Chapter 1: Introduction to Cybersecurity

Lecture by Assist. Prof. Dr. Chanankorn Jandaeng

Walailak University

Lecture Duration: 90 minutes

Goal: Build foundational understanding of cybersecurity functions and principles — the base for designing network monitoring systems.

Lecture Overview

1. What is Cybersecurity?
2. CIA Triad: Confidentiality, Integrity, Availability
3. DAD Triad: Disclosure, Alteration, Destruction
4. AAA Model
5. Threats and Vulnerabilities
6. Cybersecurity Domains

0. Security is protection of Assets

- Declare your assets first
- What are the scopes of protection

1. What is Cybersecurity?

Definition:

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, damage, or unauthorized access.

Key Aspects:

- Preventing unauthorized access
- Ensuring data confidentiality and integrity
- Maintaining operational continuity

Note for students:

Cybersecurity is not only a technical field but also a strategic and policy-driven discipline.

The Importance of Cybersecurity

- Increasing digital transformation → expanded attack surface
- Cybercrime costs expected to exceed **$10 trillion globally by 2025**
- Protecting **critical infrastructure**, **personal data**, and **national security**

Discussion Prompt:

What cybersecurity incidents have made headlines recently?

How could they have been prevented?

2. The CIA Triad

Core Security Model:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Together, these three principles define the goals of all cybersecurity mechanisms.

Confidentiality

Definition: Protecting information from unauthorized disclosure.

Mechanisms:

- Encryption
- Access control
- Data classification

Example:

Ensuring only authorized users can view patient medical records.

Integrity

Definition: Safeguarding data from unauthorized modification or destruction.

Mechanisms:

- Checksums, hashing
- Digital signatures
- Audit logs

Example:

Detecting unauthorized changes in financial transaction data.

Availability

Definition: Ensuring information and systems are accessible when needed.

Mechanisms:

- Redundancy and backups
- DDoS mitigation
- Fault tolerance

Example:

A banking system must stay online for 24/7 customer transactions.

Balancing the CIA Triad

- Trade-offs exist between **security and usability**
- Example: More encryption → higher security, but may reduce performance
- Designing secure systems requires **context-aware balance**

3. The DAD Triad

Attacker’s Perspective Model:

1. **Disclosure**
2. **Alteration**
3. **Destruction**

The **DAD Triad** represents the opposite of the CIA Triad — it helps analysts understand attacker objectives and anticipate their strategies.

Disclosure

Definition: Unauthorized exposure of confidential information.

Example Attacks:

- Data breaches
- Phishing for credentials
- Eavesdropping on network traffic

Impact:

Violates **Confidentiality** in the CIA model.

Alteration

Definition: Unauthorized modification or tampering of data or system configurations.

Example Attacks:

- SQL injection modifying database records
- Malware changing log files
- DNS poisoning

Impact:

Targets **Integrity** of data and systems.

Destruction

Definition: Irreversible deletion or corruption of data or systems.

Example Attacks:

- Ransomware wiping data
- Logic bombs
- Physical destruction of hardware

Impact:

Compromises **Availability** — systems become unusable or lost.

CIA vs. DAD Triad Comparison

Defender’s Goal (CIA)	Attacker’s Goal (DAD)	Example
Confidentiality	Disclosure	Data leakage through phishing
Integrity	Alteration	Manipulated database entries
Availability	Destruction	DDoS or ransomware attack

Insight for Students:

Network monitoring systems are designed to detect **DAD behaviors** to maintain **CIA objectives**.

Integrating CIA and DAD in Security Design

- **Defensive Strategy:** Identify and mitigate DAD activities that threaten CIA principles.
- **Network Monitoring Role:**
    - Detect disclosure attempts (data exfiltration)
    - Identify alteration behaviors (log anomalies)
    - Respond to destruction patterns (wiping or denial events)

Discussion Prompt:

How could DAD analysis improve early detection in network monitoring?

4. The AAA Model

Definition:

The **AAA Model** — *Authentication, Authorization, and Accounting* — defines the operational functions that control access and usage in a secure system.

It complements the CIA Triad by describing **how** security is enforced.

Authentication

Purpose: Verify the identity of a user or system before granting access.

Common Methods:

- Passwords, PINs
- Multi-Factor Authentication (MFA)
- Biometrics (fingerprint, facial recognition)
- Digital certificates

Example:

A network switch or VPN gateway authenticates users before allowing connection.

Authorization

Purpose: Determine **what actions or resources** an authenticated entity is allowed to access.

Mechanisms:

- Role-Based Access Control (RBAC)
- Access Control Lists (ACLs)
- Attribute-Based Access Control (ABAC)

Example:
An authenticated user can view files but not modify system configurations.

Accounting

Purpose: Track and record user actions to support auditing, compliance, and forensic analysis.

Data Collected:

- Login attempts
- Commands executed
- Resources accessed

Example:
Network devices log user activity for later review in a Security Information and Event Management (SIEM) system.

