Computer Security

Introduction

If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.
—Kahlil Gibran

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

SUNG KYUN KWAN UNIVERSITY

Course overview

Instructor: Tamer ABUHMED (tamer@skku.edu)

- This course will be delivered online on ICampus
  - ICampus will be updated regularly with lecture notes, lecture videos, additional materials, assignments, announcements, etc.
    It is your responsibility to ensure that you can access the ICampus and to keep up with the information on it.
  - Discussion related to the course will take place on Icampus discussion, but you can contact me as well.

Grading scheme

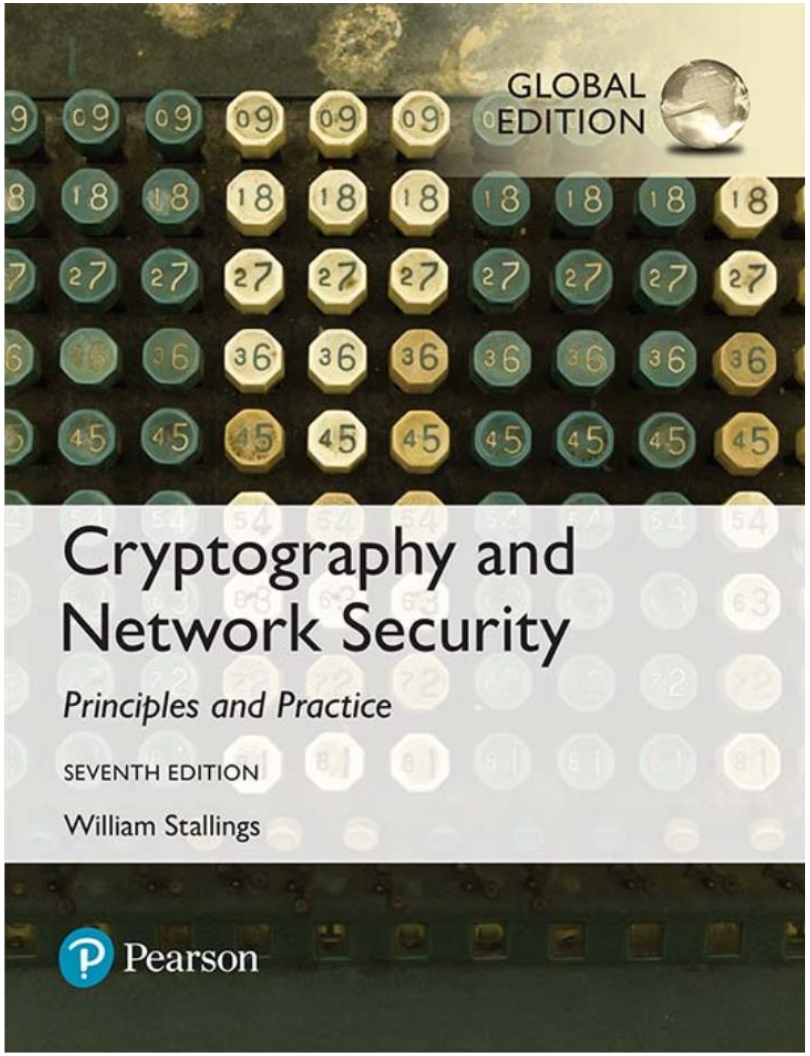
- Final (40%)
- Assignments + one min Project (50%)
- Attendance (10%)

- Regarding the assignments, you are free (even encouraged) to exchange ideas, but no sharing code or text.
- Plagiarism applies to both text and code

A note on security

- In this course, you will be exposed to information about security problems and vulnerabilities in computing systems and networks
- To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.

Required textbook



- You are expected to know
  - Most of the textbook sections
  - all the material presented in class

Course Objective

- Understand the basic principles for information and communication security, and be able to apply these principles to evaluate and criticize information system security properties
- Be able to use some important and popular security tools, like encryption, digital signatures, firewalls, intrusion detection systems (IDS)
- Be able to identify the vulnerability of the Internet systems and recognize the mechanisms of the attacks, and apply them to design and evaluate counter-measure tools

Course Contents

- Symmetric Cryptography
  - Secret key algorithms: DES/AES
- Asymmetric Cryptography
  - Public key algorithms: RSA
- Cryptographic data integrity algorithms
  - Cryptographic hash functions
    - One-way hash functions & message digests: MD5, SHA2
  - Message authentication code.
    - HMAC, CMAC
  - Digital signature
- Key management and distribution
- User authentication

Cryptography

Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

Course Contents Cont.

