01 Introduction

2020 Spring
Information Security

Teacher: Po-Wen Chi
neokent@gapps.ntnu.edu.tw

January 10, 2020

Department of Computer Science and Information Engineering,
National Taiwan Normal University

Computer Security

In the beginning, there is no Security issue.

Why?

In the beginning, there is no Security issue.

Why?

How can you attack a network system that crashes with only two characters transmission?

Definition

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 resources** (includes hardware, software, firmware, information/data and telecommunication).

— NIST Computer Security Handbook

CIA

- **Confidentiality**:
  - Data confidentiality.
  - Privacy.
- **Integrity**:
  - Data integrity.
  - System integrity.
- **Availability**

What is an Information System?

Information System

An information system (IS) is an organized system for the collection, organization, storage and communication of information.

What is an Information System?

Information System

An information system (IS) is an organized system for the collection, organization, storage and communication of information.

···Forget it. Information system is everything around you which is related to computers.

What is an Information System?

Information System

An information system (IS) is an organized system for the collection, organization, storage and communication of information.

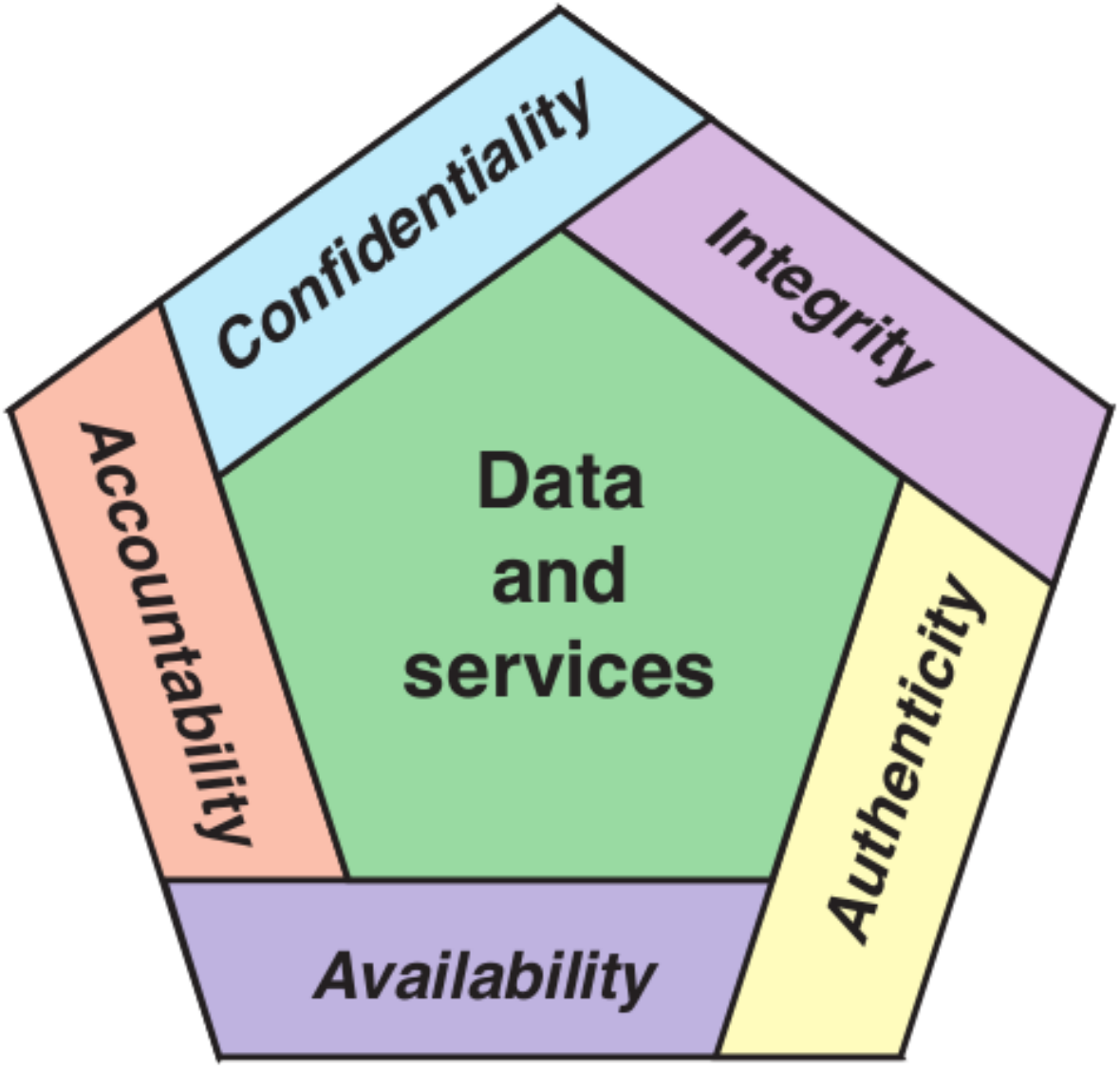
···Forget it. Information system is everything around you which is related to computers.

So, if you want to be an information security expert, you have to be an information expert first.

Other Two Security Factors

- **Authenticity**.
- **Accountability**.

