Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 03: Security Architecture and Engineering

Learning Objectives

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

- Implement secure design principles such as fail safe or fail secure, trust but verify, and zero trust
- Compare different security models
- Discuss privacy, cybersecurity, and risk frameworks
- Examine the concepts of security architecture
- Explain cloud computing, Internet of Things, microservices, and edge and fog computing

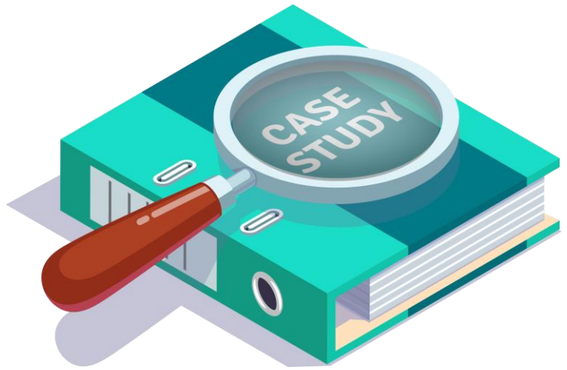
Learning Objectives

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

- Summarize the concepts of Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
- List the various advantages and disadvantages of symmetric and asymmetric cryptography
- Implement key management principles
- Explain different environmental control methods

Introduction to Security Engineering

Security Architecture and Design: Case Study



Kevin Butler, Security Administrator in the Network Firewalls division at Nutri Worldwide Inc. read the internal case study on security architecture and design.

In the previous financial year, Nutri Worldwide Inc. expected a large increase in IT infrastructure requirements. The management felt the need to implement best practices for IT service management. Hilda Jacob, the General Manager of IT security, was assigned the task of selecting the best framework to help the organization identify, plan, deliver, and support IT services. Hilda decided to select the ITIL framework.

Security Engineering

Security engineering helps in:

- Building information systems and the related architectures
- Delivering the required functionality to address the threats of information systems
- Incorporating security controls, capabilities, and behaviors into enterprise architecture and information systems to address the security principles of confidentiality, integrity, and availability

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Secure Design Principles

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

Threat Modeling

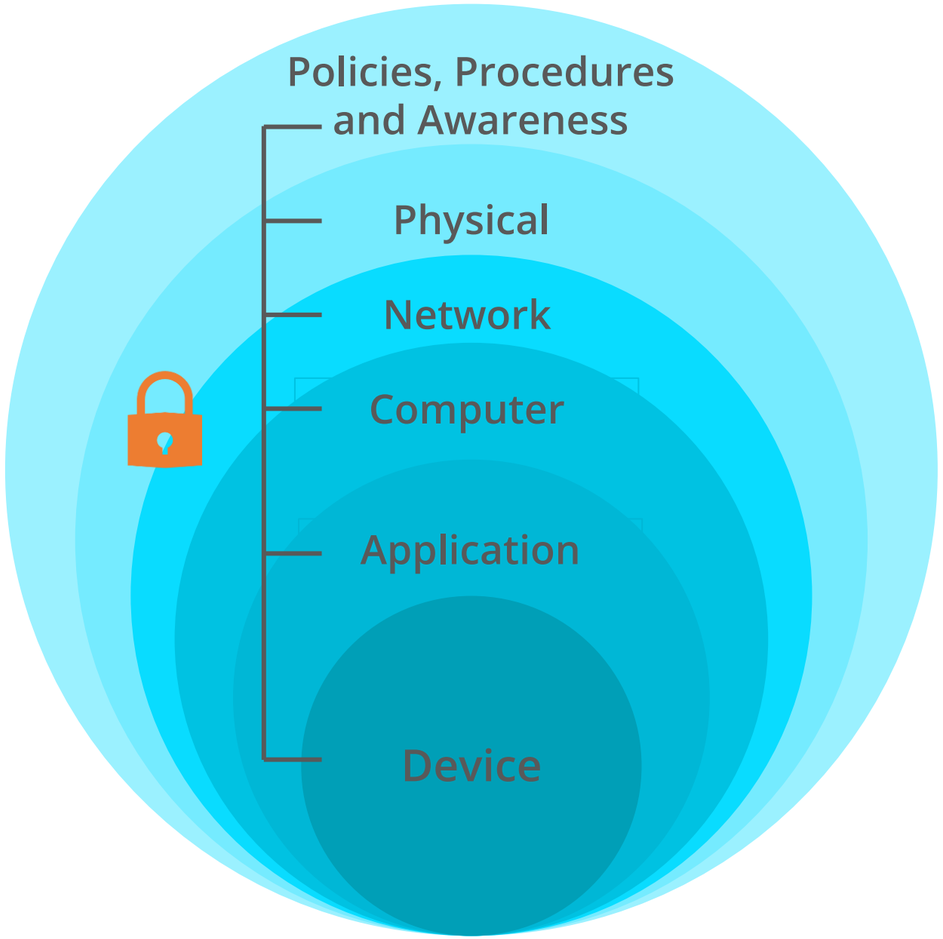
Threat modeling is a process by which:

