CS 4920/5920 Applied Cryptography

Security Overview & Chapter 1

Lecture Outline

- Security objectives and the CIA triad
- Security violation examples
- Computer security challenges and design principles
- Computer security terms
- Security attacks – passive vs. active
- Defensive Mindset and Kerckhoff's Principle
- Security by Obscurity

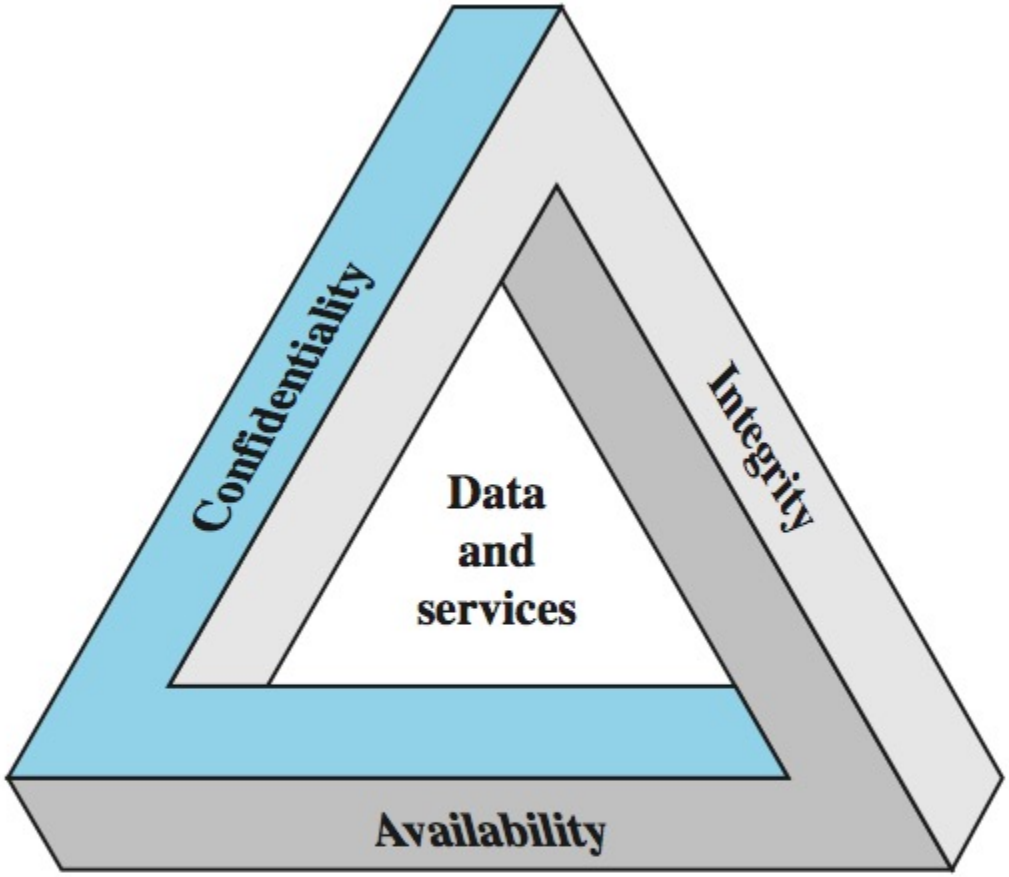
Lecture Objectives

- Identify security objectives and requirements (*e.g., what is the defense trying to protect?)*
- Define terms used in computer security
- Explain security concepts
- Define the threat scope and relevance (*e.g., what type of threat and is it important for this system?)*
- Practice the common design principles when designing secure schemes

Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)
  - NIST *Computer Security Handbook*

Key Security Concepts



(referred to as the CIA triad)

Three key objectives that are at the heart of computer security - 1

- **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.

A loss of confidentiality is the unauthorized disclosure of information.

Three key objectives that are at the heart of computer security - 2

- **Integrity:** This term covers two related concepts:
  - **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.

A loss of integrity is the unauthorized modification or destruction of information or system function.

Three key objectives that are at the heart of computer security - 3

- **Availability:** Assures that systems work promptly and service is available or accessible to authorized users.

A loss of availability is the disruption/denial of access to or use of information or an information system.

Additional Concepts

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. (Related to source integrity.)