Security Requirements



About This Course

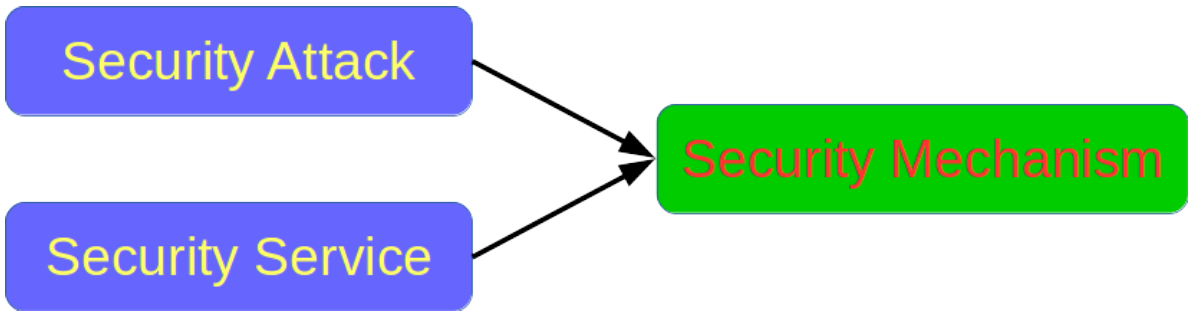
- I will give you some tools (cryptography) first.
- Then I will show you how attacks happen against previous five concepts.
- Finally, we will see how to protect with tools I give you.

OSI Security Architecture

OSI Security Architecture

ITU-T [1] Recommendation X.800, Security Architecture for OSI defines systematic way to

- Defining the requirements for security.
- Characterizing the approaches to satisfying those requirements.



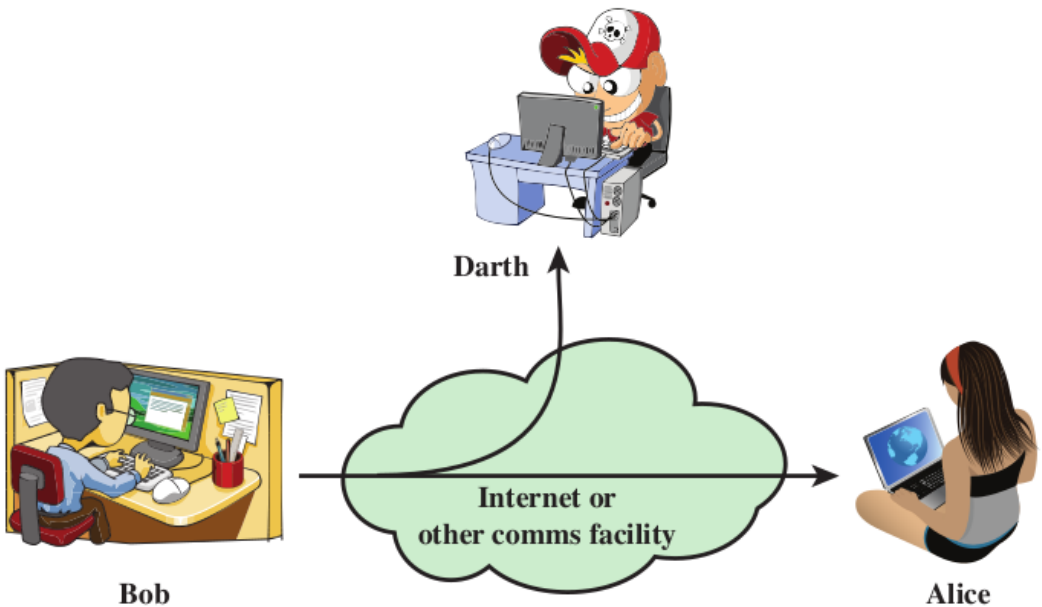
[1] The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations-sponsored agency that develops standards, called Recommendations, relating to telecommunications and to open systems interconnection (OSI).

Security Attacks

1. Passive attacks.
2. Active attacks.

Passive Attack

- Common attack:
  - Release of message content.
  - Traffic analysis.
- Hard to detect.
- Common solution: **encryption**.

