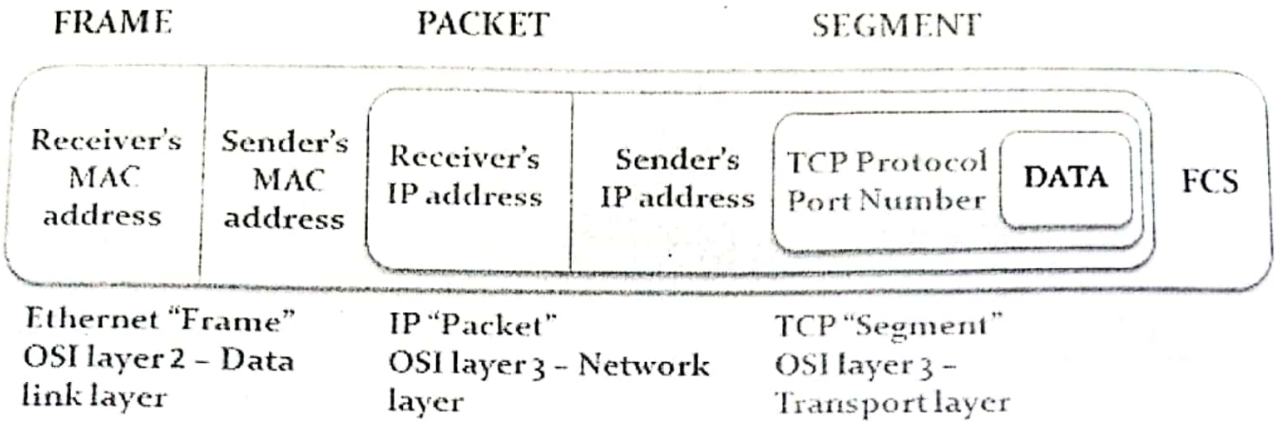
Difference Between Frame and Packet



In this article, we are going to discuss about two terms frequently used in networking as a unit of data i.e, **frame** and **packet**. The crucial difference between frame and packet is that frame is the serial collection of bits, and it encapsulates packets whereas packets are the fragmented form of data and it encapsulates segment.

