Basics of Security

Josh Wilcox (jw14g24@soton.ac.uk)

February 18, 2025

Contents

1 CIA Triad

1.1 Confidentiality

- Ensuring every piece of data can only b e accessed if authorized
- A loss of confidentiality is the unauthorized disclosure of information
- Protecting personal privacy and proprietary information

1.2 Integrity

- Guards against improper information modification or destruction
- Ensures information nonrepudiation and authenticity
  - Nonrepudiation means that a sender cannot deny having sent a message
  - Ensures that the origin of the message is verifiable
  - Provides proof of the integrity and origin of data
  - Prevents entities from denying their actions
- Making sure the application of logic is not altered inappropriately
- Loss of integrity is the unauthorized modification or destruction of information

1.2.1 Authenticity

- Authenticity means data is genuine and being able to be verified and trusted
  - Validity of transmission, message, or message originator is in confidence
  - Involves verifying:
    - Users are who they say the are
    - Each input arriving in the system comes from a trusted source

1.2.2 Accountability

- Security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
- Supports:
  - **Nonrepudiation** : Ensures that an entity cannot deny having performed a particular action, such as sending a message or making a transaction.
  - **Deterrence** : Discourages malicious activities by ensuring that actions can be traced back to the perpetrator, thereby holding them accountable.
  - **Fault isolation** : Helps in identifying and isolating the source of a fault or breach, making it easier to address and rectify issues.
  - **Intrusion detection and prevention** : Enables the monitoring and logging of activities to detect unauthorized access or anomalies, and take preventive measures.
  - **After-action recovery** : Assists in understanding the sequence of events leading to a security incident, facilitating recovery and remediation efforts.
  - **Legal action** : Provides evidence and audit trails that can be used in legal proceedings to prosecute offenders and enforce cybersecurity laws.

1.3 Availability

- Ensures timely and reliable access to and use of informatioln
- Loss of availability is the disruption of access to or use of information

2 Model of cyber security

2.1 Types of asset vulnerabilities

2.1.1 System can be corrupted

- System does the wrong thing or gives wrong answers
- Stored data values may different from what they should be
- Data may be improperly modified

2.1.2 System can become Leaky

- Someonw who should not have access to some or all of the information through the network obtains such access

2.1.3 System can become Unavailable

- A system can become very slow or unavailable such that its use is impossible or impractical

2.2 Attack Classification

- Attack occurs when a threat materialises
  - If successful, leads to an undesirable violation of security
  - Agent executing the attack is refef
- Attacks can be **active**
  - An attempt to alter assets or affect their operation
- Attacks can be **passive**
  - An attempt to learn or make use of information from the system that does not affect assets
- They can be **Inside Attacks**
  - Done by an *insider*
  - Insider is authorized but uses these permissions in a malicious way
- They can be **Outside Attacls**
  - Initiated by an unauthorized or illegitimate user of the system as a whole