Introduction to Information Security

2. Concepts in Security

Kihong Heo

KAIST

Computer Security

- Goal: understanding possible vulnerabilities in computer systems
- Computer systems?

Vulnerabilities

- Allow a malicious user to gain access to private data or full control of a machine
- Typically due to design flaws in systems
  - E.g., insecure cryptography algorithm, SW bugs
- Analysis and action needed to defend against attacks
  - E.g., removing malicious code, bug patch
- What properties should be considered to achieve secure systems?

The CIA Triad

- Three most important properties of computer security
- CIA: Confidentiality, Integrity, and Availability
- Example: a bank system
  - Confidentiality?
  - Integrity?
  - Availability?

CIA (1): Confidentiality

- Avoidance of the unauthorized disclosure of information
  - Protection of data
  - Provide access for those who are allowed to see the data
  - Disallow others from learning anything about the data
- How to achieve confidentiality?
  - Encryption: transformation of information
  - Access control: gatekeeper
  - Authentication: determination of identity

“Delecnac si ssalc txen”

Encryption

- Transformation of information using an encryption key
- Only be read by another user who has the decryption key
- Schemes: symmetric-key encryption, public-key encryption, etc
- Example:

- To be secure: make it extremely difficult to decrypt the data without the decryption key

“Delecnac si ssalc txen”

Easily Breakable Encryption

Access Control

- Rules and policies that limit access to confidential information
- Determine what users have permission to do
- Permission is determined by identity (e.g., name, serial) or role (e.g., prof, ta, student)
- Example: Linux file system

	/etc/passwd	/usr/bin/	/home/prof/exam/	/home/admin/
root	rw	rwx	rwx	rwx
prof	r	rx	rwx	–
ta	r	rx	r	–
student1	r	rx	–	–
student2	r	rx	–	–

Access Control Failure

Authentication

- Determination of the identity or role
- Typical method
  - Something you are
  - Something you know
  - Something you have

Exercise: Internet Banking

- What mechanism is used to achieve confidentiality?
  - Visit the bank website and login
  - ID and PW are sent to the server by your web browser using HTTPS
  - The server allows you to access only your account

CIA (2): Integrity

- Information has not been altered in an unauthorized way
- Benign compromise: information altered by accident
  - E.g., bit flips in memory due to cosmic ray
- Malicious compromise: information altered by attackers
  - E.g., malicious code that changes some files in a system

2021.04.11, KAIST Hacked

and me (not hacked)

Ensuring Integrity

- How to ensure the integrity of computer systems?
- Backups: periodic archiving of data
- Checksums: computation of a function that maps the data to a numerical value
- Also, encryption, access control, and authentication

Ubuntu 22.04.1 LTS (Jammy Jellyfish)

A full list of available files, including BitTorrent files, can be found below.

If you need help burning these images to disk, see the Image Burning Guide.

Name	Last modified	Size	Description
Parent Directory		-	
SHA256SUMS	2022-08-11 11:07	202	
SHA256SUMS.gpg	2022-08-11 11:07	833	
ubuntu-22.04.1-desktop-amd64.iso	2022-08-10 16:21	3.6G	Desktop image for 64-bit PC (AMD64) computers (standard download)

CIA (3): Availability

- Information is accessible and modifiable in a timely fashion
  - Information locked in a cast-iron safe box on Mars: extreme confidentiality & integrity
- How to achieve availability?
  - Physical protections: keep information available even in physical challenges (e.g., storms, earthquakes, or power outages)
  - Computational redundancies: computers that serve as fallbacks in the case of failure

"President Yoon Suk-yeol's office on Sunday said Kakao's network disturbance could even be a threat to national security."
2022.10.16

The AAA Triad

- Three most important properties of modern computer security
- AAA: Assurance (보장), Authenticity (인증), and Anonymity (익명)
- Example: Youtube, Netflix, Melon
  - Assurance?
  - Authenticity?
  - Anonymity?

AAA (1): Assurance

- How trust is provided and managed?
  - Do you trust that your bank, Melon, and Youtube will provide the promised service?
  - Do you trust that your customer pays for your service?
- Trust involves the interplay of the following:
  - Policy: What are the expected behaviors of each agent?
  - Permission: Which agent is allowed to perform the behavior?
  - Protection: How to protect the system from unauthorized users?

Example: Online Service

- For example, online music systems (e.g., Melon)
  - Policy: different plans such as 10 songs/month, unlimited, etc
  - Permission: provide limited access to people who have purchased certain songs
  - Protection: a control system that prevents abusing
- Any difference from CIA?
  - Are the songs confidential?
  - Does the abuse modify the songs?
  - Does the abuse block other users?

AAA (2): Authenticity

- How to determine that statements, policies, and permissions are genuine?
- What happens if those can be faked?
  - “I did not make the commitment. Maybe someone pretended to be me!”
- Nonrepudiation by secure authentication: authentic statement cannot be denied (오리발 방지)
  - E.g., digital signature

AAA (3): Anonymity

- Certain records or transactions are not to be attributable to any individual
- Unfortunate side effects of using personal identities in electronic communications
  - E.g., medical history, purchase history, legal records, email, etc
- Publish data in a privacy-preserving fashion
  - Aggregation: average salary, total # students, etc
  - Proxy: trusted agents that engage in action for individuals such as proxy server
  - Pseudonyms

Exercise: Who does contract COVID-19?

- Scenario: KAIST builds a system to report the information of covid contractors
  - Publish the data of new contractors every day
  - For privacy reasons, all personal data is aggregated: #contractors/class and #contractors/year-of-admission
  - For example

Class	#Constractors
CS101	8
CS230	4
CS348	7
CS420	3

YoA	#Constractors
2023	5
2022	3
2021	2
2020	5

- Question: Is this secure? Any potential privacy leaks?

Threats and Attacks

- Common list of threats and attacks that can compromise the security goals
  - Eavesdropping (도청)
  - Alteration (변조)
  - Denial-of-service (길막)
  - Masquerading (위장)
  - Repudiation (시치미, 오리발)
  - Correlation and traceback (추적)

Summary

- The goal of security: understanding possible vulnerabilities in computer systems
- The CIA triad: fundamental security properties
  - Confidentiality, Integrity, Availability
- The AAA triad: more important in modern systems
  - Assurance, Authenticity, Anonymity