Cyber Security

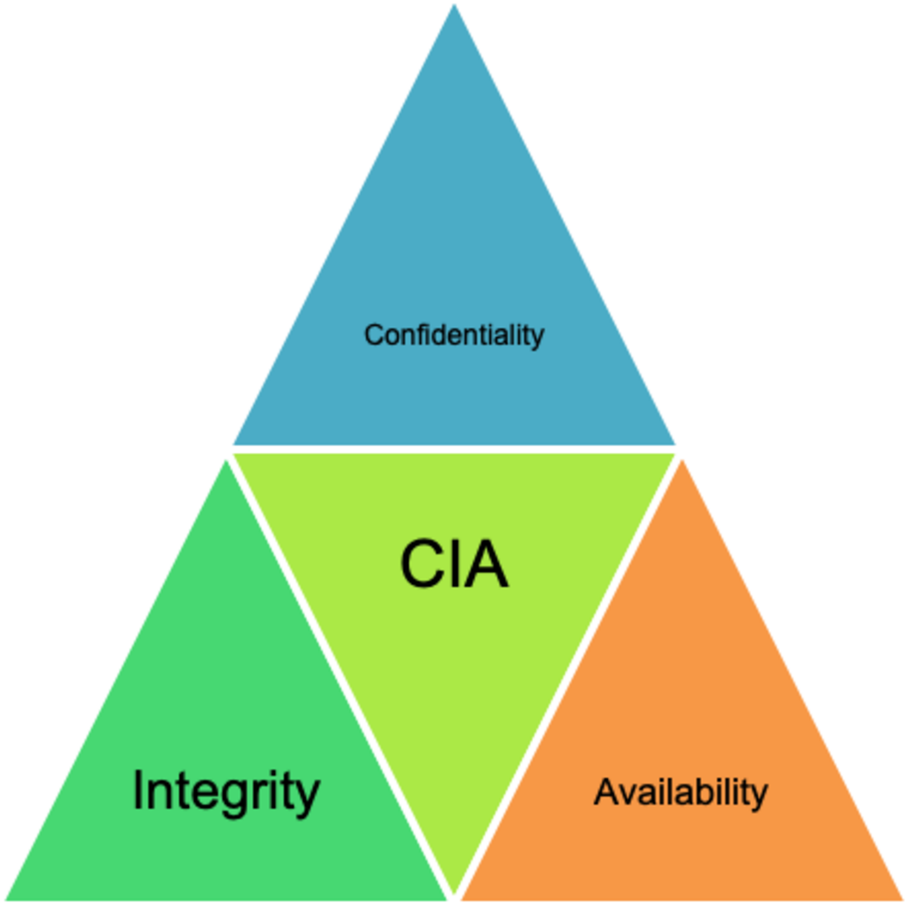
M Saeed Siddik

Course Outline

- Fundamentals: CIA Triad, Threat, Attack, Standards and Frameworks
- Cryptography: Encryption, hashing, key management, SSL, etc.
- Cyber security laws: worldwide and local laws
- Software Security: Vulnerability, memory leakge
- Information and Data Security: Malware, Virus, Phishing, Social Engineering, etc.

Cybersecurity Concepts: CIA Triad

Three principles of security control and management:
Confidentiality, Integrity, and Availability.



Confidentiality

Ensures that data is accessed only by authorized individuals. Techniques include encryption, access controls, and data classification.

- **Encryption**: Converts data into an unreadable form (e.g., AES, RSA).
- **Access Control**: Role-based access (RBAC), multi-factor authentication (MFA).
- **Data Classification**: Labeling data as public, internal, confidential, or secret.

Real-World Example: Online banking ensures that only account holders can view their statements using secure logins and encrypted sessions (HTTPS/TLS).

Integrity

Integrity ensures that data remains trustworthy, complete, and unaltered from its original state except by authorized processes.

