

IT 422 Network Security Overview

Yasser F. O. Mohammad

2010.2.22

Teaching Team

- Instructor: Yasser F. O. Mohammad
 - Computers and Systems section (Intelligent Robotics)
 - Email: yasserfarouk@gmail.com
 - Web: <http://www.ii.ist.i.kyoto-u.ac.jp/~yasser>
- TA: Eng. Maged Ashkar
- Course Website:
 - www.ii.ist.i.kyoto-u.ac.jp/~yasser/courses/NetSecCI
- Google Group:
 - Email: netsec_2010@googlegroups.com
 - Web: http://groups.google.com/group/netsec_2010

Course Syllabus

- Introduction
- Fundamentals
 - Symmetric Key Encryption
 - Hashing and Public Key Encryption
- Applications
 - Authentication Protocols
 - E-Mail Security
 - IP Security
 - Web Security
 - LAN Security
 - Intrusion Detection
 - Malicious Software
 - Firewalls

Course Philosophy

- Maximize practical sense
- Maximize field exposure
- Minimize complex mathematics

You need to USE Network Security Algorithms and Systems not to invent new ones.

Text Books

Main Text

- Network Security Essentials
 - William Stallings

Other References

- Cryptography and Network Security
 - William Stallings
- Network Security Fundamentals
 - Gert De Laet and Gert Schauwers
- Fundamentals of Network Security
 - John E. Canavan
- Applied Cryptography
 - Bruce Schneier

Let's Play a Spy Game



- Spy knows that ENEMY will attack the CAMP at 6:00
- How can he tell the CAMP about that and know that they received the information.

Security Types

- Physical and Administrative Security
- Computer Security
- Network Security
- Internet Security

ITU-T OSI X.800

- ITU-T=International Telecommunication Unit, Telecommunication Standardization Sector
- OSI=Open Systems Interconnectivity
- X.800= Security Architecture for OSI

Threats vs. Attacks

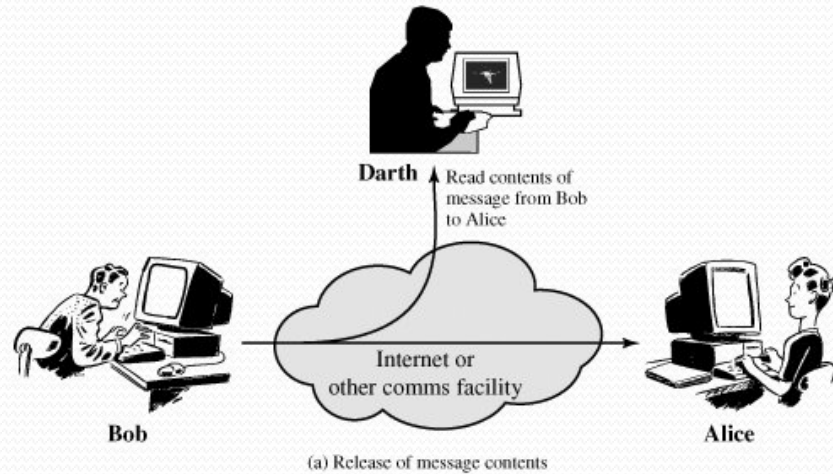
- **Threat**
A possible danger that might exploit a vulnerability.
- **Attack**
An assault on system security that derives from an intelligent threat.
- **Security mechanism**
A process that is designed to detect, prevent, or recover from a security attack.
- **Security service**
A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- **Relations Between them**
The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Attacks in X.800