- Network and Internet security
  - Denial-of-service attacks
  - viruses, worms, Trojan horses
- Securing the Internet
  - Intrusion detection systems (IDSs): host- vs. network- based, signature vs. statistical detection
    - Case study: Snort and Bro
  - Firewalls, VPN and IPsec

Outline

- What is security?
- Why do we need security?
- General Picture of Security at Computing.
- Security Fields (majors)
- Few Trends and Statistics about Security
- Security Model
- Big Picture of the Course Contents

What is security?

- Dictionary.com says:
  1. Freedom from risk or danger; safety.
  2. Freedom from doubt, anxiety, or fear; confidence.

- System correctness
  - If user supplies expected input, system generates desired output
- Security
  - If attacker supplies unexpected input, system does not fail in certain ways

System correctness

Good input $\Rightarrow$ Good output

Security

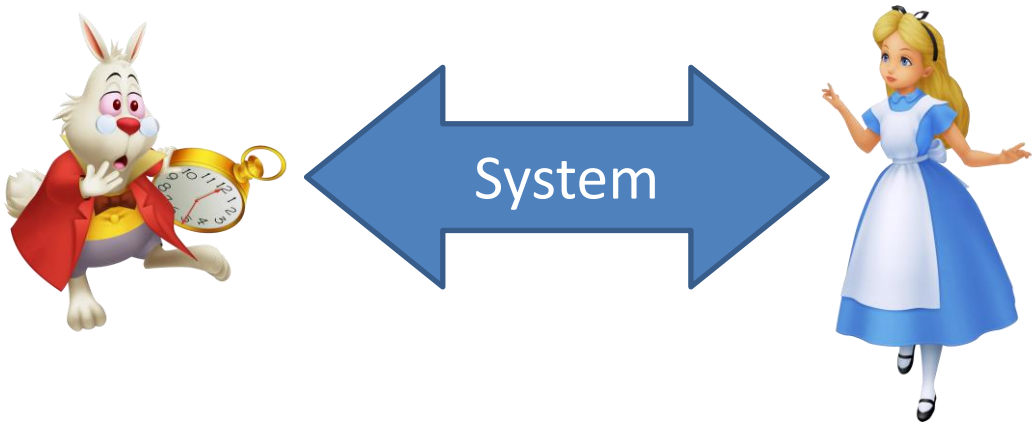
Bad input $\not\Rightarrow$ Bad output

Why do we need security?

- *Protect* vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide *authentication* and *access control* for resources
- Guarantee *availability* of resources
  - Ex: 5 9's (99.999% reliability)

General Picture of Security

- Alice and Bob are the **good guys**



Trudy is the bad "guy" 

- Trudy is our generic "intruder" adversary
  - Disrupts honest user's use of the system (Integrity, Availability)
  - Learns information intended for Alice only (Confidentiality)

Security Fields

- Network Security

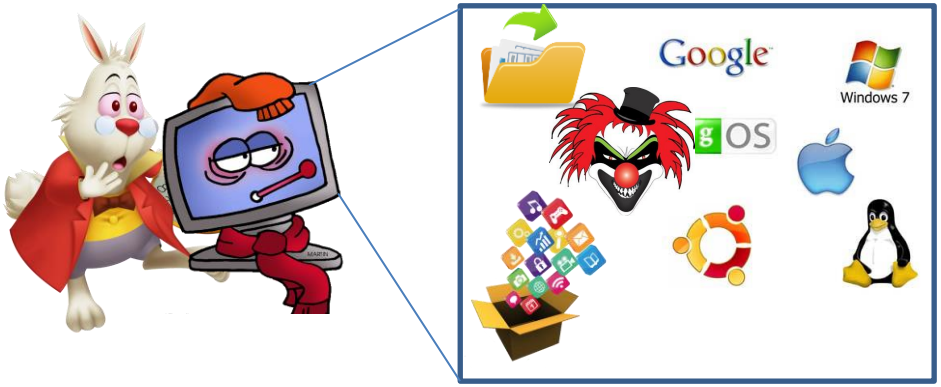
Intercepts and controls network communication

