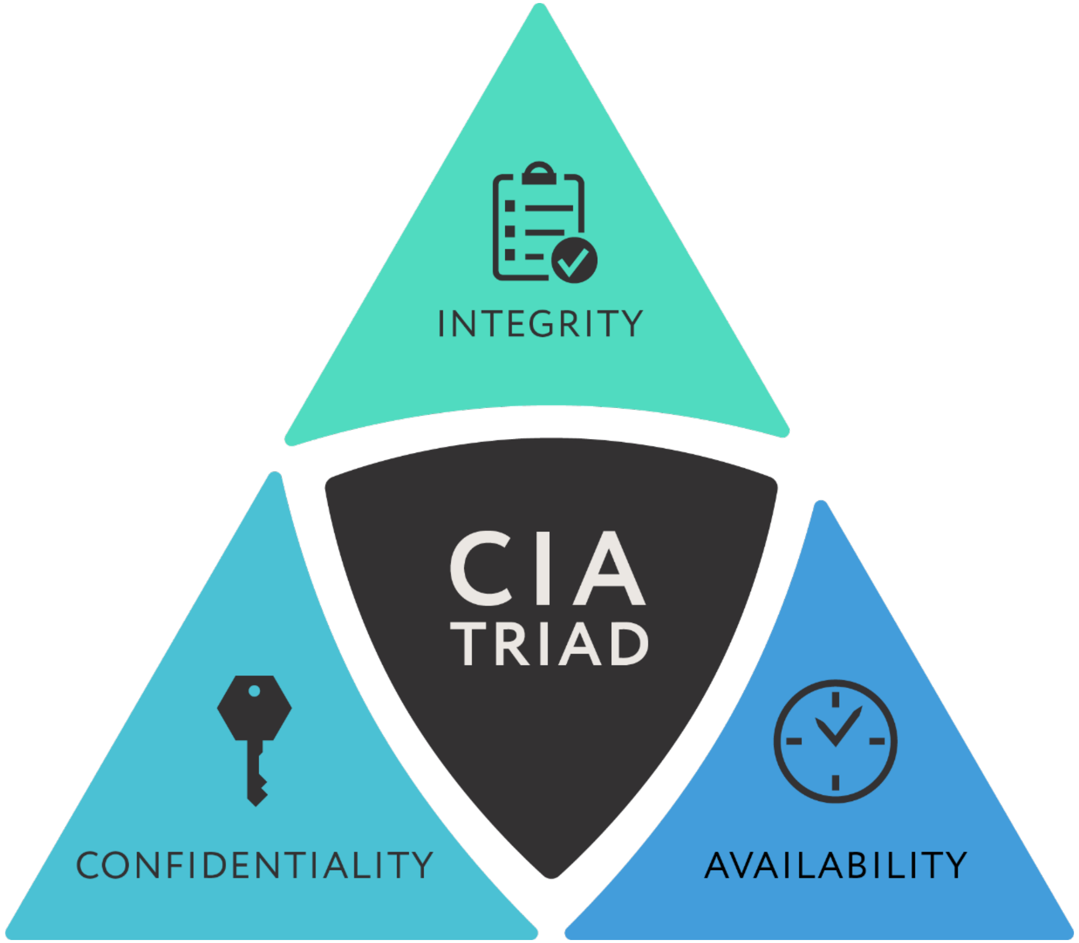
Cybersecurity

Lesson Notes 1.2.1 - CIA Triad and AAA

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

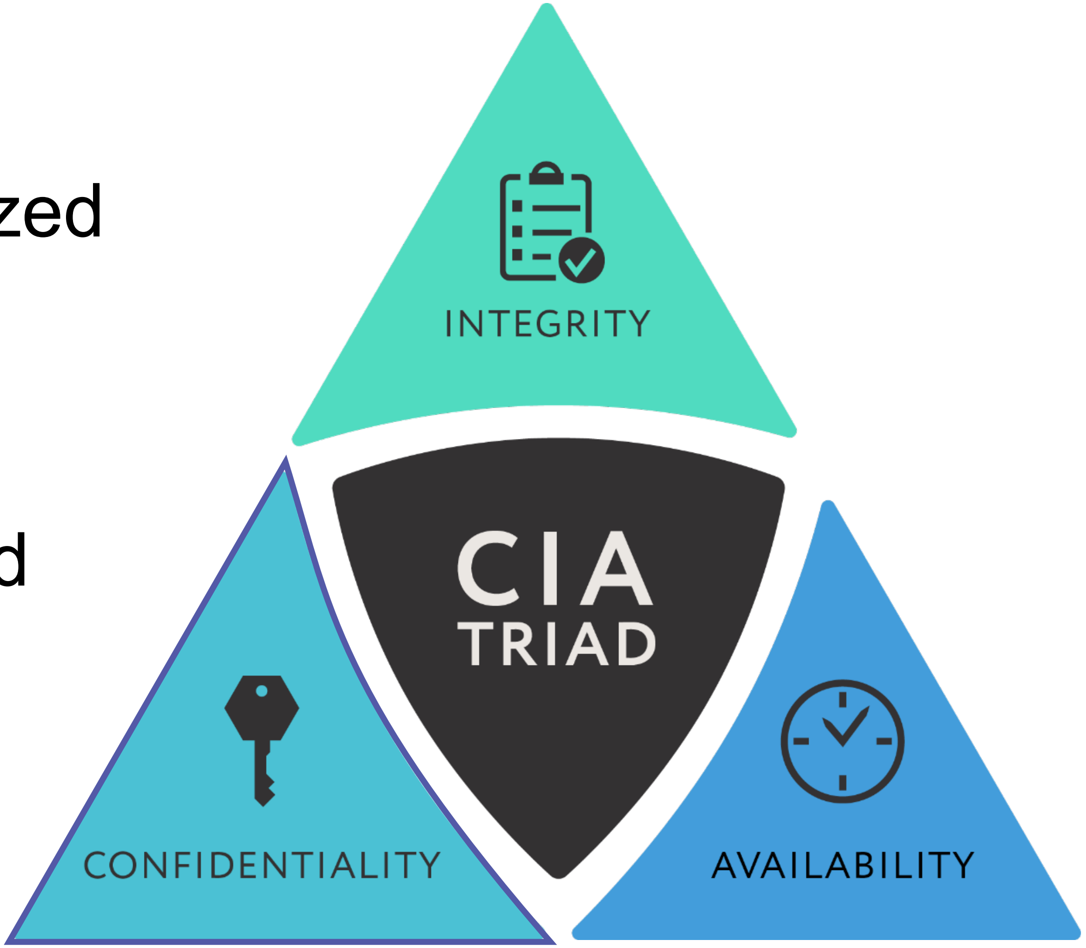
CIA Triad

- Created from the three fundamental principles of Informational Technology:
  - Confidentiality
  - Integrity
  - Availability



CIA Triad - Confidentiality

- Access and privacy controls are designed to ensure only authorized users can access confidential information
- They include the principles of identification, authentication, and authorization
- Examples of authentication controls to protect include passwords, biometrics, PINs



CYBER.ORG

CIA Triad - Integrity

- Access controls ensure that information is not tampered with or modified
- An example of security control is the use of file hashes, checksums, digital signatures, etc.
- Attacks of integrity are the most dangerous attack as they are the hardest to detect and to deter

