Network Security

Prepared By:

Sajid Majeed

Course Staff

- **Instructor:**
  - Sajid Majeed
    - Email:sajid.majeed@fuuast.edu.pk

Course Schedule

- Lectures
- Assignments
  -
- Quizes
  -
- Midterm exam
  -
- Final exam
  -

Grading Policy

- Assignments 10%
  - Late assignments are **not accepted**
- Quizes 10%
- Midterm exam 20%
- Final exam 60%

Academic Honesty

- Your work in this class **must be your own**
- If students are found to have collaborated excessively or to have cheated (e.g. by copying or sharing answers during an examination), all involved will at a minimum receive grades of 0 for the first infraction
- Further infractions will result in failure in the course.

Course Material

Reference books

- No single textbook covers the whole course!

- Lot of research papers!
  - Many will be made available
- RFCs and Internet drafts
  - Related to Network security protocols
- Web resources
  - Tutorials, white papers, reports, etc.

Course Information

- Pre-requisites
  - Computer Networks course
    - You are assumed to have good knowledge of TCP/IP protocol suite
  - Operating Systems
  - Basic understanding of programming languages

Course Contents

- Introduction to network security
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- II. NETWORK SECURITY APPLICATIONS
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
  - Network Management Security (SNMP)

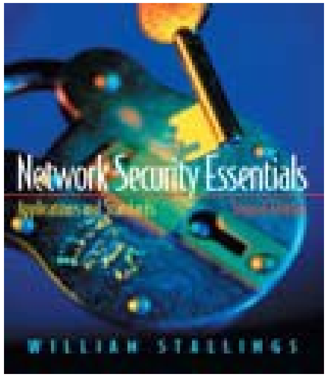
Course Contents

- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems
  - Operating System Security

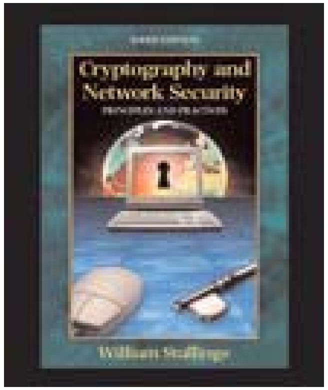
Textbooks

- One of the following three books is required for this course:

- William Stallings, Network Security Essentials

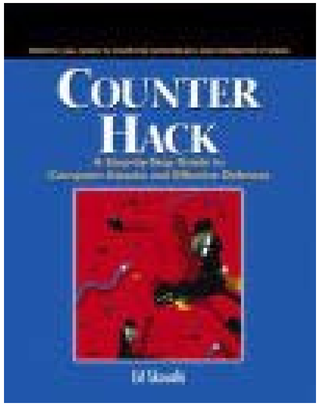


- William Stallings, Cryptography and Network Security: Principles and Practice



Textbooks

- Ed Skoudis, Counter Hack: A Step by Step Guide to Computer Attacks and Defenses



Expectations

What do you want (or expect) to learn from
this class ?

Expectations

- This class **IS** **about** …
  - Network security principles and concepts
  - Cryptography, its use, principles and major algorithms
  - Message authentication and encryption techniques
  - Security of network "system"
  - Operating system security
  - Security practices and applications

Expectations

- This class **IS NOT about …**
  - Survey of existing protocol standards
  - Survey of loopholes in current protocols
  - How to hack the network of KICSIT!
  - Tools and tips to breach Internet security
  - How you can become a good hacker …

Expectations

We will learn

Why and How

networks are made secure

Outline

- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security
- Internet standards and RFCs

Background

- Information Security requirements have changed in recent times
- Traditionally provided by physical and administrative mechanisms
- Computer use requires automated tools to protect files and other stored information
- Use of networks and communications 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 their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Aim of this Course

- Our focus 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 …

Services, Mechanisms, Attacks

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

Security Service

- Is something that enhances the security of the data processing systems and the information transfers of an organization
- Intended to counter security attacks
- Make use of one or more security mechanisms to provide the service
- Replicate functions normally associated with physical documents e.g.
  - have signatures or dates
  - need protection from disclosure, tampering, or destruction
  - be notarized or witnessed
  - be recorded or licensed

Security Mechanism

- A mechanism that is designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all functions required
- However one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
- Hence our focus is on this area

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
- Can focus on generic types of attacks
  - Note: often threat & attack mean same

