CS 686 Special Topics in CS
Privacy and Security

Definition of Security/Privacy

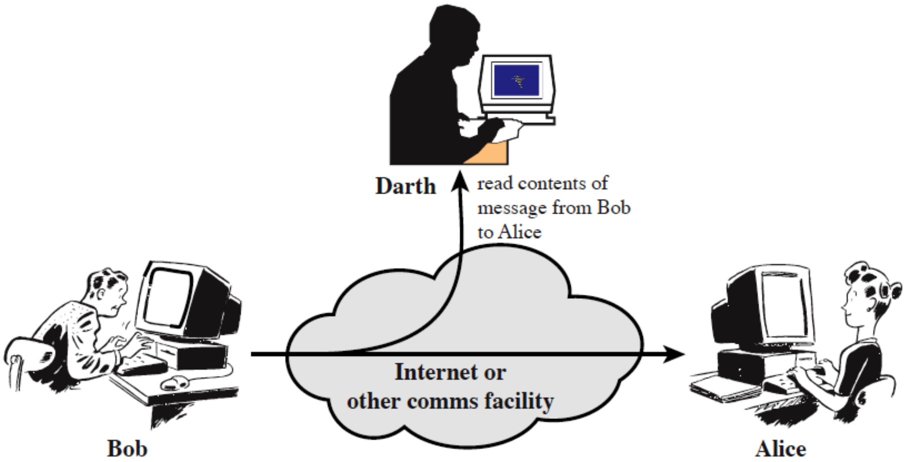
EJ Jung
ejung@cs.usfca.edu

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.

