Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 03: Security Architecture and Engineering

Learning Objectives

By the end of this lesson, you will be able to:

- Apply secure design principles like fail-safe and zero trust to strengthen system defenses against vulnerabilities
- Compare different security models to choose the best approach for strengthening system architecture against cyber threats
- Evaluate privacy, cybersecurity, and risk frameworks to create strategies for managing risks and compliance
- Investigate security architecture concepts to identify key elements for building resilient systems
- Assess various cryptography methods to ensure secure communication
- Establish environmental controls to protect infrastructure against environmental threats to maintain security

Overview of Secure Design Principles

Security Engineering

It helps in building information systems and related architectures to secure information, assets, and services. The following are its functions:

Delivering required functionality to address threats

Incorporating security controls into enterprise architecture to ensure confidentiality, integrity, and availability

Secure Design Principles

These are guidelines for building systems that resist security threats, offering a framework for developing applications, networks, and infrastructure that are less susceptible to vulnerabilities.

Secure Design Principles

1. Least privilege

The principle of least privilege means users should be granted the minimum amount of access (authorization) required to do their jobs.

Secure Design Principles

2. Threat modeling

It is a process by which:

- Potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated
- Mitigations can be prioritized

Secure Design Principles

3. Defense in depth

It is a concept in which multiple layers of security controls are placed throughout an information technology system.

Secure Design Principles

4. Secure defaults

It prioritizes security and disables unused features, ensuring the system starts in a minimal, secure state.

Secure Design Principles

5. Separation of duties (SoD)

It segregates duties to prevent fraud and errors by assigning critical or sensitive tasks to more than one person.

Secure Design Principles

6. Keep it simple

It emphasizes on keeping processes and systems simple to achieve optimal performance.

Fail Secure and Fail Safe

System failure is unavoidable and should be planned for. The following are two possible failure modes:

Fail secure (closed)

Ensures that a system defaults to a safe state in case of failure, preventing further operations

Fail safe (open)

Minimizes or prevents harm to equipment, the environment, or people in the event of a specific failure

Example

If a building catches fire, fail-safe systems would unlock doors to facilitate escape and access for firefighters, while fail-secure systems would lock doors to prevent unauthorized entry.

Trust, but Verify (TbV)

It is a security principle that emphasizes the balance between trust and skepticism, ensuring the integrity of information, systems, and processes for security.

- Promotes verification to avoid blind trust between components
- Conducts regular risk management and regulatory compliance investigations
- Performs verification audits to mitigate the risks from high-risk processes or products

Zero Trust

It is a security model based on the principle of **trusting nothing and verifying everything**.

It ensures strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are inside or outside the network perimeter.

Traditional Security vs. Zero Trust

Traditional security	Zero trust model
Uses the castle-and-moat model to establish a strong defense against outsiders	Requires all access requests to be authenticated, authorized, and encrypted
Assumes everything inside the network is automatically safe	Ensures only verified entities can access data or systems
Allows attackers who breach the network to easily move across security layers and systems	Prevents unauthorized access by enforcing strict verification for every request

Privacy by Design

It is a design-thinking approach to proactively embed privacy into the design and operation of IT systems, networked infrastructure, and business practices, by default.

The seven principles include:

1. Proactive not reactive or preventative not remedial
2. Privacy as default
3. Privacy embedded into design
4. Full functionality
5. End-to-end security
6. Visibility and transparency
7. Respect for user privacy

Source: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

Shared Responsibility Model

It is a cloud security framework that describes the cloud provider's and customer's security responsibilities.

Cloud provider

Responsible for securing the underlying infrastructure leased to customers

Cloud customer

Responsible for securing the aspects of the cloud infrastructure they control and ensuring compliance and data security

The contract (SLA) between the cloud customer and provider defines their individual and shared responsibilities.

Quick Check

You are helping an organization implement a zero-trust model. What key factor should you prioritize to ensure its success?

A. User awareness training tailored to individual needs

B. Focus on business outcomes to get leadership support

C. Follow trust-but-verify principle

D. Block access to all remote users

Overview of Fundamental Concepts of Security Models

Security Models

It is a symbolic representation of a policy.

It translates policy goals into system terms by defining the data structures and techniques for enforcement.

It converts policymakers' intentions into a set of rules that a computer system must follow.

Security Models

A CISSP candidate should be aware of the general types of security models and:

The goal addressed by a model

The evolution of a security model

Types of Security Models

- State machine model
- Multilevel lattice model
- Noninterference model
- Information flow model
- Bell–LaPadula confidentiality model
- BIBA integrity model
- Clark–Wilson integrity model
- Brewer and Nash model (Chinese wall model)
- Graham Denning model
- Take Grant model

State Machine Model

It is used to describe the behavior of a system to different inputs.

It is based on the system's state, which is a snapshot at a given moment.

It records the current permissions and instances of subjects accessing objects.

This model must define all initial system states and how inputs change them to ensure a safe final state.

State Machine Model

Once the system is in a secure state, the state machine will ensure that every time the system is accessed or changed, it will transition only from one secure state to another secure state.

Example

If any component in the OS or firewall fails, it must fail to a secure state.

State machine model characteristics

Multilevel Lattice Models

These models describe strict layers of subjects and objects, often described as lattices or discrete layers.

Subjects with different clearances use the system and the system processes data at different classification levels.

Example

A user with secret clearance can view confidential and secret documents, but not top-secret ones.

Access Control Matrix

It is a table of subjects and objects that indicates the actions or functions that each subject can perform on each object.

Subjects	Document file	Printer	Network folder share
Bob	Read	No access	No access
Mary	No access	No access	Read
Amanda	Read, write	Print	No access
Mark	Read, write	Print	Read, write
Kathryn	Read, write	Print, manage print queue	Read, write, execute
Colin	Read, write, change permissions	Print, manage print queue, change permissions	Read, write, execute, change permissions

Example of an access control matrix

Noninterference Model

The goal of this model is to ensure that high-clearance actions do not impact what low-clearance users can see, preventing any interference between their activities. It addresses the following two attacks:

Ensures that actions at one security level has no effect on another security level

- Security level
- Security level
- Security level
- Security level

Covert channel attacks

Inference attack

Source: https://www.youtube.com/watch?v=v7MHq3Kwt8k

Information Flow Model

It is based on a state machine and focuses on the flow of information rather than on access control.

It doesn't necessarily deal with only the direction of the information flow, but also the type of flow.

Information Flow Model

Here is how multilevel models manage and secure information flow across different security levels:

- The models prevent unauthorized, insecure, or restricted information flow, often between different levels of security.

- It restricts information flow between subjects and objects at the same classification level and between subjects and objects at different classification levels.

Information Flow Model

The diagram shows the flow of information between different security labels.

Bell–LaPadula Confidentiality Model

It is the first mathematical model of a multilevel security policy that defines a secure state of the system.

- Focuses on maintaining the confidentiality of objects
- Serves as a framework for systems storing and processing sensitive information
- Uses matrices and security levels to determine if a subject can access an object
- Employs subjects, objects, access operations, and security labels

Bell–LaPadula Confidentiality Model

Rules and properties

- **The simple security rule:** A subject cannot read data at a higher security level (no read up).
- **The *-property rule:** A subject cannot write data to an object at a lower security level (no write down).
- **The strong star property rule:** A subject can perform read and write functions only to objects at its same security level.

Drawbacks

- It addresses only the confidentiality of data.
- It does not address integrity or availability because it was designed in the 1970s.
- It does not support many operations that are common today, such as file sharing and networking.
- It also assumes secure transitions between security layers and does not address covert channels.

BIBA Integrity Model

It protects the integrity of the information and the activities that take place within a system. The following are the axioms of the BIBA integrity model:

Simple integrity axiom

- It states that a subject cannot read data at a lower integrity level.
- This is called a no read down (NRD).

Star integrity axiom

- It states that a subject cannot modify an object at a higher integrity level.
- This is called no write-up (NWU).

BIBA Integrity Model: Drawbacks

Addresses only integrity excluding confidentiality and availability

Focuses on protecting objects from external threats while assuming internal threats are managed programmatically

Does not prevent covert channels

Clark–Wilson Integrity Model

It is an integrity model developed after the BIBA model and is used commercially.

- It prevents unauthorized users from making modifications.
- It prevents authorized users from making improper modifications.
- It maintains internal and external consistency.

Clark–Wilson Integrity Model

The model implements the following goals of integrity:

Clark–Wilson Integrity Model

This model focuses on well-formed transactions and separation of duties.

Well-formed transaction

Identifies a series of operations that transform a data item from one consistent state to another

Access triple

Utilizes a three-part relationship of a subject, program (interchangeable with a transaction), or object

Clark–Wilson Integrity Model

This model defines the following items and procedures:

Constrained data item (CDI)

It is a data item whose integrity is protected by the security model.

Unconstrained data item (UDI)

It is a data item (input or output) that is not controlled or validated by the security model.

Integrity verification procedure (IVP)

It is a procedure that scans data items to confirm their integrity.

Transformation procedures (TPs)

They are the only procedures that are allowed to modify a CDI and form the backbone of this model.

Clark–Wilson Integrity Model

The model is illustrated below:

Brewer and Nash Model (Chinese Wall Model)

It is an information flow model that provides an access control mechanism that can change dynamically depending on a user's authorization.

Previous actions are designed to implement controls that mitigate conflict of interest.

Information flow does not happen between the subjects and objects in a way that would create a conflict of interest.

Source: https://infosectests.com/cissp-study-references/domain-3-security-engineering-and-architecting/

Graham Denning Model

The model is based on the access control matrix model.

- It defines a set of basic rights in terms of commands that a subject can execute over an object.
- Each object has an owner that has special rights on it.
- Each subject has another subject (controller) that has special rights on it.

Graham Denning Model

The model outlines eight primitive operations to ensure the secure execution of the rights a subject has over an object.

- How to securely create an object
- How to securely create a subject
- How to securely delete an object
- How to securely delete a subject
- How to securely provide the read access right
- How to securely provide the grant access right
- How to securely provide the delete access right
- How to securely provide the transfer access right

Protection rights

Take Grant Model

This model employs a direct graph to dictate how rights can be passed from one subject to another subject or object.