Model for Network Security

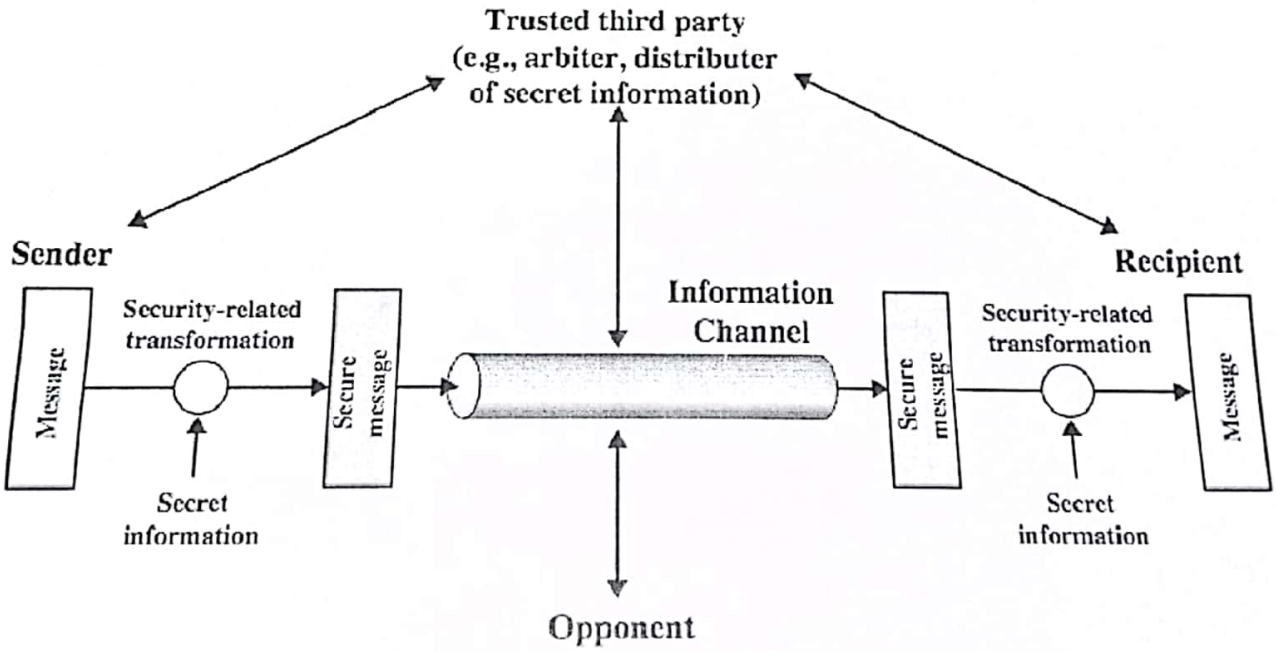


Figure 1.4 Model for Network Security

Security Services (X.800)

- **Authentication**
  - The assurance that the communicating entity is the one it claims to be
- **Access Control**
  - The prevention of unauthorized use of a resource
    - who can have access to a resource,
    - under what conditions access can occur,
    - what those accessing the resource are allowed to do
- ***Data Confidentiality***
  - The protection of data from unauthorized disclosure
- ***Data Integrity***
  - The assurance that data received are exactly as sent by an authorized entity (i.e., contains no modification, insertion, deletion or replay).
- ***Non-Repudiation***
  - Provides protection against denial by one of the entities involved in a communication of having participated in all/part of the communication.

Security Mechanisms (X.800)

Table 1.4 Relationship Between Security Services and Mechanisms

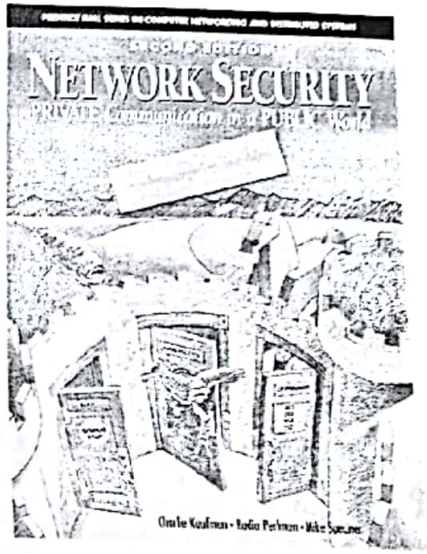
Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

http://www.itu.int/rec/T-REC-X.800-199103-I/e

The Human Element

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

-- C. Kaufman, R. Perlman, and M. Speciner.



Network Security: Private Communication in a Public World, 2/E

Kaufman, Perlman & Speciner

Prentice Hall, 2003

Security Requirements

- **Confidentiality**
  - Preserving authorized restrictions on information ***access*** and ***disclosure***, including means for protecting personal privacy and proprietary information.
- **Integrity**
  - Guarding against information ***modifications*** or ***destruction***, including ensuring information non-repudiation and authenticity.
- **Availability**
  - Ensuring timely and reliable access to and ***use*** of information

