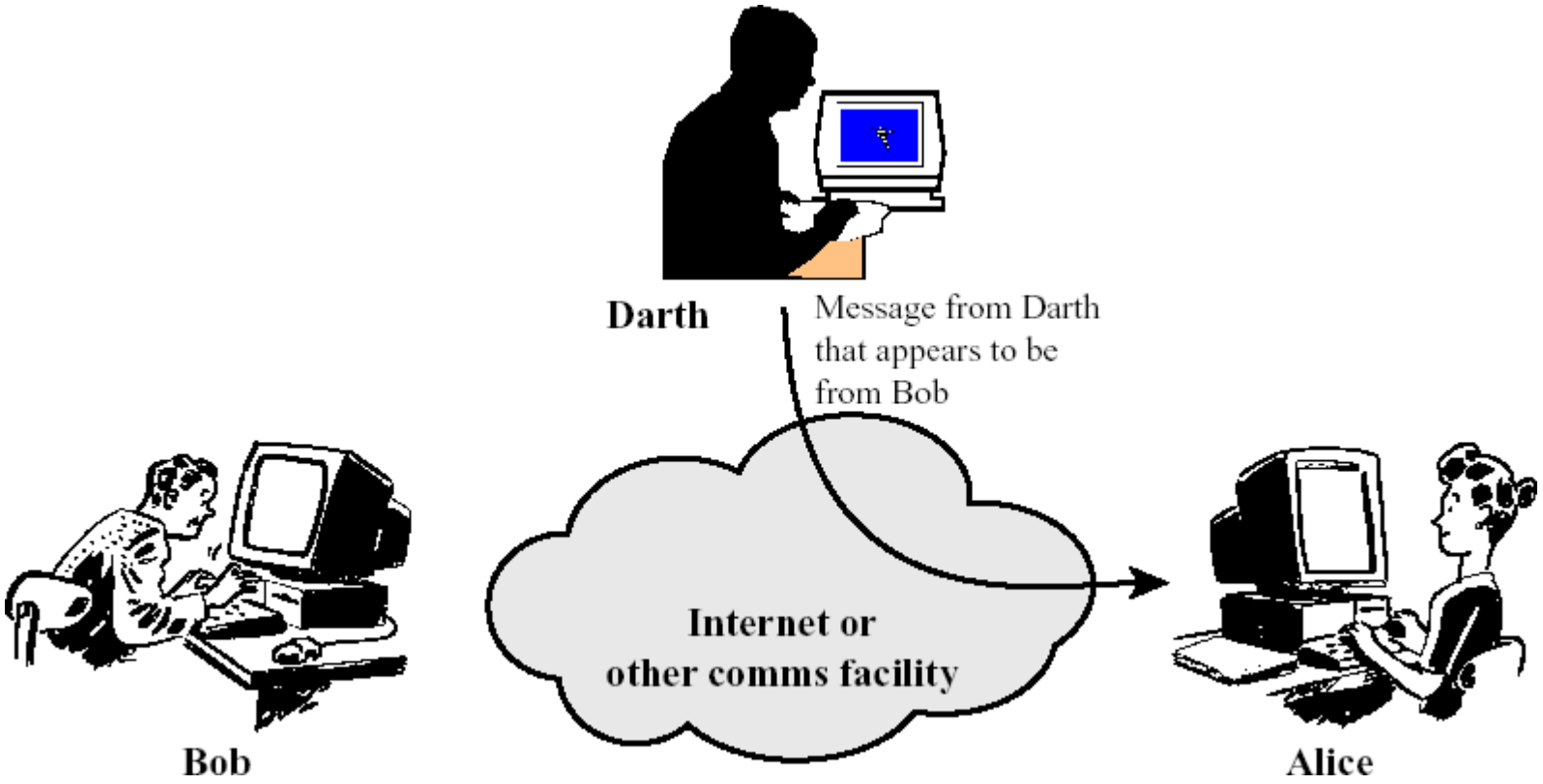
Passive Attacks: Release of Message Contents