Passive attack (1) - Eavesdrop

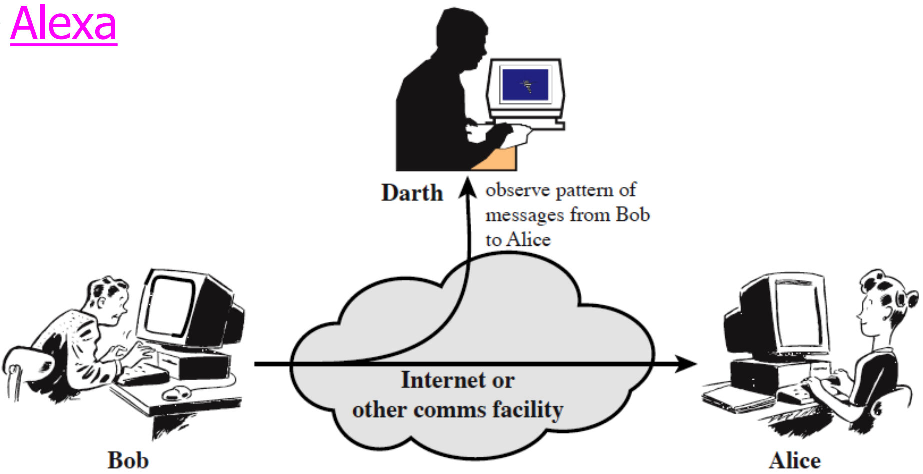
- Code talkers


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

Passive attack (2) - Analysis

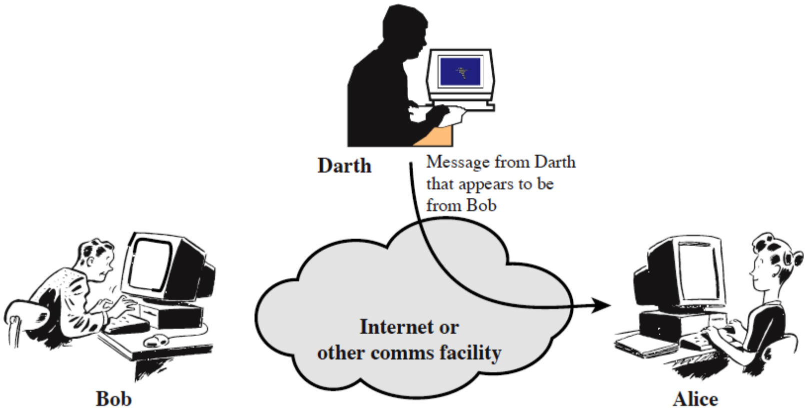
- Alexa


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

(b) Traffic analysis

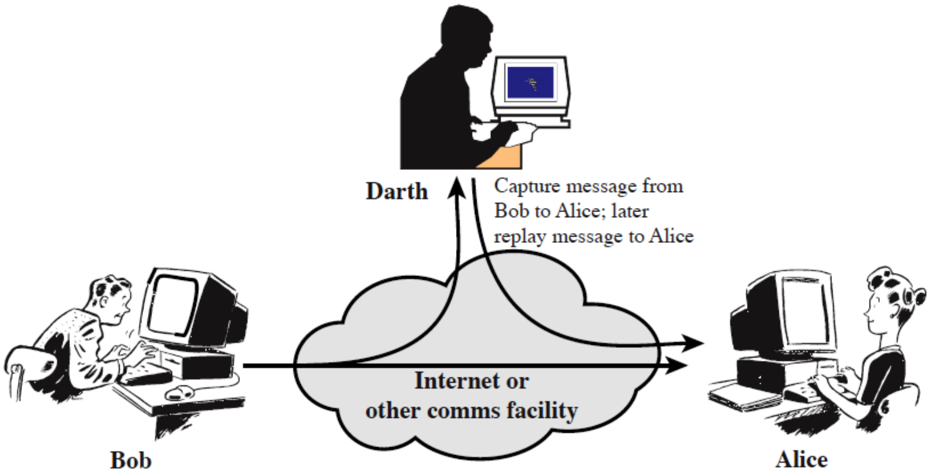
Active attack (1) - impersonation

- Impostors on Facebook


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

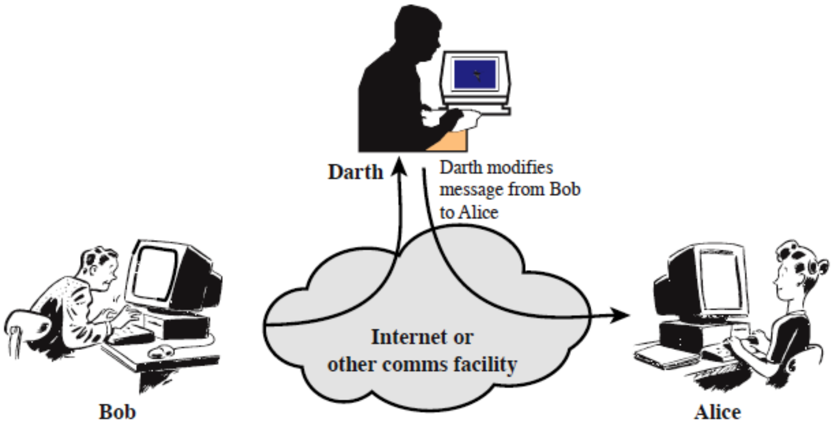
(a) Masquerade

Active (2) - replay


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

(b) Replay

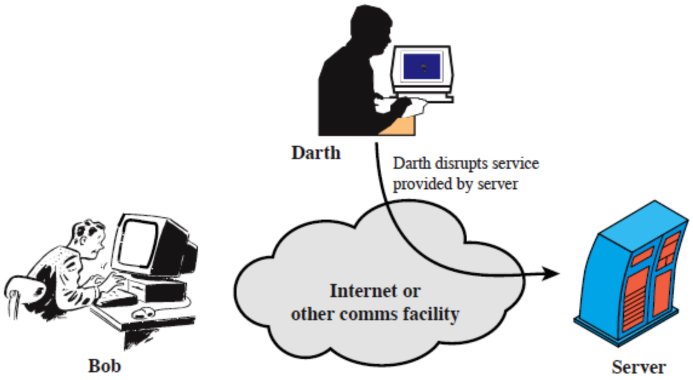
Active (3) – intercept&modify


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

(c) Modification of messages

Active (4) - DoS

- Distributed DoS


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

(d) Denial of service

Summary of attacks

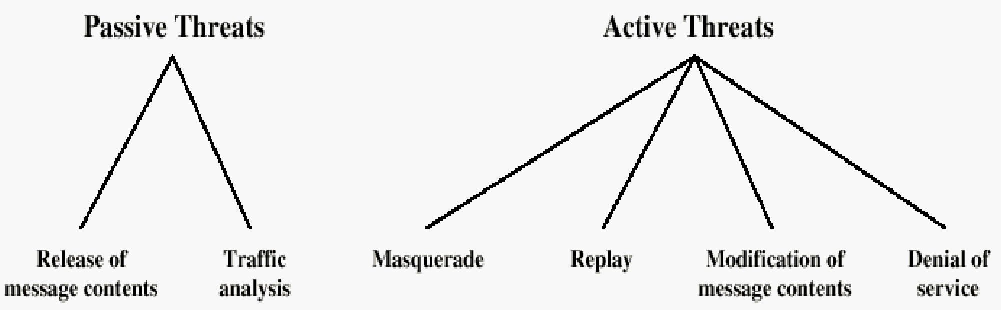


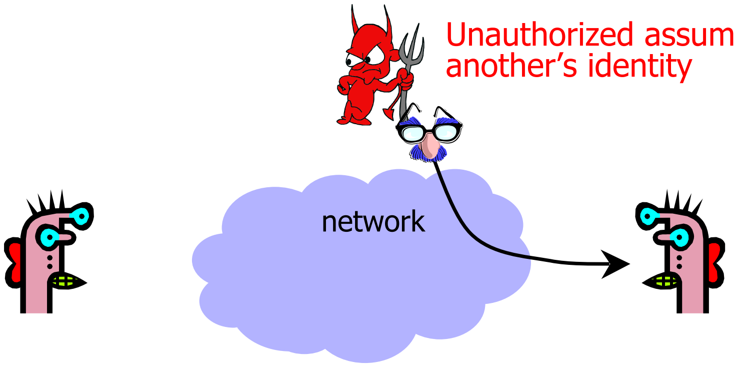
Figure 1.2 Active and Passive Security Threats

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

Attack on Authenticity

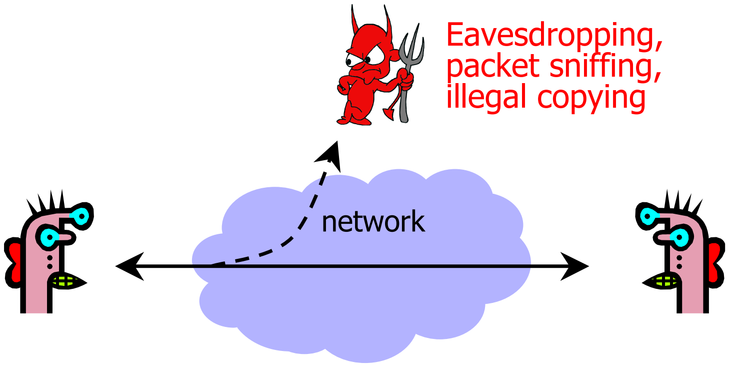
- Authenticity is identification and assurance of origin of information



Unauthorized assumption of another's identity

Attack on Confidentiality

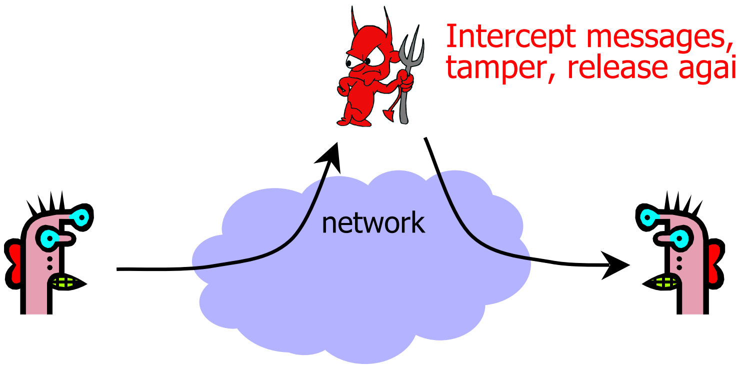
- Confidentiality is concealment of information