- Web Security

Sets up malicious site visited by victim; no control of network

Security Fields

- Application and Operating System Security



Controls malicious files and applications

The Computer Security Problem

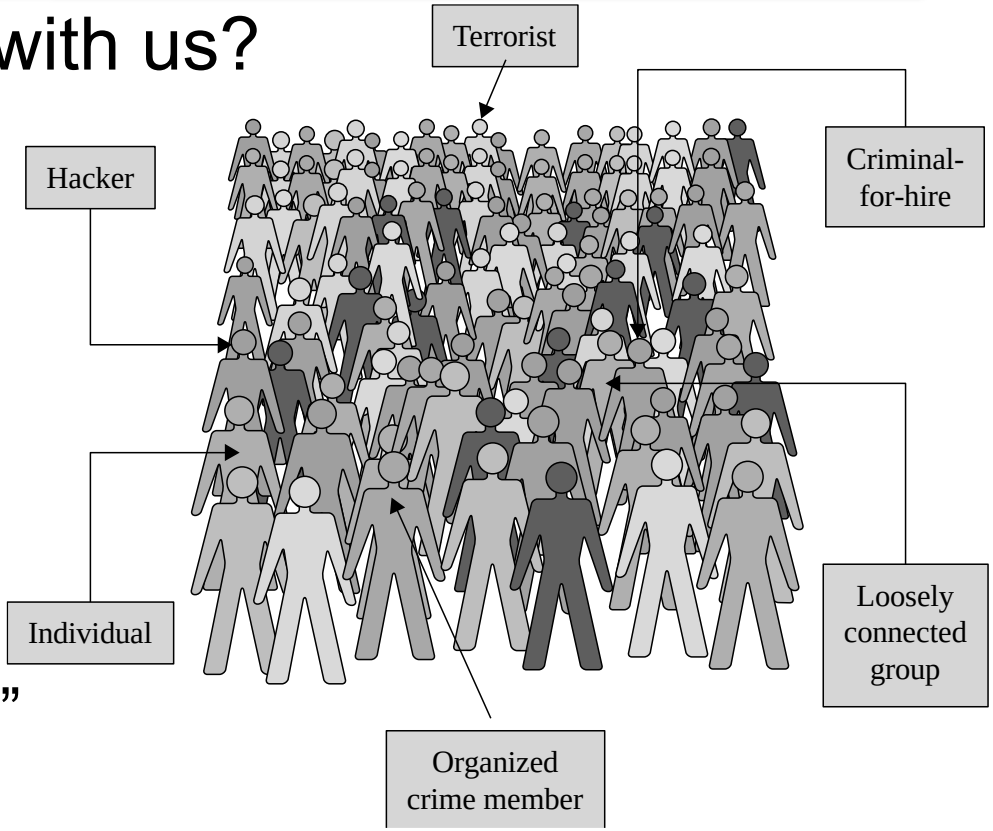
- **Lots of buggy software** (and gullible users)
- **Social engineering** (conning an individual into revealing secure information)
- **Leveraging Break-Ins of Other Systems**
- **Physical Access**

Motivations

- Military
- Terrorism
- Profits (ex. money, privileges, etc.)

Who are the adversaries?

- Who's trying to mess with us?



- Various groups:
  - Murphy
  - Amateurs
  - "Script kiddies"
  - Crackers
  - Organised crime
  - Government "cyberwarriors"
  - Terrorists
- Which of these is the most serious threat today?