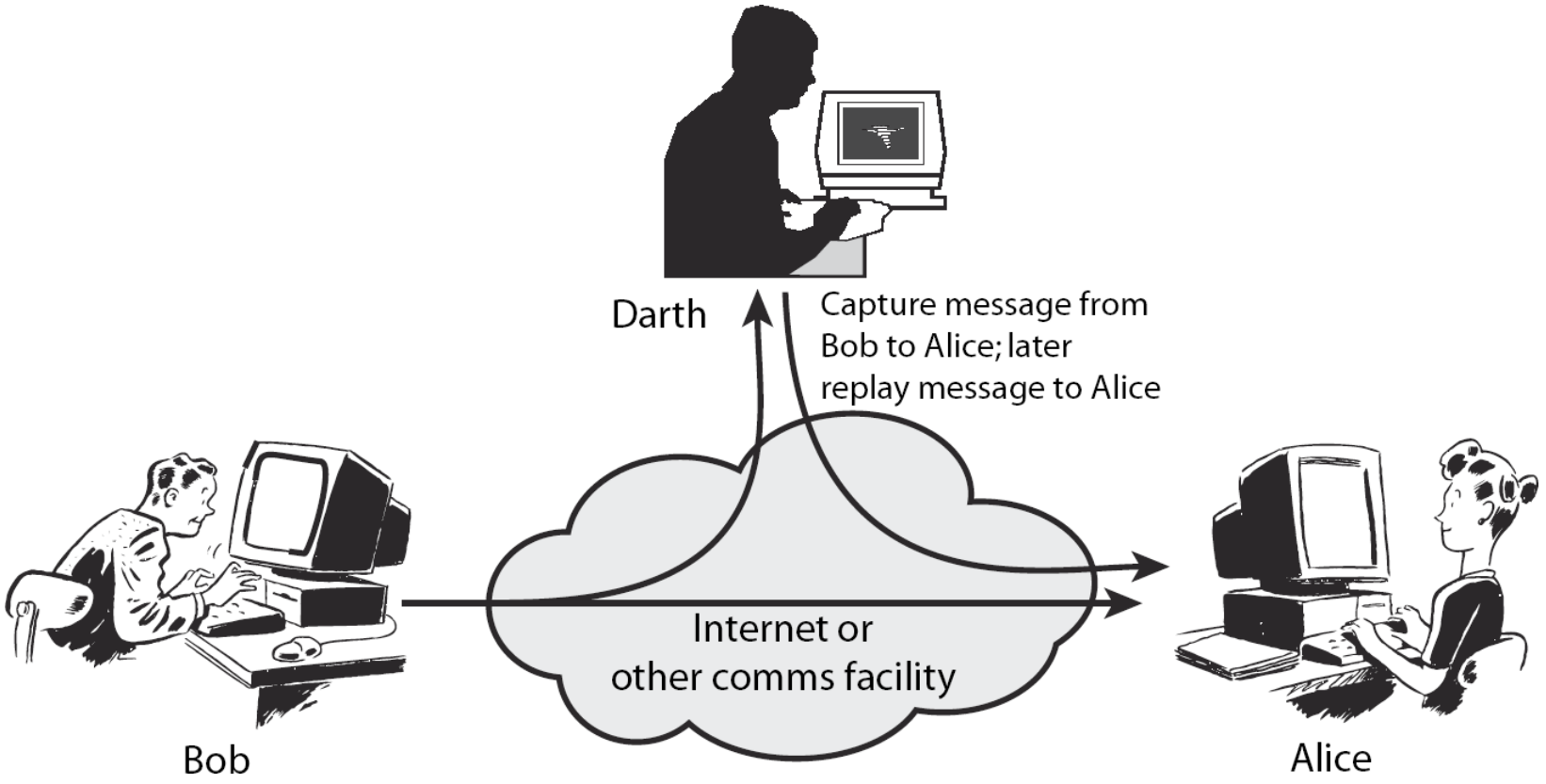
Passive Attacks: Traffic Analysis



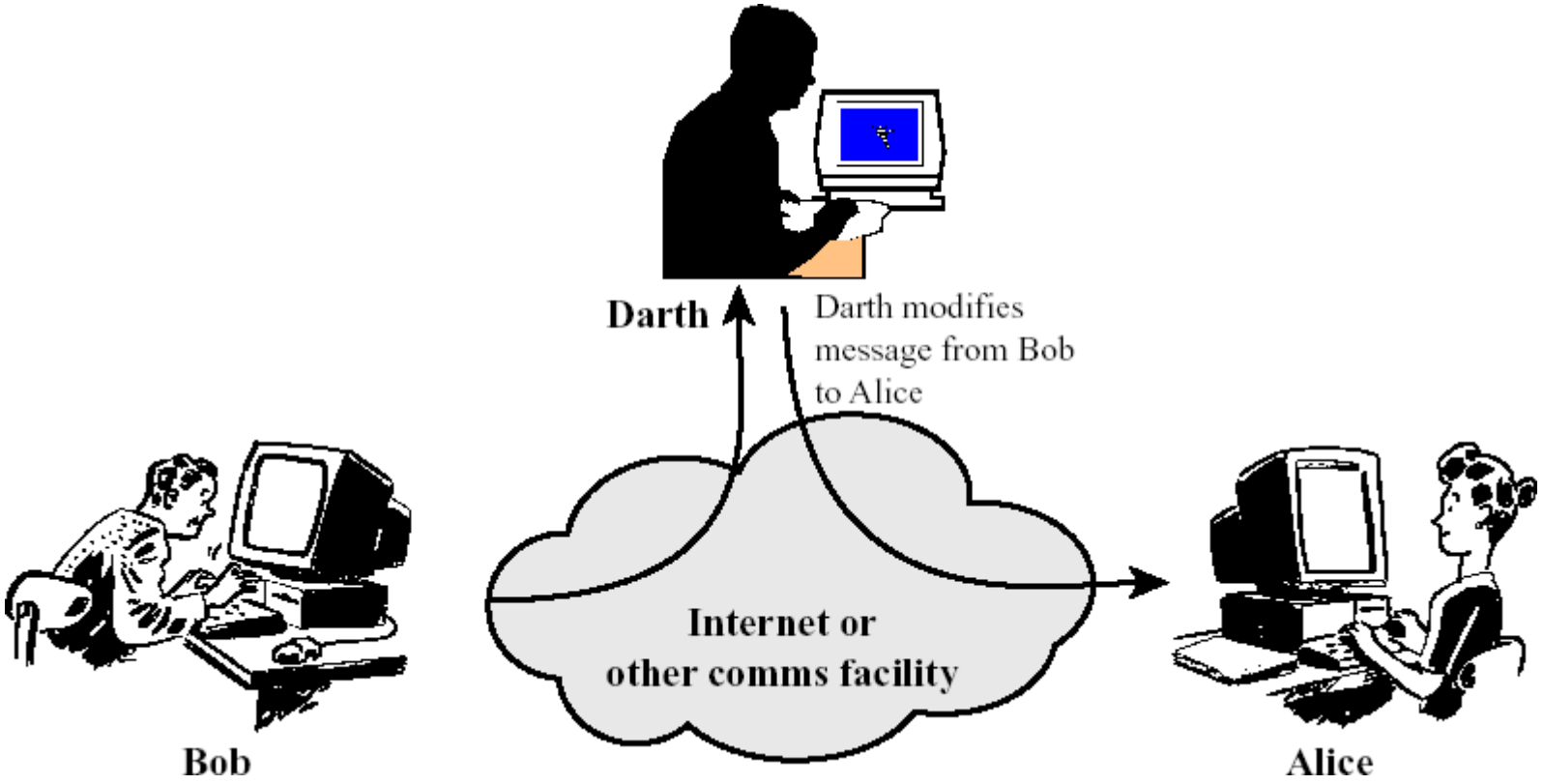
Active Attacks: Masquerade



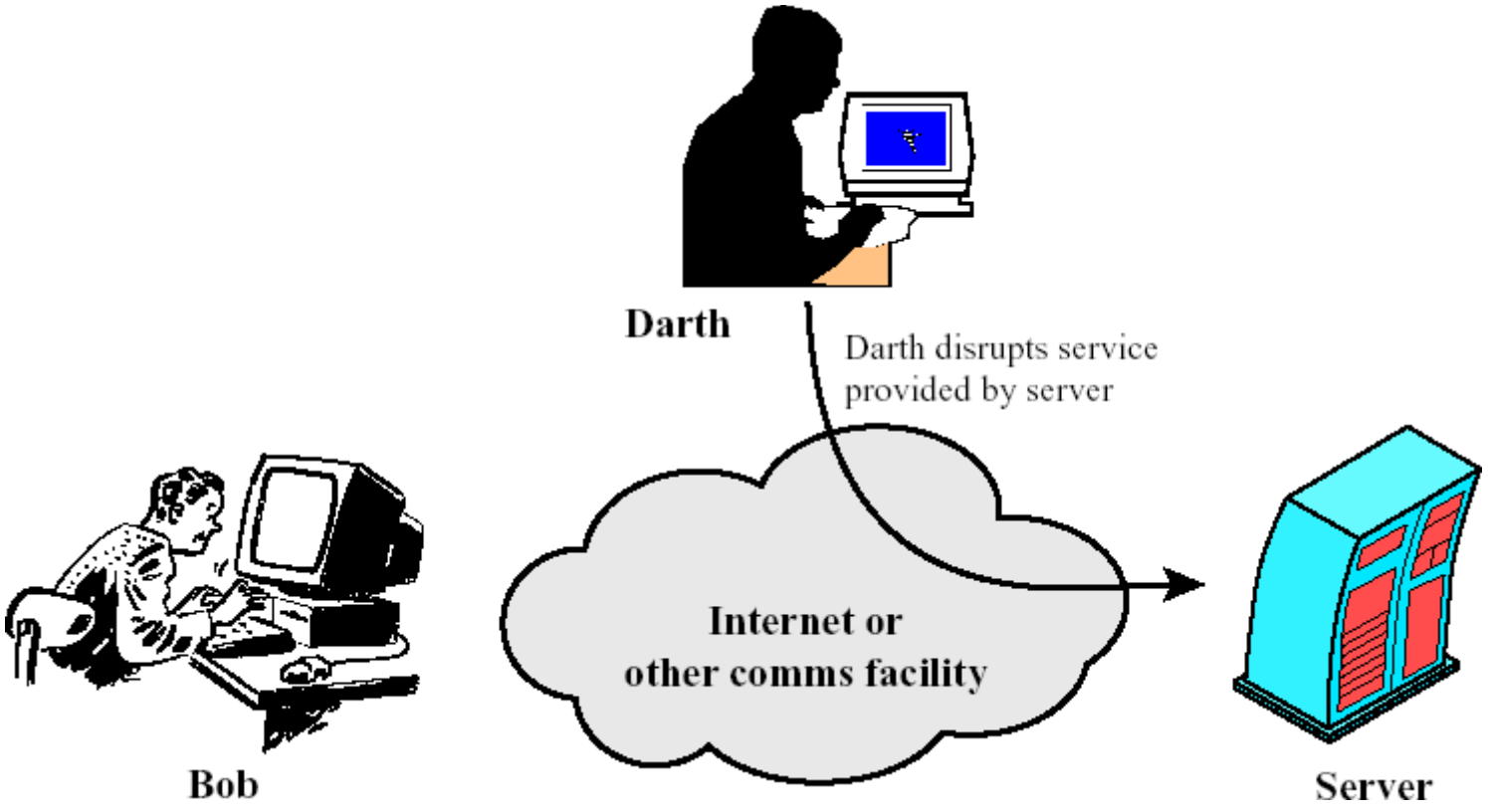
Active Attacks: Replay



Active Attacks: Modification of Messages



Active Attacks: Denial of Service



Security Service

- Intended to counter security attacks
- Enhance security of data processing systems and information transfers of an organization
  - Using one or more security mechanisms
- Often replicates functions normally associated with physical documents
  - E.g., have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800

