CS396: Security, Privacy & Society

Fall 2022

Lecture 4: Cryptographic System I

Instructor: Abrar Alrumayh

September 12, 2022

Outline

- Basic concepts and terms
- Cryptographic System I
  - Symmetric-key Encryption

Basic security concepts & terms

What is IT security?

IT security is the prevention of, or protection against

- access to information by unauthorized recipients
- intentional but unauthorized destruction or alteration of that information

Definition from: *Dictionary of Computing,* Fourth Ed.
(Oxford: Oxford University Press 1996).

IT security (informal definition)

- the protection of information systems from
  - theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide
  - any possible threat

Valuable assets

Computer systems
hardware, software, and data
have value and deserve security protection.

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

FIGURE 1-2 Computer Objects of Value

The ‘IT-security’ game: What’s at stake?

- Computer systems comprise assets that have (some) **value**
  - e.g., laptops store vast personal or important information (files, photos, email, …)
  - personal, time dependent and often imprecise (e.g., monetary Vs. emotional)
- Valuable assets deserve **security protection**
  - to **preserve** their **value**, ⇒ expressed as a **security property**
    - e.g., personal photos should always be accessible by their owner
  - or to **prevent** (undesired) **harm** ⇒ examined as a concrete **attack**
    - e.g., permanent destruction of irreplaceable photos

The ‘IT-security’ game: Who are the players?

- **Defenders**
  - system owners (e.g., users, administrators, etc.)
  - seek to **enforce** one or more **security properties** or **defeat** certain **attacks** ⇒ **property-based view**
- **Attackers**
  - external entities (e.g., hackers, other users, etc.)
  - seek to launch attacks that **break** a **security property** or **impose** the system to certain **threats** ⇒ **attack-based view**

Security properties

- General statements about the value of a computer system
- Examples
  - The C-I-A triad
    - **confidentiality, integrity, availability**
  - (Some) other properties
    - **authentication / authenticity**
    - **non-repudiation / accountability / auditability**
    - **anonymity**

Security properties

- General statements about the value of a computer system
- Examples
  - The C-I-A triad
    - **confidentiality, integrity, availability**
  - (Some) other properties
    - **authentication / authenticity**
    - **non-repudiation / accountability / auditability**
    - **anonymity**

The C-I-A triad

- Captures the three fundamental properties that make any system valuable

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)

Confidentiality

- An asset is viewed only by authorized parties
  - e.g., conforming to originally-prescribed “read” rules <subject, object, access mode, policy> via access control
  - some other tools
    - encryption, obfuscation, sanitization, …

Integrity

- An asset is modified only by authorized parties
  - beyond conforming to originally-prescribed “write” access-control rules
  - precise, accurate, unmodified, modified in acceptable way by authorized people or processes, consistent, meaningful and usable
  - authorized actions, separation & protection of resources, error detection & correction
  - some tools
    - hashing, MACs

Availability

- An asset can be used by any authorized party
  - usable, meets service's needs, bounded waiting/completion time, acceptable outcome
  - timely response, fairness, concurrency, fault tolerance, graceful cessation (if needed)
  - some tools
    - redundancy, fault tolerance, distributed architectures

The C-I-A triad

- Harm can be characterized by four acts: interception, interruption, modification, and fabrication.