Take rule
Allows the subject to take rights over an object

Grant rule
Permits the subject to grant rights to an object

Create rule
Authorizes the subject to create new rights

Remove rule
Enables the subject to remove the rights it has

Take Grant Model: Example

- Alice can create and remove privileges to secrets.
- Alice can grant privileges to Carol.
- Bob can take Alice's privileges.

Composition Theories

It is based on the notion of how inputs and outputs between multiple systems relate to one another.

Systems are usually built by combining smaller systems and the security of these components must be considered when combined into larger systems.

This theory follows how information flows between systems rather than within an individual system.

Composition Theories: Types

Cascading:

Input for one system comes from the output of another system.

A → B → C

Feedback:

One system provides input to another, which then reciprocates by providing input back to the first system, reversing the roles.

A → B

B → A

Hookup:

One system sends input to another system while also sending input to external entities.

A → B

A → C

Covert Channel

It is a type of attack that enables the transfer of information objects between processes that are not permitted to communicate by the computer security policy.

Causes

- Improper coding
- Improper access control implementation within software
- Uncontrolled shared resources

Covert Channel

It is an attack where communication is transmitted over a channel that was not intended for communication.

Types of Covert Channels

Covert storage channel

- It communicates by modifying a storage location, such as a hard drive.
- It occurs when out-of-band data is stored in messages for the purpose of memory reuse.

Example

Steganography

Covert timing channel

- It performs operations that affect the real response time observed by the receiver.
- It operates by tracking when data is transmitted between parties and monitoring the timing of operations.

Example

Monitoring cryptographic functions

Closed and Open Systems

They define the degree of interaction a system has with an external environment.

Closed system	Open system
Hides source code and internal logic from the public	Exposes source code and internal logic to the public
Works well with a narrow range of systems, typically from the same manufacturer	Works based on agreed-upon industry standards
Integrates with unlike systems with difficulty, but offers increased security	Integrates easily with systems from different manufacturers that support the same standards
Relies more on the vendor and programmer for product revisions over time	Depends on public inspection and review for product improvement
Limits external interaction	Provides interoperability

Quick Check

Which security model is employed in investment banks, between the corporate advisory area and the brokering department to separate those providing corporate advice on takeovers from those advising clients about buying shares?

A. Bell-LaPadula

B. BIBA

C. Clark Wilson

D. Brewer and Nash

Overview of Privacy, Cybersecurity, and Risk Framework

Privacy Framework

It establishes a guideline to protect personal data, ensuring compliance with privacy regulations.

Types of privacy frameworks include:

OECD privacy principles

Privacy Management Framework (PMF)

The General Data Protection Regulation (GDPR)

Source: http://www.oecdprivacy.org/
https://www.aicpa.org/interestareas/informationtechnology/privacy-management-framework.html

Cybersecurity Frameworks

It is a set of standards designed to manage and mitigate cybersecurity risk to information systems and data. Types of cybersecurity frameworks include:

ISO/IEC 270xx

HITRUST Common Security Framework (CSF)

Risk Management Framework (RMF)

Cloud Security Alliance (CSA); Security, Trust, Assurance, and Risk Registry (STAR)

Source: http://www.oecdprivacy.org/

Risk Frameworks

It is a systematic way of identifying, assessing, and managing risks across an organization.

Types of risk frameworks include:

NIST Special Publication (SP) 800-37

ISO 31000

ISACA Risk IT

Committee of Sponsoring Organizations (COSO)

Source: http://www.oecdprivacy.org/
https://www.aicpa.org/interestareas/informationtechnology/privacy-management-framework.html

Overview of System Architecture Requirement

Architecture

It describes the major components of the system and how they interact with each other.

Example

In house architecture, the house plan, electricity plan, or plumbing plan for the kitchen represents the highest or initial level in the development process.

Architecture

It serves as a tool to understand the structure and behavior of a complex system through different views.

It provides a representation of the concerns of each stakeholder.

It offers a formal description and representation of the system.

It describes the relationships, interactions, and dependencies between components.

System Architecture

It describes the major components of a system and how they interact with each other, users, and other systems. A disciplined approach to system architecture enhances:

- Interoperability
- Portability
- Security
- Extensibility

Security goals have to be defined before the architecture of a system is created (baked-in concept).

System Architecture

It is essential to ensure that security, compliance, and functional requirements are integrated seamlessly throughout the development lifecycle.

- Security addressed late in the development phase is called a baked-on concept.
- ISO/IEC 42010 is the standard for systems and software engineering architecture description.
- It is important to understand the scope of the target system before developing, architecting, or evaluating it.

Security Architecture Requirement

To safeguard sensitive information, both the government and the industry must establish robust security architecture requirements.

- They must ensure that all the systems purchased and implemented protect their secrets.
- They must develop ways to instruct vendors on how to build computer systems to meet their security needs.
- To test the products, the architecture should be developed based on the same security needs.

Security Architecture Requirement

The **Computer Security Technology Planning Study** outlines the foundational security requirements for computer systems eligible for purchase and deployment.

- It was released by the U.S. government in 1972.
- The requirements have since shaped the security architecture of nearly all systems in use today.

Security Architecture Requirement

Some of the core tenets of these requirements are:

- Trusted computing base
- Trusted platform module
- Security kernel
- Security perimeter
- Reference monitor

Trusted Computing Base (TCB)

It refers to the collection of all hardware, software, and firmware components within a system that provides security controls and enforces the security policy.

Trusted Computing Base (TCB)

It covers operating system components along with hardware, software, and firmware, as each can affect the system's security both positively and negatively.

Trusted Computing Base (TCB)

It provides extra layers of protection around these mechanisms to ensure they are not compromised, so the system runs safely and predictably.

Trusted Computing Base (TCB)

If TCB is enabled, then the system has:

A trusted path

Ensures secure communication between the user or program and the TCB

A trusted shell

Prevents exposure of actions within the interpreter or shell and blocks intrusion from other processes

Trusted Platform Module (TPM)

It is the implementation of a secure crypto-processor.

- It is a microprocessor that stores and generates cryptographic keys.
- It generates random numbers for use in cryptographic algorithms.
- It is used for cryptographic functions such as disk encryption and authentication.

Examples

Windows Server 2008 uses the disk encryption software named BitLocker.

Security Perimeter

It defines an imaginary boundary that divides trusted and untrusted components in the system.

- Reference monitor is a resource within the boundary and is considered a part of TCB components on either side of the boundary that can interact only via interfaces.
- The interfaces limit or restrict the commands and data that can be passed on either side of the boundary creating a security perimeter.

Reference Monitor

It is an access control concept, also referred to as an **abstract machine,** that provides direction on how all access control decisions are made.

- A fully secure system will require subjects to be fully authorized before access is provisioned to the objects.
- All-access decisions should be made by a core-trusted, tamper-proof component of the OS that works at the system kernel.

All system calls go through the reference monitor for security checking

Security Kernel

It comprises hardware, software, and firmware components within the TCB.

It implements and enforces the reference monitor concept.

It serves as the core of the TCB.

John	Full control
Bob	No access
David	Read
Marge	Full control
George	Write
Sean	No access
John	Full control
Bob	No access

Security Kernel Requirements

A security kernel must be:

Able to provide isolation for the processes carrying out the reference monitor concept

Small enough to be tested and verified in a complete and comprehensive manner

Invoked for every access attempt and ensure it is tamperproof

Confinement, Bounds, and Isolation

The following concepts are used in security architecture to manage and control how processes interact with memory and resources:

Confinement	Bounds	Isolation
• Allows a process to read from and write to only certain memory locations and resources • Denies and logs any action where a process attempts to initiate an action beyond its granted authority	• Defines the limits of memory a process cannot exceed when reading or writing • Specifies the bounds of a process as limits set on the memory addresses and resources it can access	• Runs a process when it is confined by memory bounds • Ensures isolation affects only the memory and resources associated with the process

Ring Model

It is a form of CPU hardware layering that separates and protects domains from each other.

- Many CPUs have four rings, ranging from ring 0 to 3.
- The innermost ring is the most trusted.
- It processes communicate between rings via system calls.

Ring 0: Kernel
Ring 1: Other OS components
Ring 2: Device drives
Ring 3: User applications

Quick Check

You moved an encrypted hard drive to a new device due to hardware failure but couldn't access the content despite knowing the password. What hardware security feature is likely causing this problem?

A. TCB

B. TPM

C. HSM

D. RSA

Overview of Industrial Control System (ICS)

Industrial Control System (ICS)

> It is a general term that encompasses several types of control systems, including **Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS),** and other control system configurations such as **Programmable Logic Controllers (PLC)** often found in the industrial sectors and critical infrastructures.
>
> ~ NIST

The following are the different types of control systems:

- Programmable logic controllers (PLC)
- Distributed control systems (DCS)
- Supervisory control and data acquisition (SCADA)

Programmable Logic Controller (PLC)

It is a small industrial computer originally designed for factory automation and industrial process control.

It can be programmed as per the process that needs to be controlled.

It has evolved into controllers with the capability of controlling complex processes and is used substantially in SCADA systems and DCS.

It is also used as the primary controller in smaller system configurations.

It is used extensively in almost all industrial processes.

Distributed Control System (DCS)

It is a specially designed automated control system used to monitor and control distributed equipment in process plants and industrial processes.

It is a system of dividing plant or process control into several areas of responsibility, each managed by its controller, with the whole system connected to form a single entity.

Supervisory Control and Data Acquisition (SCADA)

It is used to monitor and control a plant or equipment in industries (telecommunications, water, waste control, energy, oil and gas refining) and other public transportation systems.

Supervisory Control and Data Acquisition (SCADA)

SCADA SUPERVISORY CONTROL AND DATA ACQUISITION

- It consists of many remote terminal units spread geographically across for the collection of data.
- It is connected to the master station for centralized data acquisition via any communication system.
- It provides management with real-time data on production, improves plant and personnel safety, and reduces costs of operation.
- It has adopted IoT technology to significantly improve interoperability, reduce infrastructure costs, and increase ease of maintenance and integration.

SCADA: Key Components

Difference Between PLC, DCS, and SCADA

	PLC	DCS	SCADA
Usage	Controls the medium or large-scale applications	Controls the entire plant	Supervises and acquires data from remote plants
Location	Local	Local	Geographically dispersed
Communication	LAN	LAN	Any communication system
Performance	High	Medium	Slow

Security Concerns with ICS

It poses the following security concerns:

- Controls systems protocols with little or no security
- Migrates to TCP/IP networks with its inherent vulnerabilities
- Interconnects with enterprise networks
- Operates old systems and applications with poor patching practices
- Monitors control systems minimally to detect and prevent attacks
- Follows poor security practices, resulting in insecure products
- Increases risk of insider attacks by outsourced IT services
- Amplifies attacks on ICS by terrorists and foreign governments

Case Study: SFG Malware

- The SFG malware targeted the industrial control systems (ICS) within European energy companies in 2016, creating a backdoor.
- According to SentinelOne Labs, the backdoor delivered a payload that was used to extract data or potentially shut down the energy grid.

Case Study: Challenge

- The Windows-based SFG malware is designed to bypass the next-generation antivirus software and firewalls.
- It also encrypts key features of its code so that it can not be discovered and analyzed.
- It even skips features such as facial recognition, fingerprint scanners, and other advanced biometric access control systems running inside target organizations.
- It shuts down when put into a sandboxed environment or a virtual machine to escape the notice of security teams.

Case Study: Solution

- Implementing robust security measures and threat detection tools could help mitigate the risks posed by such advanced malware.

Case Study: Outcome

- The discovery of the SFG malware underscores the vulnerability of critical infrastructures and highlights the evolving tactics of cyber-criminals and nation-states.
- It emphasizes developing better defense mechanisms against future cyber threats targeting essential services.

Quick Check

You want to review the status of the industrial control systems your organization uses for building control. What type of systems should you seek access to for review?

A. SCADA

B. DSS

C. BAS

D. ICS-CSS

Overview of Information System Lifecycle

Information System Lifecycle Management

It is a systematic process involving stages, activities, and considerations for the development, deployment, and maintenance of an information system. The following are its phases:

1. Stakeholders' needs and requirements identification
2. Requirements analysis
3. Architectural design
4. Development or implementation
5. Integration
6. Verification and validation
7. Transition or deployment
8. Operations and maintenance
9. Retirement or disposal

Information System Lifecycle Management

1 Stakeholders’ needs and requirements identification

- It focuses on identifying and understanding stakeholders' needs, expectations, and requirements.
- It encompasses a comprehensive analysis of requirements from end users, managers, regulators, and other relevant parties.

Information System Lifecycle Management

2 Requirements analysis

This phase involves:

- Analyzing requirements
- Identifying functional and non-functional aspects
- Considering constraints
- Ensuring alignment with the organization’s objectives

Information System Lifecycle Management

3 **Architectural design**

It involves creating a blueprint for the information system, outlining its:

- Structure
- Components
- Modules
- Data flow
- Interfaces

Information System Lifecycle Management

4

Development or implementation

This phase involves actual coding and development of the information, involving:

- Software creation
- Hardware configuration
- Component integration

Information System Lifecycle Management

5 **Integration**

- It is the process of combining different modules or components of the system to ensure they work together seamlessly.
- It ensures that the individual elements of the system function as a unified whole.

Information System Lifecycle Management

6 Verification and validation

- It focuses on confirming that the developed system meets the specified requirements.
- It ensures that each component of the system is correctly implemented and fulfills its intended purpose.

Information System Lifecycle Management

7 Transition or deployment

This phase involves the migration of the system from the development environment to the operational environment, making it available to end users.

Information System Lifecycle Management

8 Operations and maintenance

- In this phase, the system is used in the operational environment, involving daily management, monitoring, and support.
- Maintenance ensures system functionality through updates and issue resolution.

Information System Lifecycle Management

9 Retirement or disposal

- It involves organized decommissioning of the system, focusing on data disposal and regulatory compliance.
- It also includes making decisions about the system’s future or its replacement.

Quick Check

After the CRM system has been developed and tested, which phase of the information system lifecycle would involve transferring the system to the production environment for end-users?

A. Requirement analysis

B. Development

C. Verification and validation

D. Transition or deployment

Establishing Evaluation Criteria

Evaluation Methods and Criteria

These are designed to gauge the real-world security of systems and products. Evaluation criteria help:

- Measure the security of products and systems
- Provide a common mechanism to evaluate vendor products
- Publish the findings (rating) of the product tests
- Give a level of security assurance to the product
- Customers select products based on the evaluation rating

Trust and Assurance

Trust: States the level of protection that can be expected from a system

Assurance: States that the system will be operated reliably and predictably in all computing scenarios

What is evaluated?

- The security-relevant components like the TCB, access control, kernel, reference monitor, and protection mechanisms
- The relationship and interaction between these components

Common Criteria (CC)

The Common Criteria for Information Technology Security Evaluation (CC) is the official name for the international standard (ISO/IEC 15408).

- It is an international set of specifications and guidelines that evaluates information security products, especially to ensure that the agreed-upon security standard for government deployments are met.
- The thorough evaluation is assured by rigorous evaluation of the process of implementation, specification, and testing of computer security products.
- Evaluated products are assigned evaluation assurance levels (EAL).
- It addresses functionality and assurance.

Terms Related to Common Criteria

Protection profile (PP)

It defines security requirements and objectives for products like firewalls or IDS.

Target of evaluation (TOE)

It is the target product or system whose evaluation has to be done.

Evaluation assurance level (EAL)

It is the degree or score of evaluation of the tested system or product.

Security target

It is the document that describes the target of evaluation (TOE), which includes security requirements and the operational environment.

Common Criteria Evaluation Process

Common Criteria Levels

Certification and Accreditation (C and A)

It is the two-step process used to evaluate and approve a system for use.

Certification

- It is often an internal verification and is trusted only within the organization.
- It is the technical review that assesses the security mechanism and evaluates its effectiveness.
- The process may use safeguard evaluation, risk analysis, verification, testing, and auditing techniques.
- The goal is to ensure the system is right for the customer's purpose.

Accreditation

- It is the formal declaration by the designated approving authority (DAA) that outlines how an IT system is authorized to operate.
- It is the formal management decision to approve the use of a certified system.
- Once accreditation is performed, management can formally accept the adequacy of the overall security performance of an evaluated system.

Quick Check

A government agency is evaluating a new encryption system to protect sensitive data and is considering the Common Criteria (CC) for security assessment. Which component of the Common Criteria offers a framework for defining security requirements?

A. Protection Profile (PP)

B. Security Target (ST)

C. Evaluation Assurance Level (EAL)

D. Certification Body (CB)

Overview of Cloud Computing

Cloud Computing

It is a type of computing that depends on sharing computing resources over the internet.

It is the use of remote servers on the internet to store, manage, and process data rather than a local server or computer.

Cloud Computing Models

Cloud Computing Characteristics

The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers (typically based on policies).

Cloud Computing Characteristics

It allows consumers to expand or contract the resources they use from the pool (provisioning and deprovisioning), often completely automatically.

Cloud Computing Characteristics

All resources are available over a network, without any need for direct physical access.

Cloud Computing Characteristics

Customers are charged for what they are using or consuming.

Cloud Computing Characteristics

It is the mode of operation of software where multiple independent instances of one or more applications operate in a shared environment.

Cloud Computing Characteristics

- Consumers provision the resources from the pool using on-demand self-service.
- They manage their resources themselves, without having to talk to a human administrator.

Cloud Deployment Categories

Public cloud

- The cloud infrastructure is made available to the general public or a large industry group.
- It is owned by an organization selling cloud services.

Cloud Deployment Categories

Private cloud

- The cloud infrastructure is operated solely for a single organization.
- It might be managed by the organization or by a third party.
- It might be located on-premises or off-premises.

Cloud Deployment Categories

Community cloud

- The cloud infrastructure is utilized by multiple organizations, and it supports a specific community with shared concerns.
- It might be managed by the organizations or by a third party.
- It might be located on-premises or off-premises.

Cloud Deployment Categories

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities.

Cloud Service Categories

Infrastructure as a service (IaaS)

- It offers access to a resource pool of fundamental computing infrastructures, such as compute, network, or storage.
- It is also called the Serial Peripheral Interface tiers.

Examples

Amazon EC2, Google Compute Engine, and HP Cloud

Cloud Service Categories

Platform as a service (PaaS)

- It provides cloud computing services a platform allowing customers to develop, run, and manage applications.
- It doesn’t have the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

Examples

Google App Engine, Microsoft Azure Cloud Services

Cloud Service Categories

Software as a service (SaaS)

- It is a full application that's managed and hosted by the provider.
- The consumers access it with a web browser, mobile application, or a lightweight client application.

Examples

Google Apps and Microsoft Office 365

Quick Check

You have written an application in Python. You are considering moving from a self-hosted Python environment to one where you will run the application on servers managed by a cloud provider. What type of cloud solution should you consider?

A. Software as a service (SaaS)

B. Platform as a service (PaaS)

C. Application as a service (AaaS)

D. Infrastructure as a service (IaaS)

Internet of Things (IoT) Technologies

Internet of Things (IoT)

It is a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling them to connect and exchange data.

IoT Architecture

Components of IoT

Sensors

They are the backbone of the IoT, acting as the eyes and ears of interconnected devices by gathering physical world data.

Wearables

These devices are designed to be worn, collecting real-time data and providing functionalities that seamlessly integrate with daily life.

Facility automation

It integrates internet-connected devices, sensors, and software to optimize building operations and enhance the physical environment.

Connectivity

It refers to networks such as wi-fi, Bluetooth, and cellular, which enable devices to connect to the internet.

IoT Security Challenges

Lack of standardization

- IoT lacks a standardized security framework, resulting in inconsistent security practices across devices and manufacturers.
- This fragmentation creates compatibility issues and hinders interoperability.

Data privacy concerns

- IoT devices collect and transmit vast amounts of data, including personal and sensitive information.
- Mishandling or unauthorized access to this data can lead to privacy breaches and identity theft.

Insecure communications

- IoT devices may communicate over unsecured channels.
- This makes them susceptible to eavesdropping and man-in-the-middle attacks, where attackers intercept and alter communications.

IoT Security Challenges

Lifecycle management

- IoT devices often have long lifecycles, and manufacturers may discontinue support and updates when new models enter the market.
- This leaves devices vulnerable to known security flaws that go unpatched, posing a significant security risk.

Physical attacks

- Physical access to IoT devices can allow attackers to tamper with hardware or extract sensitive data.
- Attackers with physical access can also reprogram the device for malicious purposes.

Supply chain risks

- IoT components sourced globally make supply chains vulnerable to tampering or the insertion of malicious components.
- Ensuring the integrity of the supply chain is crucial to prevent security breaches.

Top 10 IoT Vulnerabilities of OWASP

Open Web Application Security Project is a nonprofit foundation dedicated to improving the security of software applications. The following are its vulnerabilities:

1. Weak, guessable, or hard coded passwords
2. Insecure network services
3. Lack of secure update mechanism
4. Insecure ecosystem interfaces
5. Insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Lack of physical hardening
10. Insecure default settings

Edge and Fog Computing

It is a standard that defines how edge computing should work and enables the operation of computing, storage, and networking services between end devices and cloud computing data centers.

It has a decentralized computing structure.

The data is processed in the local network where the device connected to the sensor is located.

Source: https://www.e-zigurat.com/innovation-school/blog/cloud-edge-fog-computing-practical-applications/

Edge and Fog Computing

Data is processed on the edge device, IoT, endpoint, and embedded devices.

Benefits

- Real-time data analysis
- Improved response time
- Lower bandwidth consumption

Source: https://www.e-zigurat.com/innovation-school/blog/cloud-edge-fog-computing-practical-applications/

Edge and Fog Computing

Vulnerabilities

- Same security challenges as the IoT
- Increased attack surface
- Physical security concerns

These vulnerabilities can be mitigated by employing security by design and increasing network monitoring.

Source: https://www.e-zigurat.com/innovation-school/blog/cloud-edge-fog-computing-practical-applications/

Monolithic and Microservice Architecture

Monolithic Architecture

It refers to a traditional method of building applications where all software functionalities are encompassed in a single, self-contained unit.

- It describes a software style that uses a single code base for multiple business functions.
- It develops a software as a single component, with all processes tightly coupled and running as a single service.
- It resembles a giant rock with everything carved into it, illustrating a monolithic application.

Characteristics of Monolithic Architecture

01

Single codebase: The entire application's code, including the user interface (UI), business logic, and data access layers, is written and stored together in one place.

02

Tightly coupled components: Different parts of the application are highly interconnected, so a change in one component can potentially affect other parts.

03

Centralized deployment: The entire application is deployed as a single unit, so any updates or changes require redeploying the entire application.

Microservices Architecture

It breaks down an application into smaller, self-contained services that communicate with each other through well-defined APIs.

- It composes a single application from many loosely coupled and independent services in a microservices architecture.
- It handles a specific business capability, such as user authentication, payment processing, or data retrieval, with each microservice.
- It operates independently, allowing developers to work on these services separately without disrupting the entire application.

Advantages of Microservices Architecture

Agility

Empowers organizations to quickly respond to changing business needs

Scalability

Enables independent scaling to meet demand, ensuring optimal performance during traffic spikes

Faster development

Features smaller code bases and independent development cycles, accelerating development and reducing time-to-market

Easy Maintenance

Simplifies maintenance and troubleshooting by isolating services, confining issues to specific areas

Improved Fault Tolerance

Enhances fault tolerance, preventing cascading failures across services

Independence

Allows for the independent deployment of individual components

Case Study: Challenge

- Uber, like most startups, initially built their application with a monolithic architecture.
- As it expanded worldwide, they faced issues with scalability, performance, and application stability.
- Monolithic architecture combines all components into a single, popular single-tiered software application.
- These components include the client-side user interface, server-side business logic, data access layer, and integrations.

Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d
https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

Case Study: Challenge

- These components are interconnected and interdependent, which means that when one component needs to be updated, changes must be made to the entire application.
- The failure of one component can bring down the entire system.
- As the number of services grew, managing and integrating the product became complex, hindering operational efficiency and user satisfaction.

Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d
https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

Case Study: Solution

- Uber decided to break down its monolithic architecture into multiple applications, transitioning to a microservices architecture.
- Microservices divide and distribute the application workload, providing stable and scalable services.
- They decentralize data storage by managing their own data stores.

Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d
https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

Case Study: Outcome

- Uber manages each microservice individually, removing dependencies between features.
- They simplified integration and management while enhancing overall application performance.
- Independent management of each microservice enhanced stability, as the failure of one no longer jeopardizes the entire system.

Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d
https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

Monolithic vs. Microservices

The figure illustrates the difference between a monolithic architecture and a microservice architecture:

Monolithic architecture

Microservice architecture

Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d

Monolithic vs. Microservices

S.No	Feature	Monolithic architecture	Microservices architecture
1	Codebase	Single, unified codebase	Multiple, independent codebases
2	Deployment	Entire application deployed together	Individual services deployed independently
3	Scalability	Difficult to scale	Individual services can be scaled independently
4	Maintenance	Changes can be complex	Easier to modify individual services
5	Technology	Limited to chosen technologies	Different services can use different technologies
6	Communication	Simple in-memory calls	Can involve API calls, message queues

Virtualization and Related Technologies

Virtualization

It is a technology that enables running multiple operating systems side-by-side on the same processing hardware.

It adds a software layer between an operating system and the underlying computer hardware.

Traditional architecture

Virtual architecture

It leads to more efficiency, higher availability, and lower costs.

Hypervisor

It is a software that is installed to virtualize a given computer.

- **Host machine:** It is a computer on which it is installed.
- **Guest machine:** It refers to every virtual machine.

Type 1 hypervisors (bare metal) run directly on the host machine's hardware.

Example

Microsoft Hyper-V hypervisor and VMware ESX/ESXi

Type 2 hypervisors (hosted) run within an existing operating system environment.

Example

VMware Workstation and Virtual Box

Containerization

It is the process of packaging an application along with its configuration files, libraries, and dependencies to ensure it runs efficiently and without errors across various computing environments.

Source: https://tsa.com/top-5-benefits-of-containerization/

Containerization: Benefits

Source: https://tsa.com/top-5-benefits-of-containerization/

Serverless Computing

It refers to a cloud execution model where the cloud provider manages the servers and underlying infrastructure running the code.

Serverless Computing: Attributes

Event-driven

Run code in response to specific events, such as HTTP requests, without the need to provision or manage servers.

Pay per use

Pay only for what the code uses while it's executing, making it cost-effective for applications with variable traffic.

Automatic scaling

Scale resources automatically based on demand, eliminating manual server management.

Focus on code

Focus on writing and deploying the code without worrying about the underlying infrastructure.

Serverless Computing: Advantages

Reduced cost

Save costs by paying only for consumed resources

Increase scalability

Meet demand effortlessly without manual scaling

Faster deployment

Accelerate development by letting the platform manage servers

Improved maintainability

Rely on the cloud provider for server management and updates

Function-as-a-Service (FaaS)

It is a type of cloud-computing service that enables the execution of code in response to events without the complexity of building and maintaining the infrastructure.

It is a subset of serverless computing.

The server-side logic in FaaS is executed in stateless containers.

High-Performance Computing (HPC) Systems

It is the use of parallel processing for running computationally intensive operations across multiple resources. It consists of computing, network, and storage.

User or scheduler

Computer cluster

Data storage

Quick Check

A large retail chain is considering deploying edge computing devices at each store to process customer transactions and analyze real-time sales data. What is the primary benefit of using edge computing in this scenario?

A. Reduced latency for critical applications

B. Increased network bandwidth

C. Lower overall system costs

D. Improved data privacy

Overview of Cryptographic Solutions

Cryptography

It is the science of using mathematics to encrypt and decrypt data.

It enables the storage or transmission of sensitive information across insecure networks, such as the internet, ensuring that only the intended recipient can read it.

Basic Definitions

Cryptosystem	It refers to the hardware or software implementation of cryptography that contains all the necessary software, protocols, algorithms, and keys.
Cryptology	It is the study of both cryptography and cryptanalysis.
Algorithm (Cipher)	It is a set of mathematical and logical rules used in cryptographic functions.
Kerckhoff's principle	It states the concept that an algorithm should be known and only the keys should be kept secret.

Conventional Encryption

The working of a conventional encryption can be seen below:

Encryption and Decryption

Encryption is the conversion of an original message (plain text or cleartext) into a different message (ciphertext) or cryptogram.

Decryption is the extraction process by which the intended receiver extracts the plaintext from the ciphertext.

Cryptographic Key

It is a piece of information that determines the functional output of a cryptographic algorithm.

Key clustering is an instance when two different keys generate the same ciphertext from the same plaintext using the same algorithm.

Keyspace is a range of possible values used to construct keys.

It is a sequence of letters, symbols, or numbers like a password.

Strength of Cryptosystem

It is estimated using the **work factor** that assesses the effort and resources required for an attacker to breach a cryptosystem.

A good cryptosystem should be cost-efficient and less time-consuming.

A brute force attack is generally used to break a cryptosystem.

Strength of Cryptosystem

It depends on how all the following components work together:

Working of Cryptosystem Elements

A strong and secure cryptogram must:

- Use a flawless algorithm
- Select a large key size
- Employ all possible values within the key space as randomly as possible
- Protect the actual key

Cryptosystem Services

A strong cryptosystem ensures:

Confidentiality

Renders the information unintelligible except by authorized entities

Integrity

Ensures the data has not been altered in an unauthorized manner since it was created, transmitted, or stored

Authentication

Verifies the identity of the user or the system that created the information

Nonrepudiation

Guarantees that the sender cannot deny sending the message

Cryptography Methods: Substitution Cipher

It works by substituting one letter for another letter based on a key.

It is generally used on blogs to filter certain words and in combination with other ciphers.

Example

Caesar cipher or ROT13 rotates the alphabet by 13 steps.
The message **HELLO** becomes **URYYB** after ROT13 substitution.

Cryptography Methods: Transposition Cipher

It transposes the original text with long sequences of complex substitutions and permutations.

It utilizes a key to determine the positions the characters are moved to and is used in combination with substitution cipher in standard ciphers.

Example

Characters are rearranged into columns and then read off in a different order.

S	E	C	U	R	I	T	Y
E	S	U	C	I	R	Y	T

Cryptography Methods: Running Key Cipher

It uses a key that does not require an electronic algorithm and bit alterations, but cleverly uses components in the physical world.

Example

The sender and receiver agree to use a set of books as the algorithm. The key here could be a book page, line number, or column count.

The message **CRYPTOGRAPHY 149l6c7.299l3c7.911l5c8** could likely mean:

Book 1, page 49, line 6, column 7

Book 2, page 99, line 3, column 7

Book 9, page 11, line 5, column 8

Cryptography Methods: Concealment or Null Cipher

It is a message within a message.

Example

If the key value is set to every third word, the recipient would extract and write down every third word from the message to reveal the hidden information.

The message, **the saying: “The time is right” is not cow language, so is now a dead subject** reveals the real message to be **The right cow is dead**.

Cryptography Methods: Steganography

It is the art of hiding the existence of a message by hiding it in some other media such as a picture, audio, or video file.

- It is used to insert digital watermarks on images to identify illegal copies.
- It is employed to send secret messages through emails.

XOR Function

It is a basic mathematical function used in cryptography and returns a true value when only one of the input values is true.

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Here, 0 represents false and 1 represents true.

If both values are false or both values are true, the output of the XOR function is false.

Modulo (Mod) Function

It is also a mathematical function used in cryptography and is the value that is left over (remainder) after a division operation is performed.

Number	Divisor	MOD Function
15	4	3
10	2	0
7	3	1
90	10	0
77	8	5

It is as important to cryptography as logical operations.

Initialization Vector (IV)

It is a random value used with algorithms to ensure more randomness to the encryption process.

- They must be used with keys and encrypted when being sent to the destination.
- If they are not used, then two identical plaintext values encrypted with the same key will create the same ciphertext.

One-Time Pad

It is also known as Vernam cipher and is considered unbreakable when implemented properly.

It uses a binary mathematical function called exclusive OR (XOR) secure implementation and is:

- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender’s and receiver’s sites
- At least as long as the message

Encryption Methods

Symmetric key algorithm

Asymmetric key algorithm

Symmetric Encryption

In this, both encryption and decryption of a message are performed using only a single cryptographic key which is held by each pair of communicating users.

- It can provide confidentiality because of the same key, but not authenticity or nonrepudiation.
- It is used to send secret messages where confidentiality is the main criterion.
- It is used in both wired and wireless networks.
- Number of keys = n(n-1)/2

Note:

Keys must be securely shared between communicating parties.

Examples

Blowfish, AES, IDEA, RC4, RC5, RC6, DES, and 3DES

Symmetric Key Ciphers

Block cipher and stream cipher are the two primary types of symmetric key ciphers:

Block Cipher

It converts a fixed-length block of plaintext data to a block of ciphertext data of the same length.

- The text is operated on preset blocks (64,128, and 192 bits).
- A combination of substitution and transposition is used.
- Although stronger than stream-based ciphers, it is more expensive and computationally more exhaustive.
- It is mainly implemented in software.
- It is used in ciphers like DES and AES.

Stream Cipher

It is generated by combining the keystream (sequence of bits) with plaintext data bit by bit using XOR operations.

- It ensures non-repeating pattern of bits in keystream for security.
- It is mainly implemented in hardware.
- It is most used in voice or video communication.

Stream Cipher vs. Block Cipher

Stream cipher	Block cipher
Faster than block cipher	Slower than stream cipher
Processes the input element continuously, producing output one element at a time	Processes one block at a time, producing output for each block
Requires less code	Requires more code
Uses keys only one time	Allows reuse of key
Easier to implement in hardware	Easier to implement in software
Application: SSL (secure connection on web)	**Application:** Database, file encryption

Data Encryption Standard (DES)

- It is based on a symmetric-key cryptosystem.
- It is a block encryption algorithm that works with fixed-sized 64-bit blocks.
- It uses a 56-bit key, along with 8 bits for parity.
- It employs 16 rounds of transposition and substitution to encrypt data.
- It is no longer considered secure enough for modern applications.

The Feistel function (F function) of DES

Data Encryption Standard (DES) Modes

Electronic Code Book

It is the simplest and the weakest form of DES and is suitable only for shorter messages.

- The message is broken into independent (64-bit) blocks which are encrypted.
- Each block is encoded independently of the other blocks (no chaining).
- The operations can be run in parallel, which decreases processing time.
- The errors are contained.

Electronic Code Book

It has the following limitations:

It cannot carry out preprocessing functions before receiving plain text.

It involves generation of identical ciphertext by identical plaintexts and keys.

It is susceptible to known plaintext attacks.

The repetitive information contained in the plaintext may show in the ciphertext if aligned with blocks.

If the same message is encrypted (with the same key) and sent twice, its ciphertext remains the same.

Cipher Block Chaining

It is stronger than ECB and solves its security deficiencies and is commonly used for bulk encryption.

Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining

- It uses an IV (initialization vector) to add some randomness to encryption and make the previous ciphertext IV for the next block using a chaining function.
- It uses 64-bit plaintext blocks which are XORed with 64-bit IV.
- It encrypts repeated plaintext blocks into different ciphertext blocks by chaining each previous ciphertext block with the current plaintext block.

Cipher Feedback

It divides plaintext into 1, 8, 64, or 128-bit segments (the four sub-modes of CFB) and can encrypt any number of bits.

Example

Single bits or single characters (bytes)

- S=1: bit stream cipher
- S=8: character stream cipher

Cipher Feedback

- A ciphertext segment depends on the current and all preceding plaintext segments.
- A corrupted ciphertext segment during transmission will affect the current and next several plaintext segments.
- The size of the ciphertext must be the same as the block of plaintext.
- It operates as a stream cipher, encrypting data bit-by-bit or byte-by-byte, depending on the sub-mode.

Output Feedback

It feeds the encrypted keystream of the previous block to the next block to create the next portion of the keystream.

- It is very similar to CFB.
- It uses a block cipher as a stream cipher.
- It is appropriate when data arrives in bits or bytes and when error propagation is not accepted.
- It requires the keystream to be of the same size as the block of plaintext.

Output Feedback

Output Feedback (OFB) mode encryption

Advantages

- More resistant to transmission errors; a bit error in a ciphertext segment affects only the decryption of that segment
- Ensures random generation of IV each time and sends it with the ciphertext

Use

- Stream encryption over noisy channels (digital video and audio signals)

Counter

- It uses a 64-bit random data block counter as the first IV.
- It uses an IV counter that increments for each plaintext block that needs to be encrypted.
- It ensures different IV for each plaintext.
- It encrypts the IV and key and then XORs the value with each plaintext block or ciphertext block.
- It generates a keystream values by encrypting CTR, which is then XORed with the message stream.
- It needs to be unknown and unpredictable.
- It is any function that produces a sequence that is guaranteed not to repeat for a long time.

Counter

Advantages

- It needs only the encryption algorithm.
- It enables random access to encrypted data blocks.
- It processes (encrypted or decrypted) blocks in parallel.
- It makes encryption or decryption simple and fast.

Uses

High-speed network encryptions, encrypting ATM cells, IPSec, and Wireless 802.11i

Triple DES

- It uses three 56-bit keys instead of one and uses 48 rounds of transposition and substitution (instead of 16).
- It is approximately 256 times stronger than DES.
- It is used in secure electronic transmission of data.
- It can be configured for use in VPN connectivity (such as IPsec).

Advanced Encryption Standard (AES)

It is a symmetric block cipher and is the current U.S. standard for encryption.

It uses the following for encryption:

- 128-bit keys (10 rounds of encryption)
- 192-bit keys (12 rounds of encryption) or
- 256-bit keys (14 rounds of encryption)

It uses the Rijndael algorithm with variable block sizes (128, 192, and 256-bit) and key lengths (128, 192, and 256-bit).

Other Symmetric Systems

IDEA

- It stands for international data encryption algorithm.
- It uses 64-bit blocks, 128-bit key, and 8 rounds of computation.
- It is used in e-mail encryption software and pretty good privacy (PGP).

Blowfish

- It uses 64-bit block size.
  - 32 – 448 bits (in steps of 8 bits) key size and 16 rounds of computation
- It is optimized for 32-bit micro-processors.

Twofish

- It is a modification of Blowfish using 128-bit blocks.
- It uses variable key length up to 256 bits.

Other Symmetric Systems

RC5

- It uses block sizes of 32, 64, or 128-bits, with key lengths up to 2040 bits.
- It is created as a candidate algorithm for AES.

RC6

- It uses key sizes of 128, 192, and 256-bits and has a block size of 128 bits.
- It is based on RC5 and was also a candidate for AES.

Symmetric Keys: Round Up

Algorithm	Block size	Key length	Comments
DES	64 bit	56 bit + 8-bit parity	16 rounds of processing
2DES	64 bit	112 bit	Compromised by meet-in-the-middle attack
3DES	64 bit	168 bit	
Rijndael	128,192,256 bits	128,192,256 bits	Performs variable rounds of operation
IDEA	64 bit	128 bit	• Performs eight rounds transposition and substitution • Used in PGP
CAST	64 bit	40 to 128 bits	
SAFER	64 to 128 bit	64 to 128 bit	Used in Bluetooth
Blowfish	64 bit	Variable key size	
Twofish	128 bit	128, 192, 256 bits	
RC5	16,32,64 bits	0 to 2040 bits	
AES	128 bit	128, 192, 256 bits	

Asymmetric Encryption

It is also called public-key encryption and uses two keys that are linked mathematically. but are mutually exclusive.

- It needs a pair of keys, one for encryption and one for decryption
- The public key is usually shared, while the private key is secured by the owner.
- In a **secure message format,** the message is encrypted with the receiver's public key (confidentiality).
- In an **open message format,** the message is encrypted with the sender’s private key (authenticity).

Examples

RSA, Diffie-Hellman, Elliptic curve cryptosystem (ECC), El Gamal, and Digital signature algorithm (DSA)

Asymmetric Encryption

Its working is illustrated below:

Goals of Asymmetric Encryption

Authentication

Ensures the ability to authenticate the identity of communicating entities

Confidentiality

Assures the ability to send data in a secure or confidential manner

Non-repudiation

Enables the ability to permit or deny the sending of data

Asymmetric Encryption: Pros and Cons

Pros

- It is highly scalable, making it suitable for large systems.
- It provides confidentiality, authentication, and non-repudiation of data.
- It offers a better key distribution mechanism, enhancing overall security.

Cons

- It is slower when compared to symmetric key algorithms.
- It also requires complex mathematical computations and demands more processing power for implementation.
- It needs a larger key size.

Secure Message Format: Flow

This type of communication is essential for achieving confidentiality, ensuring that data is transmitted in a secure form.

1

Charles wants to send data to Alice that should only be read by her.

Charles

Alice

Secure Message Format: Flow

Charles generates a private and public key pair and exchanges his public key with Alice's public key.

2

Alice
public key

Charles

Charles
private key

2

Charles
public key

Alice
private key

Alice also generates a private and public key pair and exchanges her public key with Charles's public key.

Alice

Secure Message Format: Flow

After the exchange, Charles has his private key along with Alice's public key.

3

Similarly, Alice has her private key along with Charles's public key.

3

Charles

May the force be with you

Avce1ksldldna sd#$sdvdee

Avce1ksldldna sd#$sdvdee

May the force be with you

Alice

To ensure confidentiality, Charles encrypts the data using Alice's public key.

4

5

Alice decrypts the data using her private key, which ensures confidentiality.

Open Message Format: Flow

1

Charles wants to send data to Alice, ensuring she can authenticate him as the sender and cannot deny receiving the message.

Charles

Alice

Open Message Format: Flow

Charles generates private and public keys and exchanges his public key with Alice's public key.

Alice also generates private and public keys and exchanges her public key with Charles' public key.

2

Alice
public key

Charles
private key

2

Charles
public key

Alice
private key

Charles

Alice

Open Message Format: Flow

After the exchange, Charles has his private key along with Alice's public key.

Similarly, Alice has her private key along with Charles's public key.

Charles

May the force be with you

3

Avce1ksldldna sd#$sdvdee

Avce1ksldldna sd#$sdvdee

3

May the force be with you

Alice

To assure authentication and non-repudiation, Charles encrypts the data using his private key.

4

5

Alice decrypts using Charles's public key, ensuring authentication and non-repudiation.

Introduction to RSA Algorithm

It stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of this algorithm.

It is a worldwide de facto standard.

It is based on the difficulty of factoring the product of two large prime numbers, securing the cryptosystem.

It provides digital signatures, encryption, and secret key distribution.

It is used in web browsers with SSL, systems that use public-key cryptosystems.

Types of Asymmetric Cryptography: Elliptic Curve Cryptosystems (ECC)

It generates keys through the properties of the elliptic curve equation, instead of the product of very large prime numbers.

- An ECC key of 160 bits provides the same protection as a 1024-bit RSA key.
- It is more efficient than RSA.
- It provides encryption, digital signature, and key exchange.
- It is used in devices with limited processing, storage, and bandwidth capacity.

Examples

Wireless and cell phone

Zero-Knowledge Proof

Asymmetric cryptography is based on this concept which means that someone can tell something that can be trusted without giving more information than needed.

It is applicable in public-key cryptography.

Example

Trusting a message based on half the key pair (public key), without needing to know the other half of the pair (private key)

Zero-Knowledge Proof

Application

Ownership

Confirms owning a private key

Membership

Establishes being a part of a group, without revealing the identity

Sealed bid auction

Validates who won, without revealing the bid

Types of Asymmetric Encryption: Diffie-Hellman Key Exchange

It is a key distribution asymmetric algorithm that uses a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome.

- It allows two users to exchange a secret key.
- It requires no prior secrets.
- It denies encryption or digital signature functions.

Types of Asymmetric Encryption: Diffie-Hellman Key Exchange

- It is vulnerable to man-in-the-middle attack.
- It is based on the difficulty of calculating discrete logarithms in a finite field.
- It is currently used in many protocols, namely:
  - Secure sockets layer (SSL) or transport layer security (TLS)
  - Secure shell (SSH)
  - Internet protocol security (IPSec)
  - Public key infrastructure (PKI)

Hybrid Key Cryptography (Digital Envelope)

It is a hybrid system that combines the symmetric and asymmetric methods that encrypts a message using a secret key.

- The symmetric secret key is encrypted using a recipient's public key with an asymmetric algorithm.
- The message is encrypted with that secret key and the encrypted symmetric secret key is sent to the recipient.

Hybrid Key Cryptography (Digital Envelope)

- The recipients use their private key to decrypt the secret key.
- The secret key is then used to decrypt the message.
- A symmetric algorithm is used for bulk encryption.
- To distribute the symmetric key, the asymmetric algorithm is used.

Session Key

It is a single-use symmetric key that is used to encrypt or decrypt communication between two users for a single session.

- It’s more secure than static symmetric keys.
- It is decided by the peers and used till the session is over.
- It makes eavesdropping difficult and proves breaking the keys to be futile.

Symmetric vs. Asymmetric Cryptography

Symmetric cryptography	Asymmetric cryptography
It uses the same key for encryption and decryption.	It uses a pair of keys, one for encryption and the other for decryption.
It consumes less computing power.	It consumes more computing power.
It is much faster.	It is slower and are used to distribute the symmetric key.
It is synonymous with a secret key or session key.	It refers to the public key (encryption key) or private key (decryption key) of an asymmetric key pair.

Advantages and Disadvantages

Types of cryptography	Advantages	Disadvantages
Symmetric cryptography	• Very fast to encrypt or decrypt, secure, and affordable • Best for encrypting large files	• Presents the challenge of key management • Does not provide authenticity, nonrepudiation
Asymmetric cryptography	• Enables better key distribution than symmetric systems • Offers better scalability due to ease of key distribution • Provides authenticity and nonrepudiation, in addition to confidentiality and integrity	• Much slower operation than symmetric systems • Vulnerable to man-in-the-middle attacks

One-Way Hash

A hash function uses an algorithm without any key for encryption. This encryption cannot be reversed and hence is called **one-way.**

- A fixed-length hash value (message digest or hash) is created or **hashed** from variable-length plaintext.
- It guarantees data integrity by changing the hash value with changes to plaintext.
- It can be applied to data blocks of any size.
- It produces fixed-length output.

One-Way Hash

Characteristics

- It is computed over the entire message.
- It is a one-way function.
- If given a message and hash value, it makes computing another message with the same hash value impossible.
- It is resistant to birthday attacks.

Hashing Algorithms

A hash function is any algorithm or subroutine that maps large data sets of variable length to smaller data sets of a fixed length.

MD5

- It is the most widely used of the MD (Message-digest algorithm) family of hash algorithms.
- It is harder to break; for input of any length, it creates a 128-bit hash value.

SHA-1/ SHA-2

- It belongs to the secure hash algorithm (SHA) family.
- It generates a 160-bit hash value.
- SHA-2 includes SHA-224, SHA-256, SHA-384, and SHA-512, termed after the length of the hash value each creates.

Hashing Process

1

Charles wants to send an email to Alice and ensure that it is not tampered with during transit.

Charles

Alice

Hashing Communication Process at Sender's End

Hashing Communication Process at Receiver's End

Alice

5

a3421hjkgds

6

#

7

a3421hjkgds

a3421hjkgds

a3421hjkgds

Alice, on receiving the email appended with hash, separates email and hash digest.

Alice inputs the email received from Charles into the hashing algorithm, and creates a fixed-length digest again.

Fixed length digest created at the receiver end and the one received from the sender is compared.

If they are the same, then no tampering has occurred during the transit.

Application of Hashing

Password verification

Stores passwords as hashes instead of normal text files to enhance security

Signature verification

Generates and verifies digital signatures using mathematical processes to confirm the authenticity of documents or messages

Data integrity checks

Produces checksums for data files to assure users about the correctness and integrity of the data

Message Authentication Code (MAC)

It is also known as a tag and is a short piece of information that authenticates a message to confirm that the message is received from the stated sender and has not been changed.

Sender sends MAC with the message

Client computes the MAC and compares with the MAC sent

The MAC value protects both a message's data integrity as well as its authenticity by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

Birthday Attack

It is based on the statistical probability that with 23 people in a room, there is more than 50% probability that two people have the same birthday.

- If the algorithm does produce the same value for two distinctly different messages, it is called a hash collision.
- A birthday attack attempts to exploit the probability of two messages producing the same message digest by using the same hash function.
- SHA-1 (160 bits) may require approximately 280 computations to find a hash collision.
- A hashing algorithm that has a larger bit output is more resistant to birthday attacks as it makes it harder to find a collision.

Salting

Salt is a random value that is added to password hash to prevent dictionary attacks and hash collisions.

- It makes it difficult for the attacker to break into a system by using the strategy of password hash-matching.
- It randomly generates a new salt for each password.
- It stores the output of the cryptographic hash function, instead of the original password, in the database.
- It is used in Unix systems and for internet security.

Password creation

Digital Signatures

- They are used for signing the document cryptographically.
- To digitally sign the data:
  - Create the hash of a data
  - Encrypt that hash with the sender's private key
- To verify the digital signature:
  - Hash the data
  - Find the sender’s public key
  - Decrypt the signature with the sender's public key
  - Check whether the hash you have created matches the hash which you received
- Hashing provides message integrity; signing of hash provides authentication and nonrepudiation.
- It also involves encrypting the hash value of a message with a private key.

Digital Signatures

The working of digital signature is illustrated below:

Quick Check

Bob wants to digitally sign a message he's sending to Alice so that Alice can be sure the message came from him without modification while in transit. Which key should he use to encrypt the message digest?

A. Bob's public key

B. Bob's private key

C. Alice's public key

D. Alice's private key

Overview of Digital Signature Process

Digital Signature Process

It combines asymmetric cryptography and hashing to authenticate messages, ensure their integrity, and prevent repudiation.

Digital Signature Process

Charles wants to send an email to Alice and wants the email not to be tampered with in transit.

Alice wants to ensure not only integrity but also authentication and nonrepudiation
is maintained.

Charles

Alice

Digital Signature Process

Charles generates a private and public key pair, then exchanges his public key with Alice's public key.

Alice also generates her own private and public key pair and exchanges her public key with Charles's public key.

Charles

Alice public key

Charles private key

Charles public key

Alice private key

Alice

Digital Signature Communication at Sender's End

Charles inputs an email into a hashing algorithm.

A fixed-length digest is created as the output.

The message digest is encrypted (digital signature) using the private key of the sender (Charles).

This digital signature is appended to the email and sent to the receiver.

Digital Signature Communication at Receiver’s End

Alice, upon receiving the email appended with the digital signature, separates the digital signature from the email.

The digital signature is decrypted with the sender's public key. Correct decryption ensures authentication and nonrepudiation.

After decrypting with the sender's public key, the hash digest received from the sender becomes visible.

The email is then fed into a hashing algorithm to generate a hash digest.

Both hash digests are compared. If they are the same, it means the email has not been tampered with, ensuring integrity.

Application of Digital Signatures

Communication security

Enables the sender to encrypt the mail with the recipient's public key and sign it with their private key

Code security

Helps protect the code against tampering by digitally signing it

Secure software updates

Helps protect against tampering by digitally signing the updates and providing users with their public key to verify

Financial sectors protection

Protects against tampering with financial documents

Advantages of Digital Signature

Highly robust:

Sturdy in security and stability compared to alternative signature verification algorithms

Better speed:

Faster in key generation compared to the RSA algorithm and such

Less storage:

Reduced storage space requirements to work its entire cycle

Patent free:

Exempted from patents, enabling global, cost-free use

Quick Check

Allen wants to send a secure message to Bob and ensure its authenticity. Which of the following best describes how Allen creates a digital signature for his message to Bob?

A. Allen encrypts a message digest with his private key.

B. Allen encrypts a message digest with his public key.

C. Bob encrypts a message digest with his private key.

D. Bob encrypts a message digest with his public key.

Overview of Public Key Infrastructure

Public Key Infrastructure (PKI)

> It is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

PKI: Characteristics

- It provides CIA and nonrepudiation.
- It includes certificate authority (CA), digital certificates, registration authorities (RA), policies and procedures, certificate revocation, time-stamping, nonrepudiation support, and security-enabled applications.
- A digital certificate is required by each participant, which contains a particular participant's public key and other identifying information.
- It is signed by a trusted CA and the authenticity of the public key is the liability of the CA.
- It is mainly used in online banking and e-commerce.

Certificate Authority (CA)

It is a trusted third party responsible for the issuance and maintenance of digital certificates and can also be internal to an organization.

- It also handles the revocation of certificates.
- It updates and maintains the revoked certificates stored in the certificate revocation list (CRL).

Registration Authority

It establishes and confirms the identity of the individual, initiates the registration process with CA, and performs certificate lifecycle management.

- It performs the registration duties.
- It verifies all the necessary information before allowing a request to go to CA.
- It cannot issue certificates.

PKI Certificate

It is also known as a digital certificate and is used to cryptographically link ownership of a public key with the entity that owns it.

It is used for sharing public keys to be used for encryption and authentication.

Source: https://searchsecurity.techtarget.com/definition/encryption
https://searchsecurity.techtarget.com/definition/digital-signature

PKI Certificate

It includes the following:

- Public key being certified
- Information about the entity that owns the public key
- Metadata relating to the digital certificate
- Digital signature of the public key created by the issuer of the certificate

Note:

X.509 is the standard that dictates the fields used in the certificate and the valid values that can be populated in the fields.

Source: https://searchsecurity.techtarget.com/definition/encryption
https://searchsecurity.techtarget.com/definition/digital-signature

Enrollment Process

It is the process by which a user proves their identity to a certificate authority (CA) to obtain a digital certificate.

Enrollment Process

Enrollment steps

Step 1
The user proves their identity to obtain a digital certificate.

Step 2
The user seeking the certificate provides their public key after the verification process done by the CA is complete.

Step 3
The CA creates an X.509 digital certificate containing the user's identification information and public key.

Step 4
The CA digitally signs the certificate and provides the user with a copy of the signed digital certificate.

Verification Process

When a user receives a digital certificate from a person with whom they wish to communicate, they must verify if:

The CA digital signature is authentic

The CA is trusted by the user

The certificate contains trusted data

The certificate is not listed on a CRL

Revocation Process

Occasionally, a certificate authority needs to revoke a certificate. This might occur because:

- The certificate was compromised
- The certificate was erroneously issued
- The details got changed
- The security association was changed

Certificate Revocation List (CRL)

Certificate revocation list

- It is maintained by various certificate authorities.
- It contains the serial numbers of certificates that have been issued by a CA and have been revoked along with the date and time of revocation.

Online certificate status protocol (OCSP)

- It carries out real-time validation of certificates and reports it back to the user.
- It checks the CRL that is maintained by the CA.

PKI Process

Step 1

User A and User B participate in the PKI process.

Step 2

User A generates public key and private key at their system.

Step 3

User A sends public key and identification information to the CA.

Step 4

The RA or CA verifies the information provided by User A.

Step 5

The CA generates an X.509 digital certificate with the user's public key embedded.

Step 6

The CA digitally signs the certificate and sends it to User A.

Step 7

User A presents the certificate to User B to communicate.

Step 8

User B takes the certificate and verifies the digital signature.

Step 9

After verification, User B trusts the public key of User A and securely communicate.

Key Management

It is the most challenging part of cryptography and can be handled manually or automatically.

- Its features include:
  - Generating, destroying, and recovering keys
  - Protection of keys against capturing, modification, corruption, or disclosure to unauthorized individuals
  - Updating keys and distributing them to the right entities regularly
- Distribution protocols (asymmetric) include:
  - RSA
  - Diffie-Hellman
- The Kerberos key distribution center (KDC) is an example of automated key management.

Key Management Principles

It includes taking backup copies and adopting multi-party key recovery.

The rules states that the key should be:

- Stored and transmitted by secure means
- Randomly generated
- Properly destroyed at the end of their lifetime
- Long enough to provide the necessary level of protection

Their lifetime should correspond with the sensitivity of the data it is protecting.

M of N Control

It is a tool that prevents the recreation of private and public key material from the backup.

- It requires a minimum number of agents (M) out of the total number of agents (N) to work together, to perform high-security tasks.
- The key materials are backed up and then mathematically distributed across several systems or devices.

Example

Implementing three of eight controls would require three key escrow recovery agents to work together to pull a single key out of the key escrow database, illustrating that M is always less than or equal to N.

Source: https://slideplayer.com/slide/12293221/

Quick Check

You realize that a digital certificate used by your organization has been compromised and want to add it to the certificate revocation list (CRL). What element of the certificate goes on the CRL?

A. Serial number

B. Public key

C. Digital signature

D. Private key

Types of Cryptanalytic Attacks

Cryptanalysis

It is the study of ciphertext, ciphers, and cryptosystems to understand how hackers work and find better techniques for defeating or weakening them.

It is used to breach cryptographic security systems and decipher the contents of encrypted messages, even without knowing the cryptographic key.

Cryptanalytic Attacks

The different types of cryptanalysis attacks include:

Brute force	Ciphertext-only	Known-plaintext	Frequency analysis
Chosen-plaintext	Chosen-ciphertext	Implementation	Side-channel
Fault injection	Man-in-the-middle (MITM)	Pass-the-hash	Ransomware

Brute Force

It is an attempt to break the key by systematically checking all possible combinations of characters until the correct one is found.

Bits	Cipher	Number of keys	Attack time@ 10^{13} decryptions/sec
56	DES	7.2×10^{16}	1 hr.
128	AES	3.4×10^{38}	5.3×10^{17} yrs
168	3DES	3.7×10^{50}	5.8×10^{29} yrs
192	AES	6.3×10^{57}	9.8×10^{36} yrs
256	AES	1.2×10^{77}	1.8×10^{56} yrs

It is always successful if the time for the attack is not limited.

Ciphertext Only

In this attack, the attacker has the ciphertext of several messages and each message is encrypted using the same encryption algorithm.

The goal is to discover the key used in the encryption process.

It is the hardest attack to succeed at because the attacker has very little information about the encryption process.

Known-Plaintext

It is a cryptanalysis method where the attacker:

- Owns the plaintext and corresponding ciphertext of one or more messages
- Analyzes the relationship between the plaintext and the ciphertext
- Aims to discover the key used to encrypt the messages

Frequency Analysis

It is the study of the frequency of letters or groups of letters in a ciphertext.

- It is based on the fact that, in any given written language, certain letters and combinations of letters occur with varying frequencies.
- It is used as an aid to breaking classical ciphers such as the Ceaser cipher.

Chosen-Plaintext

It is a cryptanalysis technique where the attacker:

- Knows the algorithm used for encryption
- Runs samples of plaintext to obtain the corresponding ciphertexts
- Compares ciphertexts to possibly discover the encryption key

In an adaptive chosen-plaintext, the attacker modifies the chosen plaintext based on the resulting ciphertext.

Chosen-Ciphertext

In this attack, the attacker:

Accesses the system used for decryption

Chooses the ciphertext to be decrypted and gets access to the resulting decrypted plaintext

Gains access to an unattended decryption system through **lunchtime**, **midnight** attacks

Implementation Attacks

The attacker exploits implementation weaknesses in the software, protocol, or encryption algorithm.

Side-Channel Attacks

The attacker analyzes the following information retrieved from the encryption device:

Power consumption statistics

Radiation emissions

Error information

Time taken for encryption and decryption

Sound

Fault Injection

It is a physical attack on the device to inject a fault in the system deliberately to change its intended behavior.

Electromagnetic interferences

Power supply disturbances

Radiation-based fault injections

The goal is to retrieve the secret key with a very small number of experiments.

Man-in-the-Middle (MITM)

In this attack, the attacker tries to break the ciphertext by analyzing the time taken to execute the encryption and decryption algorithms for various inputs.

- The attacker intercepts and relays messages between two targets.
- It makes the client and the server believe that they are directly communicating with each other.

Pass-the-Hash

In this attack, the attacker captures a password hash and uses it to gain access as an authorized user.

- The attacker doesn’t need to decrypt the hash to obtain a plaintext password.
- This technique can be performed against any system which accepts NTLM authentication.

Ransomware

It is a form of malware that encrypts a victim's data and important files.

The attacker then demands a ransom from the victim for the decryption key to restore access to the data.

If the victim doesn’t pay on time, the data is gone forever.

Quick Check

You receive a call from a colleague who is unable to access important project files on their computer. When they try to open the files, a message appears demanding payment in exchange for a decryption key to restore access. What type of malware is this?

A. Rootkit

B. Spyware

C. Ransomware

D. Trojan Horse

Applying Security Principles to Site and Facility Design

Site and Facility Design Criteria

They establish key principles for secure environments by prioritizing physical security.

Physical security is an essential part of a security plan and forms the basis of all other security measures, including personnel and information.

The most important goal in planning a site is the protection of life, property, and operations.

A security professional must review all aspects of construction as part of the standard operational procedure.

Site and Facility Design Criteria

Layered approach is a strategy that includes examining physical security measures starting at the site perimeter and working down to the desktop computer.