Security Threats / Attacks

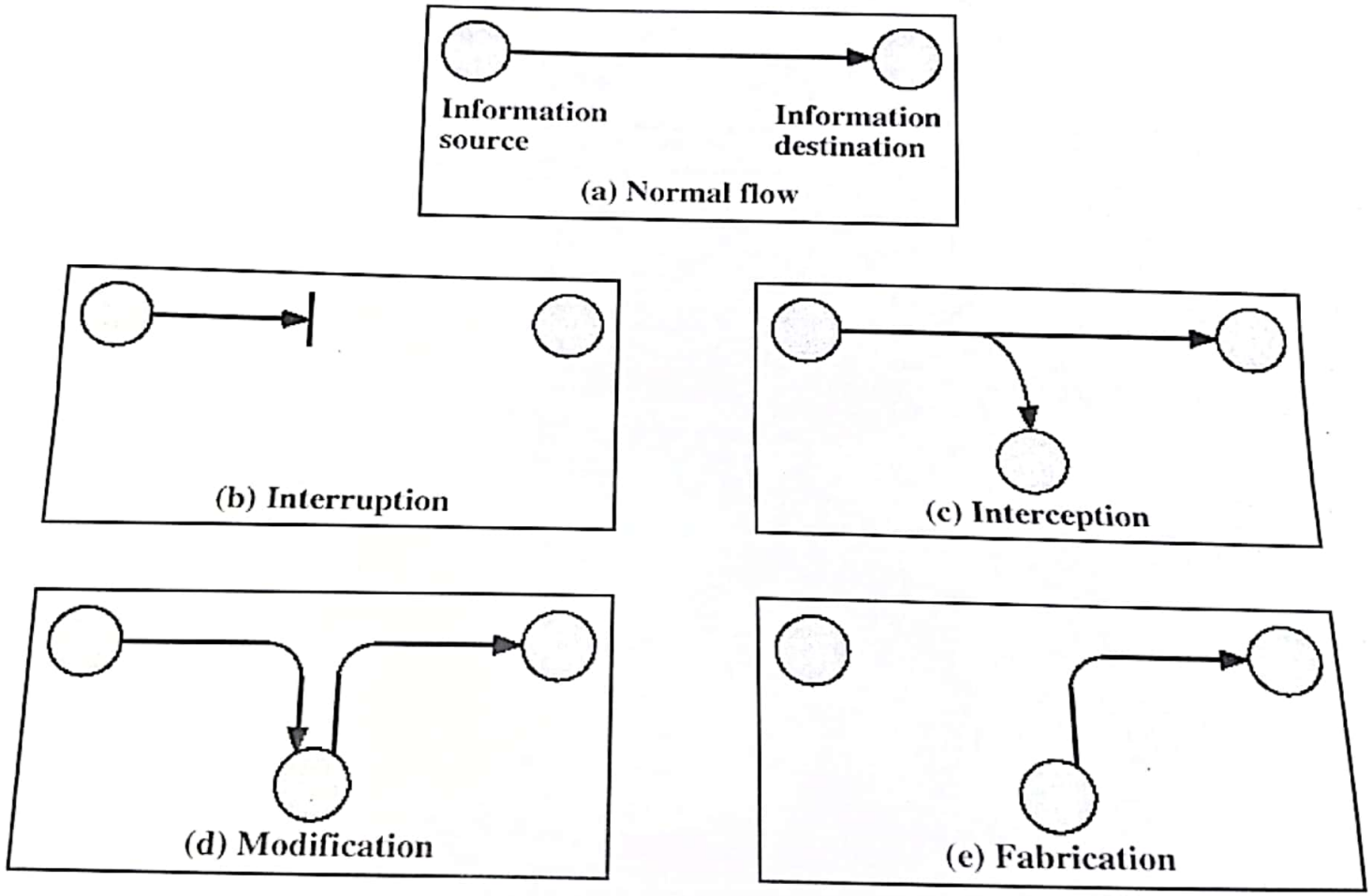