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - Nonrepudiation, fault isolation, …

Examples of Security Violations - 1

- *Scenario* User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure.
- *Violation* User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission

Examples of Security Violations - 2

- *Scenario* A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer.
- *Violation* User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Examples of Security Violations - 3

- *Violation* Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

Quiz 1

- For the following two examples,
  -- Identify which of the followings are being violated (among *confidentiality*, *integrity*, *availability*, *authentication*, and *accountability*)
  -- Explain the potential impact of the violations and describe a scenario that highlights such impact

Quiz 1A. Examples of Security Violations - 4

- *Scenario* An employee is fired. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action.
- *Violation* The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.

Quiz 1B. Examples of Security Violations - 5

- *Scenario* A message is sent from a customer to a stockbroker with instructions for various transactions.
- *Violation* Subsequently, the investments lose value and the customer denies sending the message.

Levels of Impact

- Can define 3 levels of impact from a security breach
  - Low
    - E.g., minor degradation of service, minor damage to assets, minor financial loss, minor harm individuals.
  - Moderate
    - E.g., significant degradation of service, significant …
  - High
    - E.g., severe degradation of service, severe…

Examples of Security Requirements

- Confidentiality
  - passwords (high), student grades (moderate), directory information (low)
- Integrity
  - patient allergy information (high), Web forum for registered users (moderate), anonymous online poll (low)
- Availability
  - authentication service (high), public Web site for a university (moderate), online telephone directory lookup application (low)

Computer Security Challenges

1. not simple (even when requirements seem to be straightforward, mechanisms can be complex)
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought in system design
10. regarded as impediment to using system

Fundamental Security Design Principles, 1

- 1. *Economy of mechanisms*: Simple and small design
- 2. *Fail-safe default*: E.g., most file access system have the access decisions based on permissions rather than exclusion
- 3. *Complete mediation*: Every access must be checked against access control; resource-intensive
- 4. *Open design*: Related to Kerckhoff's Principle
- 5. *Separation of privilege:* Multiple privilege attributes are required to achieve access to a restricted resource
- 6. *Least privilege:* Use the least set of privileges necessary to perform the task

Fundamental Security Design Principles, 2

- 7. *Least common mechanism:* Minimize the functions shared by users
- 8. *Psychological acceptability:* Security should not interfere with the work of users
- 9. *Isolation:* Logical (and physical) isolation for file or subsystem access
- 10. *Encapsulation:* Encapsulation of procedures or data objects
- 11. *Modularity: E*.g., plug-and-play
- 12. *Layering*: Multiple, overlapping protection approaches, e.g., defense in depth
- 13. *Least astonishment*: Reduce user's astonishment

Security Terms

- **Vulnerability** – a weakness/opening allowing attacker threat
- **Threat** – a potential for violation of security
- **Risk** - where a threat intersects with a vulnerability, risk is present (also accounts for the threat impact)
- **Attack** – an assault on system security, a deliberate attempt to evade security services
- **Security mechanism** - a process/device 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; can incorporate one or more security mechanisms

