Introduction to Cryptography

Jibi Abraham

COEP TECHNOLOGICAL UNIVERSITY

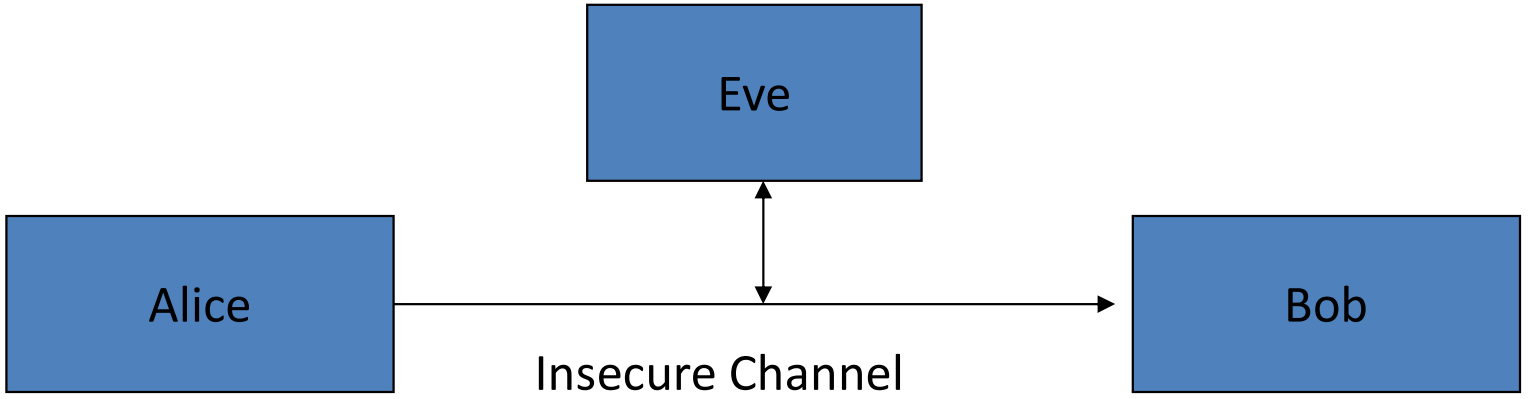
Shivajinagar, Pune-411 005

(A Unitary Technological University of Govt. of Maharashtra)

Information Security

- Traditionally is provided by
  - Physical Mechanisms
    - eg. rugged filing cabinets with locks
  - Administrative mechanisms
    - eg. Personnel screening procedures during hiring process
- Growing computer use implies a need for automated tools for protecting files and other information stored on it
- Use of networks and communications links requires measures to protect data during transmission

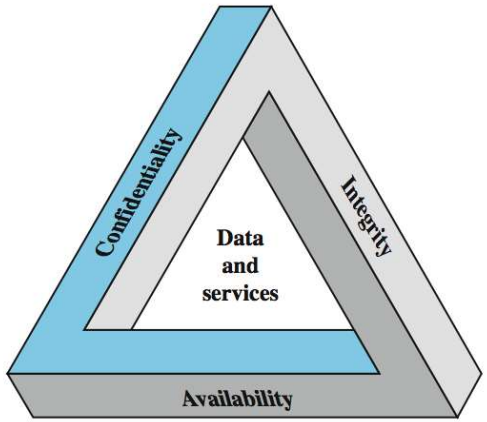
Cryptography Goals



- Encryption – Prevent Eve from intercepting message
- Authentication – Prevent Eve from impersonating Alice

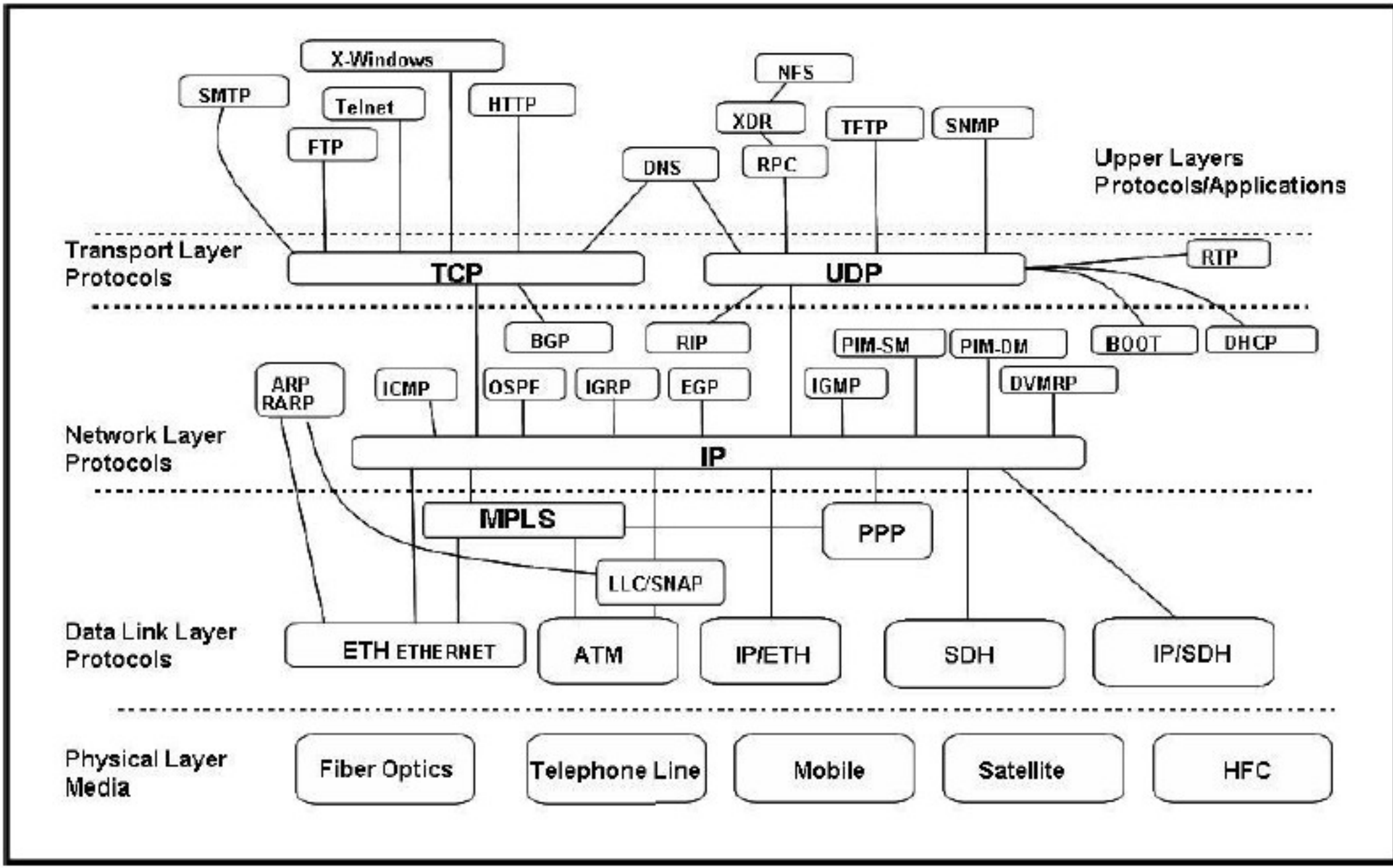
Information Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the
  - Integrity
  - availability and
  - Confidentiality