Security Attacks

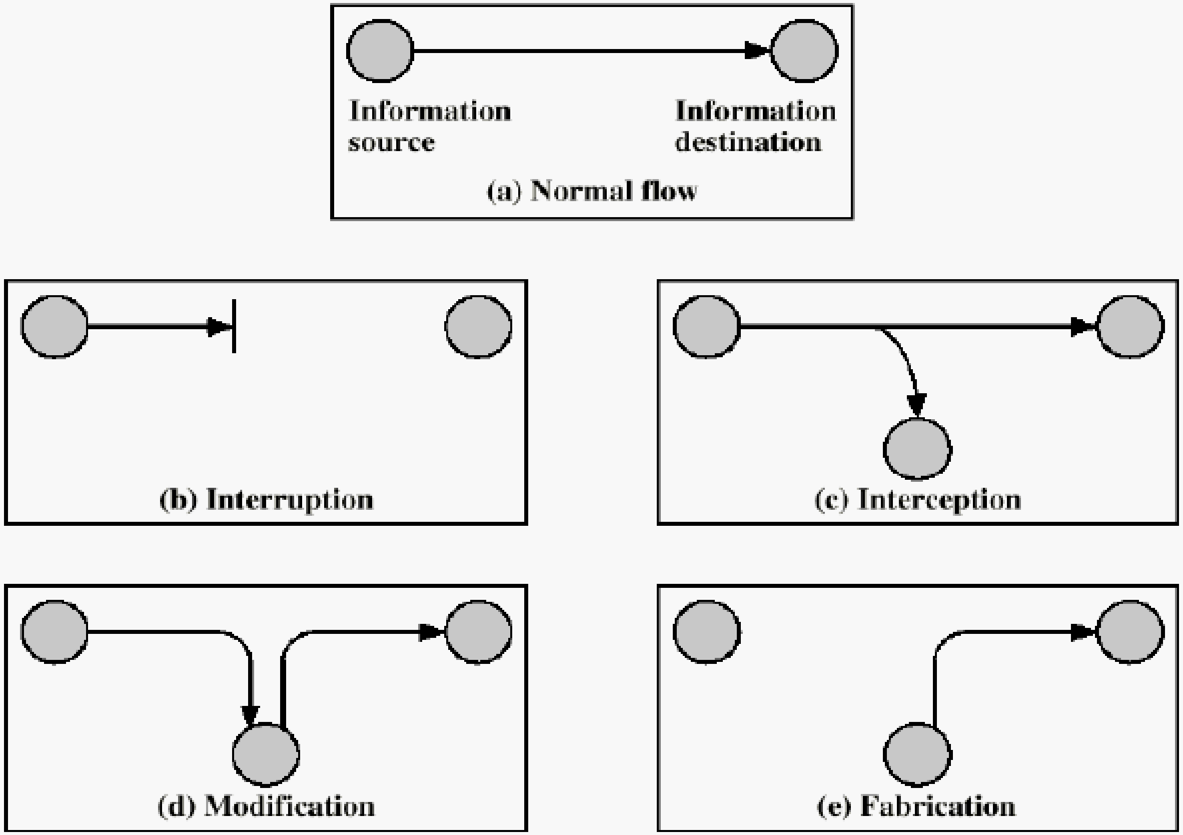
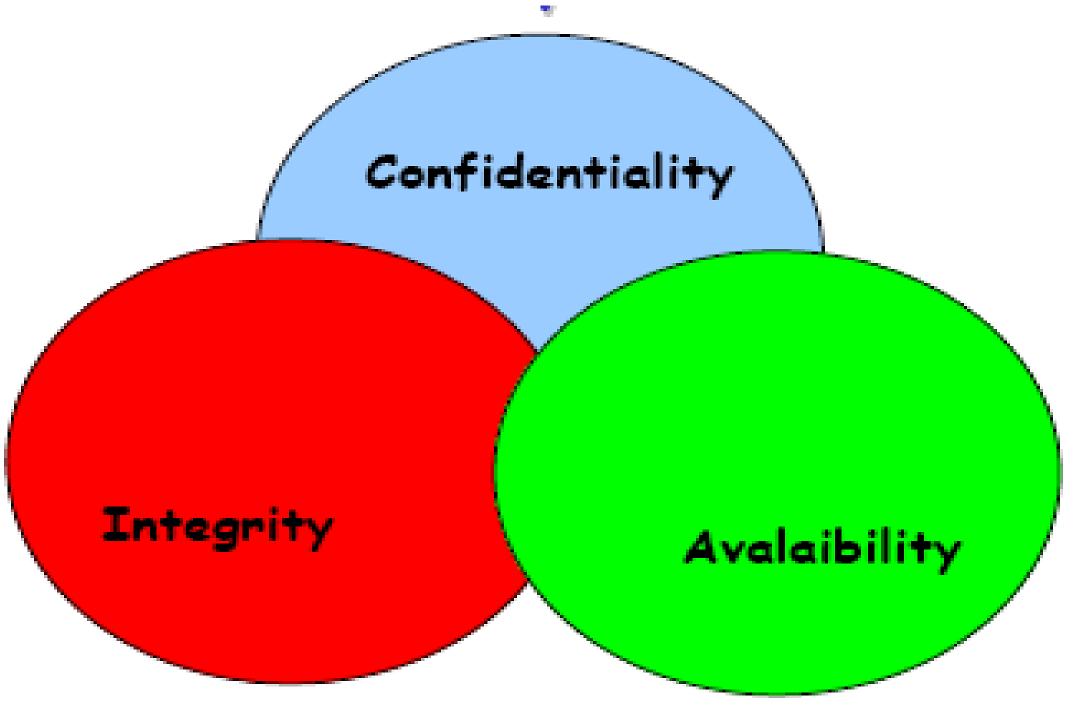


Figure 1.1 Security Threats

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Security Goals



Summary: Attacks, Services and Mechanisms

- **Security Attack:** Any action 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

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

Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources

Security Services (X.800)

- X.800 defines security services in 5 major categories
  - ***Authentication*** - assurance that the communicating entity is the one claimed
  - ***Access Control*** - prevention of the unauthorized use of a resource
  - **Data Confidentiality** –protection of data from unauthorized disclosure
  - **Data Integrity** - assurance that data received is as sent by an authorized entity
  - **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Services

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

– Denial of Service Attacks

– Virus that deletes files

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment: Converting data into form that is not readable
  - Digital signatures: To check authenticity and integrity of data
  - Access controls: Enforcing access rights to resources
  - Data integrity
  - Authentication exchange
  - Traffic padding: Insertion of bits to frustrate traffic analysis
  - Routing control: Selection of secure routes
  - Notarization: Use of trusted third party for data exchange