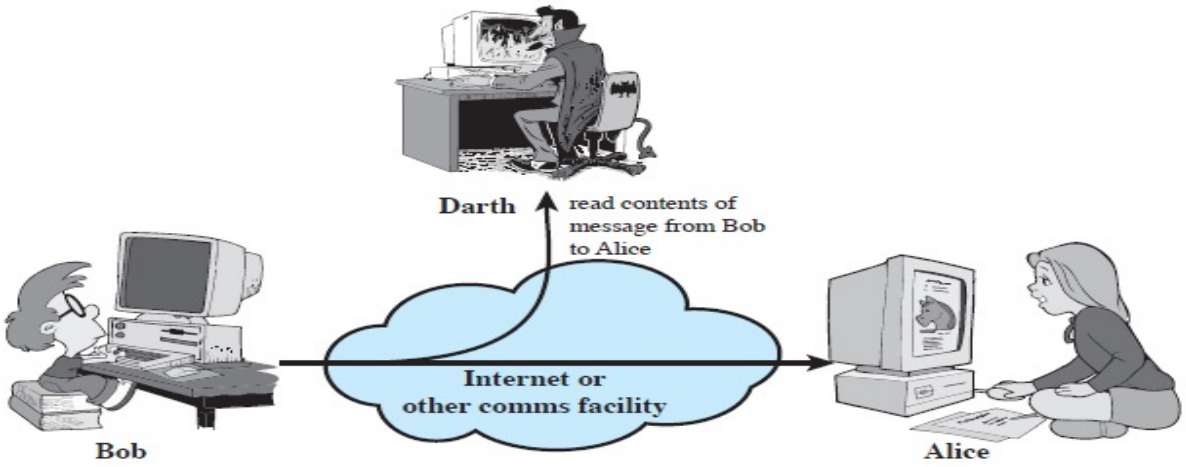
Security Attack

- Passive Attacks
  - A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Active Attacks
  - An active attack attempts to alter system resources or affect their operation.

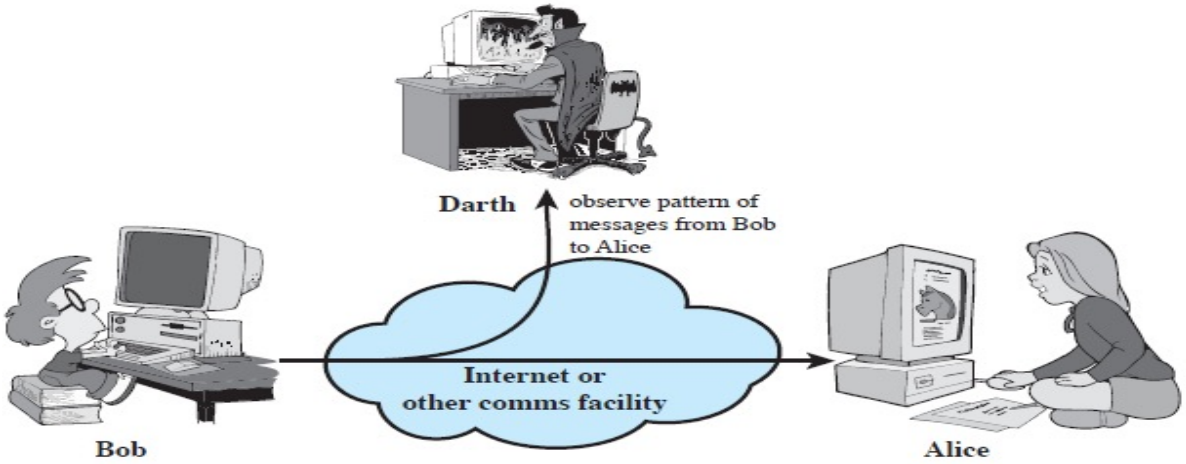
Passive Attacks

- Two types of passive attacks are:
  - Release of message contents
  - Traffic analysis
    - Monitor traffic flow to determine location and identity of communicating hosts and could observe the frequency and length of messages being exchanged

- Passive attacks are difficult to detect because they do not involve any alteration of the data.
- Our main goal is to prevent their success



(a) Release of message contents



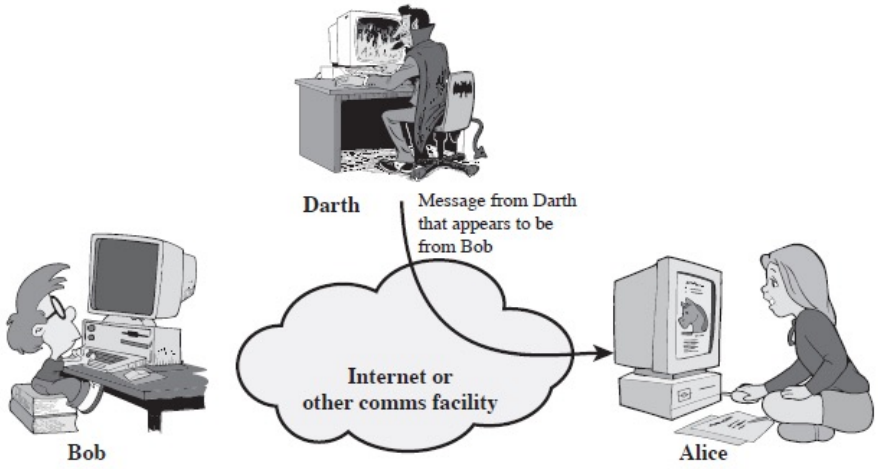
(b) Traffic analysis

Figure 1.2 Passive attacks.