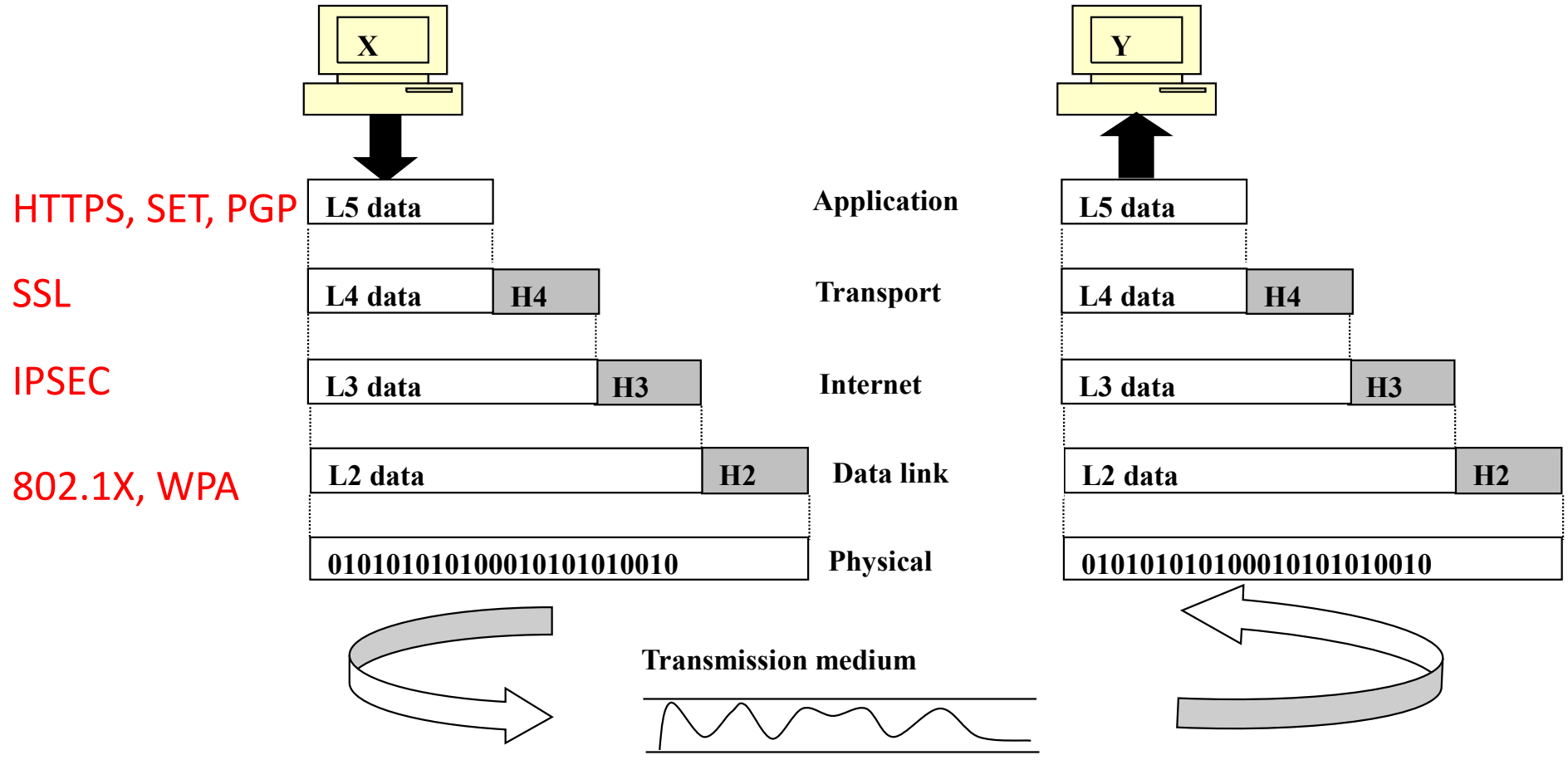


- of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

TCP/IP Protocol Suit



Data Exchange using TCP/IP Layers



Secure Electronic Transaction (SET) – to protect credit card transaction
Pretty Good Privacy (PGP) – To secure email
Secure Socket Layer (SSL)-Located between the Application and Transport Layers Located
IPSEC – at Network Layer

Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
- RSA Labs (de facto)

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 in a network
- **Internet Security** - measures to protect data during its transmission over a collection of interconnected networks
- **Cryptography** = the science (art) of encryption
- **Cryptanalysis** = the science (art) of breaking encryption
- **Cryptology** = cryptography + cryptanalysis

OSI Security Architecture

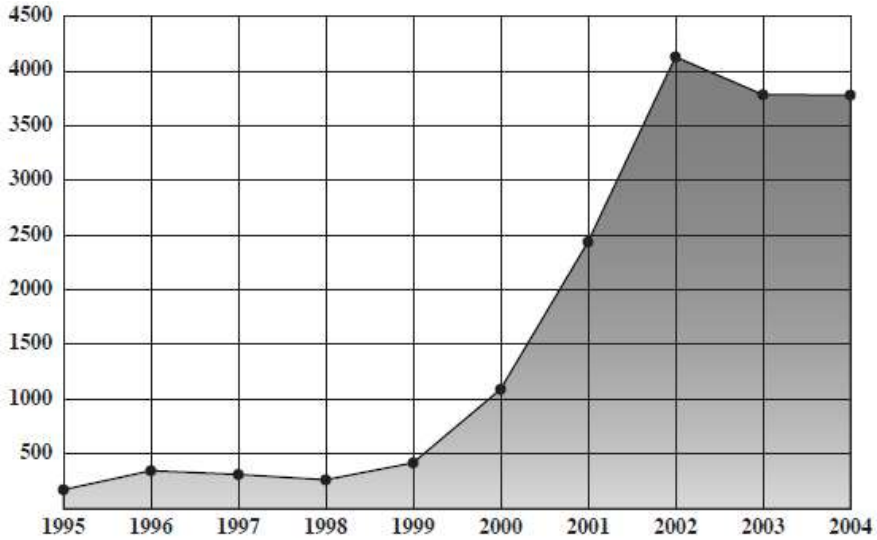
- ITU-T X.800 Security Architecture for OSI
- A systematic way of defining and providing security requirements
- It provides a useful, abstract overview of concepts
- 3 Aspects of Info Security
  - **Security Attacks**
    - Any action that compromises the security of information.
  - **Security Services**
    - A service that enhances the security of data processing systems and information transfers
    - Makes use of one or more security mechanisms
  - **Security Mechanisms**
    - A mechanism to detect, prevent, or recover from a security attack

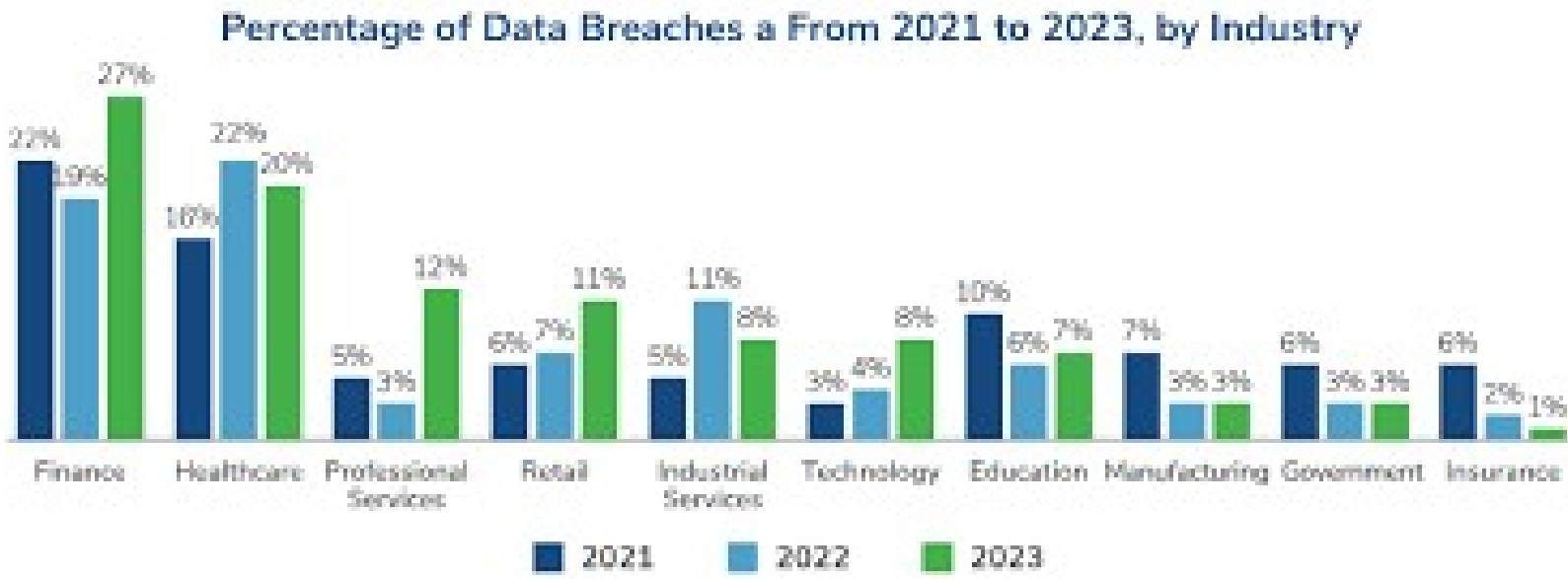
Threats

- A potential for violation of security, which exists when there is a circumstance, capability, action or an event that could breach security and cause harm
- ie. a threat is a possible danger that might exploit a vulnerability