- **Hash Functions**: Generate a unique digital fingerprint (e.g., SHA-256) to detect tampering.
- **Digital Signatures**: Verify authenticity of software updates or documents.
- **Checksums & Version Control:** Ensure files and code remain consistent over time.

Real-World Example: When downloading software, a checksum or hash is often provided so users can verify the file hasn't been modified by attackers.

Availability

Availability ensures that information and systems are accessible to authorized users whenever they need them. Even the most secure system is useless if legitimate users cannot access it.

- **Redundancy**: Backup servers, failover systems, RAID storage.
- **Disaster Recovery Plans**: Procedures for restoring services quickly after outages.
- **Monitoring and Maintenance**: Detecting performance issues before they lead to downtime.

Real-World Example: Cloud service providers use geographically distributed data centers to guarantee high uptime for their customers.

Threats to CIA Triad

Threats to Confidentiality: Data breaches, insider threats, eavesdropping, and shoulder surfing.

Threats to Integrity: Malware infections, man-in-the-middle attacks, unauthorized configuration changes, accidental file corruption.

Threats to Availability: Distributed Denial-of-Service (DDoS) attacks, power outages, hardware failures, and ransomware that locks files.

Cybersecurity standards and framework

- ISO/IEC 27001
- NIST Cybersecurity Framework (CSF)
- Open Web Application Security Project (OWASP)

ISO/IEC 27001

ISO/IEC 27001 is an internationally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). An ISMS is a systematic approach to managing sensitive information, including people, processes, and technology, to ensure it remains secure. The current version is ISO/IEC 27001:2022.

ISO/IEC 27001

- Internationally recognized standard (by ISO/IEC).
- Focuses on building and maintaining an Information Security Management System (ISMS).
- Risk-based approach to security.
- Requires documented policies, procedures, and controls.
- Certifiable — organizations can get ISO 27001 certification.
- Emphasizes continuous improvement (Plan-Do-Check-Act cycle).
- Covers people, process, and technology aspects of security.

NIST Cybersecurity Framework (CSF)

- Developed by the U.S. National Institute of Standards and Technology.
- Voluntary, but widely adopted across industries.
- Organized into 5 core functions: Identify, Protect, Detect, Respond, Recover.
- Provides categories and subcategories of controls, not prescriptive steps.
- Flexible and scalable suitable for organizations of all sizes.
- Maps to other standards (ISO 27001, COBIT, CIS controls).
- Focused on risk management and improving cybersecurity posture.

OWASP (Open Worldwide Application Security Project)

- Community-driven, open-source project.
- Focuses specifically on application and web security.
- Publishes the OWASP Top 10 (most critical web application security risks).
- Provides best practices, cheat sheets, and testing guides.
- Not a certifiable standard more of an awareness and education framework.

WASP Top 10 (2021 edition)

- **Broken Access Control** – Users can access data or functions they shouldn't (e.g., changing another user's data).
- **Cryptographic Failures** – Sensitive data is not properly protected, often due to weak encryption or exposure of secrets.
- **Injection** – Malicious data (like SQL, NoSQL, or OS commands) is sent to the application, leading to unauthorized actions or data breaches.
- **Insecure Design** – Weaknesses in the design phase of the application that can't easily be fixed later.
- **Security Misconfiguration** – Incorrectly configured servers, databases, or applications, leaving vulnerabilities open.

WASP Top 10 (2021 edition)

- **Identification and Authentication Failures** – Weak login, session management, or credential handling, allowing attackers to impersonate users.
- **Software and Data Integrity Failures** – Code or critical data can be tampered with, e.g., via untrusted updates or CI/CD pipeline issues.
- **Security Logging and Monitoring Failures** – Insufficient logging, alerting, or monitoring, making it hard to detect breaches.
- **Server-Side Request Forgery (SSRF)** – The server can be tricked into making requests to unintended locations, potentially exposing internal systems.
- **Vulnerable and Outdated Components** – Using libraries, frameworks, or software with known security flaws.

Thank You

saeed.siddik@iit.du.ac.bd