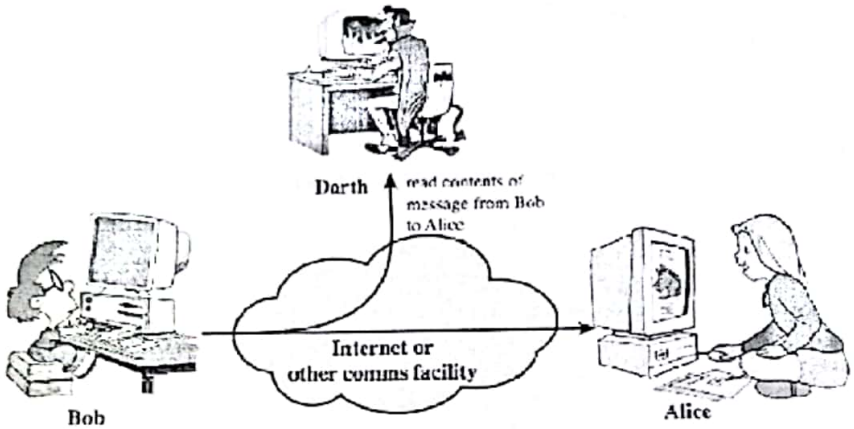
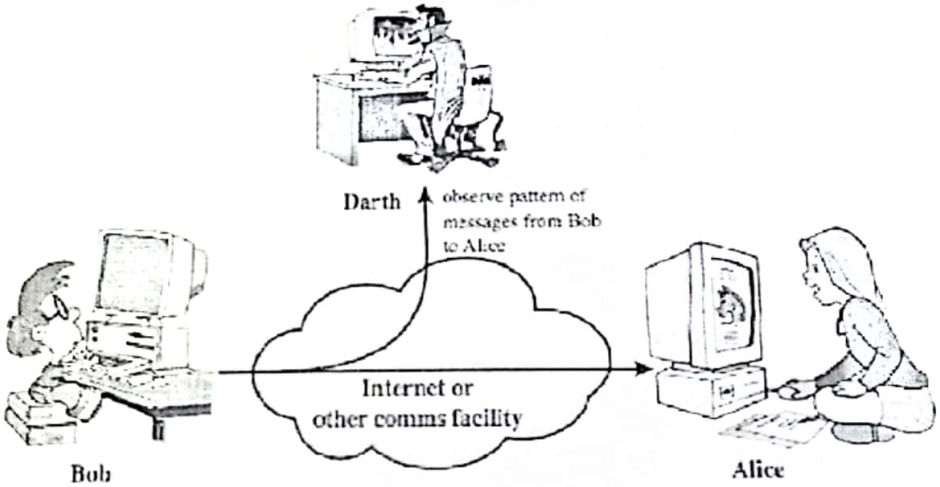