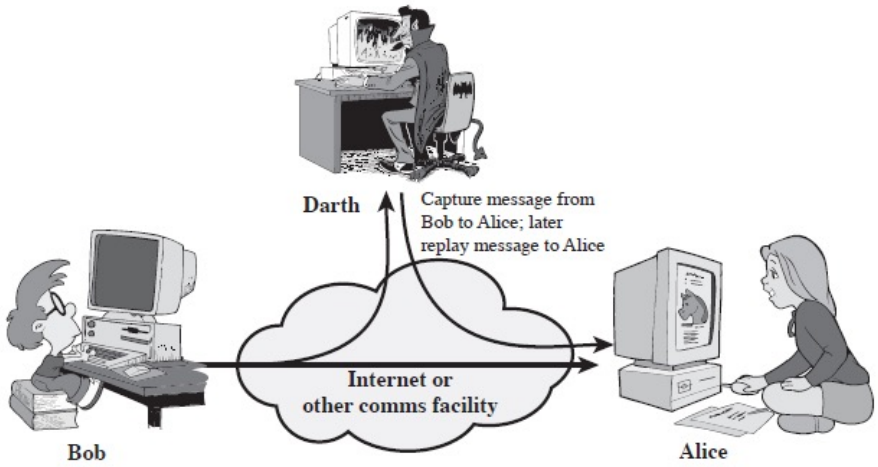
Active Attacks

- Four types of active attacks are:
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service (DoS)

- Active attacks are difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities.
- Our main goal is to detect them and to recover from any disruption or delays caused by them.

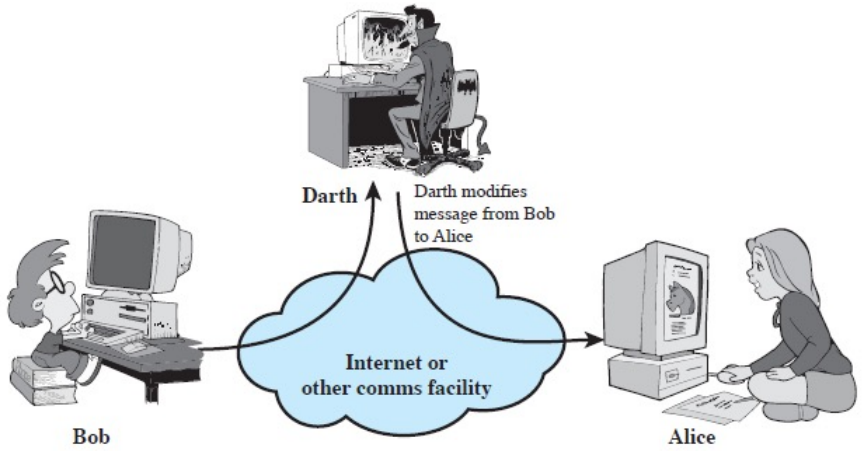


(a) Masquerade

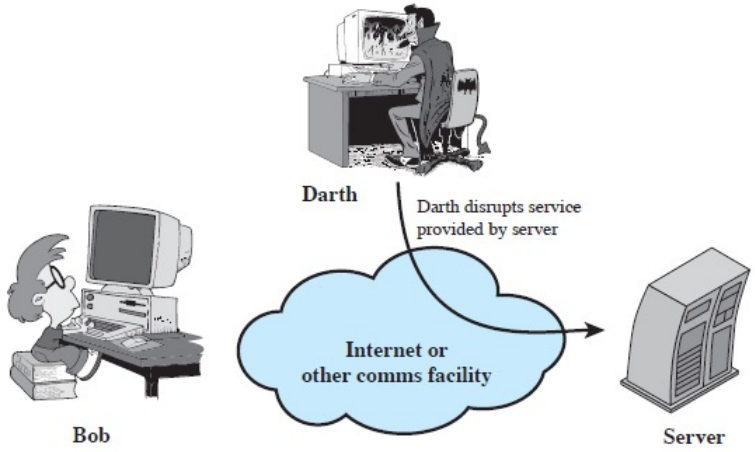


(b) Replay

Figure 1.3 Active attacks (page 1 of 2)