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

Secure Design Principles

Defense in Depth

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



Secure Design Principles

Secure Defaults	The default behavior of the system is to be secure. If you use 10% of the features 90% of the time, the other features can be disabled.
Separation of Duties (SoD):	• Separation of duties (also known as **segregation of duties**) is the concept of having more than one person to complete a critical or sensitive task. • The goal of separation of duties is to prevent fraud and error.
Keep It Simple	Keep it simple is a design principle that states that most processes or systems work best if they are kept simple rather than made overly complicated.

Fail Secure and Fail Safe

Failure is unavoidable and should be planned for. There are two possible failure modes: fail secure and fail safe.

Fail Secure (Closed)

- Fail secure is a design feature that in the event of a failure, it should fail to a state that prevents further operations.
- For example, a firewall must be configured to fail securely. In the event of an operational failure of the firewall, all traffic is subsequently denied.

Fail Safe (Open)

- Fail safe is a design feature that in the event of a specific type of failure, it should cause minimal or no harm to other equipment, the environment, or people.
- For example, if a building catches fire, fail-safe systems would unlock doors to ensure quick escape and allow firefighters inside, while fail secure would lock doors to prevent unauthorized access to the building.

Trust but Verify

Trust but Verify (TbV) promotes the idea that system components should not blindly trust each other.

For example, even if the data source is reliable, always verify the data for accuracy and integrity.

Organizations must regularly perform risk management and regulatory compliance investigations.

Verification audits can be conducted to mitigate the negative consequences of high-risk processes or product use.

Zero Trust

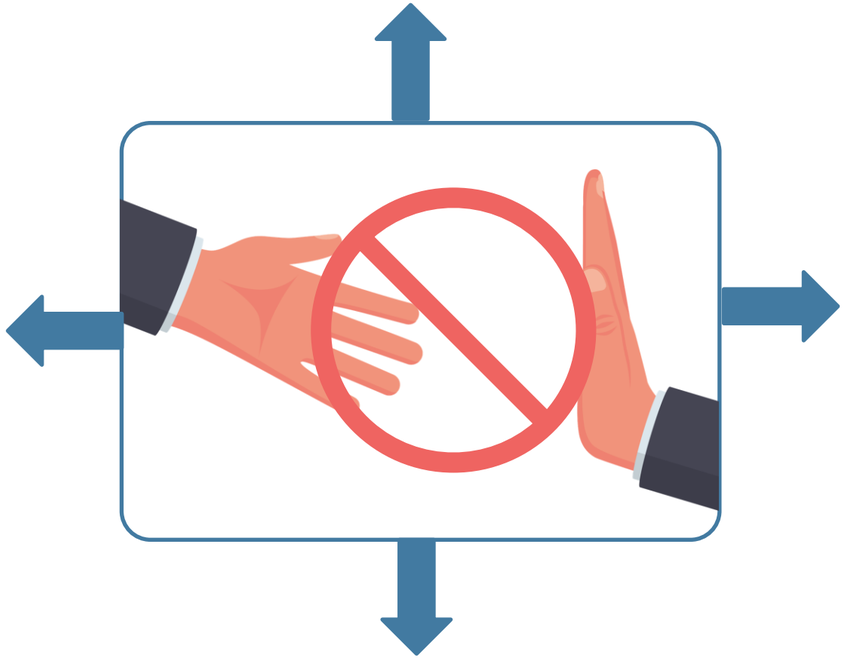
Zero trust is a security model based on the principle of
trust nothing and verify everything.

It is a holistic approach to network security wherein every person and device trying to access resources on a private network must require strict identity verification, regardless of whether they are inside or outside the network perimeter.

Zero Trust

While it is difficult to obtain access from outside the network, everything inside the organization's network is trusted by default.

The traditional IT network security model is based on the castle-and-moat concept.



Every access request is fully authenticated, authorized, and encrypted before granting access.

Under this broken trust model, if an attacker gains access to the network, they can easily move across security layers and systems.

Privacy by Design

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

Seven principles of Privacy By Design:

1. **Proactive not reactive or preventative not remedial**: Anticipate, identify, and prevent privacy-invasive events before they happen.
2. **Privacy as default**: Personal data is automatically protected in any given IT system or business practice.
3. **Privacy embedded into design**: Privacy is a fully integrated component of the system and not bolted on as an add-on.
4. **Full functionality**: Positive-sum, not zero-sum: employ a win-win approach to all legitimate interests and objectives, without making any unnecessary trade-offs.

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

Privacy by Design

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

Seven principles of Privacy By Design:

5. **End-to-end security:** Lifecycle protection: extend securely across the entire lifecycle of the data from collection to retention to destruction at the end of the process.
6. **Visibility and transparency:** Assure stakeholders that business practices and technologies are operating according to stated promises and objectives and subject to independent verification.
7. **Respect for user privacy**: Keep things user-centric. Prioritize an individual's privacy interests by offering such measures as strong privacy defaults, appropriate notice, and user-friendly options.

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

Shared Responsibility

- A shared responsibility model is a cloud security framework that describes the security responsibilities of the cloud provider and the cloud customer.
- The cloud provider is responsible for the security of the underlying infrastructure that they lease to their customers, while customers are responsible for the security of the areas of the cloud infrastructure over which they have control.
- Typically, the contract (SLA) between the cloud customer and the cloud provider is used to clarify their individual and shared responsibilities.
- Cloud customer is ultimately responsible for compliance and data security.