CERT report

- Computer Emergency Response Team reported Internet related vulnerabilities over 10 years

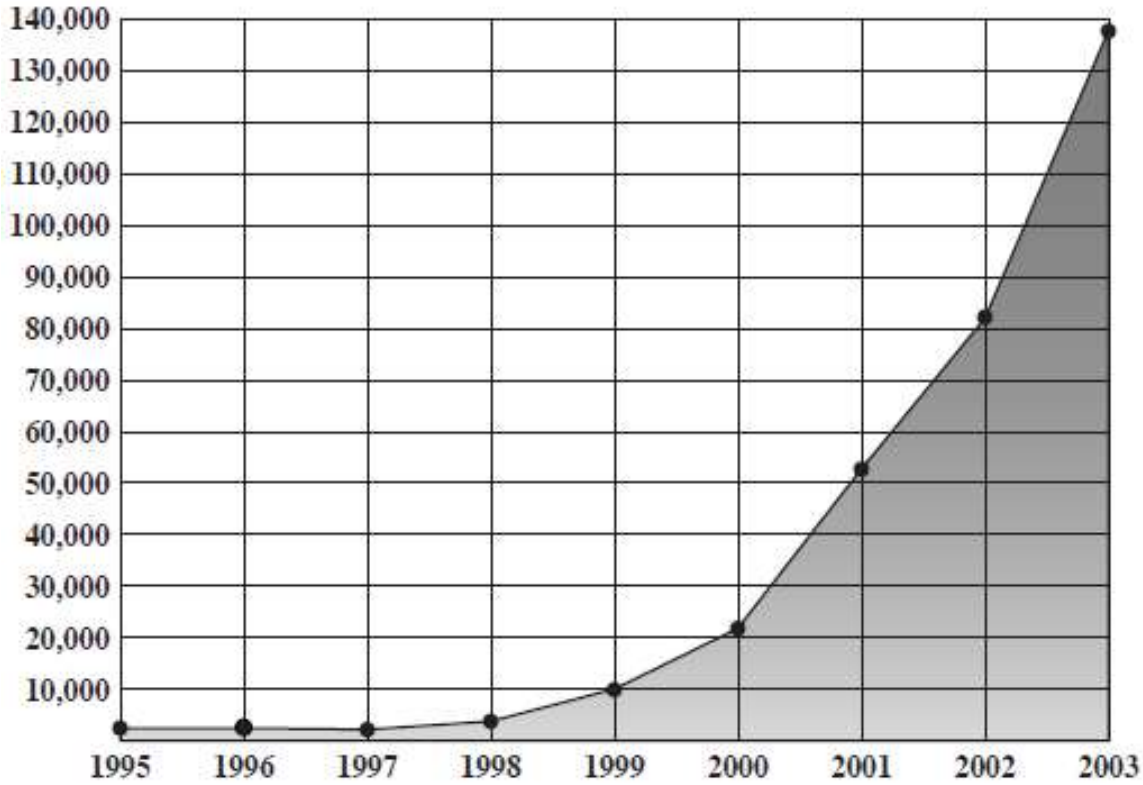




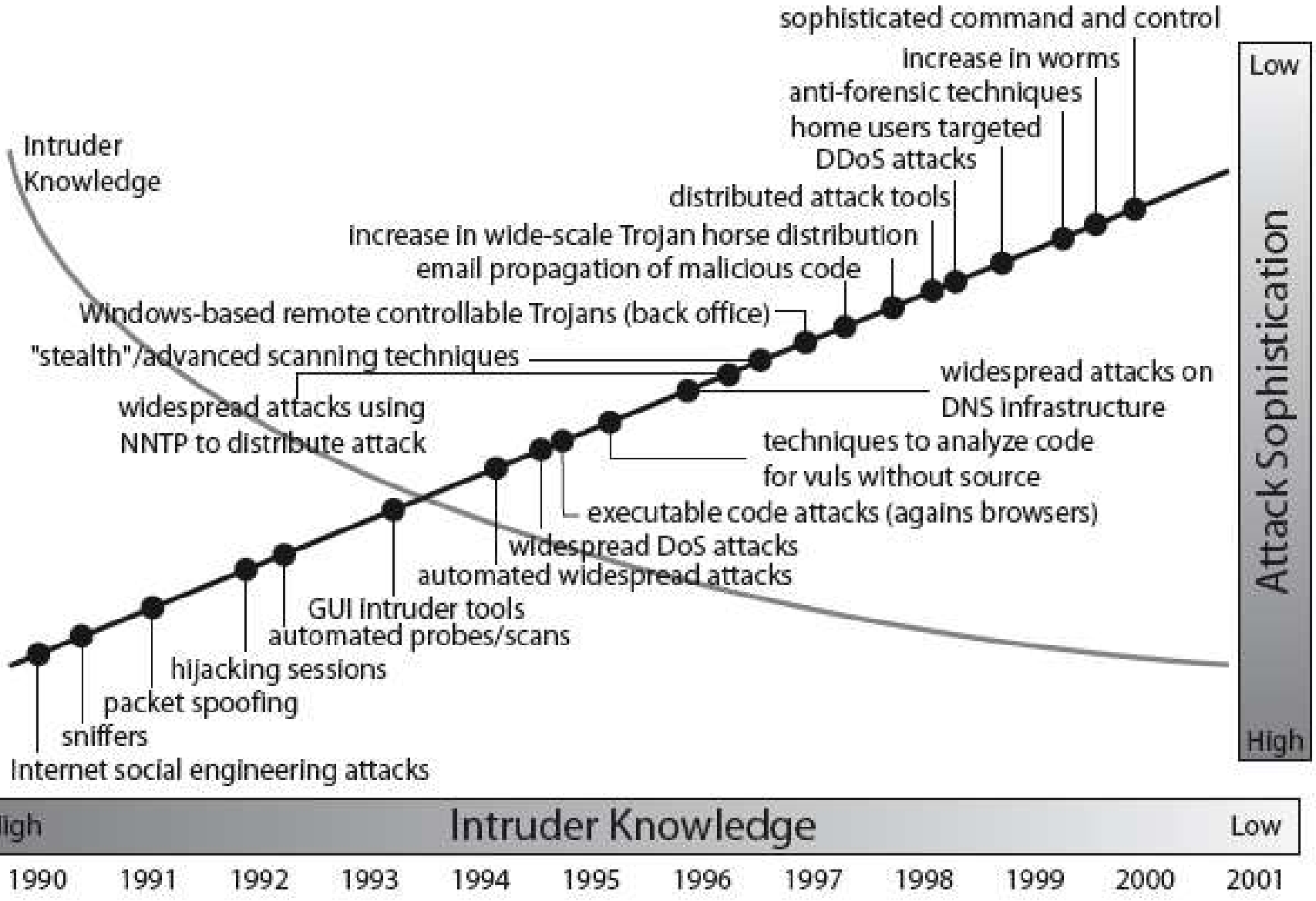
COEP Tech

Attack

- An assault on system security that derives from an intelligent threat, ie, an intelligent act that is a deliberate attempt to evade the security service and violate the security policy of the system
- CERT reported Incidents



Security Attacks Trends



Source: CERT

Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Low Impact

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
  - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  - (ii) result in minor damage to organizational assets;
  - (iii) result in minor financial loss; or
  - (iv) result in minor harm to individuals