  "A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828

  "A processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

- Data Confidentiality (privacy)
  - Protection of data from unauthorized disclosure
- Authentication (who created or sent data)
  - Assurance that the communicating entity is the one claimed
- Data Integrity (no alteration)
  - Assurance that data received is as sent by an authorized entity

Security Services (X.800)

- Access Control (misuse of resources)
  - Prevention of the unauthorized use of a resource
- Non-Repudiation (trust on transaction)
  - Protection against denial by one of the parties in a communication
- Availability (permanence, non-erasure)
  - Denial of service attacks
  - Viruses that delete files, etc.

Security Mechanism

- A 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**

Security Mechanisms (X.800)

1. Encipherment
   - Converting data into form that is not readable
2. Digital signatures
   - To check authenticity and integrity of data
3. Access controls
   - Enforcing access rights to resources
4. Data integrity

Security Mechanisms (X.800)

5. Authentication exchange
6. Traffic padding
   - Insertion of bits to frustrate traffic analysis
7. Routing control
   - Selection of secure routes
8. Notarization
   - Use of trusted third party for data excha

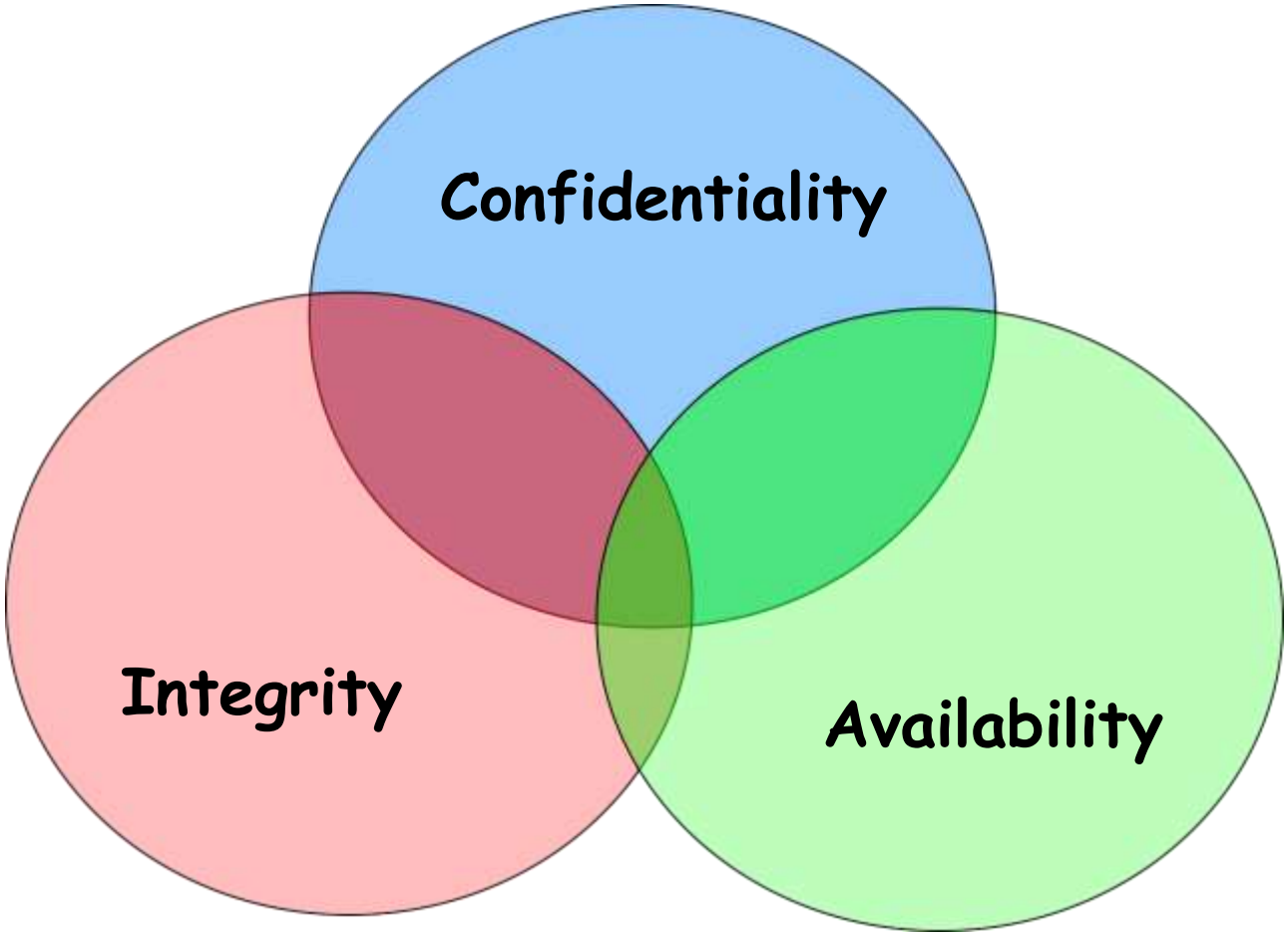
Pervasive Security Mechanisms (X.800)