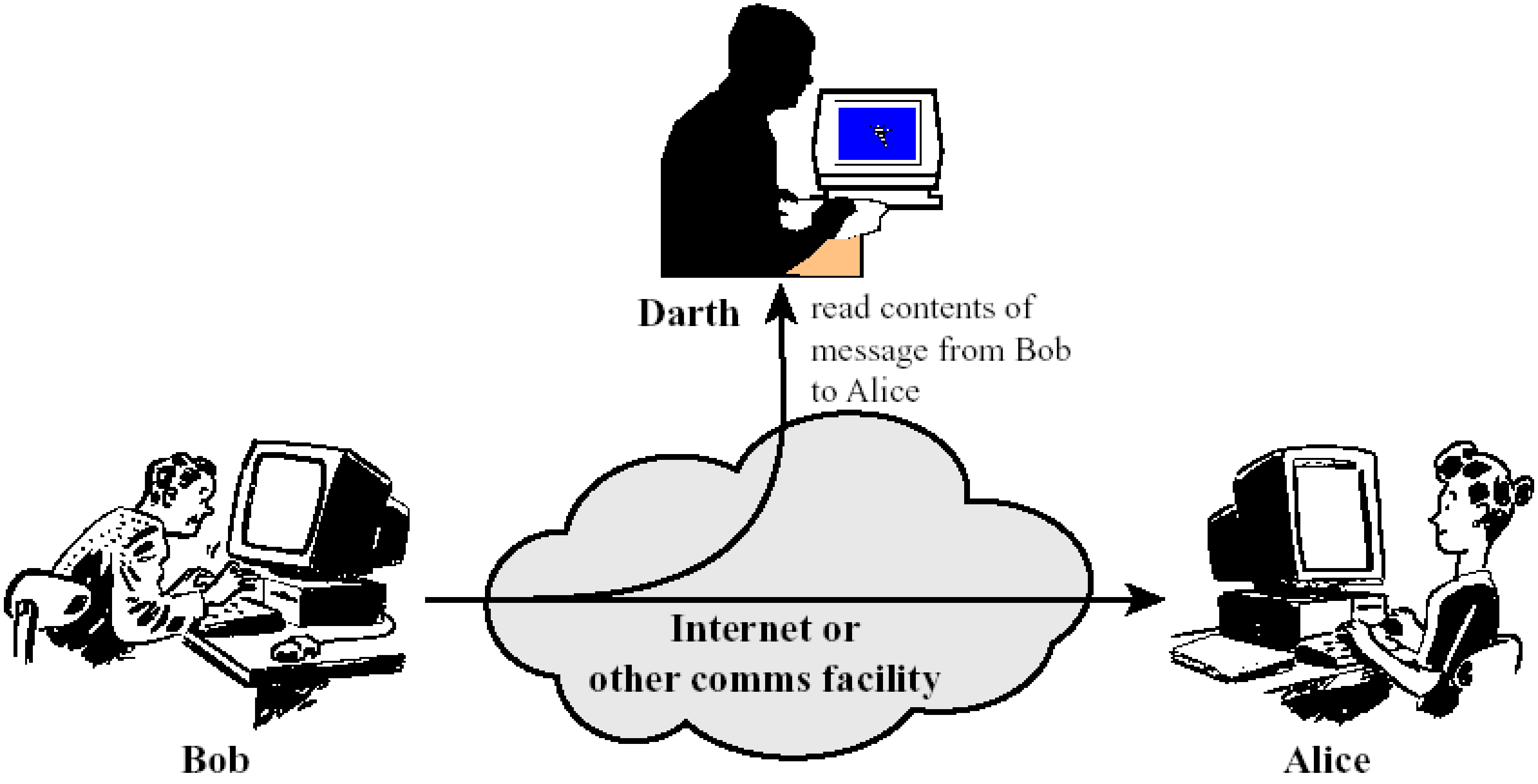
Security Mechanisms (X.800)

- Pervasive security mechanisms:
  - trusted functionality: percieved to be correct with respect to some criteria
  - security labels:
  - event detection: detection of security relevant events
  - security audit trails:
  - security recovery:

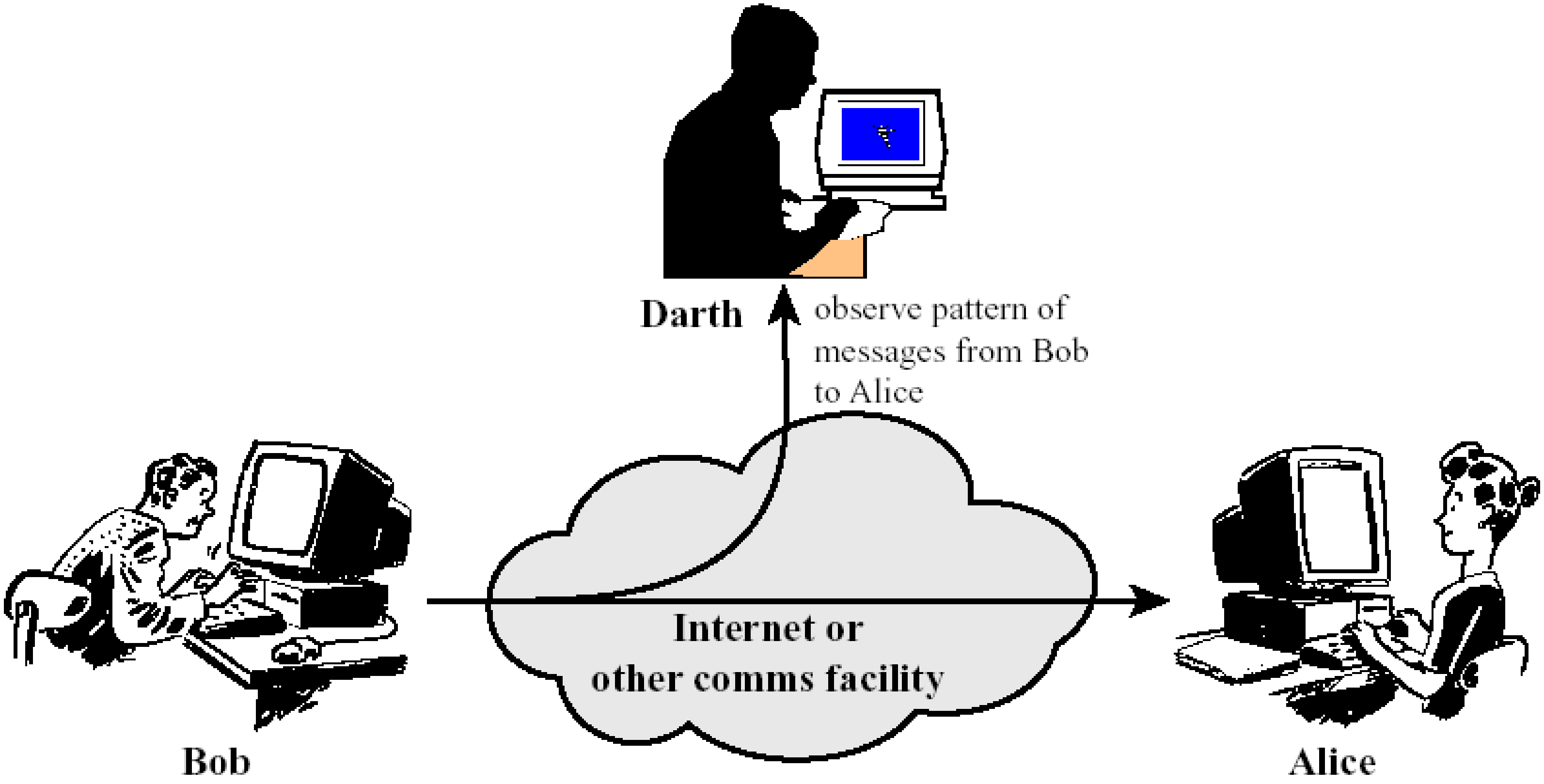
Classify Security Attacks as

- **Passive attacks -** eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **Active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

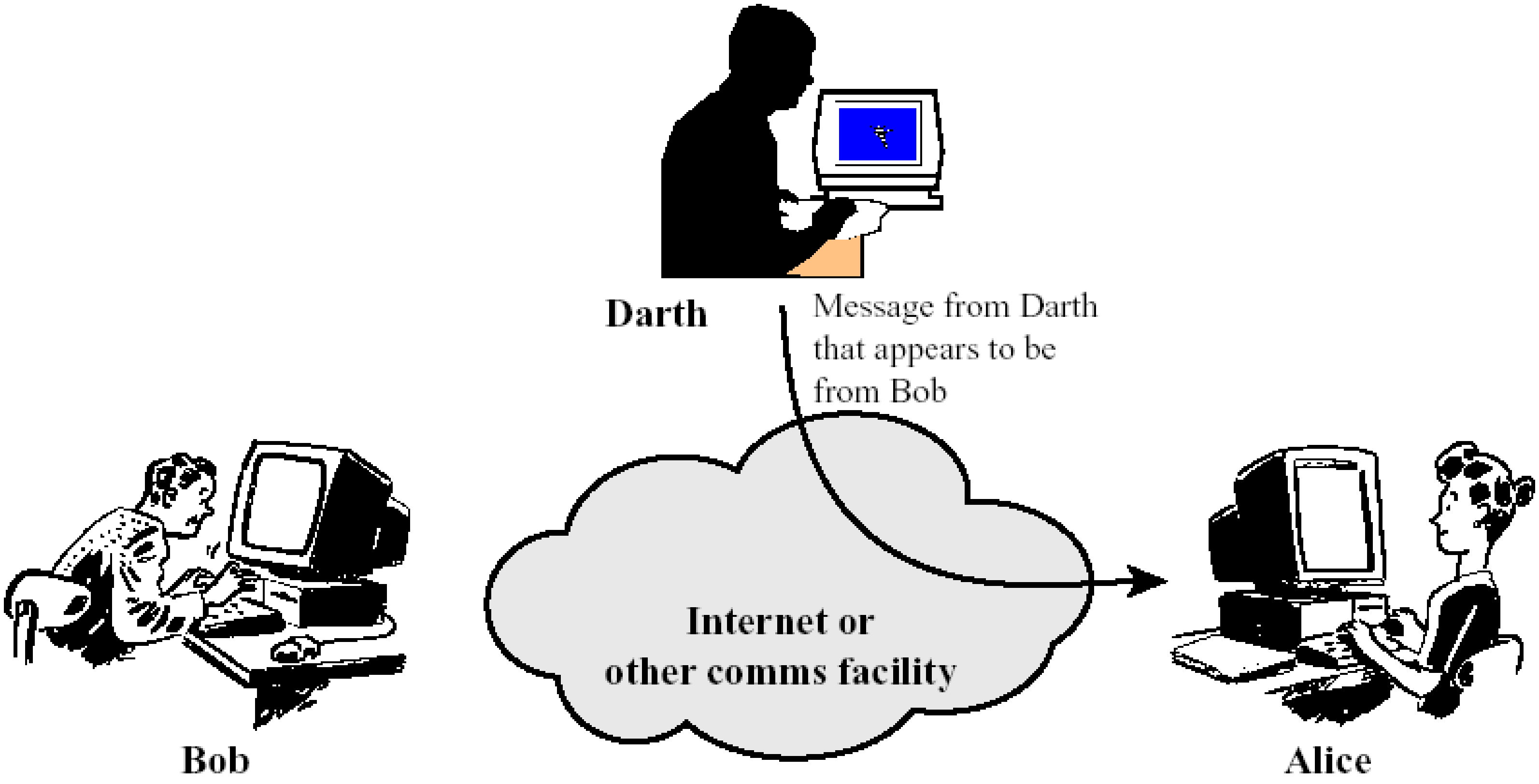
Passive Attacks: Release of Message Contents