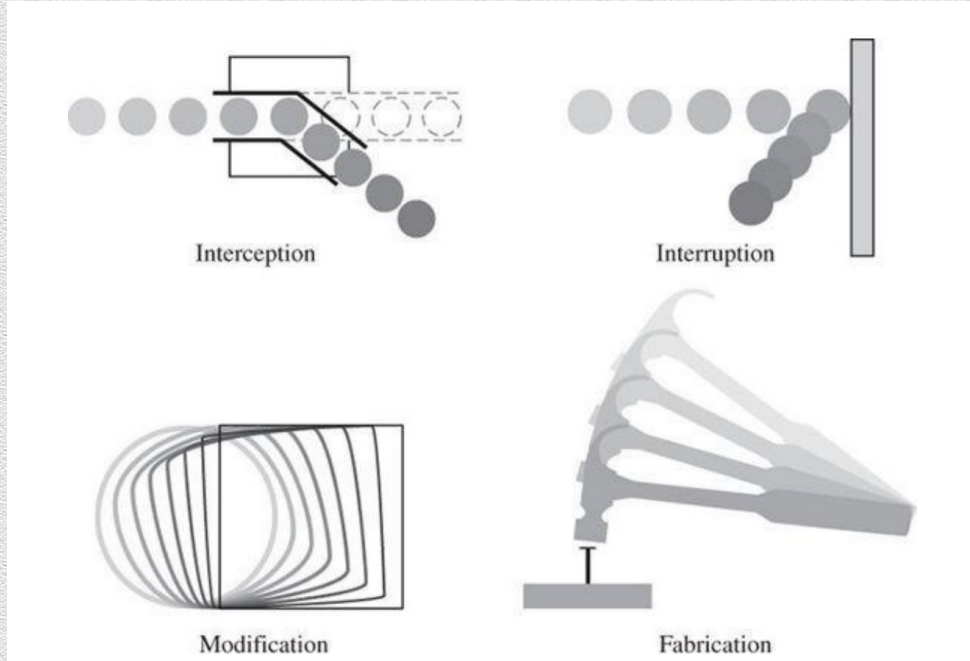


FIGURE 1-5 Four Acts to Cause Security Harm

Authenticity

- The ability to determine that statements, policies, and permissions issued by persons or systems are genuine
  - some tools
    - digital signatures

Non-repudiation

- The assurance that someone cannot deny the validity of something
  - the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity.
- Some tool:
  - Digital signatures (cryptographic computations that allow entities to commit to the authenticity of their documents in a unique way)
    - achieve non-repudiation (authentic statements issued by some person or system cannot be denied)

Non-repudiation

- Digital signatures is a protocol used to mark that only the sender can make but that other people can easily recognize as belonging to the sender.
  - confirms agreement to a message

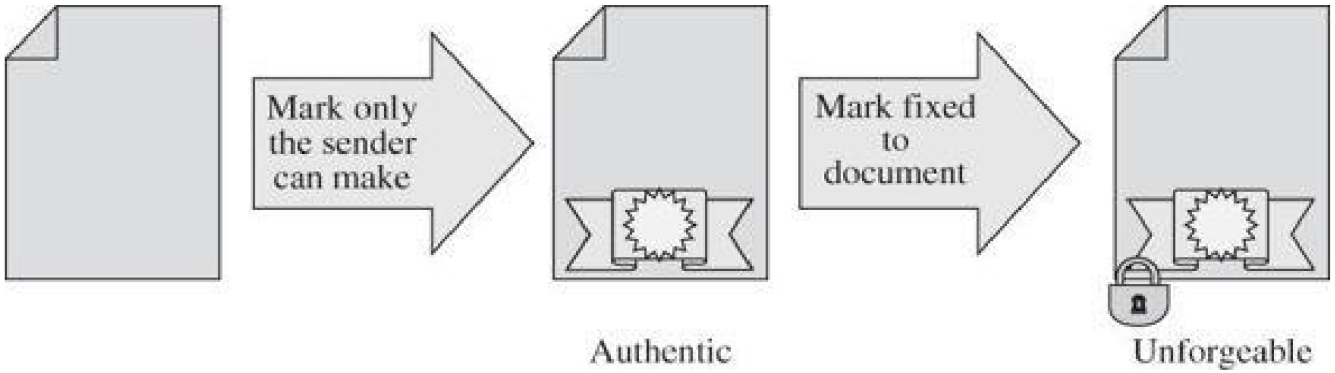


FIGURE 2-26 Digital Signature Requirements

Anonymity

- The property that certain records/transactions cannot be attributed to any individual
- some tools
  - aggregation
    - disclosure of statistics on combined data from many individuals that cannot be tied to any individual
  - proxies
    - trusted agents interacting on behalf on an individual in untraceable way
  - pseudonyms
    - fictional identities, known only to a trusted party, that fill in for real identities

Discussion

1. Cloud-based storage
2. e-banking
   - What is a **valued asset**?
   - What does it mean to **preserve** this value?
   - What is a corresponding desired **security property**?
   - What is a **harm** that must be prevented?