[See this article]

Some terminology

- Assets

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

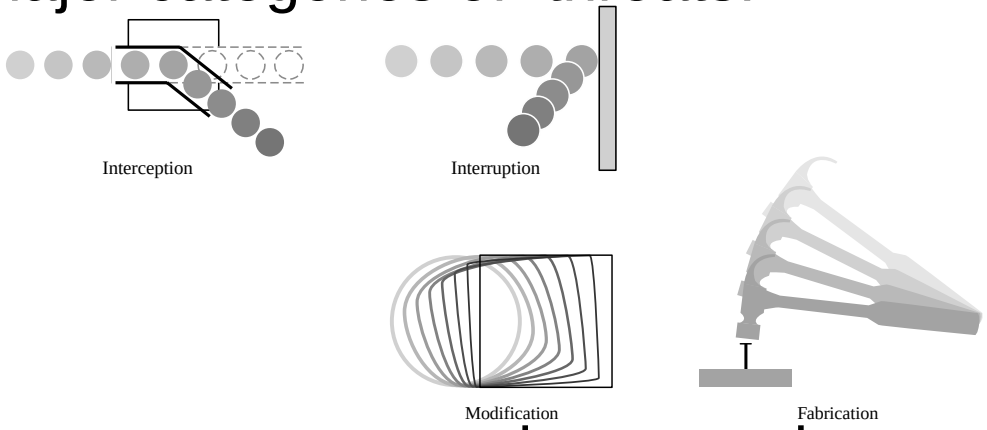
Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

- Vulnerabilities
  - Weaknesses in a system that may be able to be exploited in order to cause loss or harm
  - e.g., a file server that doesn't authenticate its users