Moderate Impact

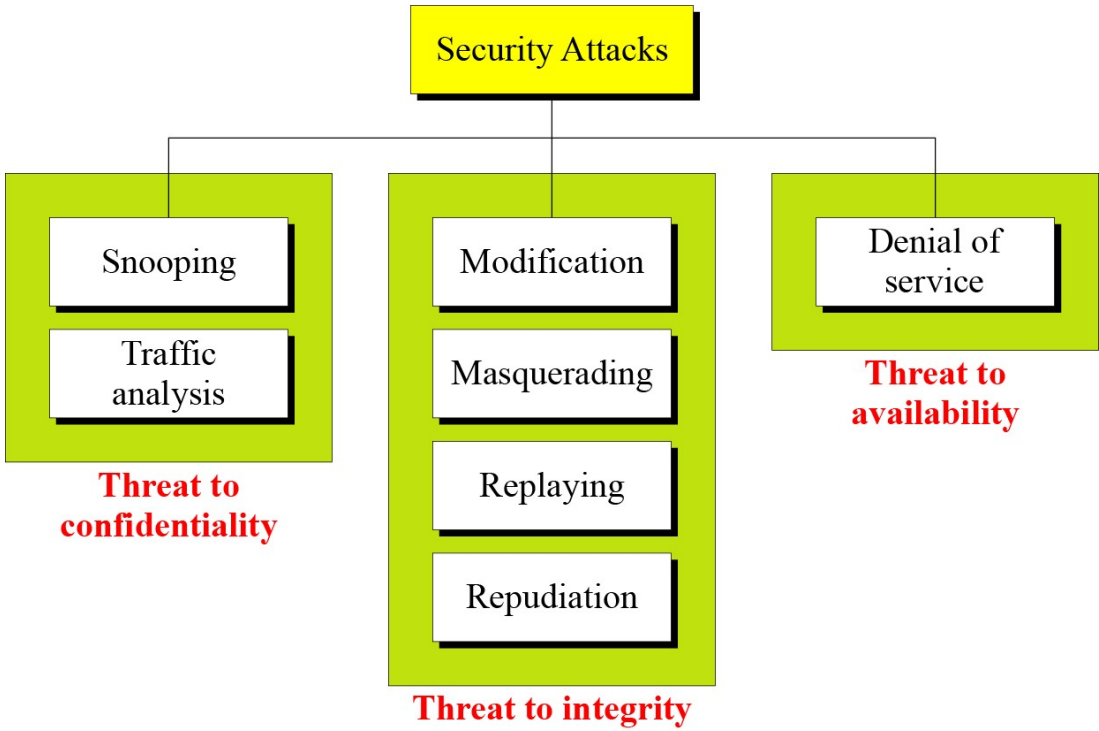
- The loss could be expected to have a serious adverse effect on organizational operations, assets, or individuals.
- A serious adverse effect means that, e.g., the loss might
  - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - (ii) result in significant damage to organizational assets;
  - (iii) result in significant financial loss; or
  - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High Impact

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss might
  - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  - (ii) result in major damage to organizational assets;
  - (iii) result in major financial loss; or
  - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

