Information System and Network Security

ICT 5301

Introduction

Information System

Network Security

- Security Violation
- Internetwork Security
  - Confidentiality
  - Authentication
  - Nonrepudiation
  - Integrity

Introduction

Security Service

- Electronic form of traditional document system
  - Difficult to differentiate between original and copy
  - Altering documents may not leave any trace
  - Authenticity may not be proved correctly
- Common Integrity Functions
  - Identification
  - Authorization
  - Signature
  - Certificate of origination and receipt
  - Access
  - Authenticity
  - Approval / Disapproval
  - Privacy

Introduction

Mechanism – Cryptographic Techniques

Threat

- Possible danger that may exploit a vulnerability

Attack

- Assault on system security
  - Gain unauthorized access to information
  - Impersonating
  - Disavow liability
  - Interfere unauthorized communication channel
  - Privacy breach

Computer Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

The Challenges of Computer Security

Security is not as simple as it might first appear to the novice. But the mechanisms used to meet those requirements can be quite complex

In developing a particular security mechanism or algorithm, one must always consider potential attacks

The procedures used to provide particular services are often counterintuitive

Having designed various security mechanisms, it is necessary to decide where to use them

Security mechanisms typically involve more than a particular algorithm or protocol

Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them

The Challenges of Computer Security

There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment

Security is still too often an afterthought to be incorporated into a system after the design is complete

Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Open System Interconnection (OSI) Arch.

ITU-T recommends X.800 “Security Architecture for OSI”

Defines a systematic way of defining and providing security requirements

It provides a useful, if abstract, overview of concepts we will study

Open System Interconnection (OSI) Arch.

Security attack

- Any actions that compromises the security of information owned by an organization (or a person)

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 the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service

Security Attacks

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.
- A threat is a possible danger that might exploit a vulnerability.

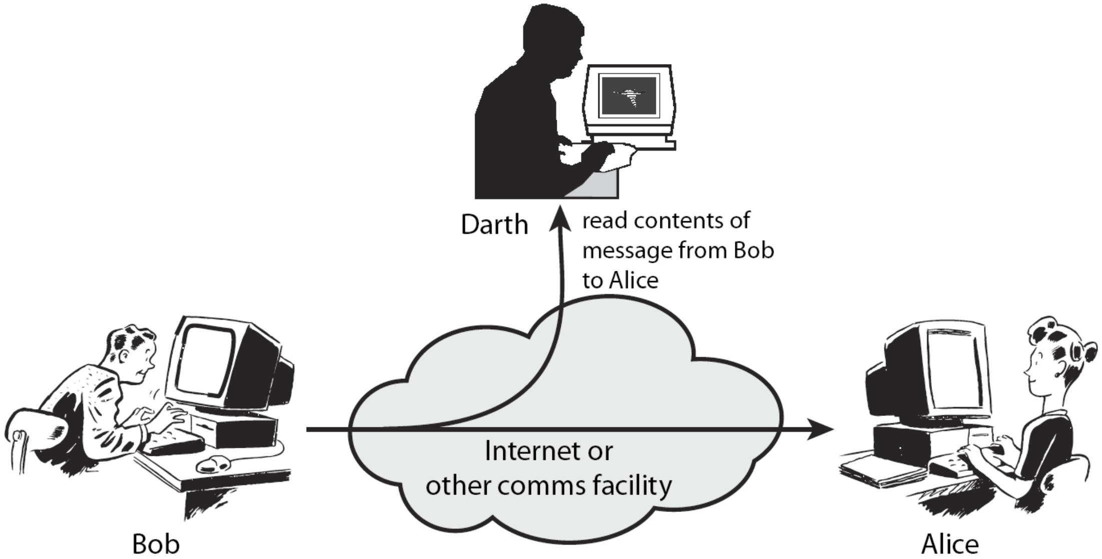
Attack

- An assault on system security that derives from an intelligent threat
- That is a deliberate attempt

Security Attacks

Passive attacks – Attempts to learn unauthorized information without modifying original message