Securing Information Environment

In case of an emergency, a security professional must consider:

Protecting life, property, and operations

Minimizing risk of theft, destruction, and unauthorized access

The areas of consideration are crime prevention through environmental design (CPTED), site location, construction, and support facilities.

Crime Prevention Through Environmental Design (CPTED)

It is a crime reduction technique used in areas such as streets, parks, museums, government buildings, houses, and commercial complexes.

The three environmental strategies of CPTED are:

Territoriality: Makes users feel safe and ensures the potential offender is aware of a substantial risk of apprehension

Surveillance: Creates the perception that people can be seen

Access control: Limits the opportunities for crime

Site Location

When selecting a site location for the facility, the following factors must be considered:

- Existing boundary protection
- Location and access
- Stable power supply
- Local crime
- Joint tenants
- Visibility
- Wind and surface traffic
- Natural hazards
- Emergency access

Construction

The areas that require attention during the construction planning stage are:

- Floor slab
- Raised flooring
- Walls
- Ceilings
- Windows
- Doors

Overview of Facility Security Controls

Facility Security Controls

These are measures to secure a facility's physical infrastructure, safeguard assets, and ensure the safety of personnel.

They include access management, surveillance, environmental protection, and emergency responses to mitigate risks and ensure safety and continuity.

Support Facilities

They play a crucial role in physical security by providing essential services and infrastructure. Follow these best practices when using support facilities:

HVAC	As an IT manager, be aware of who is responsible for HVAC (heating, ventilation, and air conditioning).
Water	Turn off power to the equipment, drain water, place all affected equipment or media in an air-conditioned area, and wipe with water displacement spray.
Electricity	Install user surge protectors, uninterruptible power supply (UPS), backup sources for critical systems, and anti-static carpets.
Earthquakes	Keep computers away from glass windows and high surfaces, use shock absorbers and anchors, and ensure objects do not fall on computers.
Lightning	Switch off the systems, unplug them, and store the backup tapes away from the building's steel support.

Data Center (DC) Security: Guidelines

DCs, server rooms, and wiring closets should be at the core of the facility.

Wiring closets in a multistory building should be placed directly above or below each other to help with the easier connectivity of wires across the building.

Access to DC should be via only one door. If there are additional doors, they should function as one-way exit doors.

DC should not be in the basement or upper floors of a building.

The data processing center should be constructed as one room rather than different individual rooms.

DC should have a positive air pressure, and any contaminants should be prevented. Place water detectors under raised floors and on dropped ceilings.

The HVAC system should be implemented for temperature and humidity control.

Personnel Access Control

It is important to prevent the following unauthorized entries to the facilities:

Piggybacking

When a person follows through a door with the permission of the person who has received access

Tailgating

When a person, whether an employee or not, passes through a secure door without the knowledge of the person who has gained legitimate access through the secure door

Mantraps and Turnstiles

Turnstiles

- It is a form of a gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction.
- It is the equivalent of a secured revolving door.

Mantraps

- It is a double set of doors that is often protected by a guard or some other physical layout that prevents piggybacking.
- It can trap individuals at the discretion of security personnel.

Access Controls

Smart card

- It is a security ID with an embedded magnetic strip, bar code, or integrated circuit chip.
- It can process information or store a reasonable amount of data in memory and can be used in multifactor authentication to improve security.
- It is vulnerable to physical security attacks.

Memory card

- It is a machine-readable ID card with memory sticks.
- It can hold a small amount of data in memory but cannot process it.
- It is easy to copy or to duplicate.

Proximity reader

- It is a passive device or transponder that can be used to control physical access.
- It is typically worn by an individual, that alters the magnetic field generated by the reader when detected and processed.

Media Storage Security

They are used to store media.

Passive locking safes can detect if someone attempts to tamper with them, in which case extra internal bolts will fall into place to ensure it cannot be compromised.

Examples

Thermal locking safes can identify temperature changes and implement additional locks.

Media Storage Security: Safe Types

Safe type	Characteristic
Wall safe	Embedded into the wall and easily hidden
Floor safe	Fixed into the floor and easily hidden
Chests	Stand-alone safe
Depositories	Contain slots, allowing valuables to be slipped in
Vaults	Large enough to allow walk-in

Fire Prevention, Detection, and Suppression

Prevention

- Training employees for fire safety
- Supplying the right equipment and ensuring their working conditions
- Storing combustible materials in a proper manner

Detection

Placing fire detectors at strategic points to detect smoke or fire

Suppression

Using a suppression agent to put out a fire

Stages of Fire

The earlier the fire is detected, the easier it is to extinguish.

Stage 1
Incipient stage

Only the air is ionized with no smoke.

Stage 2
Smoke stage

Smoke is visible from the point of ignition.

Stage 3
Flame stage

The flame can be seen with the naked eye.

Stage 4
Heat stage

The fire is considerably higher.

Fire Detection Devices

Smoke-activated

- Senses the presence of smoke particles in the air
- Photoelectric device: It detects a variation in light intensity and produces a beam of light. If the light is obstructed, an alarm is produced.

Fire Detection Devices

Heat-activated

- **Fixed temperate:** An alarm is generated when a particular temperature is reached.
- **Rate-of-raise:** An alarm is generated when the temperature rises over time.
  - These sensors usually provide a quicker warning than fixed-temperature sensors, but they are prone to false positives.

Classes of Fires

The following are the classes of fires:

Class A fires

Class B fires

Class C fires

Class D fires

Class K fires

Classes of Fire

The table given below indicates the types of fires and the corresponding extinguishing methods:

Class	Description (fuel)	Extinguishing method
A	Common combustibles such as paper, wood, and clothing	Water, Foam
B	Burnable fuels such as gasoline or oil	Inert gas, CO2
C	Electrical fires such as computers and electronics	Inert gas, CO2 (Note: As the first step, turn off electricity)
D	Special fires, such as chemical or metal	Dry powder (May require total immersion or other special techniques)
K	Commercial kitchens	Wet chemical

Water-Based Suppression System

It is a method to suppress fire by releasing water through pipes and sprinklers.

Wet pipe	• It is always full of water, usually discharged by temperature control sensors. • It is also called closed-head systems.
Dry pipe	• It contains compressed air instead of water. • It fills the pipes with water and discharges when the water valve is opened.
Preaction	• It is the combination of wet and dry pipes and the water is not held in the pipes until the fire is detected. • It releases water only after the sprinkler head activation triggers are melted by sufficient heat.
Deluge	• It is another form of dry pipe system that uses larger pipes. • It can deliver a significantly larger volume of water.

Gas Suppression

Gas discharge systems remove oxygen from the air and should not be used in environments where people are located.

It is more effective than water suppression systems.

Example

Halon is an effective gas suppression system but is banned because it degrades the environment.

Effective replacements for Halon are:

- FM200
- NAF-S-III
- Argon
- Inergen

Motion Detectors

The following motion detectors help check intrusion:

Infrared

Monitors for significant changes in the infrared lighting pattern of a monitored area

Heat-based

Observes for significant changes in the heat levels of a monitored area

Wave pattern

Transmits low ultrasonic frequency signals and monitors for significant changes in the reflected patterns

Capacitance

Supervises the changes in the electrical or magnetic field surrounding a monitored object

Photoelectric

Watches visible light levels in a monitored area

Passive audio

Listens for abnormal sounds in a monitored area

Alarm Types

Alarms are security mechanisms designed to detect unauthorized access.

Deterrent

- It triggers deterrent actions.
- The goal is to make intrusion attempts more difficult.

Repellent

- It triggers sound or light.
- The goal is to discourage intruders.

Notification

- It triggers notifications to security analysts.
- It is silent from an attacker's perspective but gives warning signals to the security team.

Alarm Categories

Local alarm system

- It must broadcast an audible alarm signal that can be heard within 400 feet.
- The security guards should be stationed nearby.

Central station

- The alarm is silent locally, but offsite monitoring agents are notified.

Auxiliary system

- The notifications are sent to emergency services such as the fire, police, and medical teams.
- It can be added to either a local or a centralized system.

Emanation Security: Electronic Emanation

It refers to the protection against unintended electromagnetic signals or emissions from electronic devices that could be intercepted and exploited by attackers.

Hardware or electronic devices emit electronic signals which, if captured, can reveal useful information.

TEMPEST is used to protect against emanation leaks.

Emanation Security: Electronic Emanation

Controls against electronic emanation are:

Faraday cage

It is a closed enclosure with external metal mesh that fully surrounds the enclosure, absorbing EM signals.

White noise

It broadcasts false traffic to mask and hide the presence of real emanations.

Control zone

- It implements zones so that the emanations are controlled within the environment.
- It uses Faraday Cage or white noise in those zones.

Heating, Ventilation, and Air-Conditioning (HVAC)

Low humidity causes static electricity, while high humidity can lead to corrosion, making it essential to maintain temperature and humidity within reasonable limits.

- It employs positive pressure and drainage.
- It maintains humidity at recommended levels of 40% to 55%.

Note:

The recommended set point temperature range for a data center is 68 to 77°F (20–25°C).

Power Supply

Reliable power supply is critical for any data center.
The following are common threats to the power system:

Power excess

- **Surge:** Prolonged high voltage
- **Spike:** Momentary high voltage

Power loss

- **Blackout:** Extended, complete loss of electric power
- **Fault:** Brief power outage

Power degradation

- **Brownout:** Protracted reduction in voltage
- **Sag or dip:** Temporary reduction in voltage

Training and Awareness

Physical security awareness and training are very critical.

- Employees should receive training on how to operate emergency power systems.
- It is essential to provide training on the proper use of fire extinguishers.
- Evacuation routes must be prominently displayed throughout the building.
- Regular fire drills should be conducted to ensure preparedness.

Quick Check

You are facing issues with the leakage of critical electronic information due to emanations. What physical security control broadcasts false emanations to mask true electromagnetic emanations from computing equipment?

A. Faraday cage

B. Copper-infused windows

C. Shielded cabling

D. White noise

Key Takeaways

- An architecture framework provides a structure used for developing a broad range of security designs.
- The various types of evaluation criteria are trusted computer system evaluation criteria, information technology security evaluation criteria, common criteria, and payment card industry data security standards.
- System security architecture is focused on designing security services within individual computing systems.
- The various types of distributed systems are virtualization, hypervisor, and cloud computing.
- Physical security is an essential part of a security plan and forms the basis of all other security measures, including personnel and information.

Thank You