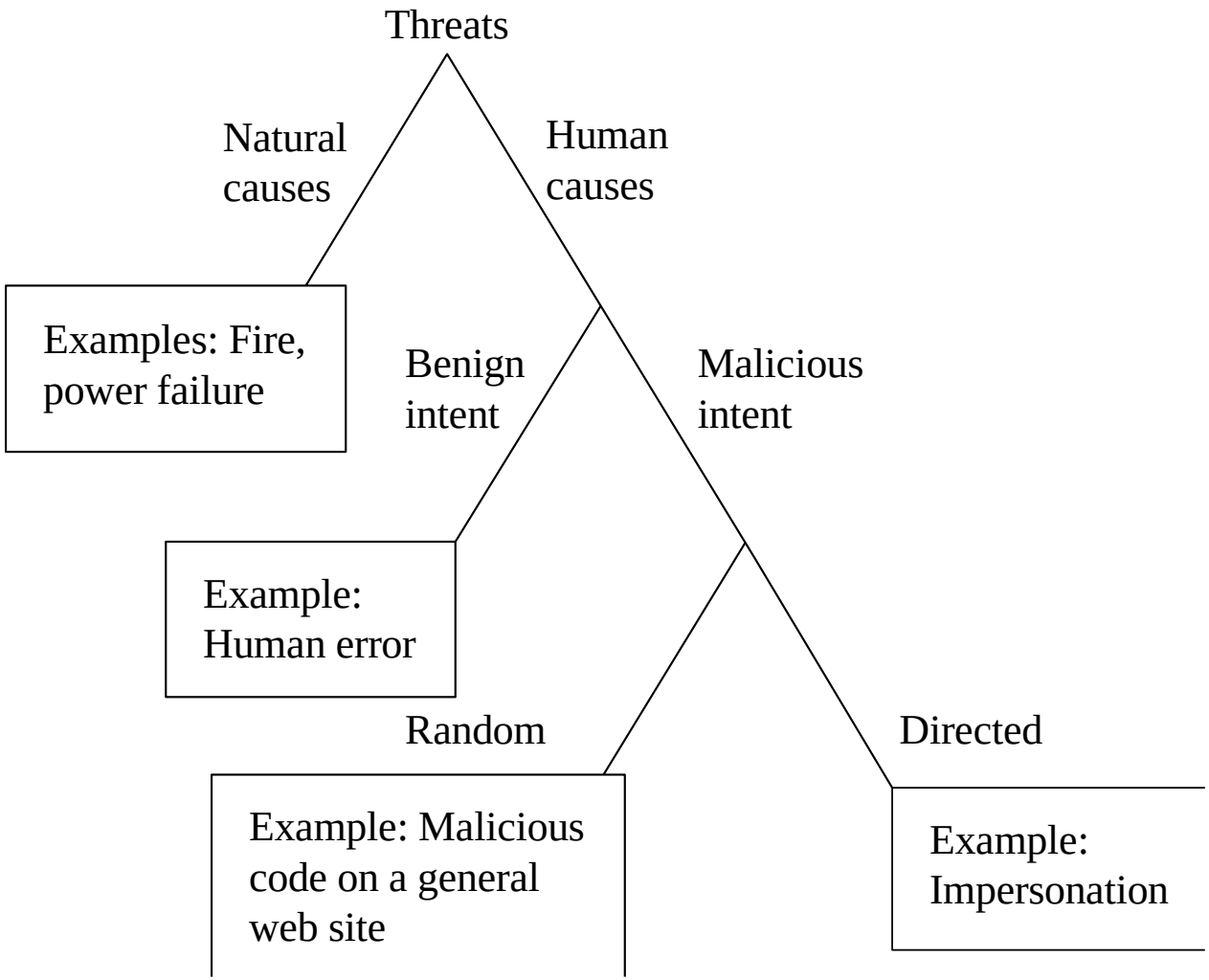
Some terminology

- Threats
  - A loss or harm that might befall a system
  - e.g., users' personal files may be revealed to the public
  - There are four major categories of threats:
    1. Interception
    2. Interruption
    3. Modification
    4. Fabrication



  - When designing a system, we need to state the threat model
    - Set of threats we are undertaking to defend against
    - Whom do we want to prevent from doing what?

Types of Threats



Some terminology

Attack

An action which exploits a vulnerability
e.g., telling the file server you are a different user in an attempt to read or modify their files

Control

Removing or reducing a vulnerability
You control a vulnerability to prevent an attack and block a threat.
How would you control the file server vulnerability?
Our goal: control vulnerabilities

Methods of defence

- How can we defend against a threat?
  - Prevent it: prevent the attack
  - Deter it: make the attack harder or more expensive
  - Deflect it: make yourself less attractive to attacker
  - Detect it: notice that attack is occurring (or has occurred)
  - Recover from it: mitigate the effects of the attack
- Often, we'll want to do many things to defend against the same threat
  - "Defence in depth"

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation

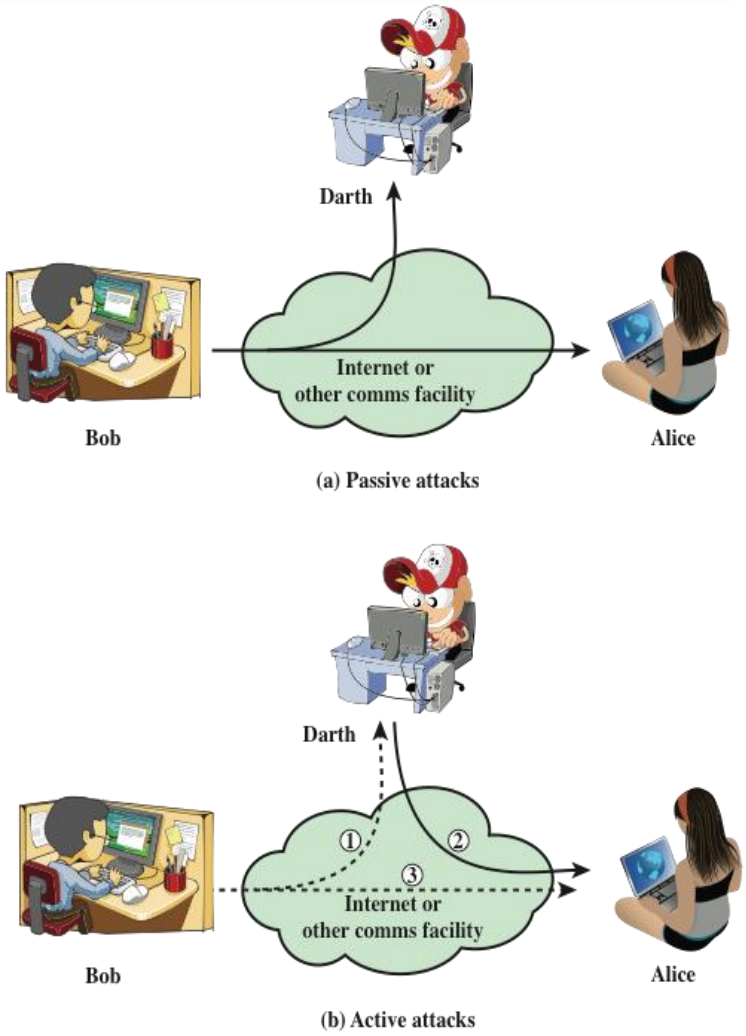
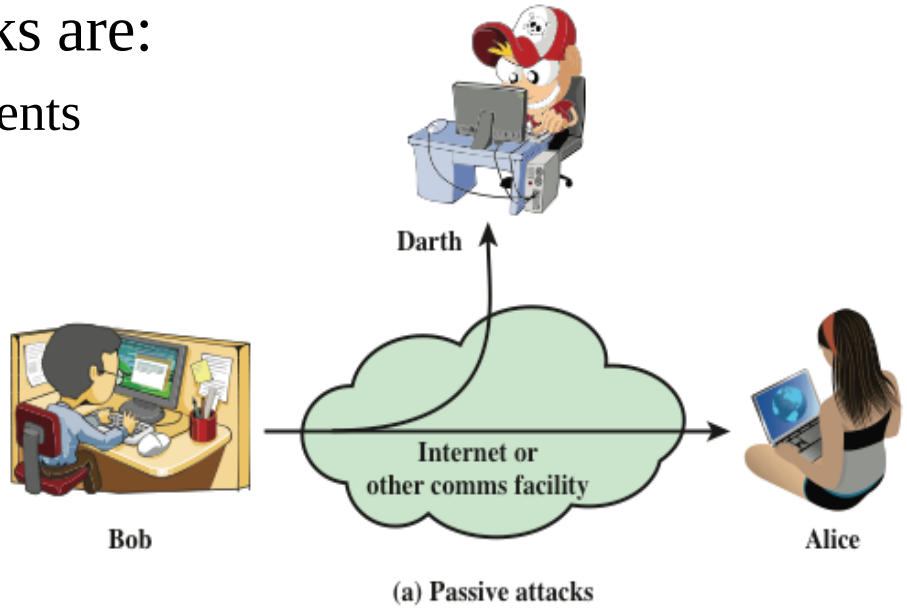


Figure 1.2 Security Attacks

Passive Attacks

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis



(a) Passive attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

Active Attacks

- Involve some **modification** of the data stream or the creation of a false stream
- **Difficult** to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to **detect** attacks and to **recover** from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

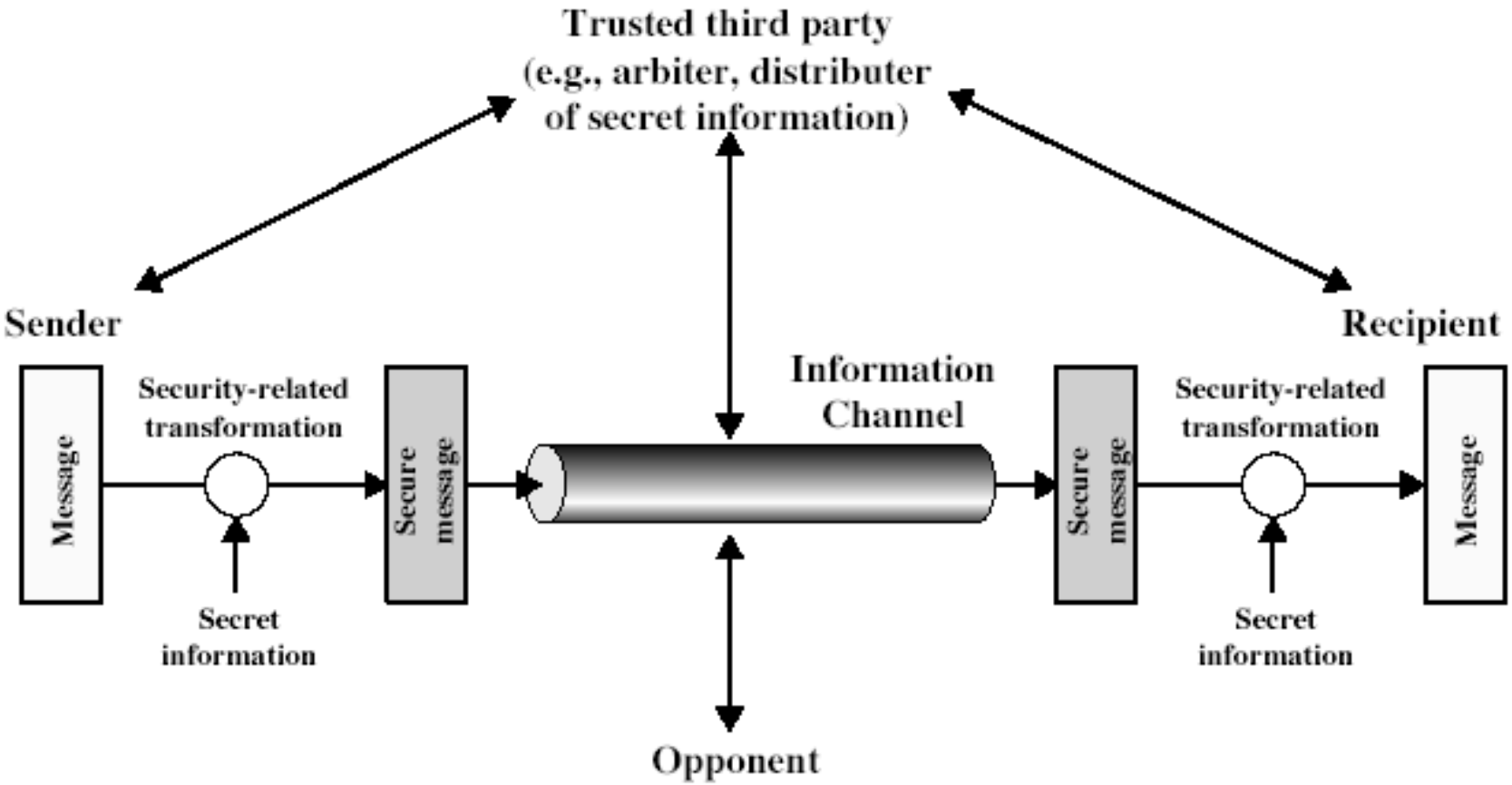
- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security Model