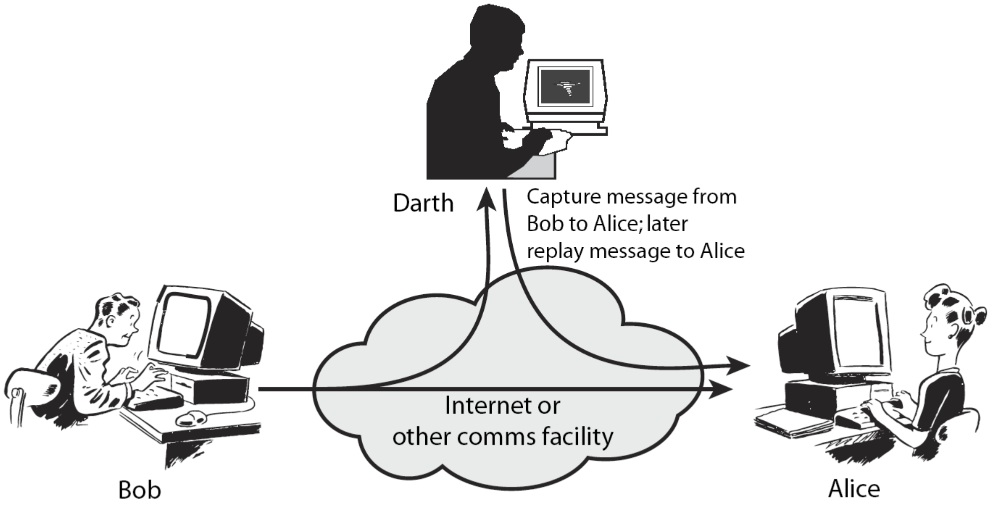
- Release of message contents
- Traffic analysis


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

Security Attacks

Active attacks – Involves modification or creation of data stream

- Masquerade - Impersonating
- Replay – Capturing data unit and replaying for unauthorized effect
- Modification of messages
- Denial of service – Prevents normal use o communication facilities
  - Suppress all messages directed to a particular destination
  - Disruption of an entire network – Disabling network / overloading network with messages


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

Security Service

Authentication – Assure communicating parties to be authentic ones

- Peer Entity Authentication
- Data Origin Authentication

Access Control – Prevent unauthorized access

- Who? When? What?

Data confidentiality – Protection against unauthorized access

- Connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality
  - From observation (source, destination, frequency, length, etc.)

Security Service

Data integrity – Assurance of proper data transfer

- Connection based
  - Connection-oriented – Check duplication, insertion, modification, reordering, replays
  - Connectionless – Generally provides protection against modification only
- Recovery based
  - With recovery – Detects violation only, manual intervention needed to recover
  - Without recovery – Attempts to recover data when violation is detected

Nonrepudiation – Protection against denial by of any party participated in a communication

Availability

Security Mechanism (X.800)

Specific Security Mechanism

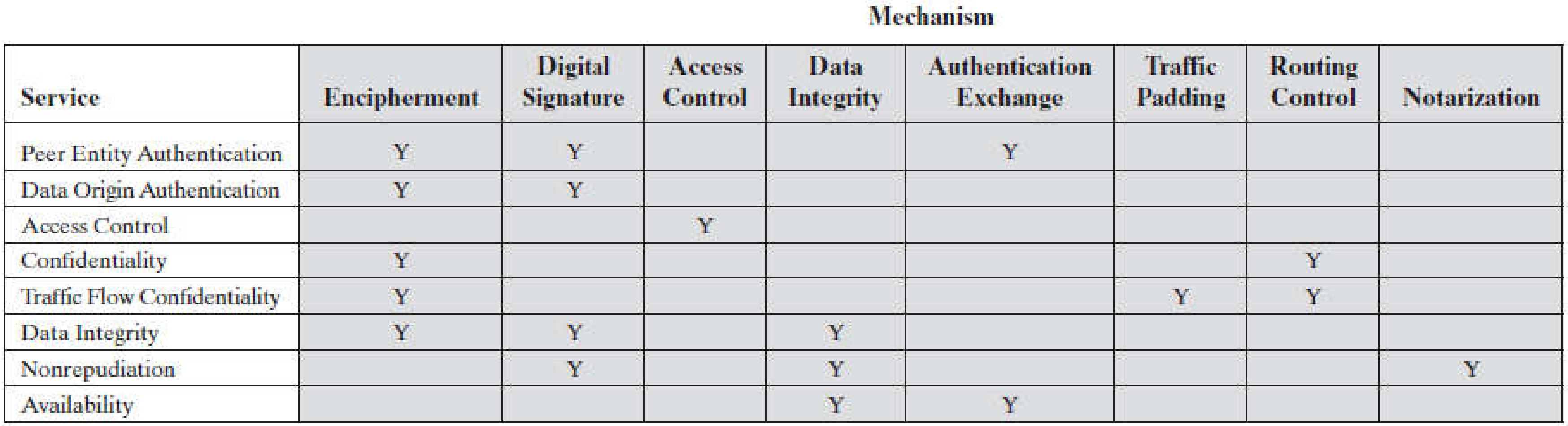
- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization

Security Mechanism (X.800)