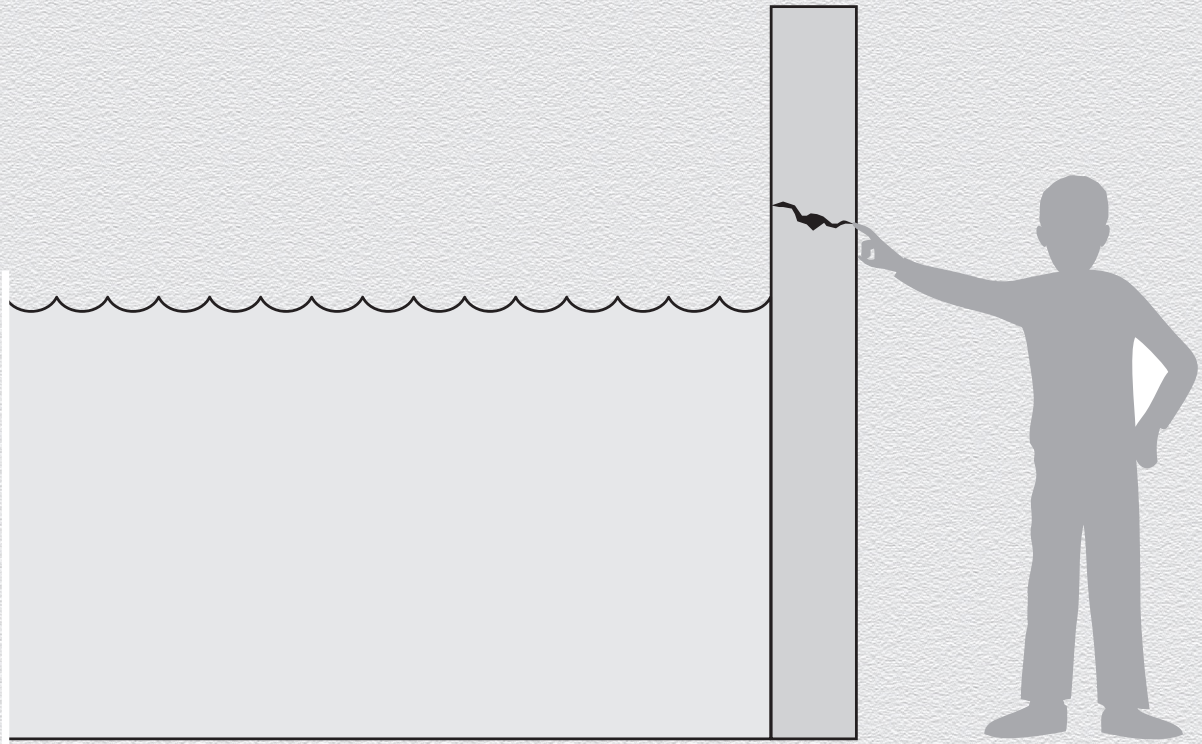
The “Vulnerability - Threat - Control” paradigm

- A **vulnerability** is a weakness that could be exploited to cause harm
- A **threat** is a set of circumstances that could cause harm
- A **security control** is a mechanism that protects against harm
  - i.e., countermeasures designed to prevent threats from exercising vulnerabilities

Thus

- **Attackers** seek to **exploit** vulnerabilities in order to **impose** threats
- **Defenders** seek to **block** these threats by **controlling** the vulnerabilities

A “Vulnerability - Threat - Control” example



Example of threat

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel