

# Security Goals

# Information Security (44 U.S. Code § 3542)

- (1) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
  - (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
  - (C) availability, which means ensuring timely and reliable access to and use of information.

# Information Security Triad: CIA





# Confidentiality

- **Protecting information from disclosure** to unauthorized parties
- Access to information should be granted only on a **need-to-know basis**
- **Data categorization** according to the amount and type of possible damage should it fall into wrong hands

## Supporting Principles (🔒)

- Authentication, Authorization, Encryption, Anonymity, Secrecy

# Integrity

- Protecting information from being modified by unauthorized parties
- Being correct or **consistent with the intended state** of information
- Ensuring that the **information is not tampered** whenever it travels from source to destination or even stored at rest

## Supporting Principles ()

- Hashing, Digital Signatures, Non-repudiation, Tamper-evident packaging



# Availability

- Ensuring that authorized parties are **able to access information** when needed
- Ensuring that the services of an organization are available

## Supporting Principles ()

- Accessibility, Fault Tolerance, Redundancy, Backup, Testing

## Exercise 2.1 (📌)

1. Which security goals are at risk by the following threats?

| Threat                      | C | I | A |
|-----------------------------|---|---|---|
| Network Sniffing            |   |   |   |
| DDoS Attack                 |   |   |   |
| Rogue WiFi Access Point     |   |   |   |
| Electromagnetic Pulse (EMP) |   |   |   |
| Whistleblower               |   |   |   |
| Social Engineering          |   |   |   |

# Attacker Behavior vs. Security Goals

|           | Active | Passive | Threatened Security Goals                |
|-----------|--------|---------|--|
| Observing | (✓)    | ✓       | Confidentiality                          |
| Altering  | ✓      | ✗       | Confidentiality, Integrity, Availability |



# Extended CIA Models

# Parkerian Hexad (1998)

- Confidentiality
- Possession / Control (NEW)
- Integrity
- Authenticity (NEW)
- Availability
- Utility (NEW)

## Possession / Control

- Protecting against the idea that **confidential data can be possessed/controlled by an unauthorized individual or party**
- Loss of control or possession of information should not automatically lead to the breach of confidentiality

### Supporting Principles ()

- Encryption, Authentication

## Authenticity

- Assurance that a message or transaction is from the source it claims to be from

### Supporting Principles ()

- Identification, Digital Certificates

## Utility

- Usefulness of data or information

### Supporting Principles ( )

- Compatibility, Accessibility

---

Information may be available and therefore usable but it doesn't necessarily have to be in a useful form to be defined as available. [<sup>1</sup>]

# CIA<sup>3</sup> (2016)

- Confidentiality
- Integrity
- Availability
- Accountability (NEW)
- Assurance (NEW)



## Accountability

- Allowing to answer questions like "*Who did it?*" or "*Who is accountable?*"
- Considering **legal consequences** and contractual obligations
- Encompassing **segregation of duties** and awareness training

### Supporting Principles ( )

- **Integrity**, Non-repudiation, Authenticity, Design, Governance, Policy

## Assurance

- Introduces **control activities** for the aforementioned security goals
- Periodic controls **assuring that all security measures** (both technical and operational) **work as intended**

### Supporting Principles ( )

- Auditing, Measuring, Monitoring, Continuous Improvement



# Dependency Model of CIA<sup>3</sup>



## Exercise 2.2 (📌)

1. Define at least three supporting measures for each CIA<sup>3</sup> security goal, distinguishing between technical and organizational measures

| Security Goal   | Technical Measures | Organizational Measures |
|-----------------|--------------------|-------------------------|
| Confidentiality |                    |                         |
| Integrity       |                    |                         |
| Availability    |                    |                         |
| Accountability  |                    |                         |
| Assurance       |                    |                         |

## Exercise 2.3 (🏠)

1. Which of the "classic" CIA security goals could have been compromised in each of the [Motivation: Case Studies](#)?
2. Explain each ✓ briefly

| Case Study                | C | I | A |
|---------------------------|---|---|---|
| <a href="#">Marriot</a>   |   |   |   |
| <a href="#">Equifax</a>   |   |   |   |
| <a href="#">VTech</a>     |   |   |   |
| <a href="#">CloudPets</a> |   |   |   |