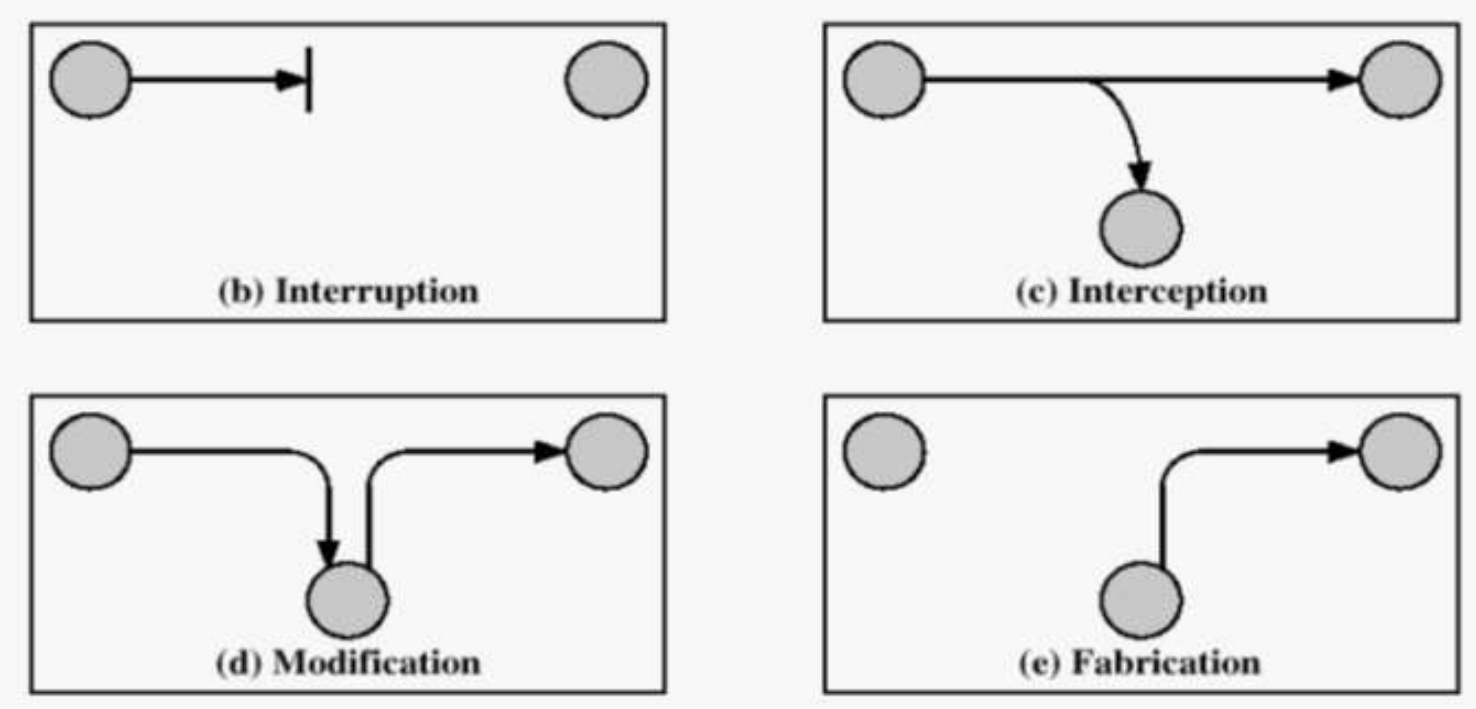
Classification of Security Attacks

- **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



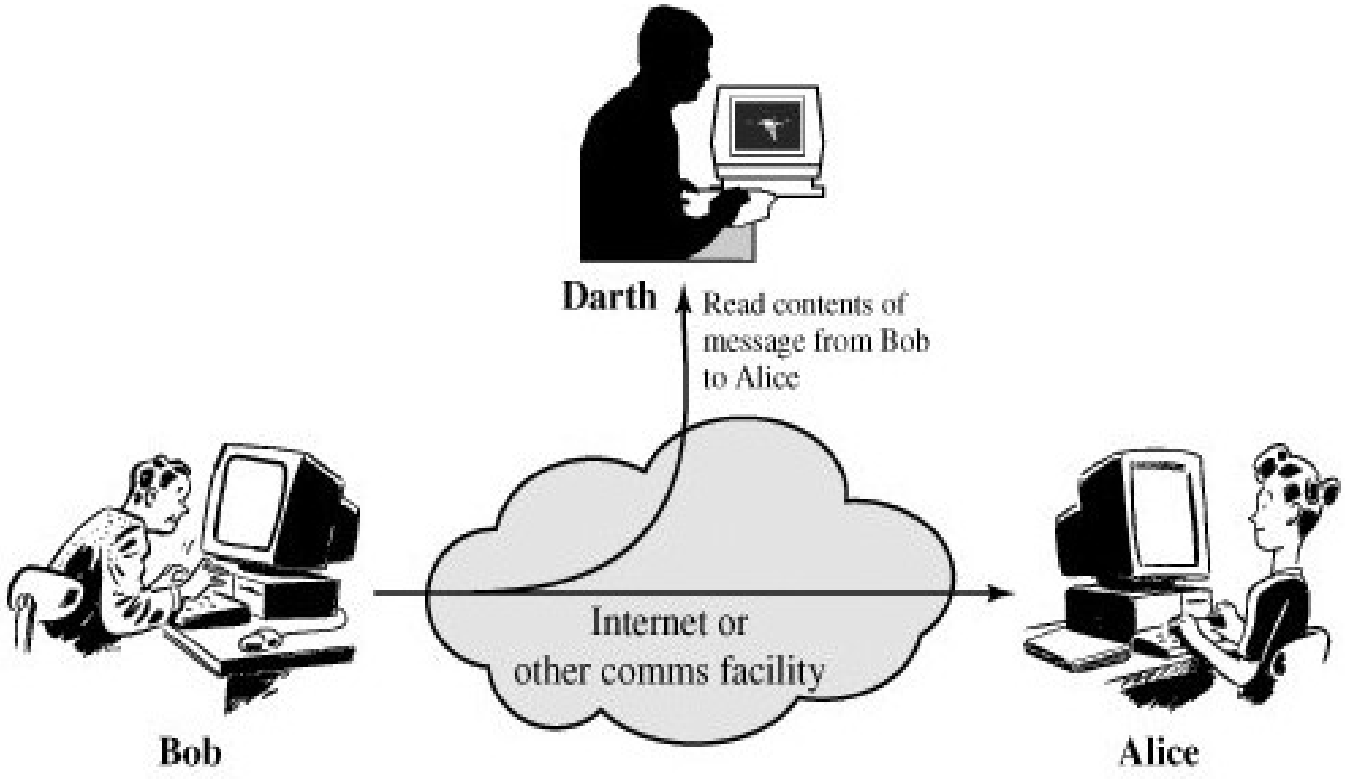
Network Security Attacks

- Have a wide range of attacks



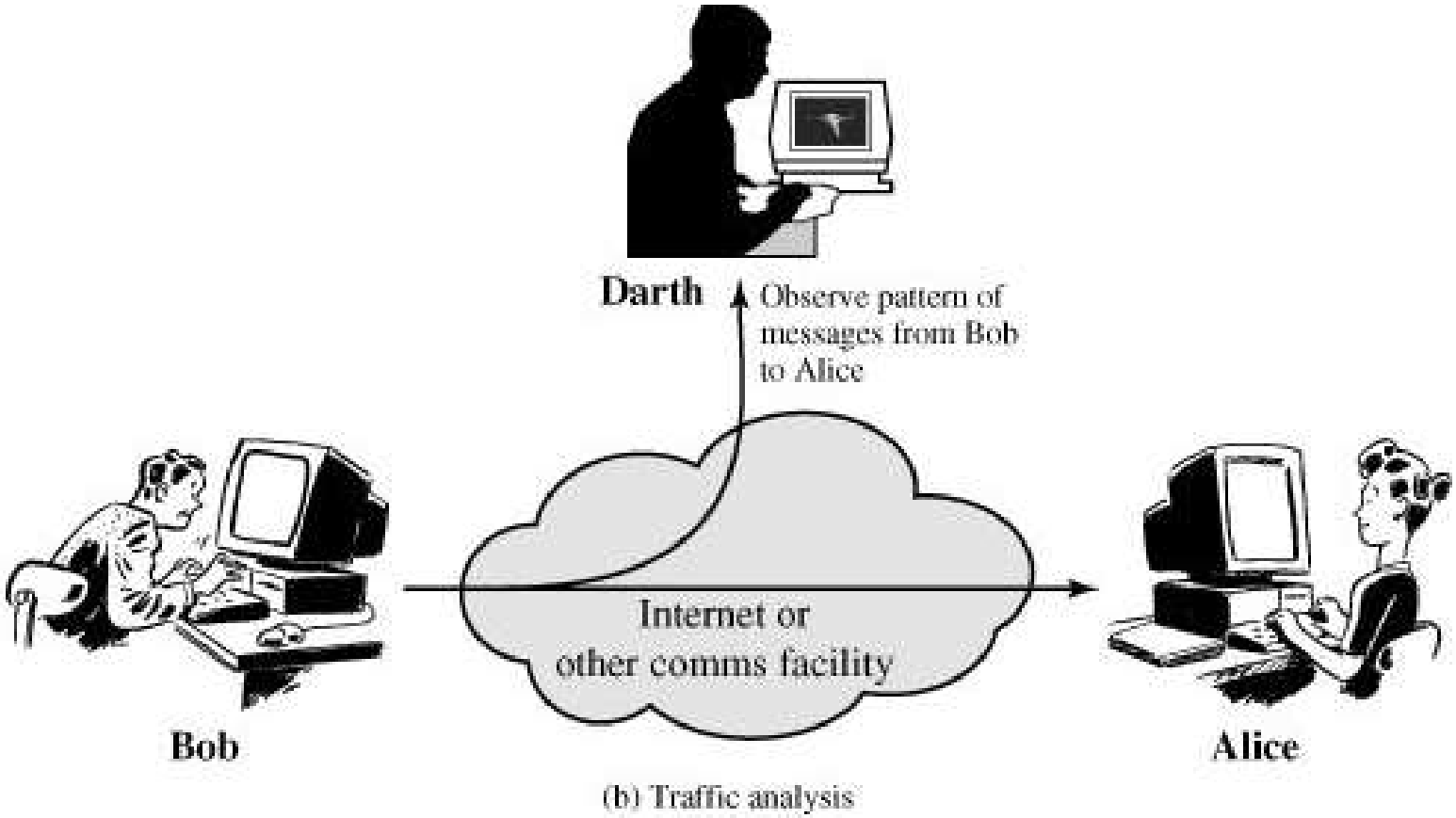
Passive Attack- Release of Message Contents

