Information and Network Security Concepts

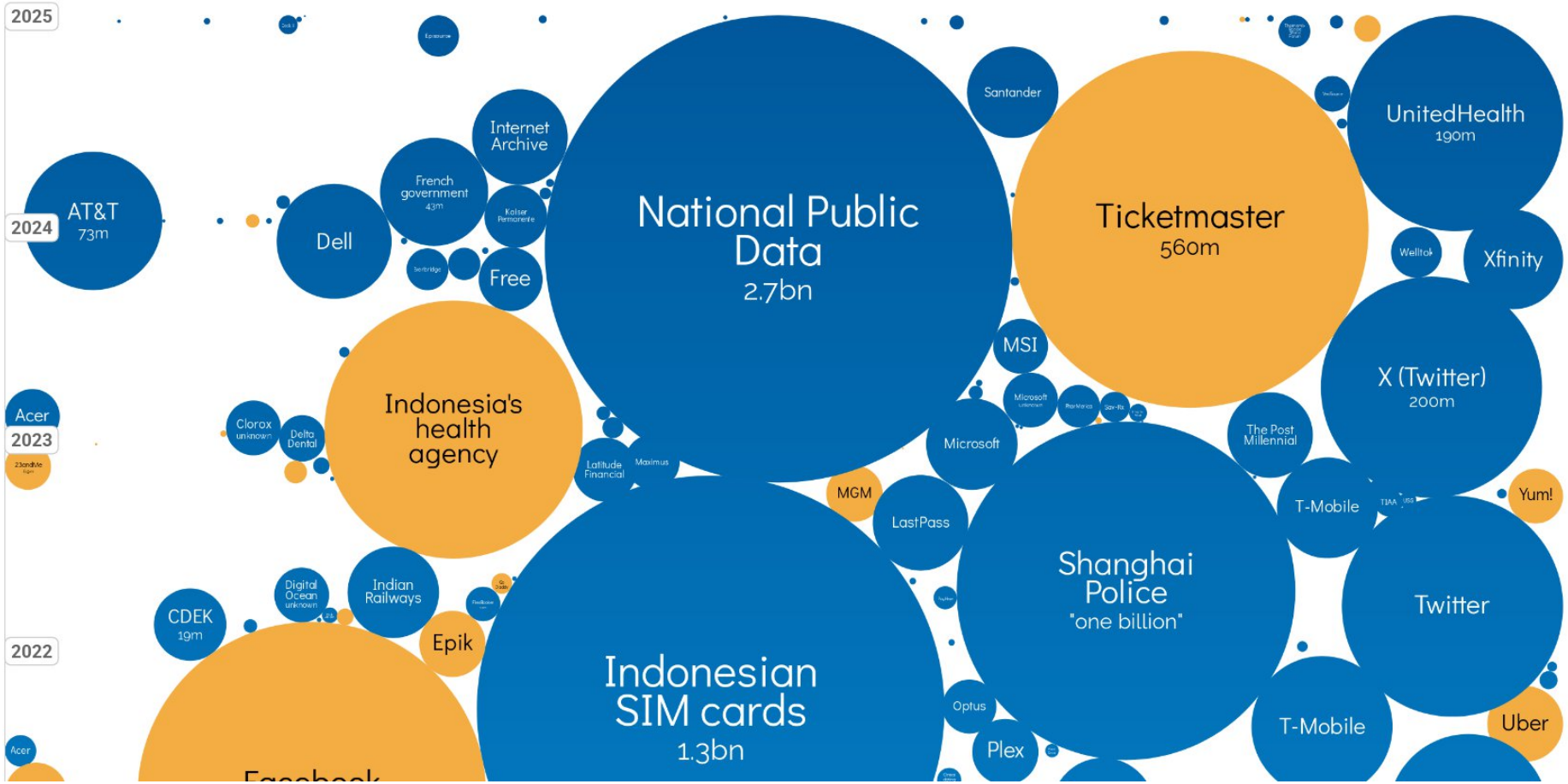
IT3122 Computer Security

2025.08.25

Intended Learning Outcomes

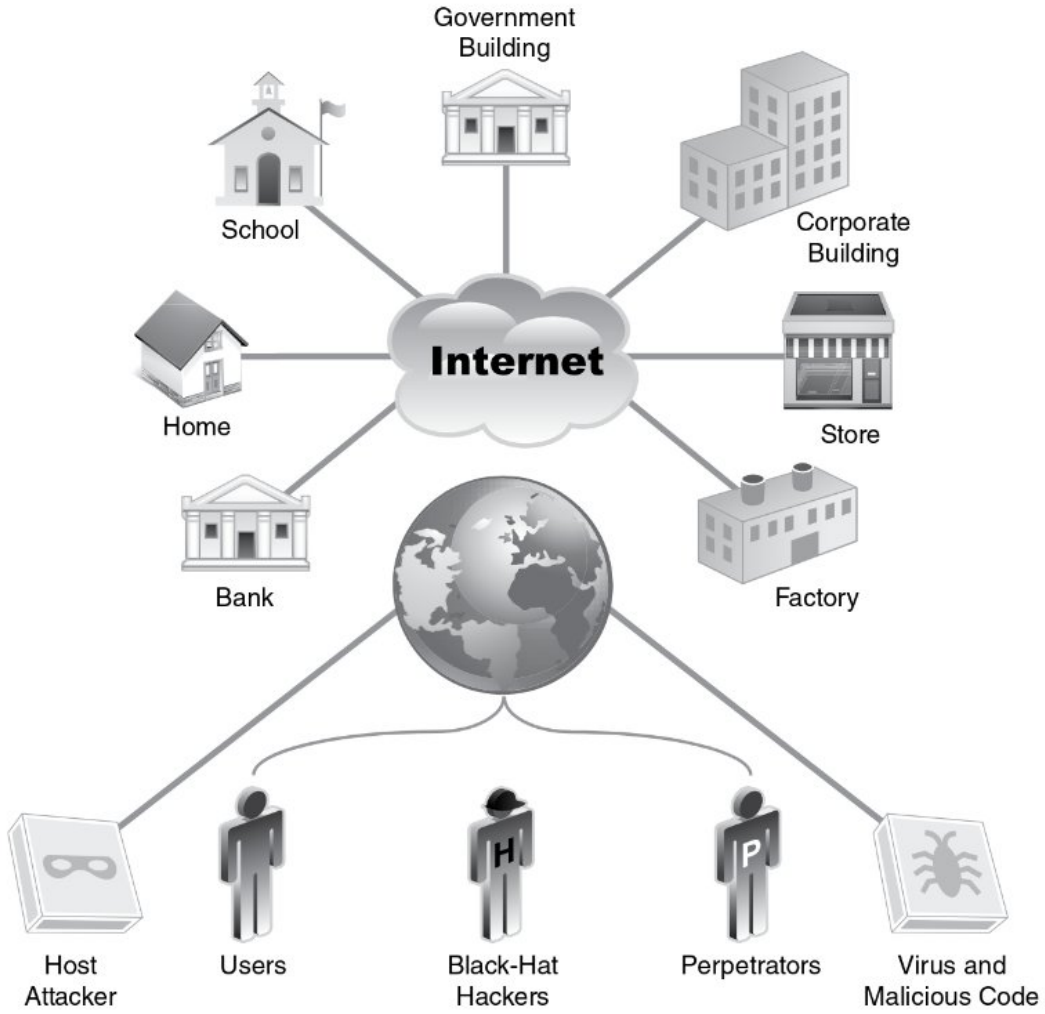
- Describe how unauthorized access can lead to a data breach.
- Describe the key security requirements of confidentiality, integrity, and availability.
- Distinguish between risks, threats, and vulnerabilities.

World’s Biggest Data Breaches & Hacks



2025.08.25 https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Cyberspace: The New Frontier



Cybersecurity

- **Cybersecurity** is the protection of information that is stored, transmitted, and processed in a networked system of computers, other digital devices, and network devices and transmission lines, including the Internet.
- Cybersecurity encompasses **information security**, with respect to electronic information, and **network security**.