Model for Network Security



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

Alice's Online Bank

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Trudy view the situation?

The Basic Components 1/3

- AOB must prevent Trudy from learning Bob's account balance
- **Confidentiality:** prevent unauthorized *reading* of information
  - Cryptography used for confidentiality

The Basic Components 2/3

- Trudy must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- **Integrity:** detect unauthorized *writing* of information
  - Cryptography used for integrity

The Basic Components 3/3

- AOB's information must be available whenever it's needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a timely manner when needed
- Availability is a "new" security concern
  - Denial of service (DoS) attacks

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Cryptography

- “Secret codes”
- The book covers
  - Classic cryptography
  - Symmetric ciphers
  - Public key (Asymmetric) cryptography
  - Hash functions++
  - Advanced cryptanalysis

Protocols

- "Simple" authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Real-world security protocols
  - SSH, SSL, IPSec, Kerberos
  - Wireless: WEP, GSM

Access Control

- Authentication
  - Passwords
  - Biometrics
  - Other methods of authentication
- Authorization
  - Access Control Lists/Capabilities
  - Multilevel security (MLS), security modeling, covert channel, inference control
  - Firewalls, intrusion detection (IDS)

Think Like Trudy

- In the past, no respectable sources talked about “hacking” in detail
  - After all, such info might help Trudy
- Recently, this has changed
  - Lots of books on network hacking, evil software, how to hack software, etc.
  - Classes teach virus writing, SRE, etc.

SRE: Site Reliability Engineer

Think Like Trudy

- Good guys must think like bad guys!
- A police detective…
  - …must study and understand criminals
- In information security
  - We want to understand Trudy's methods
  - Might think about Trudy's motives
  - We'll often pretend to be Trudy

Think Like Trudy

- Is all of this security information a good idea?
- Bruce Schneier (referring to *Security Engineering*, by Ross Anderson):
  - "It's about time somebody wrote a book to teach the good guys what the bad guys already know."

Think Like Trudy

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice's and/or Bob's stupidity
- But, we **cannot** act like Trudy
  - Except in this class…

In This Course…

- Think like the bad guy
- Always look for weaknesses
  - Find the ***weak link*** before Trudy does
- It's OK to break the rules
  - What rules?
- Think like Trudy
- But don't do anything illegal!