- Trusted functionality
  - Perceived to be correct with respect to some criteria
- Security labels
- Event detection
  - Detection of security relevant events
- Security audit trails
- Security recovery

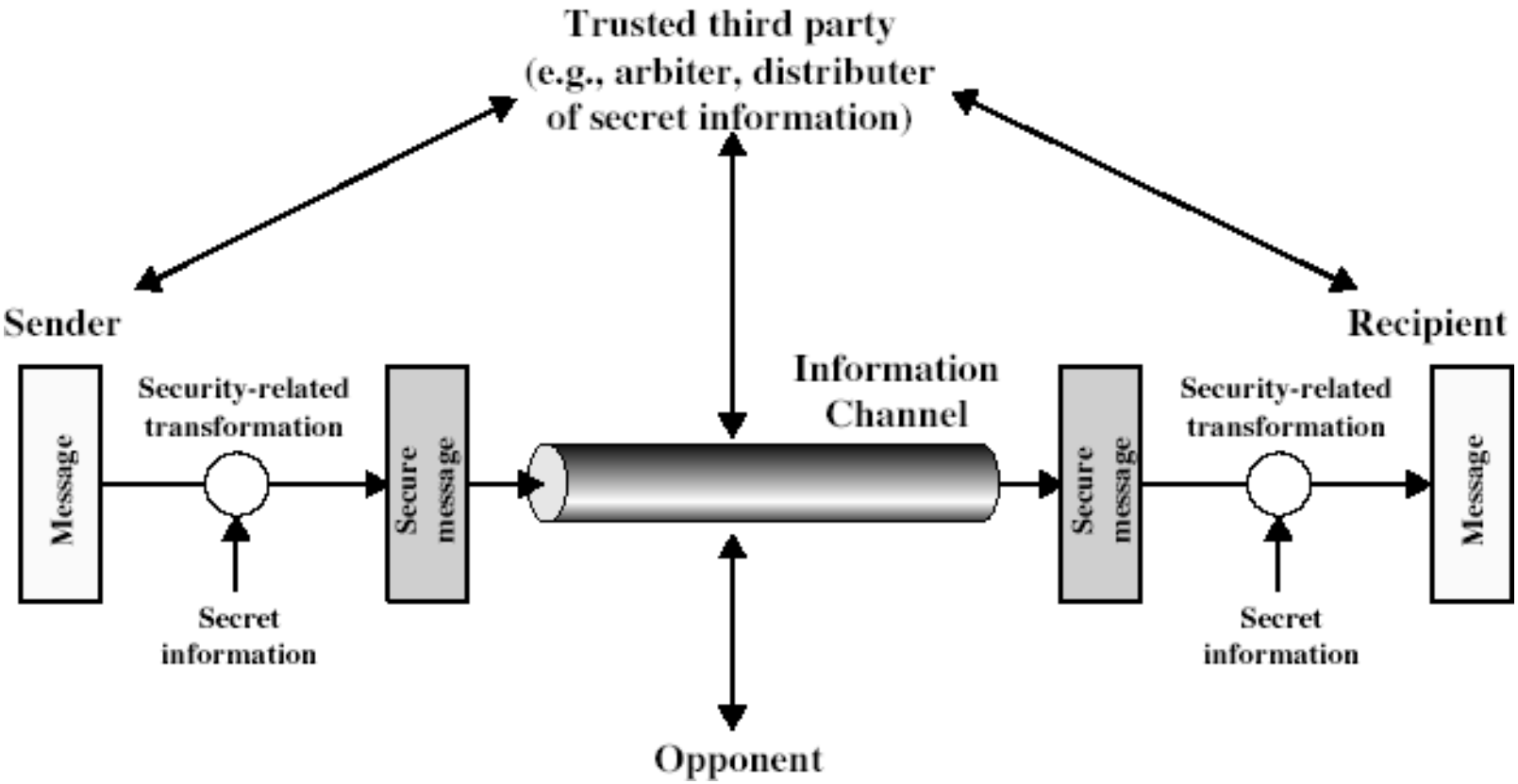
Summary

- Security Attack
  - Any action that compromises 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 security of data processing systems and information transfers; makes use of one or more security mechanisms

Security Goals