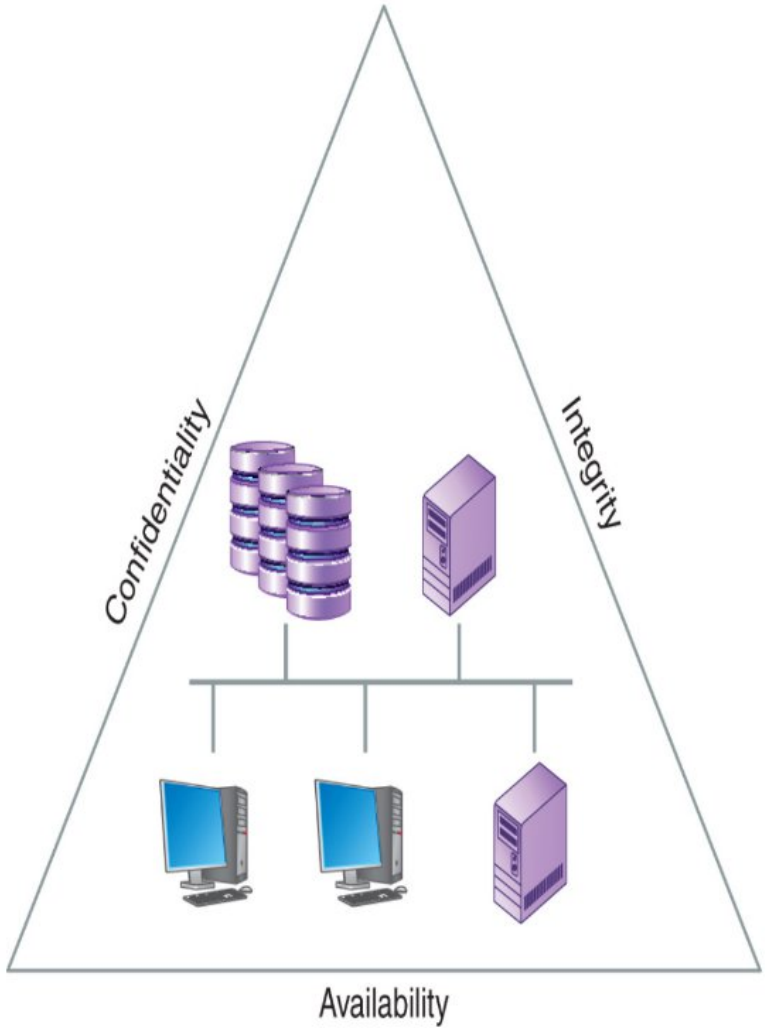
Information Security

- **Information security** refers to preservation of confidentiality, integrity, and availability of information.
- Information security also is concerned with physical information.

Network Security

- **Network security** refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

Security Triad



Security Triad

- **Confidentiality**—Only authorized users can view information.
- **Integrity**—Only authorized users can change information.
- **Availability**—Information is accessible by authorized users whenever they request the information.

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.

Integrity

- **Data integrity**: Assures that data 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.

Availability

- Assures that systems work promptly and service is not denied to authorized users.