(c) Modification of messages



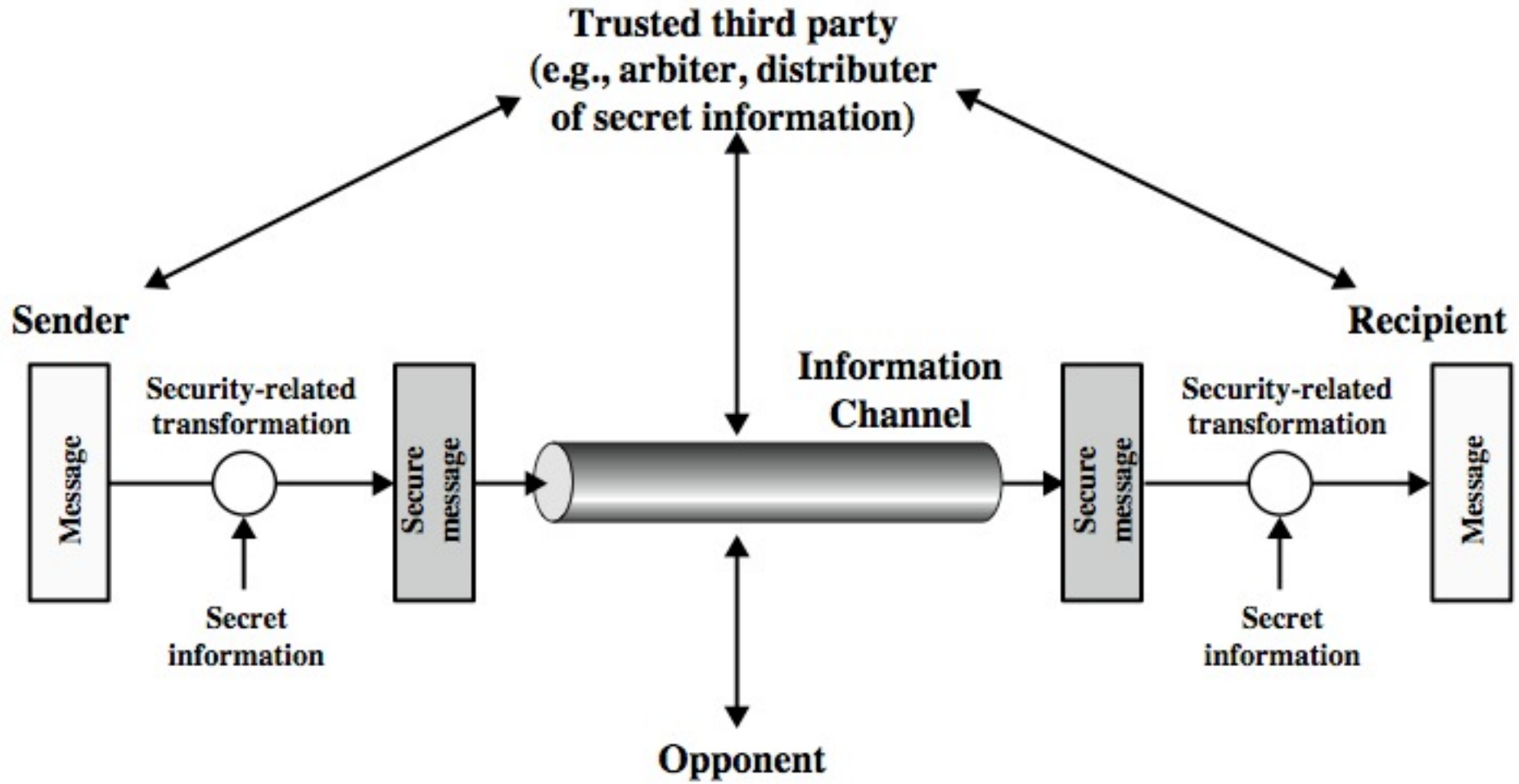
(d) Denial of service

Figure 1.3 Active Attacks (page 2 of 2)