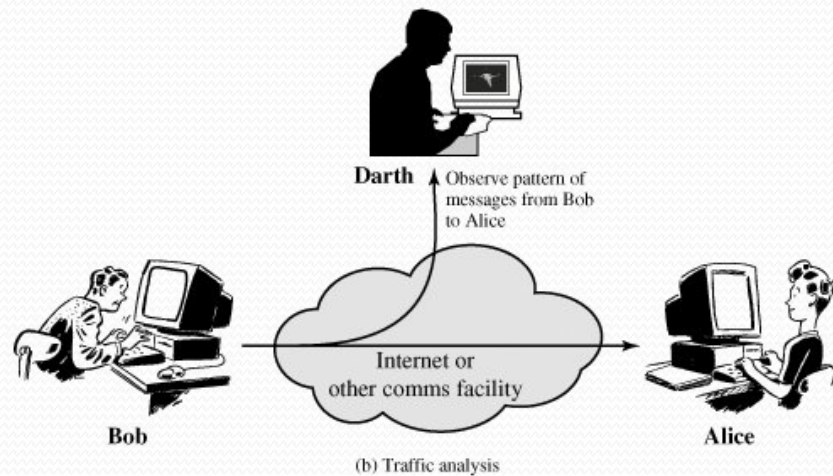
- Passive Attacks
- Active Attacks

Passive Attacks

Release of Message Contents



Traffic Analysis



Active Attacks

Masquerade



Darth
Message from Darth
that appears to be
from Bob



Bob



Internet or
other comms facility



Alice

(a) Masquerade

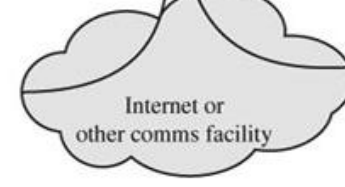
Modification



Darth
Darth modifies
message from Bob
to Alice



Bob



Internet or
other comms facility



Alice

(c) Modification of messages

Replay



Darth
Capture message from
Bob to Alice; later
replay message to Alice



Bob



Internet or
other comms facility



Alice

(b) Replay

DoS



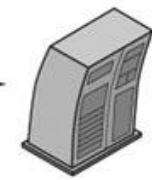
Darth
Darth disrupts service
provided by server



Bob



Internet or
other comms facility



Server

(d) Denial of service

Security Services in X.800

1. Authentication
 - Peer entity authentication
 - Data origin authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Nonrepudiation
6. Availability