Preserve Security Mechanism

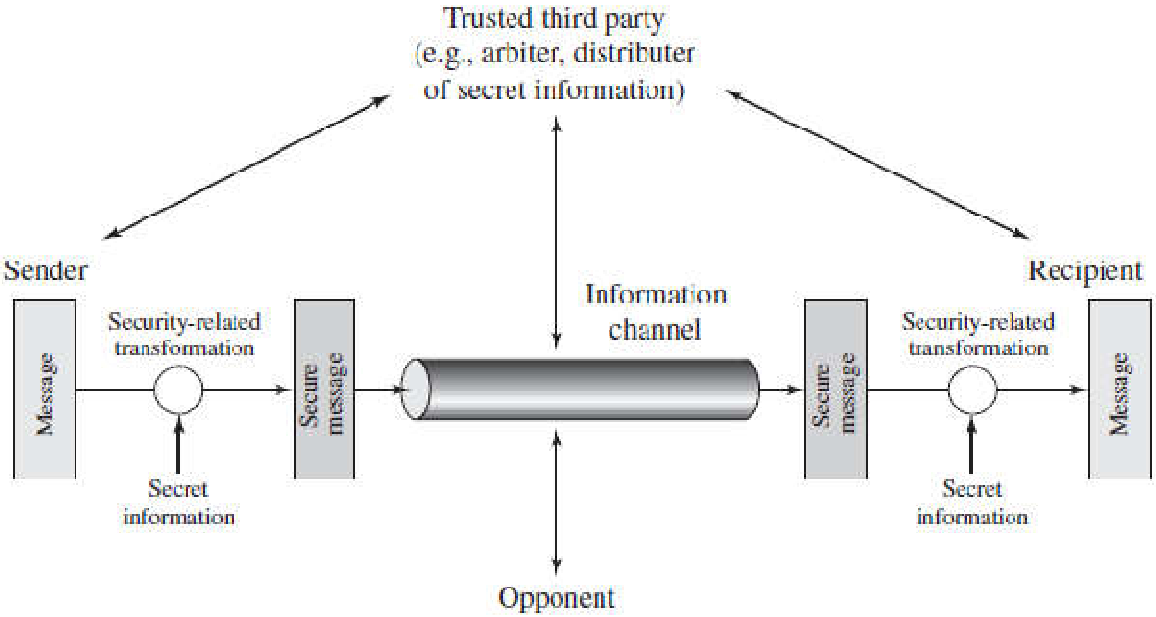
- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

Security Mechanism



	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
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			

Model for Network Security



Model for Network Security

Design an algorithm for performing the security related information

Generate the secret information to be used in the algorithm

Develop methods for the distribution and sharing of the secret information

Specify a protocol to be used

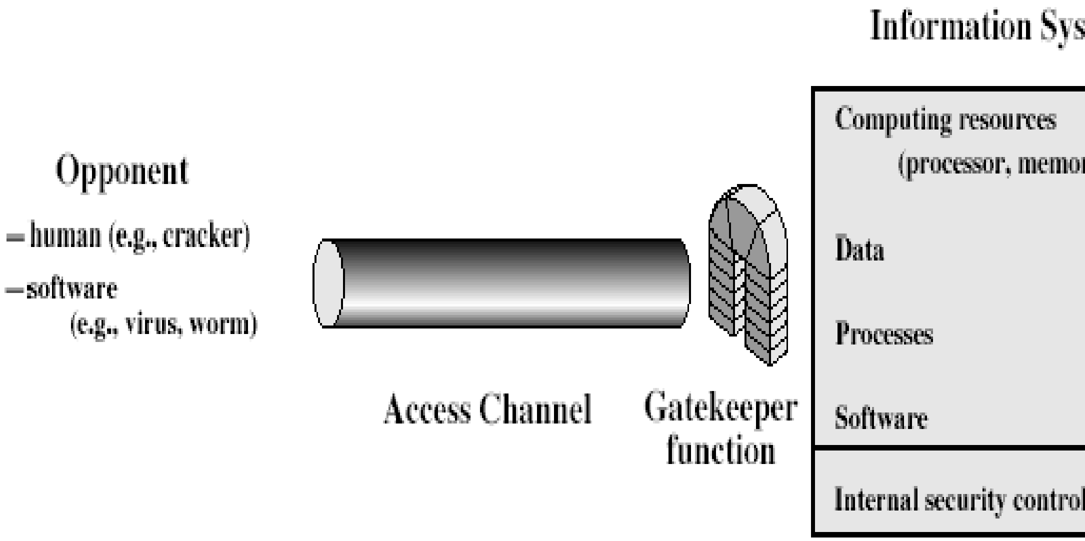
Model for Network Security

Information access threats

- Intercept or modify data on behalf of users who should not have access to that data.

Service threats

Exploit service flaws in computers to inhibit use by legitimate users



Model for Network Security

Select appropriate gatekeeper functions to identify users

Implement security controls to ensure only authorised users access designated information or resources

Reference books

Cryptography and Network Security Principles and Practices

- William Stallings

Network Security PRIVATE Communication in a PUBLIC World

- Chalie Kaufman, Radia Perlman, Mike Speciner

Marks Distribution

Mid 1 – 5th / 6th week – 30%

Mid 2 – 9th / 10th week - 30%

Final – After 14th week – 40%