Figure 1.1 Security Threats

Passive Attacks



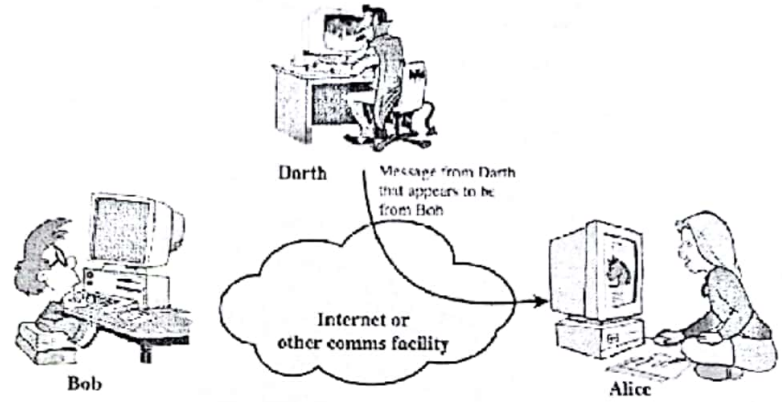
(a) Release of message contents



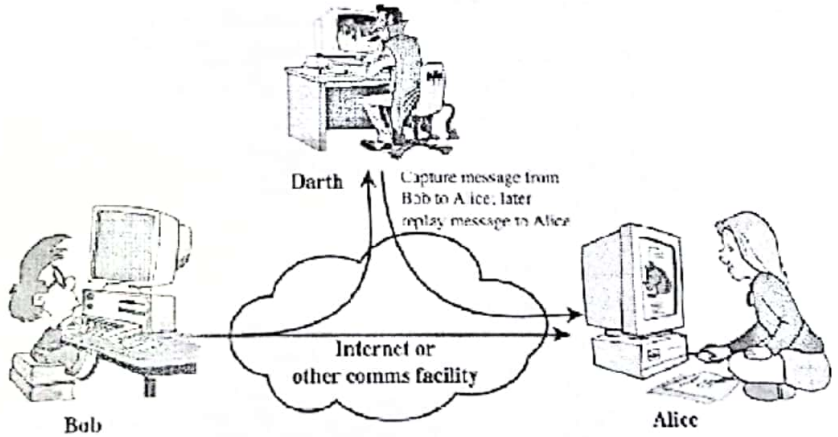
(b) Traffic analysis

Figure 1.2 Passive attacks.

Active Attacks (1)



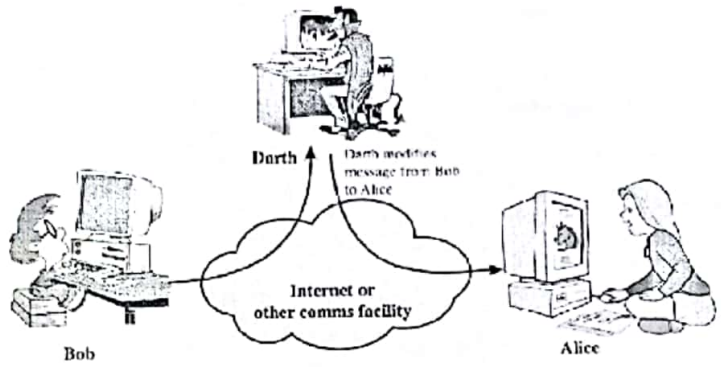
(a) Masquerade



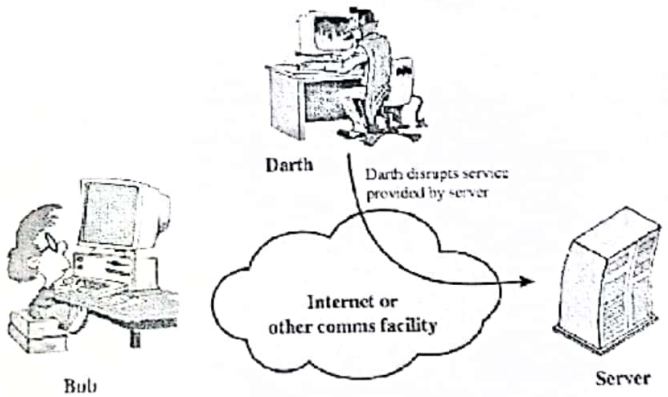
(b) Replay

Figure 1.3 Active attacks (page 1 of 2)

Active Attacks (2)



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active Attacks (page 2 of 2)

Threats & Attacks

Table 1.1 Threats and Attacks (RFC 2828)

Threat

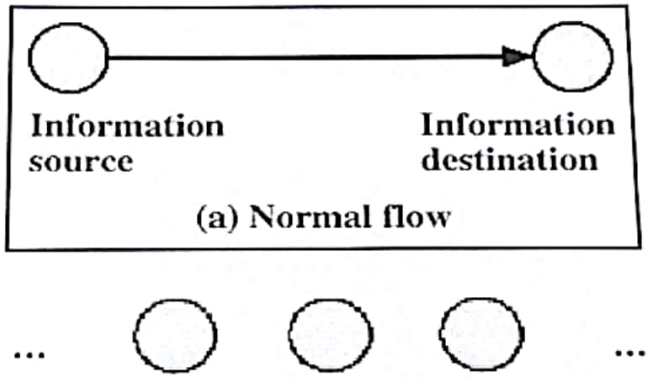
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

… but *threat* and *attack* used nearly interchangeably

Security Threats / Attacks



Security Attacks, Mechanisms & Services

- **Security *Attack***
  - Any action that compromises the security of information
- **Security *Mechanism***
  - A process / device that is designed to detect, prevent or recover from a security attack.
- **Security *Service***
  - A service intended to counter security attacks, typically by implementing one or more mechanisms.