AAA in Context

Component	Function	Example
Authentication	Verify identity	Username & password
Authorization	Grant permissions	File access rights
Accounting	Record activities	System logs

Integration:

- AAA supports **Confidentiality** (via access control)
- Reinforces **Integrity** (by restricting modification rights)
- Enhances **Availability** (through controlled, accountable access)

Relation to Network Monitoring

Network monitoring tools often integrate with AAA systems to:

- Validate authorized users
- Detect abnormal authentication patterns
- Correlate access logs with threat intelligence

Example:
A SIEM alerts administrators to repeated failed authentication attempts — possible brute-force attack.

Reflection Prompt

- How do AAA and CIA models complement each other?
- Why is accounting critical for incident response and network forensics?

5. Threats in Cybersecurity

Threat: Any circumstance or event that can exploit a vulnerability to cause harm.

Types of Threats:

- **Human:** hackers, insiders, social engineers
- **Technical:** malware, ransomware, zero-day exploits
- **Environmental:** natural disasters, power outages

Example: A phishing attack that steals user credentials.

Vulnerabilities

Definition: Weakness or flaw in a system that can be exploited by a threat.

Examples:

- Unpatched software
- Weak passwords
- Misconfigured firewalls

Note for Students:
A vulnerability by itself is not an attack — it becomes a risk when combined with a threat and exposure.

Threats vs. Vulnerabilities vs. Risks

Concept	Description	Example
Threat	Potential cause of harm	Hacker attempts intrusion
Vulnerability	Weakness exploited	Outdated OS
Risk	Probability × Impact	Data breach likelihood and cost

6. Overview of Cybersecurity Domains

Major Domains:

1. **Network Security**
2. **Application Security**
3. **Information Security**
4. **Cloud Security**
5. **Operational Security (OpSec)**
6. **Incident Response & Forensics**
7. **Security Governance & Risk Management**

6.1 Network Security

Focus: Protecting network infrastructure and data in transit.

Components:

- Firewalls and IDS/IPS
- VPNs and segmentation
- Monitoring and logging systems

Connection to this course:

This domain directly supports network monitoring design and threat detection.

6.2 Application Security

Goal: Secure software from vulnerabilities during design and development.

- Code review and testing
- Secure SDLC principles
- OWASP Top 10

Example: Preventing SQL injection and cross-site scripting.

6.3 Information Security

Concerned with: Data protection in all forms — physical and digital.

- Data governance
- Encryption policies
- Data loss prevention (DLP)

6.4 Cloud Security

Challenges:

- Shared responsibility model
- Identity and access control
- Data protection in virtualized environments

Example: Securing AWS/Azure cloud workloads.

6.5 Operational Security (OpSec)

Focus: Procedures and policies that protect information during daily operations.

- Access control policies
- Data handling procedures
- Employee training and awareness

6.6 Incident Response & Forensics

Key Steps:

1. Preparation
2. Detection
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Forensics: Collecting and analyzing evidence to understand and prevent future incidents.

6.7 Governance, Risk & Compliance (GRC)

- Frameworks: ISO 27001, NIST, COBIT
- Policy creation and enforcement
- Risk assessment and management

Example: University IT governance aligning with national cybersecurity frameworks.

7. From Concepts to Practice

Foundation for Network Monitoring

Why Network Monitoring?

- Early threat detection
- Performance optimization
- Compliance and audit readiness

Core Functions:

- Collecting and analyzing traffic data
- Detecting anomalies and attacks
- Generating alerts and reports

Network Monitoring Tools and Techniques

Examples:

- SIEM (Security Information and Event Management)
- IDS/IPS (Intrusion Detection/Prevention Systems)
- NetFlow and Packet Capture

Skill Focus:

Understanding data patterns → forming actionable cybersecurity intelligence.

CIA & DAD in Network Monitoring

Principle	Monitoring Focus	Example
Confidentiality / Disclosure	Detect data exfiltration	Unusual outbound traffic
Integrity / Alteration	Identify tampering attempts	Log anomalies
Availability / Destruction	Ensure uptime	Detect DDoS patterns

Case Study Discussion

Scenario:

University network experiences unusual outbound traffic at midnight.

Questions for Students:

- Which part of the CIA or DAD triad is at risk?
- What tools would you use to investigate?
- What mitigation actions are appropriate?

Key Takeaways

- CIA Triad defines **defensive objectives**
- DAD Triad reveals **attacker motivations**
- Understanding both aids in designing effective **network monitoring systems**
- Cybersecurity domains interconnect to protect data, systems, and operations

Reflection and Discussion

- How can cybersecurity principles guide network monitoring design?
- What balance exists between monitoring privacy and data protection?
- How could AI assist in future network monitoring solutions?

Thank You

Assist. Prof. Dr. Chanankorn Jandaeng

Walailak University

Contact: chatchanan.ja@mail.wu.ac.th