Eavesdropping



(a) Release of message contents

Passive Attack- - Traffic Analysis

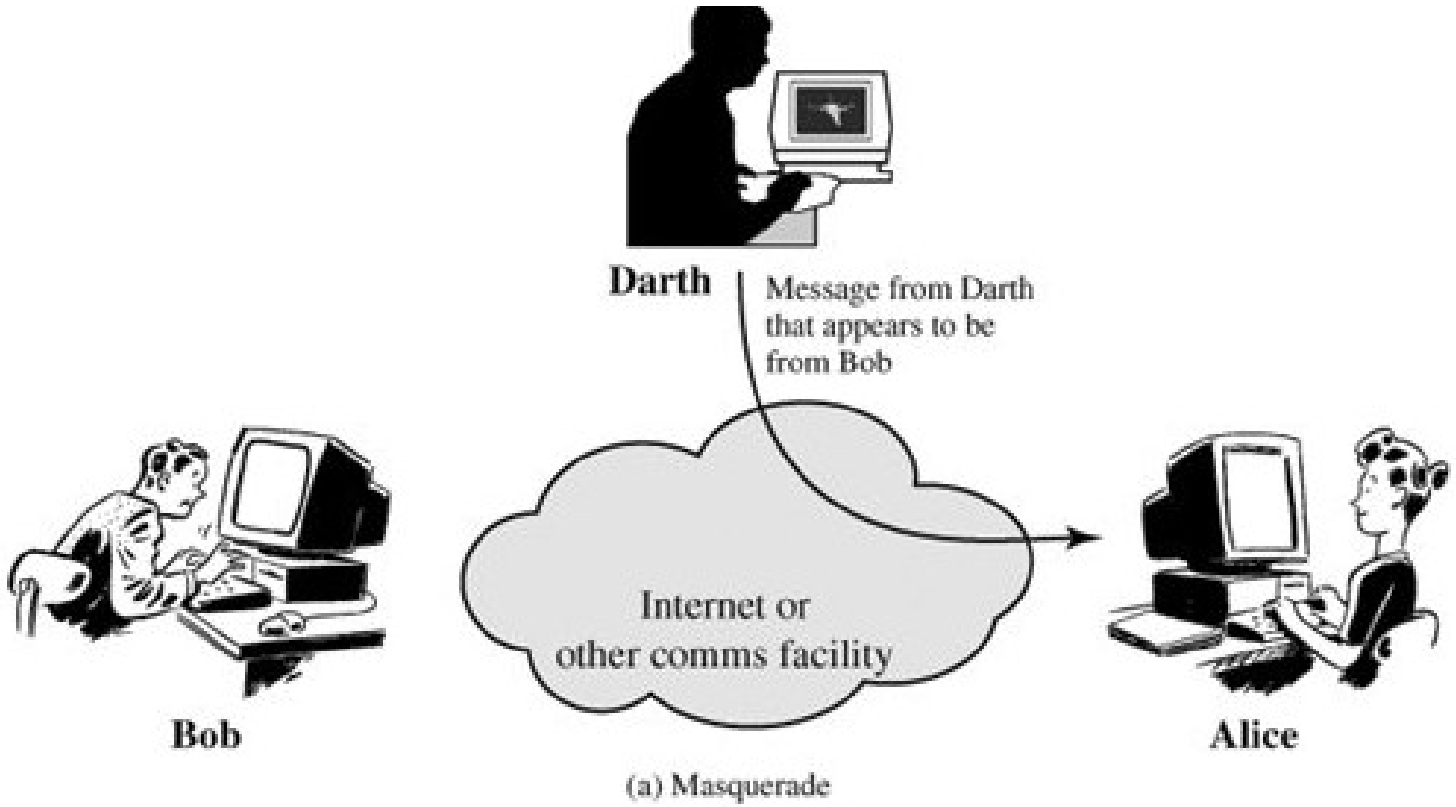


(b) Traffic analysis

Packet Sniffing

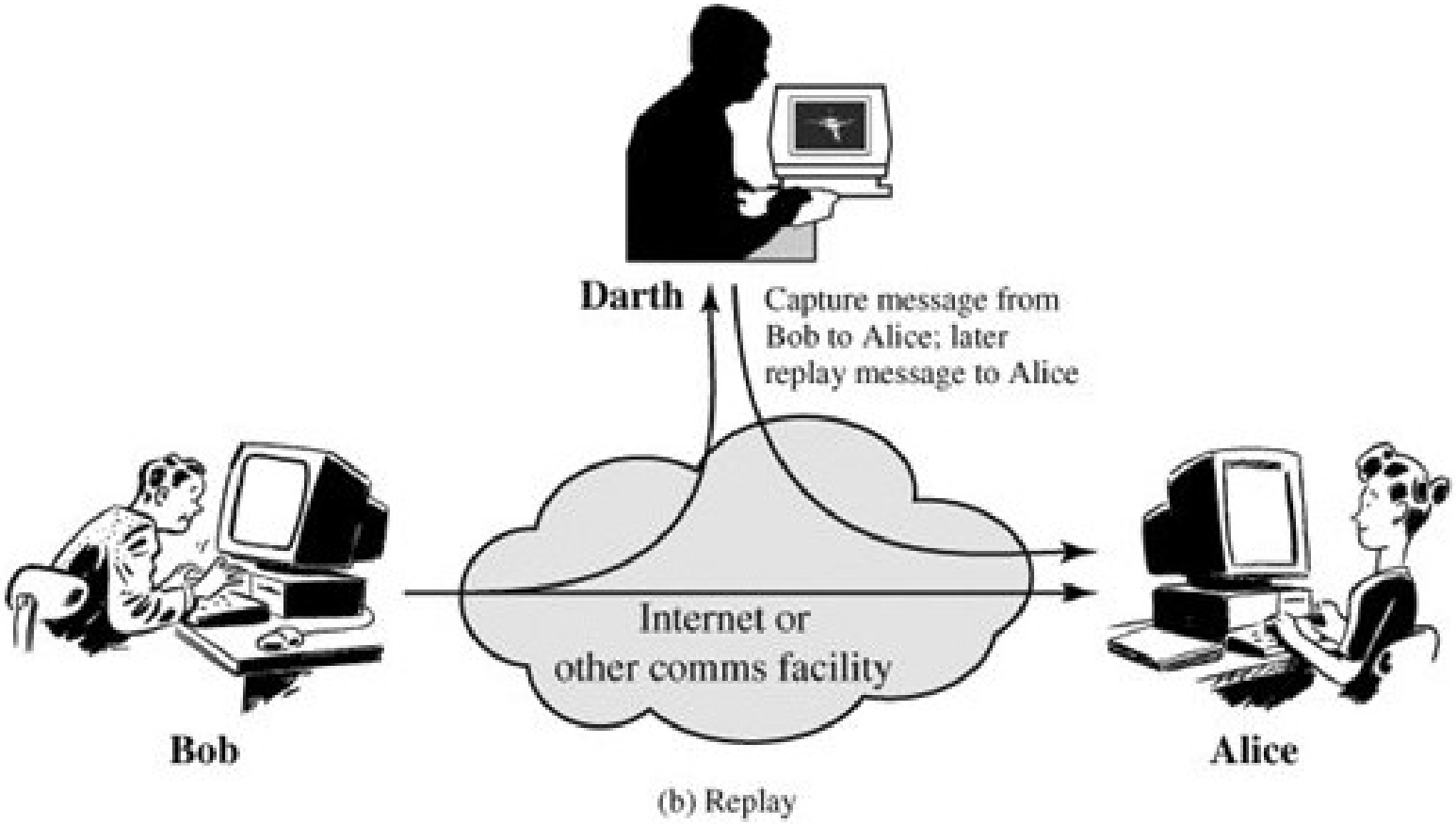
- A passive attack on an ongoing conversation.
- Broadcast nature of LAN
- NIC Promiscuous mode
- Wireshark took
- PCAP file
- Remedy – Encryption
  - Link encryption
  - End-to-end encryption

Active Attack- Masquerade



(a) Masquerade

Active Attack- Replay

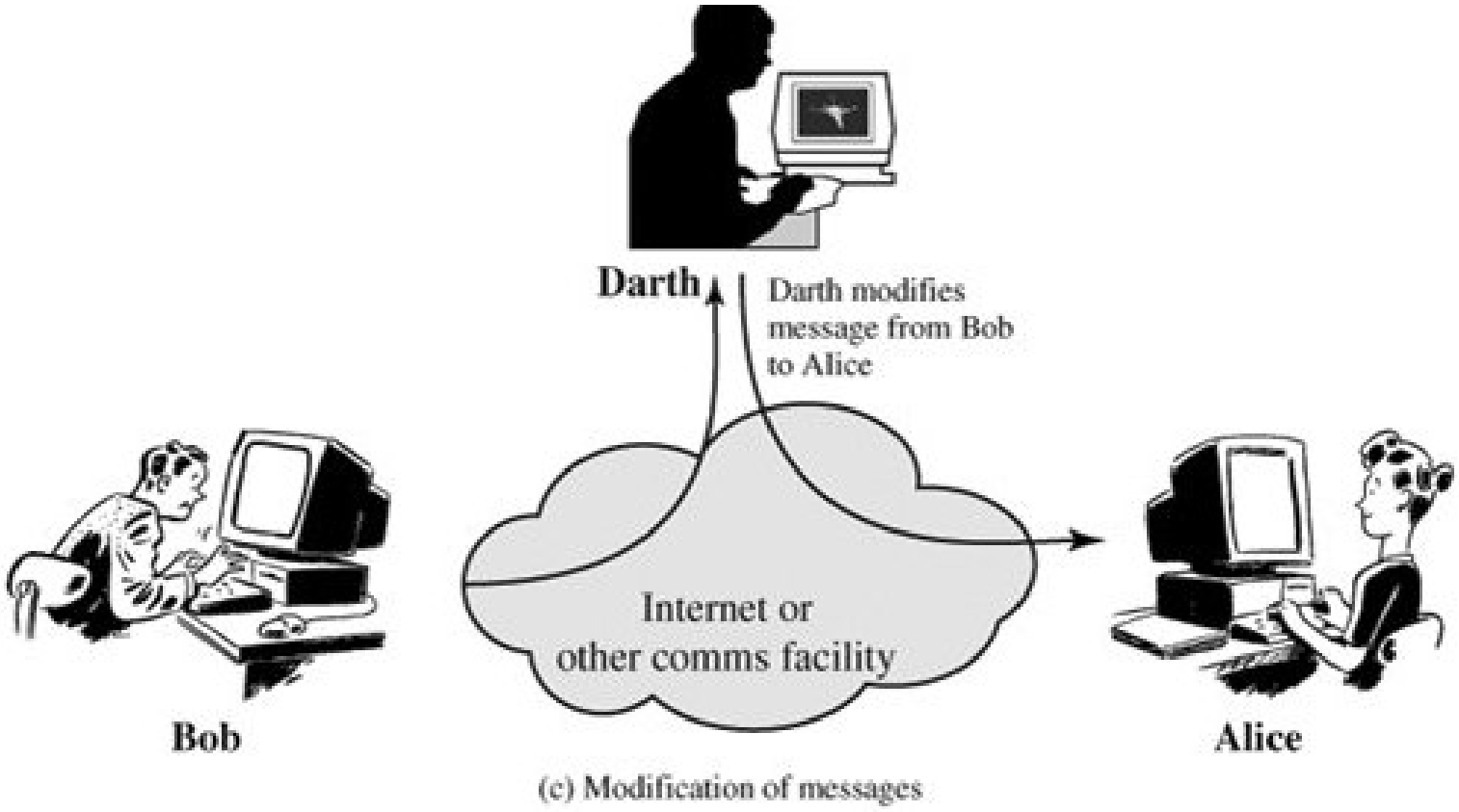


(b) Replay

Packet Spoofing

- Attacker sends packets with a false source address, receiver replies to forged address
  - Attacker can intercept, if he is in between them
  - Attacker need not have to see the reply in case like DoS