Common Vulnerabilities and Exposures

- Published by MITRE: https://cve.mitre.org/

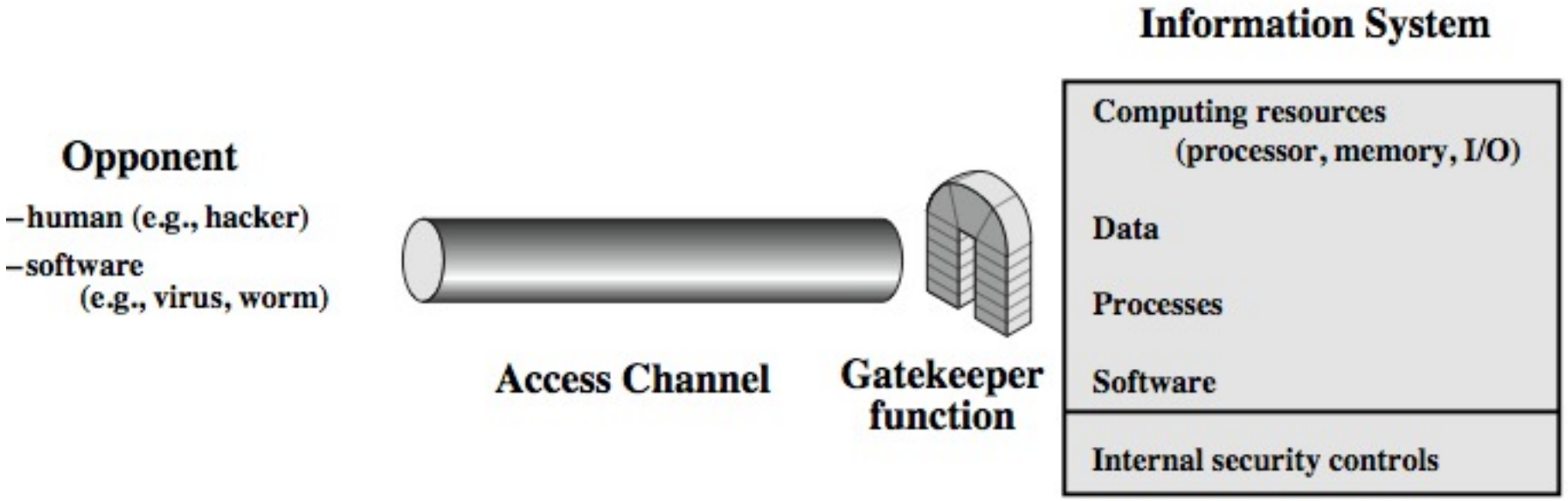
Model for Network Security



Model for Network Security

- Using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate the secret information (keys) used by the algorithm
  3. Develop methods to distribute and share the secret information
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- Using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorised users access designated information or resources

The Art of War: Defensive Mindset

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

***—The Art of War,* Sun Tzu**

(Wu Sun, an ancient Chinese military general, strategist and philosopher)

The Art of War: Defensive Mindset

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

***—The Art of War,* Sun Tzu**

(Wu Sun, an ancient Chinese military general, strategist and philosopher)

Prepare for threats and assume worse case

Kerckhoff's Principle

- Open Design or Shannon's Maxim ("the enemy knows the system")
- Security implementations and protocols known to the adversary
- Security relies on the secrecy of keys
- Common design principle among security experts

- **In contrast to** security-by-obscurity approaches, e.g., steganography
- History shows that security-by-obscurity is vulnerable against persistent attackers

Kerckhoff's Principle

- Open Design or Shannon's Maxim ("the enemy knows the system")
- Security implementations and protocols known to the adversary
- Security relies on the secrecy of keys
- Common design principle among security experts

- **In contrast to** security-by-obscurity approaches, e.g., steganography
- History shows that security-by-obscurity is vulnerable against persistent attackers

Steganography

- an alternative to encryption
- hides existence of message ☺
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks ☹
  - high overhead to hide relatively few info bits
- advantage is can obscure encryption use ☺

Quiz 1C. Steganography

- Find the steganographic message in the following text:

Since everyone can read, encoding text in neutral sentences is doubtfully effective

Steganography Example
(A Puzzle for Inspector Morse)

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basis O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Summary

- Security concepts:
  - confidentiality, integrity, availability, authenticity, accountability
- Security challenges and design principles
- Security vulnerabilities and threats
- Kerckhoff's Principle and Security by Obscurity, e.g., steganography
- Models for network (access) security