Eavesdropping,
packet sniffing,
illegal copying

Attack on Integrity

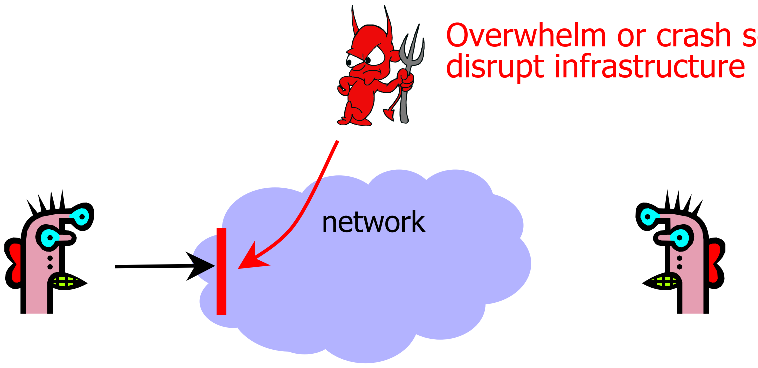
- Integrity is prevention of unauthorized changes



Intercept messages, tamper, release again

Attack on Availability

- Availability is ability to use information or resources desired



Overwhelm or crash servers, disrupt infrastructure

Famous words

- Encrypt and decrypt
- Plaintext and ciphertext
  - encrypt plaintext -> ciphertext
  - decrypt ciphertext -> plaintext
  - easy example: XOR
- Digital signature
  - as you sign on paper
  - for non-repudiation and accountability
- Session
  - one conversation/communication unit

Model for Network Security

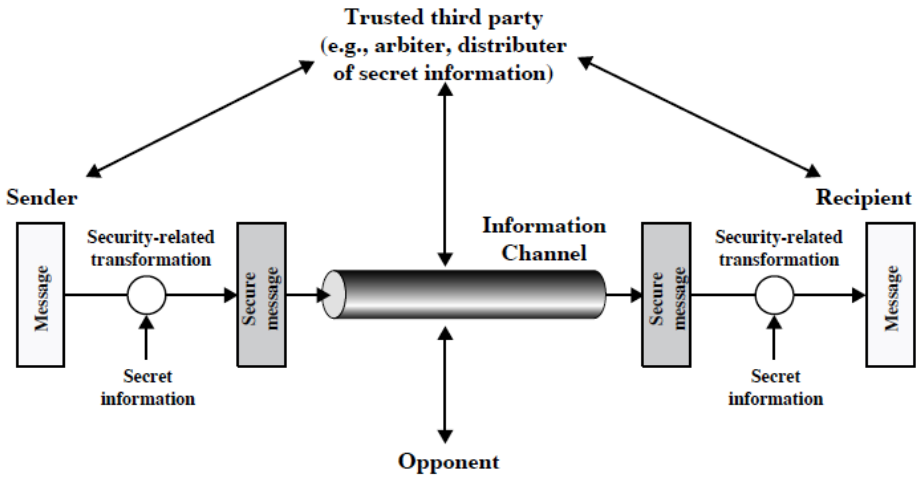


Figure 1.5 Model for Network Security

Access Control Model

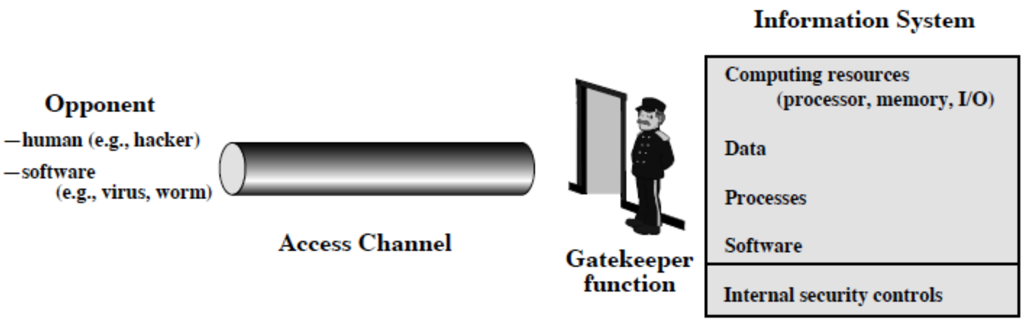


Figure 1.6 Network Access Security Model