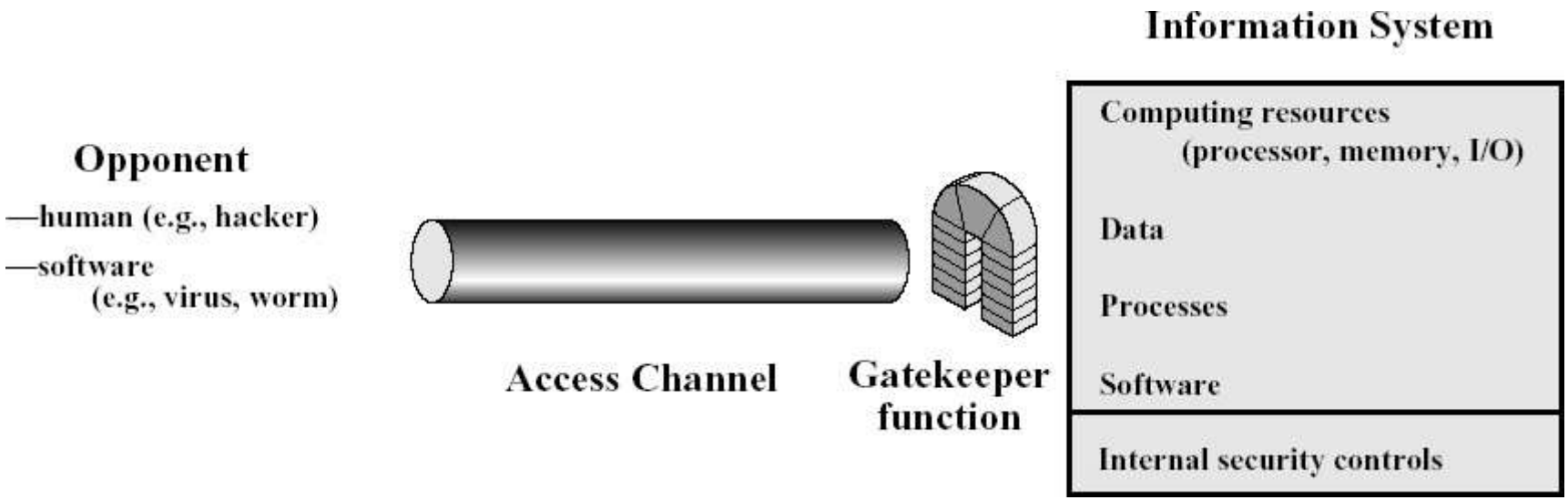
Model for Network Security



Model for Network Security

- Using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate secret information (keys) used by the algorithm
  3. Develop methods to distribute and share the secret information
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- Using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorised users access designated information or resources
- Trusted computer systems can be used to implement this model