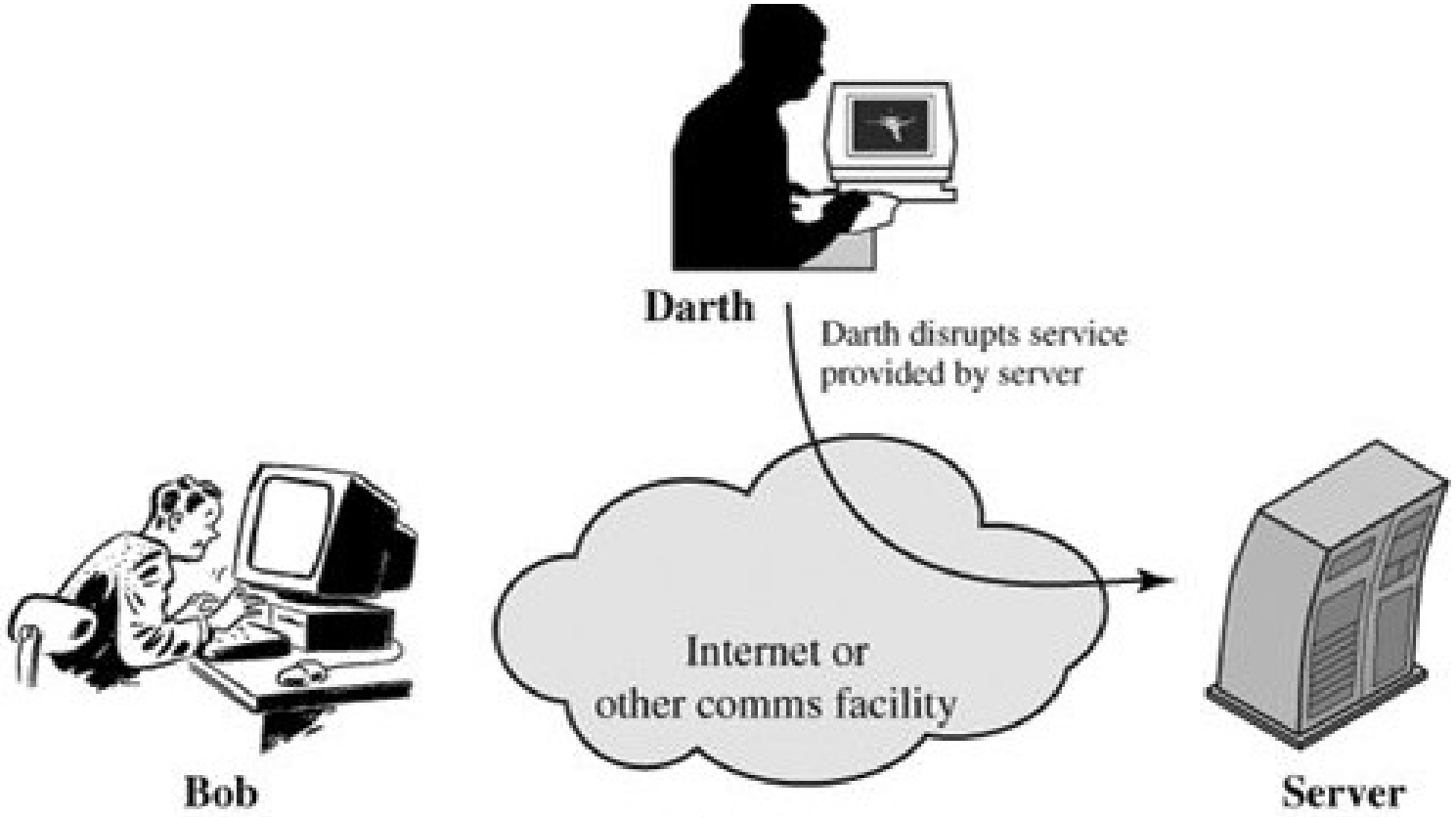
Active Attack- Modification of Messages



(c) Modification of messages

Active Attack- Denial of Service

- TCP SYN Flood
- ICMP Flood
- UDP Flood



(d) Denial of service

Other famous attacks

- Phishing
  - an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data to utilize or sell the stolen information
  - Phishing prevention options
    - DNS records verification keeps such emails in spam folder, sender's email address is not associated with a legitimate domain name etc.
- Pharming (DNS Spoofing)
  - Malware infects a victim's computer and stealthily makes changes to the victim's host's file
- How can Secure Socket Layer (SSL) prevent Phishing and Pharming?

Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

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)

- **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

X.800 - Security Services

- AUTHENTICATION
  - The assurance that the communicating entity is the one that it claims to be.
  - Peer Entity Authentication
    - Used in association with a logical connection to provide confidence in the identity of the entities connected. Ex: TCP connection
  - Data Origin Authentication
    - In a connectionless transfer, provides assurance that the source of received data is as claimed. Ex: Email
  - Explore Windows/Unix user login authentication mechanism
    - Passwd command is setuid set with root as owner

X.800 - Security Services (contd)

- ACCESS CONTROL
  - The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

X.800 - Security Services (contd)

- DATA CONFIDENTIALITY
  - The protection of data from unauthorized disclosure.
  - Connection Confidentiality
    - The protection of all user data on a connection.
  - Connectionless Confidentiality
    - The protection of all user data in a single data block (flow)
  - Selective-Field Confidentiality
    - The confidentiality of selected fields within the user data on a connection or in a single data block.
  - Traffic Flow Confidentiality
    - The protection of the information that might be derived from observation of traffic flows: source, destination, frequency, length

X.800 - Security Services (contd)

- DATA INTEGRITY
  - The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - Connection Integrity with Recovery
    - Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - Connection Integrity without Recovery
    - As above, but provides only detection without recovery.
  - Selective-Field Connection Integrity
    - Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
  - Connectionless Integrity
    - Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
  - Selective-Field Connectionless Integrity
    - Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

