HPCNC

01219325 Software Development Security
Lecture 1: Principles of Information Security

Asst. Prof. Usa Sammapun, Ph.D.

Chawanat Nakasan, D.Eng. [*]

[*] Today’s Instructor

Outline

Core Principles: C-I-A

Risk and Risk Management

Threats

Various Fields of Information Security

Key Disciplines & Skimming the Rest of the Course

Core Principles

C-I-A, the Core Principles

Confidentiality

- Protection from unauthorized use and disclosure
- Encryption, Access control
- Related: Secrecy, Privacy, Classification (การจัดชั้นความลับ)

Availability

- Uninterrupted access
- Includes both data and infra
- Threats incl. Denial of Service
- Business Continuity Plan, High Availability, Disaster Recovery, etc.

Integrity

- Protection from unauthorized modification
- Data not altered or deleted
- Hashing, Checksums, Digital Signature, etc.
- Requires Confidentiality as primary basis

“AAA” Services

Identity

- Claiming who you are and that you are initiating AAA.

Authentication

- Proving who you are.
- This includes person, device, system, all of them.

- Solutions include passwords, MFA, biometrics, OpenID (Sign in with [app]), Digital Certificates and Signatures.

Authorization

- Determine the correct set of rights, things you can do in a system.
- Solutions include basic file permissions, role-based access control (RBAC), access control lists (ACL).

Auditing

- Monitoring, tracking, recording
- Audit trails, logging, tracing
- Requires OS, system, and other skills.

Accountability

- Proving human action or inaction.
- Compliance
- Legal and Regulatory Basis

Non-Repudiation

- Prevent denial of things that happened.
- Digital certs, session IDs, txn logs, etc.

Protection Mechanisms

Protection Mechanisms

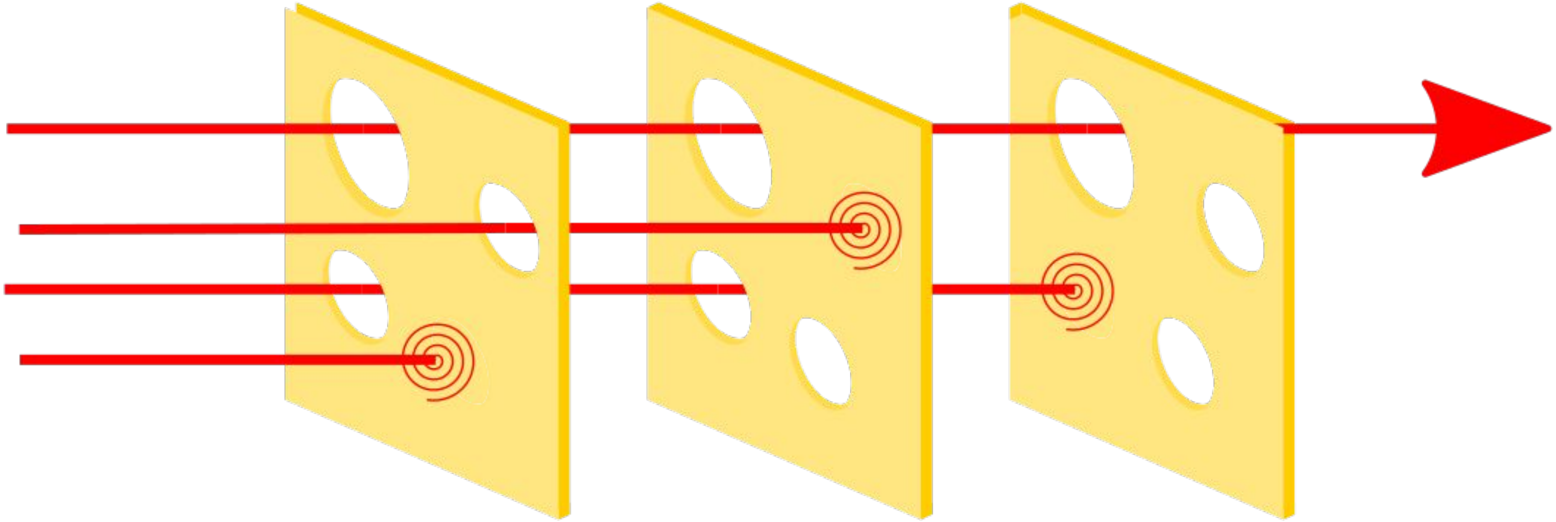
Layering = Defense in Depth

Abstraction = Assigning classes and roles (NOT same as layering)

Data Hiding

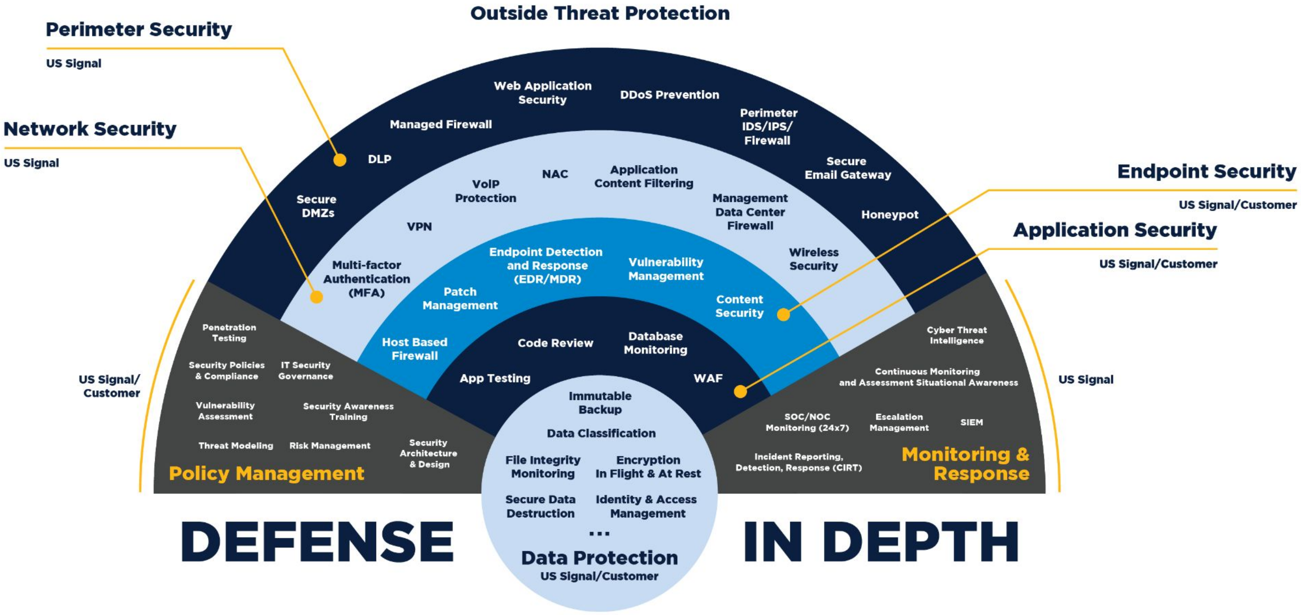
Encryption

Layering (Defense in Depth)



📷: Wikipedia

Layering (Defense in Depth)



📷: US Signal

Data Hiding

Encryption