Security Mechanisms in X.800

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

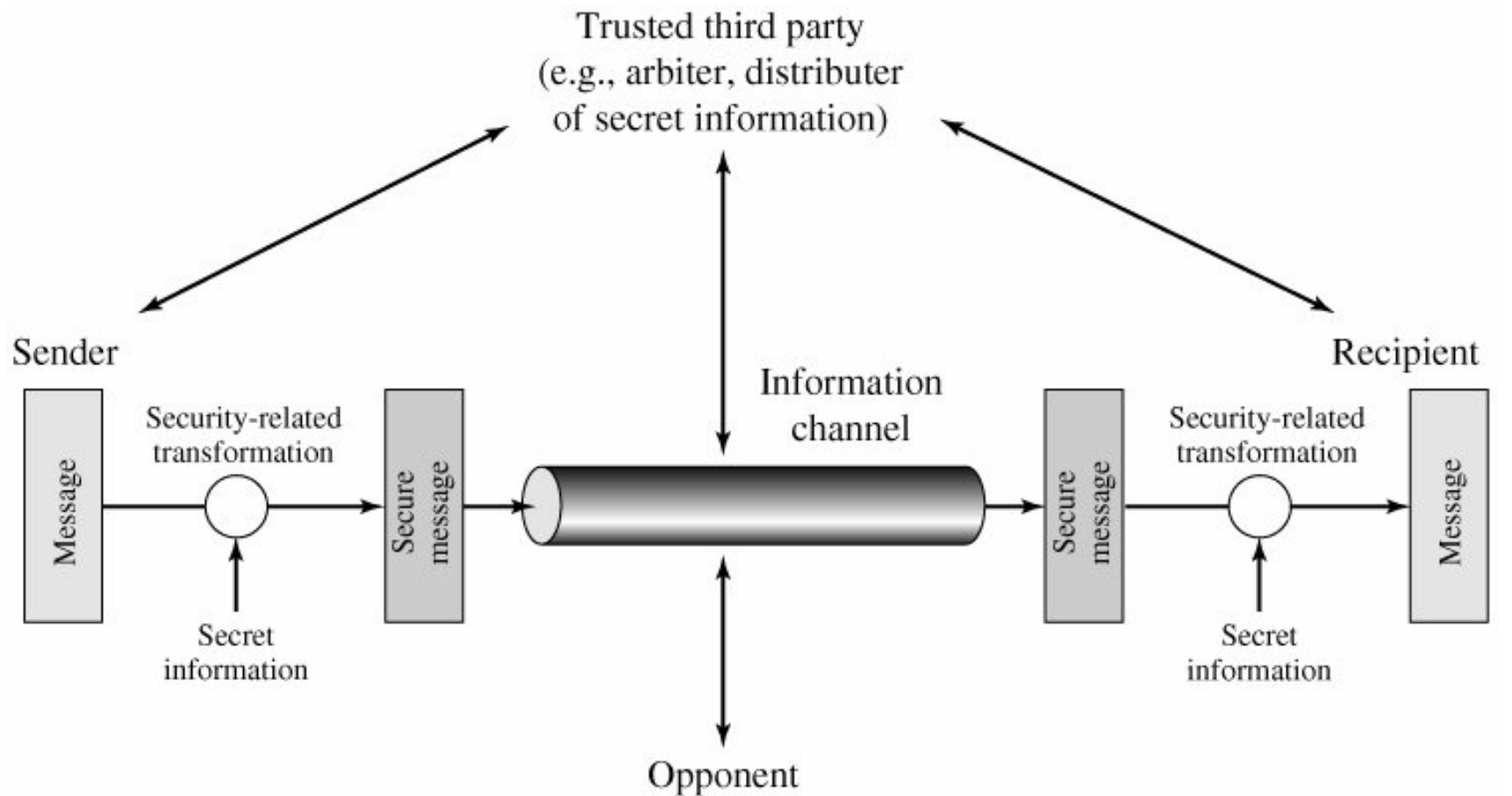
Security Mechanisms in X.800

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

Services and Mechanisms

Service	Mechanism							
	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



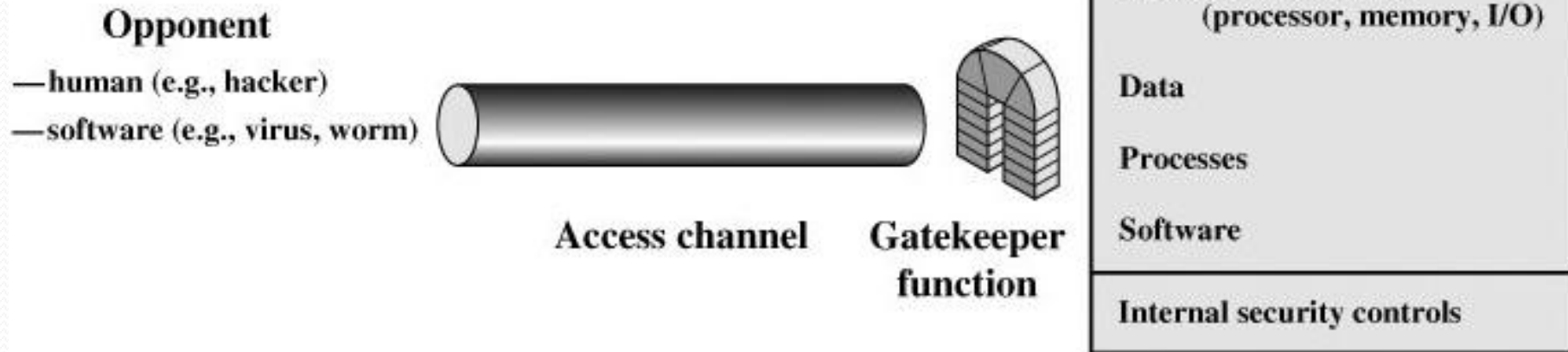
Security Techniques

- Data Transformation
 - Encryption
 - Hashing
 - Padding
- Secret Information
 - Keys
 - Algorithms

Steps of any security techniques

- Algorithm Design
- [Optional] Secret Information Generation
- [Optional] Secret Information Distribution
- Protocol Specification

Network Access Model



First Assignment

- Self Read: Section 1.6 of ‘Network Security Essentials’ about Standards and Internet Society
- Suggest as many solutions as you can to the Spy game