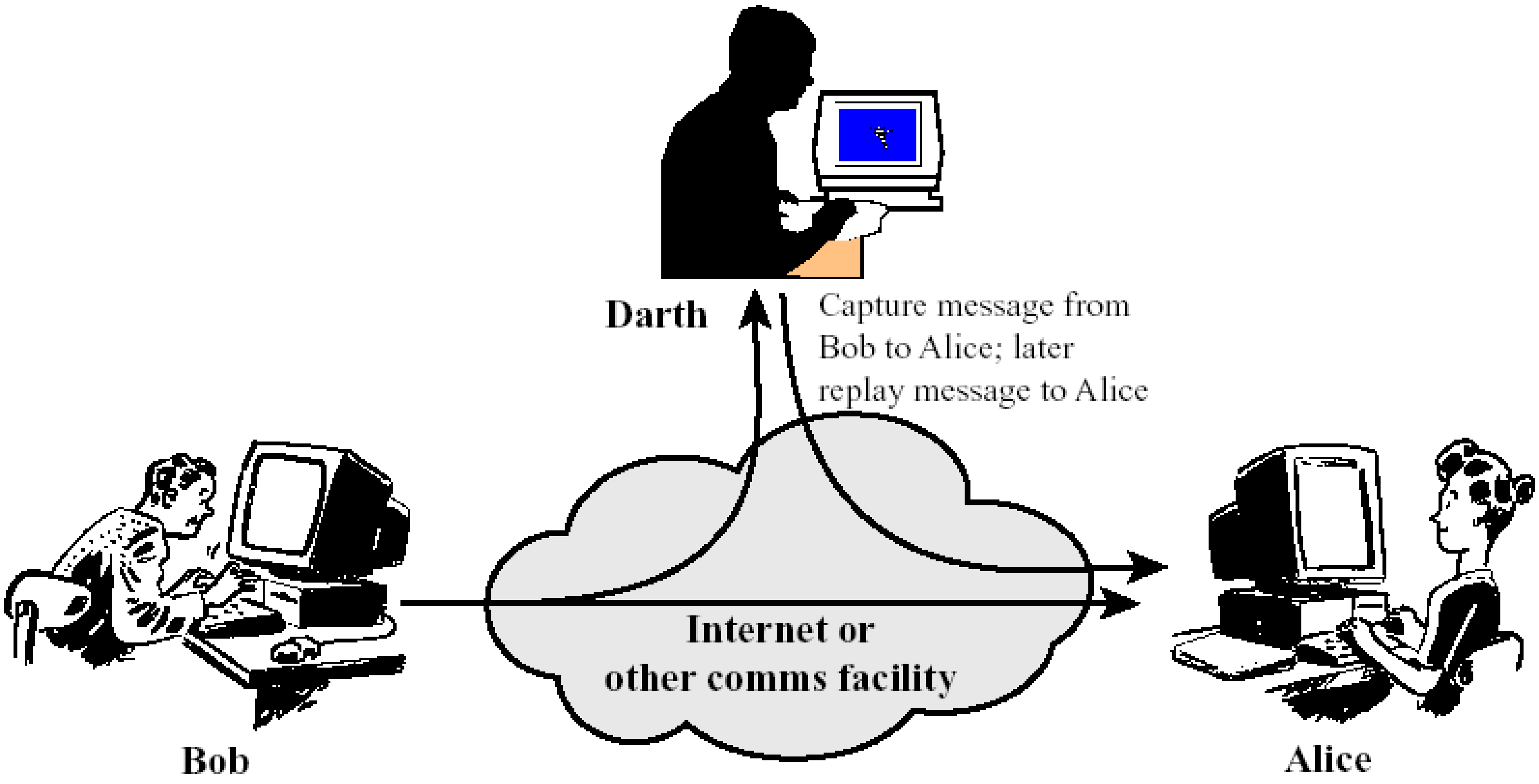
Passive Attacks: Traffic Analysis


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

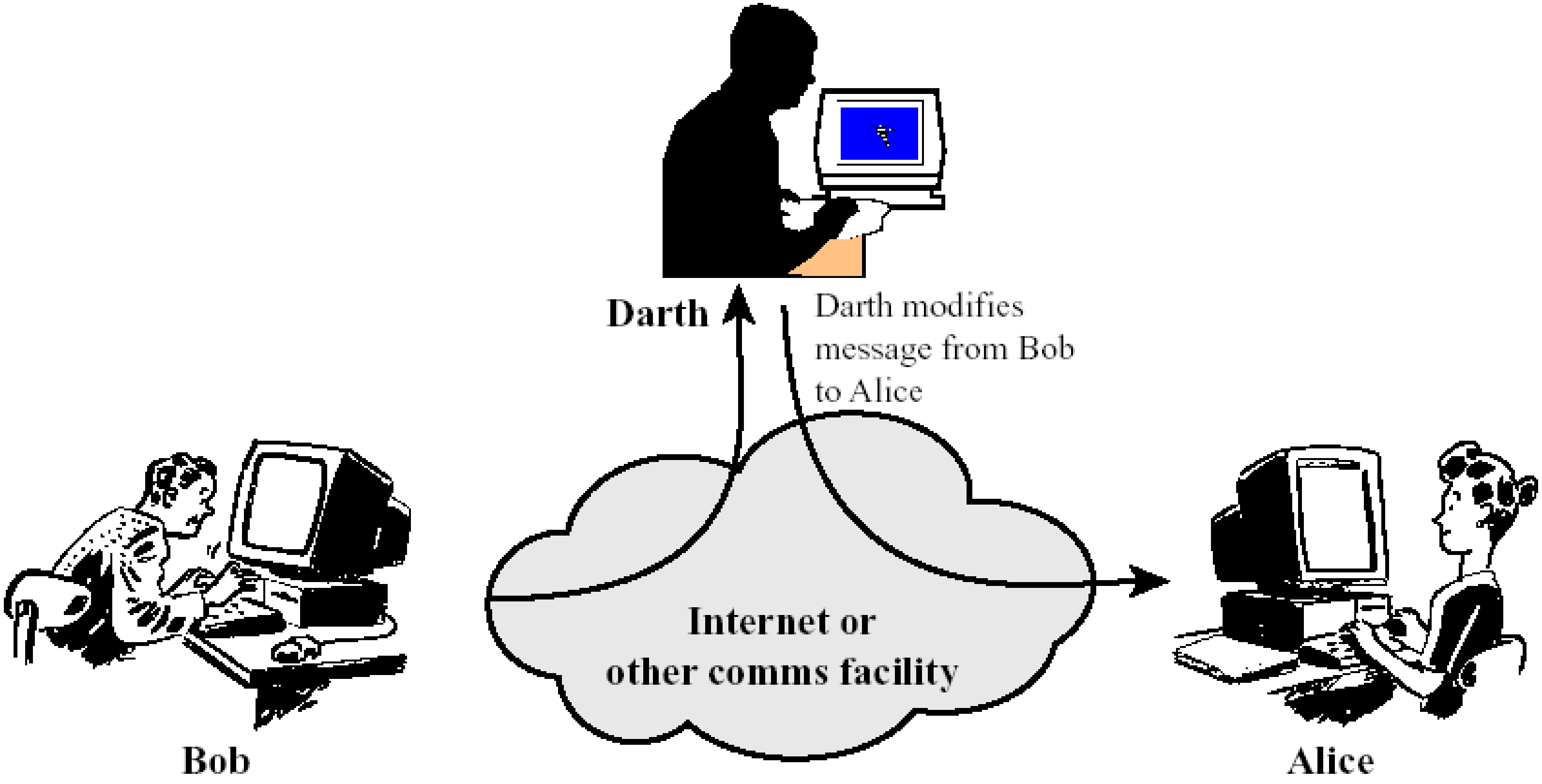
Active Attacks: Masquerade