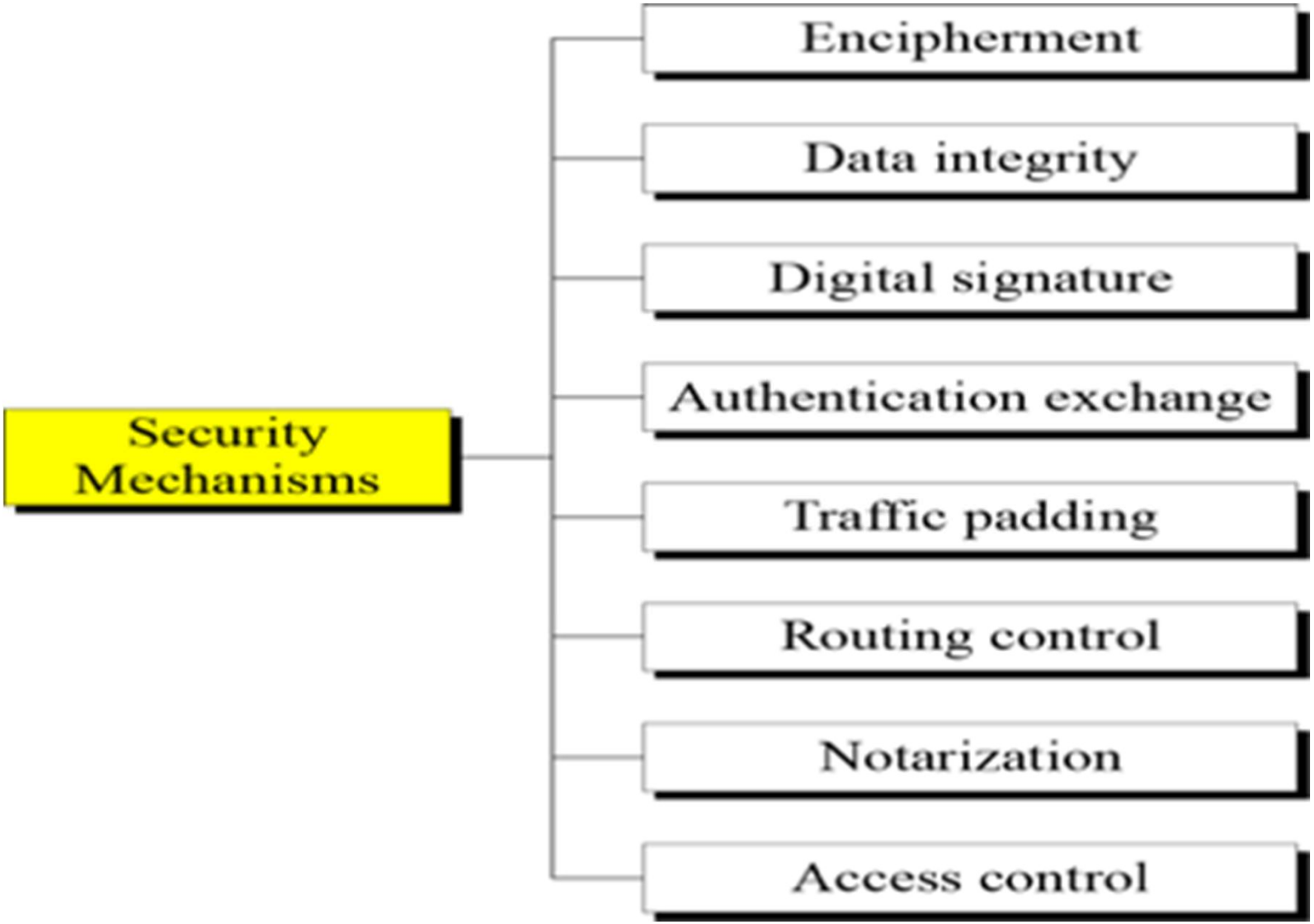
X.800 - Security Services (contd)

- NONREPUDIATION
  - Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
  - Nonrepudiation, Origin
    - Proof that the message was sent by the specified party.
  - Nonrepudiation, Destination
    - Proof that the message was received by the specified party.

Security Mechanisms

- 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**

Security Mechanisms (X.800)



Mechanisms to Implement Security

- Two techniques are prevalent today:
  - Cryptography
    - Science and art of transforming messages to make them secure and immune to attacks
  - Steganography
    - Means "covered writing"
    - E.g. covering data under color image

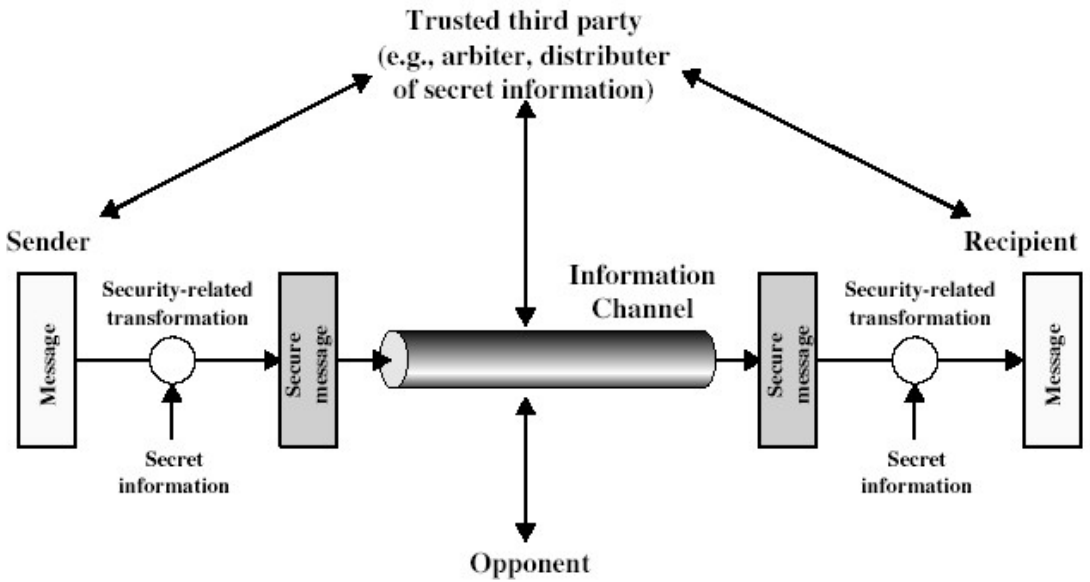
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Relationship between Services and Mechanisms

	Mechanism				
Requirement	Encipherment	Digital Signature	Access Control	Data Integrity	Routing Control
Authentication	Y	Y			
Access control			Y		
Confidentiality	Y				Y
Data integrity	Y	Y		Y	

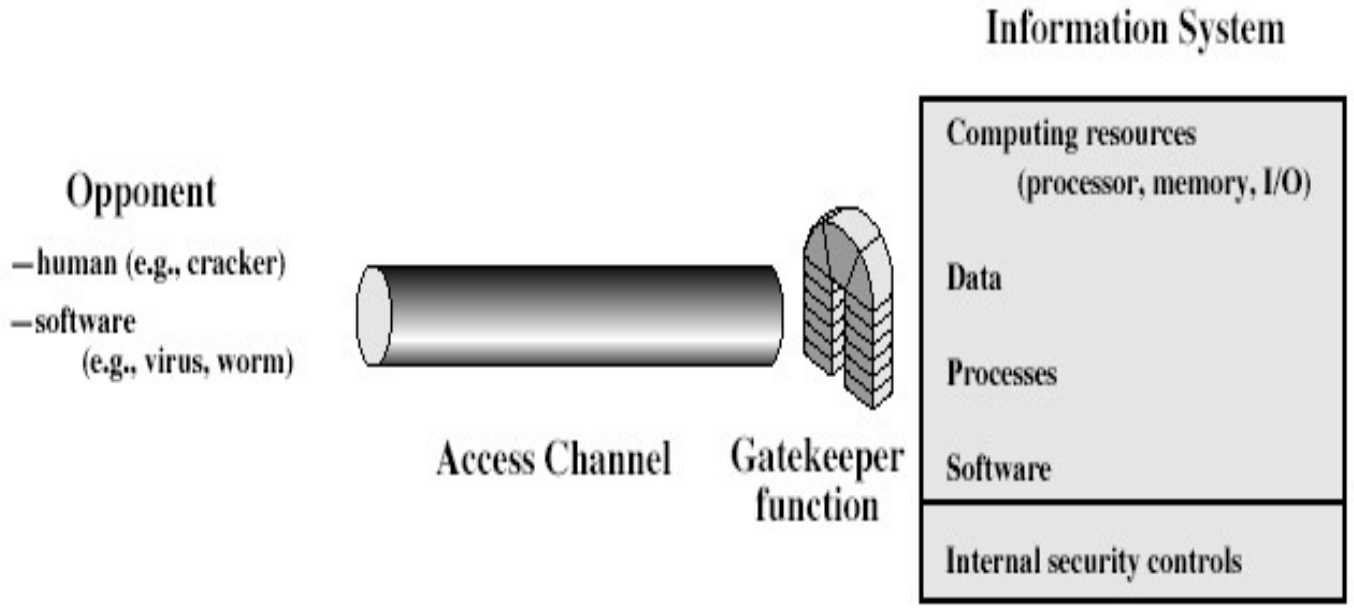
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

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 Using

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

Design a Security Service

1. Design an algorithm for security related transformation.
2. Generate the secret information to be used with the algorithm
3. Develop methods for the distribution and sharing the secret information
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service

- *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure..*

  — On War, Carl Von Clausewitz

Aim of Course

- Focus is on
- **Cryptography**
  - is the practice and study of techniques for secure communication of information over a network in the presence of adversarial behavior
  - Secret key functions
  - Public key functions
  - Hash functions
- **Network Security Mechanisms**
- **Authentication and Web security protocols**