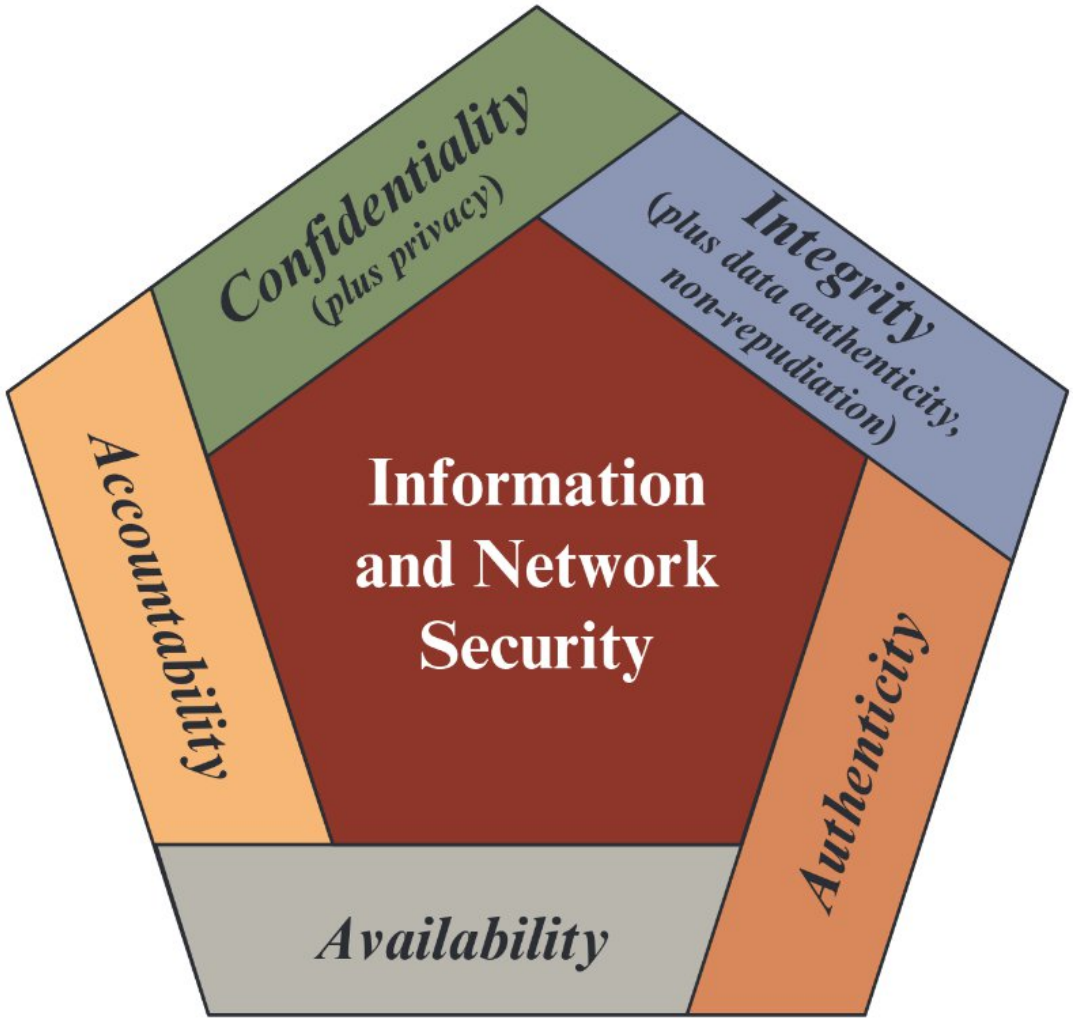
Authenticity

- 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.
- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Essential Information and Network Security Objectives



The Challenges of Information Security

- Security is not as simple as it might first appear to the novice.
- In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.
- The procedures used to provide particular services are often counterintuitive.
- Having designed various security mechanisms, it is necessary to decide where to use them.

The Challenges of Information Security

- Security mechanisms typically involve more than a particular algorithm or protocol.
- Information and network security are essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
- There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
- Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.

The Challenges of Information Security

- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
- Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The OSI Security Architecture

- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is 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.

Risks, Threats, and Vulnerabilities

- An **asset** is any item that has value to an organization or a person.
- **Risk** is the level of exposure to some event that has an effect on an asset, usually the likelihood that something bad will happen to an asset.
- A **threat** is any action, either natural or human induced, that could damage an asset.
- A **vulnerability** is a weakness that allows a threat to be realized or to have an effect on an asset.

References

- W. Stallings, “Information and Network Security Concepts,” in *Cryptography and Network Security, Principles and Practice*, 8th edition, 2023, pp. 21–43.
- D. Kim, and M. G. Solomon, “Information Systems Security,” in *Fundamentals of Information Systems Security*, 4th edition, 2023, pp. 35–105.