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

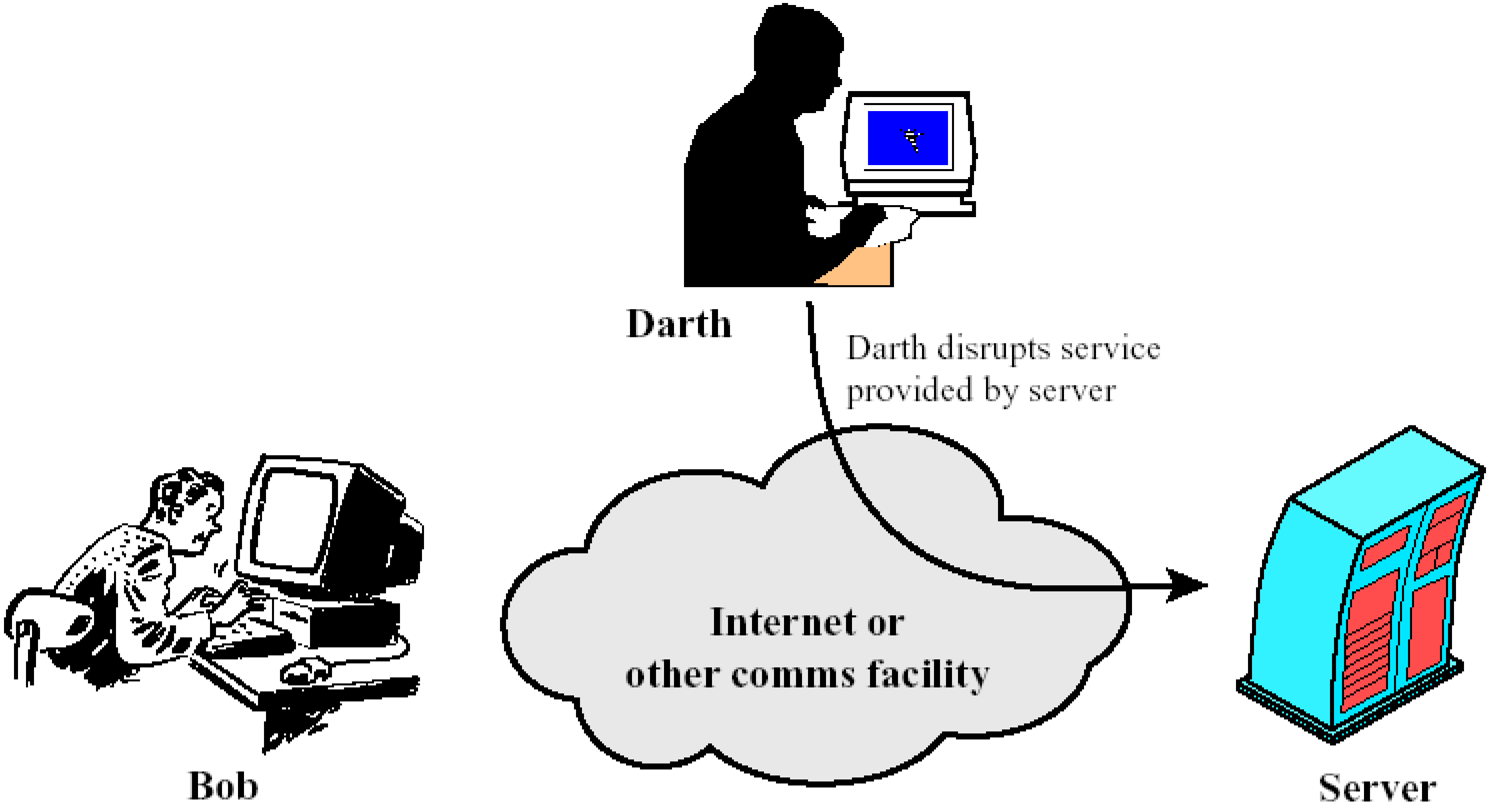
Active Attacks: Replay

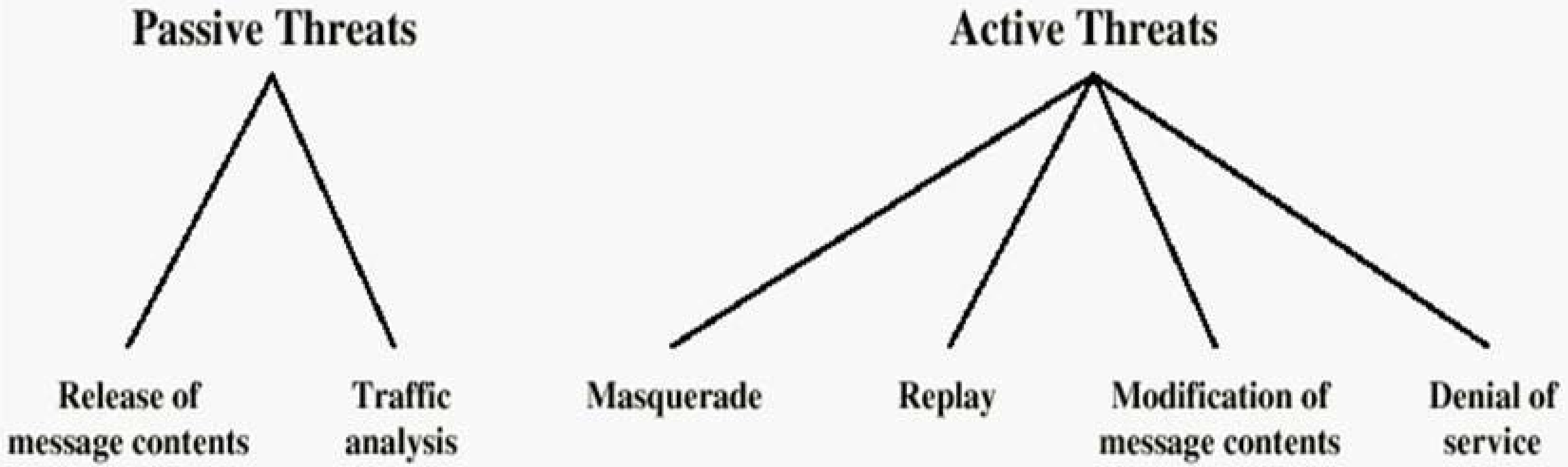

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attacks: Modification of Messages


Darth
Darth modifies message from Bob to Alice
Bob
Internet or other comms facility
Alice

Active Attacks: Denial of Service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server