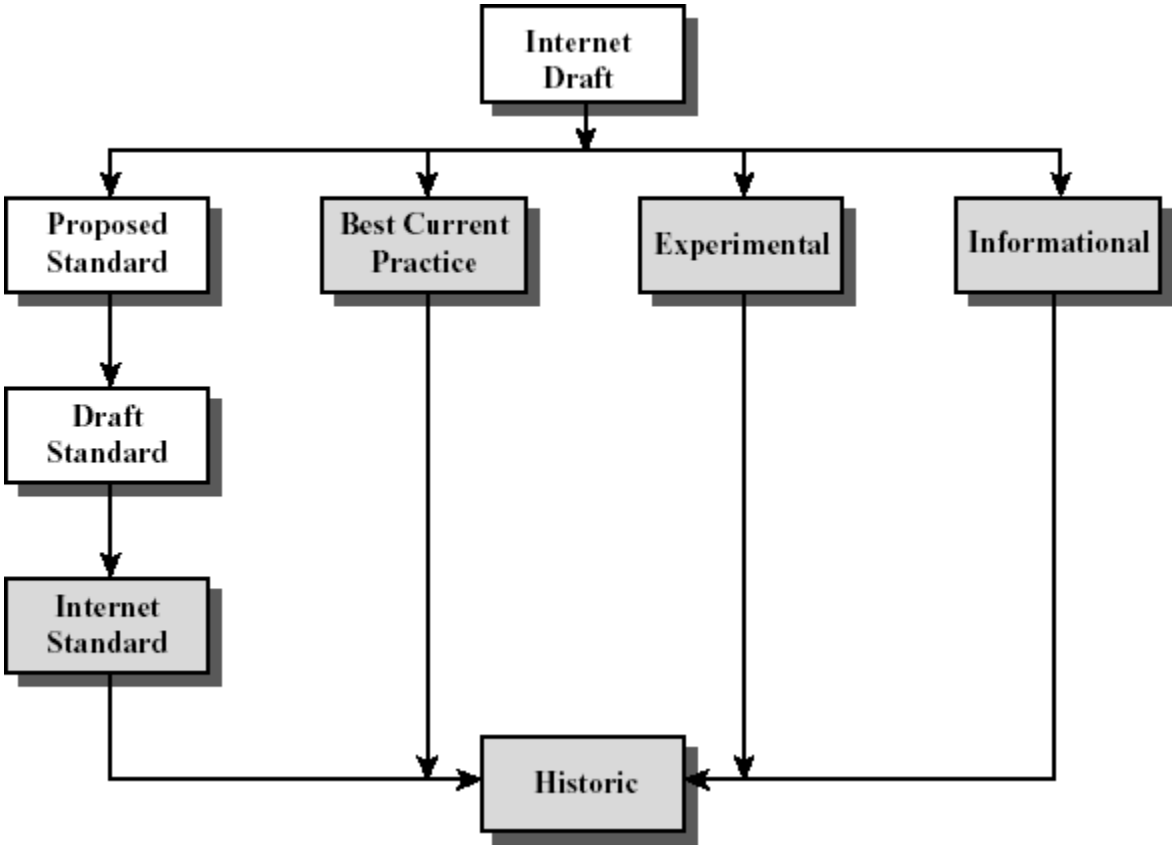
Methods of Defense

- Policies
  - Frequent changes of passwords
- Encryption
- Software Controls
  - Access limitations in a data base
  - Operating system protects each user from other user
- Hardware Controls (smartcard)
- Physical Controls

Internet standards and RFCs

- The Internet society
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)

Internet RFC Publication Process



Summary

- Have considered:
  - Definitions for:
    - Computer, network and internet security
- X.800 standard
- Security attacks, services, mechanisms
- Models for network (access) security

Any question ?