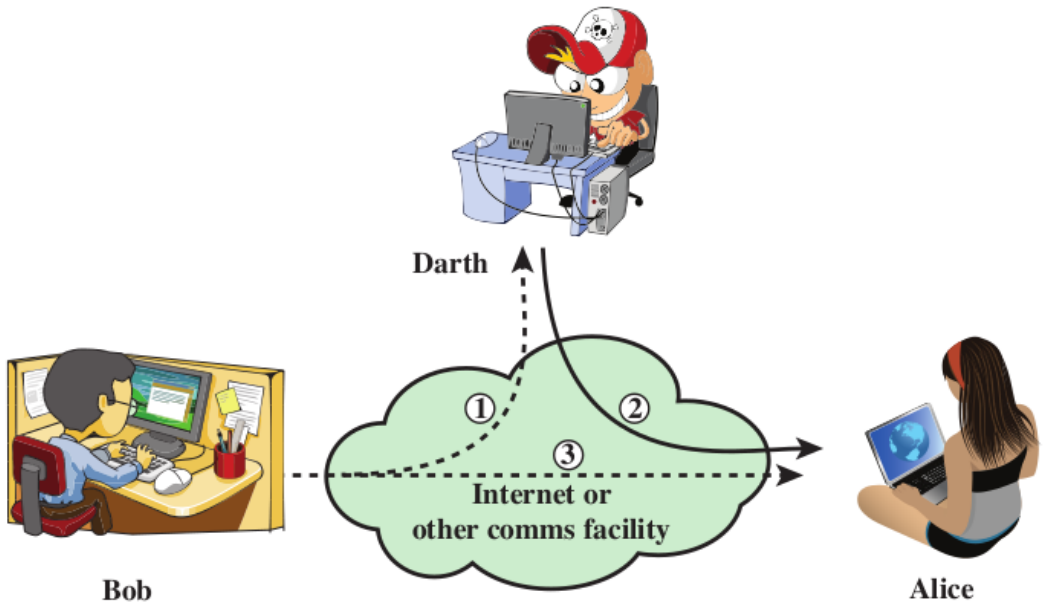


Quiz

Would you please tell me how to eavesdrop the communication between Alice and Bob?

Active Attack

- Common attack:
  - Masquerade.
  - Replay.
  - Message modification.
  - Denial of service.
- Hard to prevent.
- Common solution: **detection** and **recovery**.



Security Service

X.800 Recommendation divides security services into 5 categories:

1. Authentication
2. Access Control.
3. Data Confidentiality.
4. Data Integrity.
5. Non-Repudiation.

Authentication

Make sure who you are and who he/she is.

- Peer entity authentication.
- Data-origin authentication.

Access Control

You can only do what you are allowed.

Data Confidentiality

Data cannot be accessed by unauthorized entities.

- Connection confidentiality.
- Connectionless confidentiality.
- Selective-field confidentiality.
- Traffic-flow confidentiality.

Data Integrity

Data received are exactly as sent.

- Connection integrity with recovery.
- Connection integrity without recovery.
- Connectionless integrity.
- Selective-field connection integrity.
- Selective-field connectionless integrity.

Non-Repudiation

You cannot deny what you have done.

- Non-repudiation source.
- Non-repudiation destination.

Security Mechanism

Specific Security Mechanism:

- Encipherment.
- Digital signature.
- Access control.
- Data integrity.
- Authentication exchange.
- Traffic padding.
- Routing control.
- Notarization.

Pervasive Security Mechanism:

- Trusted functionality.
- Security label.
- Event detection.
- Security audit trail.
- Security recovery.

Fundamental Security Design Principle

Economy of Mechanism

KISS: Keep it simple and stupid.

Fail-safe Defaults

Default setting should be Safe.

EX: Default firewall rule should be **Reject**.

Complete Mediation

Every access should be checked.

EX: sudo cache.

Open Design

The algorithm should be opened so that can be reviewed by other experts.

EX: 國安局。

Separation of Privilege

Multiple attributes are required.

Least Privilege

Should operate using the least set of privileges necessary to perform the task.

EX: Linux root.

Least Common Mechanism

Mechanisms used to access resources should not be shared.

Reduce the amount of HW and SW.

Psychological Acceptability

Frankly speaking $\cdots$almost impossible.

Isolation

EX:

- DMZ.
- Sandbox.
- Hinet data center isolation.

Modularity

Using existed security functions.

Layering

Multiple overlapping protection.

Layering

Multiple overlapping protection.

Quiz: Why one layer protection is not enough??

Least Astonishment

Frankly speaking ···almost impossible.

Should I Remember All These Terms?

- The Above Definitions Come From the Textbook.
- Remember those definitions can let you have common language with others, but nothing good to your skills.
- XXX Security:
  - If you have no knowledge about XXX, how can you know how to attack it or how to protect it?

Appendix: Hacker

Hacker

In computing, a hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.

How to be skilled?

Hacker

In computing, a hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.

How to be skilled? **Interests, Interests Interests.**

Hacker Ethics

- Access to computers and **anything** that might teach you something about the way the world works should be unlimited and total.
- All information should be **free**.
- **Mistrust authority**.
- Hackers should be **judged by their hacking**, not bogus criteria such as degrees, age, race, or position.
- You can create **art and beauty** on a computer.
- Computers can change your life for the**better**.

Appendix: 很壞很壞的駭客

Joke

https://blog.longwin.com.tw/2005/05/badbadcrack_joke/

Appendix: How To Ask Questions The Smart Way

Reference Link

http://www.catb.org/~esr/faqs/smart-questions.html

Questions that You Should NOT ASK

- Where can I find program or resource X?
- How can I use X to do Y?
- How can I configure my shell prompt?
- Can I convert an AcmeCorp document into a TeX file using the Bass-o-matic file converter?
- My program, configuration, SQL statement doesn't work
- I'm having problems with my Windows machine. Can you help?
- My program doesn't work. I think system facility X is broken.
- I'm having problems installing Linux or X. Can you help?
- How can I crack root/steal channel-ops privileges/read someone's e-mail?