Passive Threats

Release of message contents

Traffic analysis

Active Threats

Masquerade

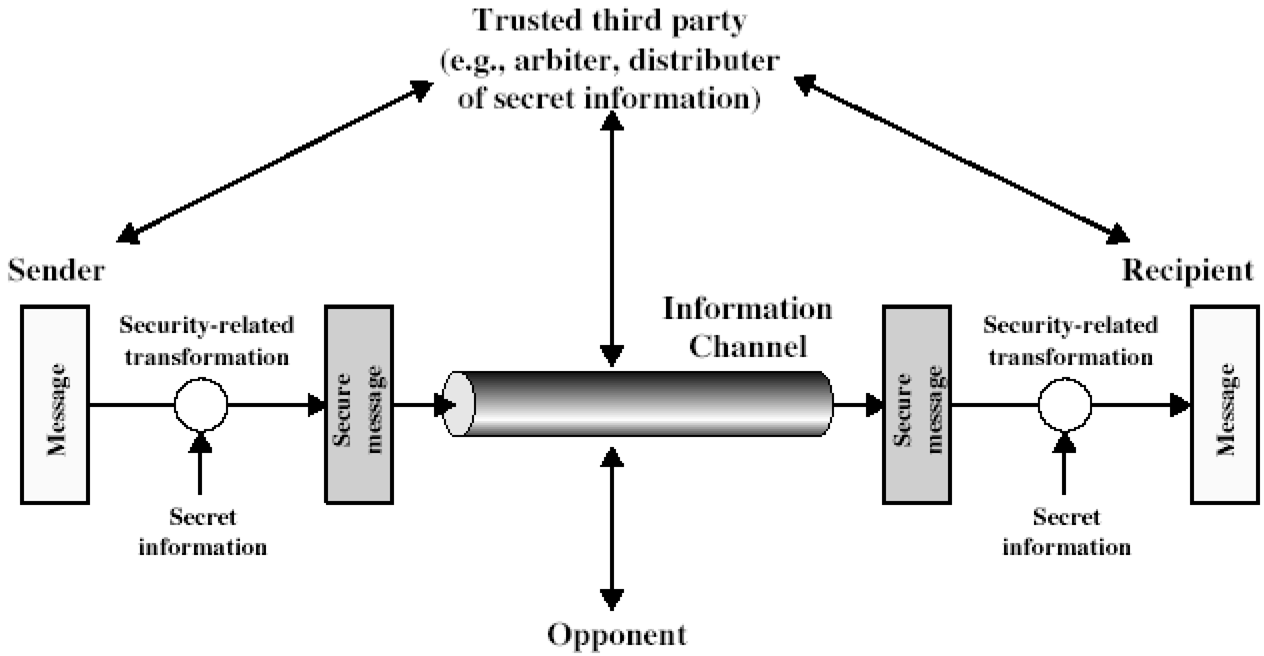
Replay

Modification of message contents

Denial of service

Active and Passive Security Threats

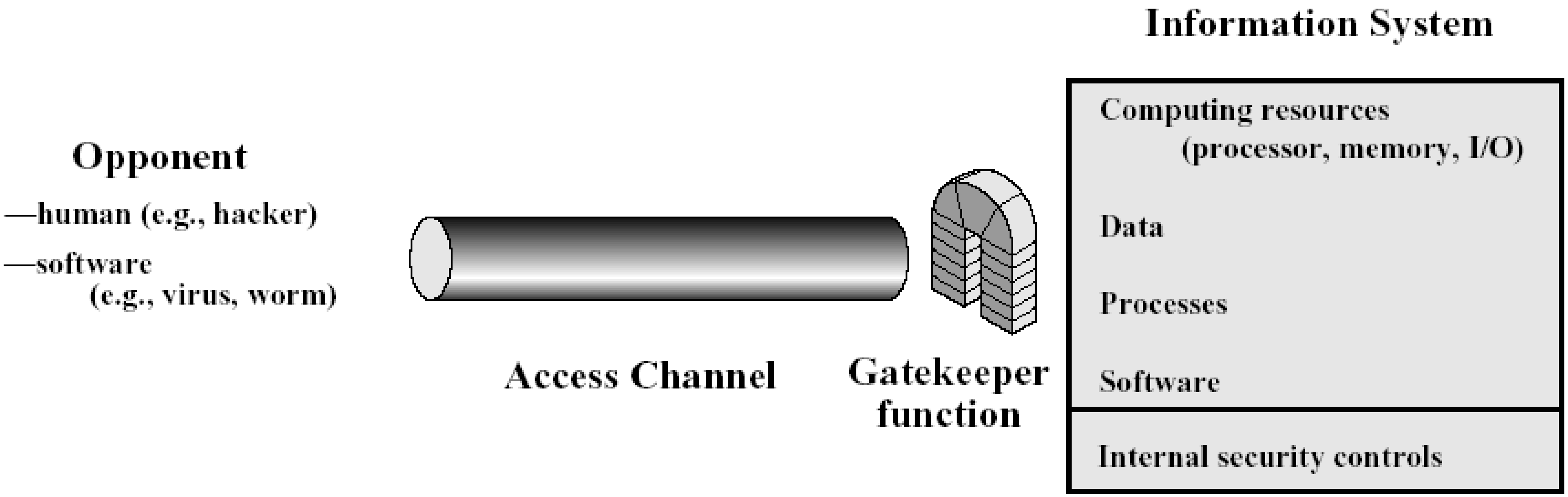
Model for Network Security



Model for Network Security

- **Using this model requires us to:**
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Information System

Computing resources
(processor, memory, I/O)

Data

Processes

Software

Internal security controls

Opponent

—human (e.g., hacker)

—software
(e.g., virus, worm)

Access Channel

Gatekeeper function

Model for Network Access Security

- Using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - 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

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords)
- Physical Controls

Internet standards and RFCs

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

Summary

- Have considered:
  - computer, network, internet security def's
  - security services, mechanisms, attacks
  - X.800 standard
  - models for network (access) security