INTEGRITY
CIA
TRIAD
CONFIDENTIALITY
AVAILABILITY

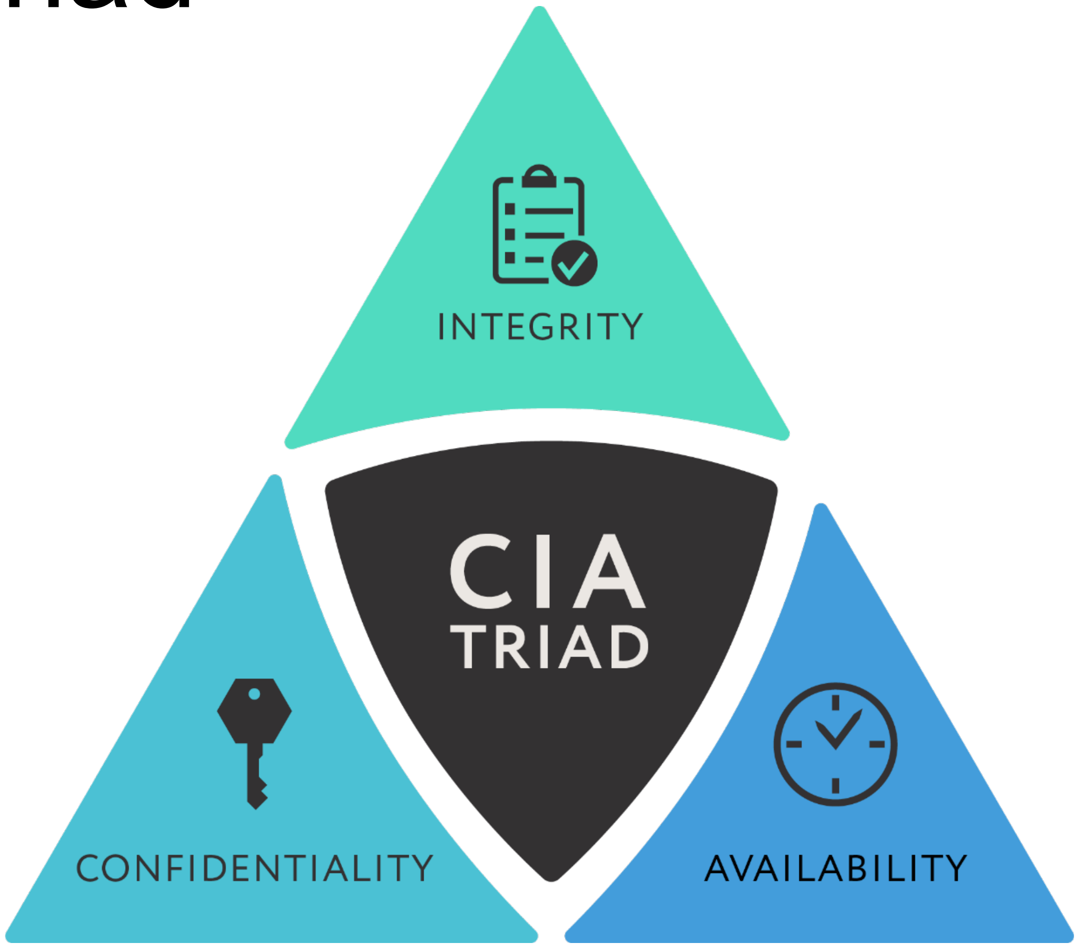
CIA Triad - Availability

- Ensuring that services are available when needed to the people who need them
- Availability can be impacted by natural (fire, floods, hurricanes), environmental (power outage), or artificial (DDoS attack) events.
- Redundancy, recovery, and performance monitoring are crucial

INTEGRITY
CIA TRIAD
CONFIDENTIALITY
AVAILABILITY

Importance of the CIA Triad

- Provides a simple and understandable framework for developing and implementing security controls
- Organizations can effectively balance various security risks and prioritize their resources accordingly
- Flexible and can be applied to different types of information systems and organizations, regardless of size or industry.



Digital Forensics

- When it comes to forensic analysis with information and data, there must be non-repudiation, or no doubt that it was tampered with.
- The earliest state of the data, know as provenance must be available.

AAA Framework

- Used to understand security surrounding the accessibility of individuals
- Process of Identification passes:
  - Authentication
  - Authorization
  - Accounting

AAA Framework – Authenticating People

- Verifying claims of identity which is crucial for
  - Protecting sensitive information
  - Preventing unauthorized access
  - Maintaining security
- Examples:
  - Knowledge based methods
    - Passwords, pins, security questions
  - Possession based
    - Key cards, tokens, smart cards
  - Biometric
    - Fingerprint, face or voice recognition
  - Multi-factor Authentication
    - Combination of two or more listed above

AAA Framework – Authenticating Systems

- Verifying the identity of a device, computer, or application to ensure authorization to resources and other systems while preventing unauthorized access
- Credential-Based
  - Username and password, API keys
- Token-Based
  - Hardware or software tokens
- Biometric
  - Fingerprinting or behavioral metrics
- Mutual
  - Client and server authentication
- Zero-Trust Architecture
  - Assumes no system is trustworthy

AAA Framework – Authorization Models

- The set of rules and policies that govern who can access and what actions can they perform within a system
- Determined by several factors
  - System complexity
  - Data sensitivity
  - Compliance requirements
  - Management
  - Flexibility

Authorization Model Types

- Access Control Lists (ACL)
  - Assigns permissions directly to people or groups
  - Simple with smaller numbers, but can become complex with larger systems
- Role-Based Access Control (RBAC)
  - Assigns permissions based on roles and users are assigned these roles
  - Examples include administrators, guests, editors, etc.
- Attribute-Based Access Control (ABAC)
  - Assigns permissions based on attributes such as department, location, device type, time, etc.
  - Well-suited for complex systems with dynamic needs

Authorization Model Types cont’d

- Rule-Based Access Control (RuBAC)
  - Rules define access conditions, often expressed as if-then statements
  - Allows specific security requirements
- Mandatory Access Control (MAC)
  - Enforces restrictions based on security labels to users and resources
  - Centrally controlled and often used in high-security environments
  - High protection but less flexible for user needs