Understand the Fundamental Concepts of Security Models

Security Models

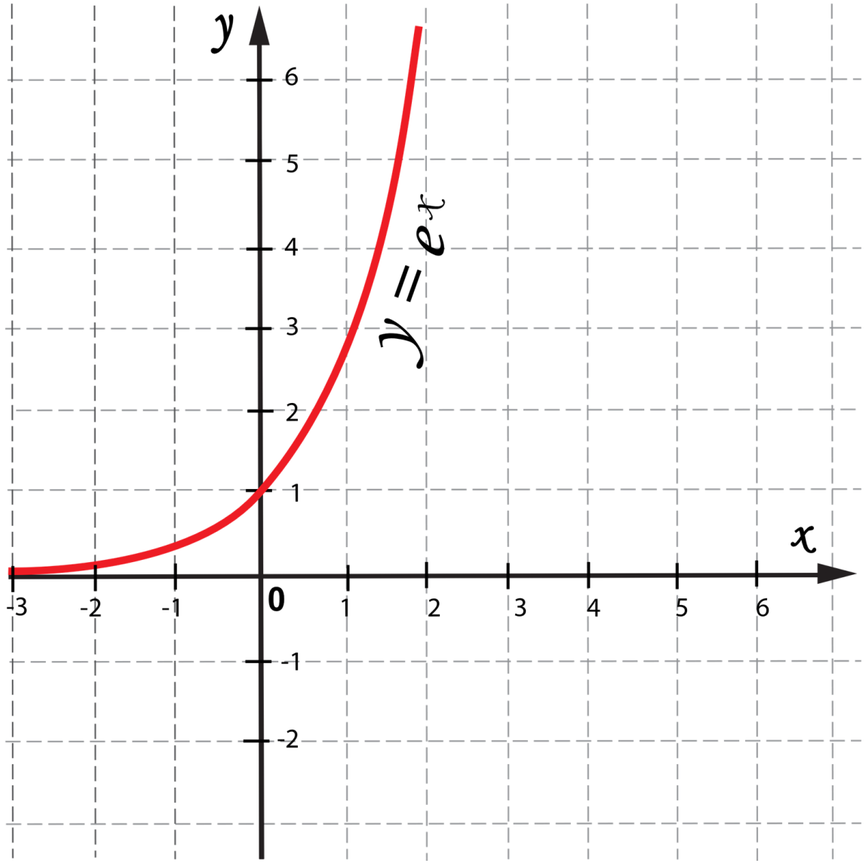
A model is a symbolic representation of a policy.

It maps the desires of the policymakers to a set of rules that a computer system must follow.

It maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy.

Security Models

- It is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code.
- For example, if a security policy states that the subjects need to be authorized to access objects, the security model would provide the mathematical relationships and formulas explaining how x can access y only through the outlined specific methods.



Security Models

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

Some examples:

State Machine Model

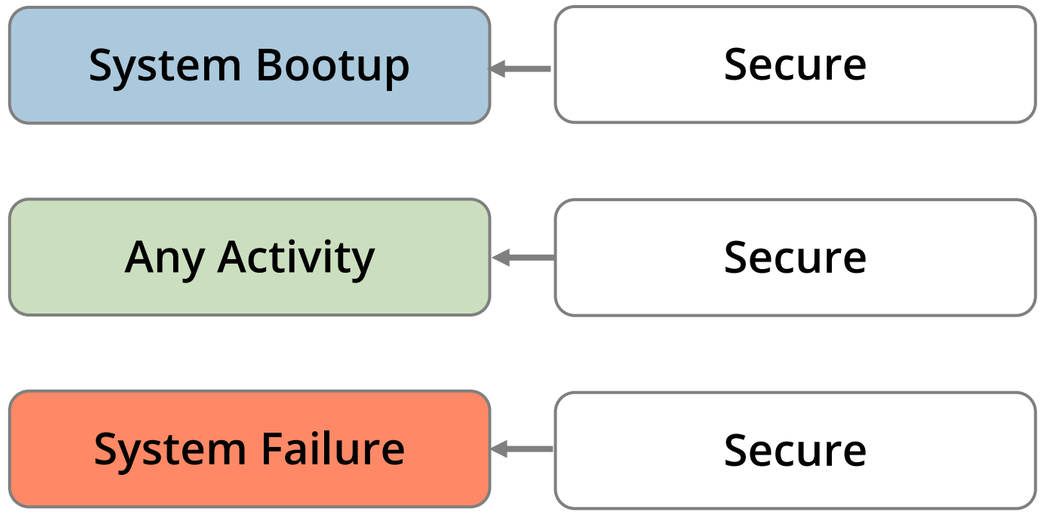
This is used to describe the behavior of a system to different inputs.

- It is based on the state of a system.
  - State is the snapshot of the system at one moment in time.
  - Current permissions and current instances of subjects accessing objects must be captured.
- This model must identify all the initial states of the system and outline how these values will be changed by various inputs so that it is always safe in the 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.

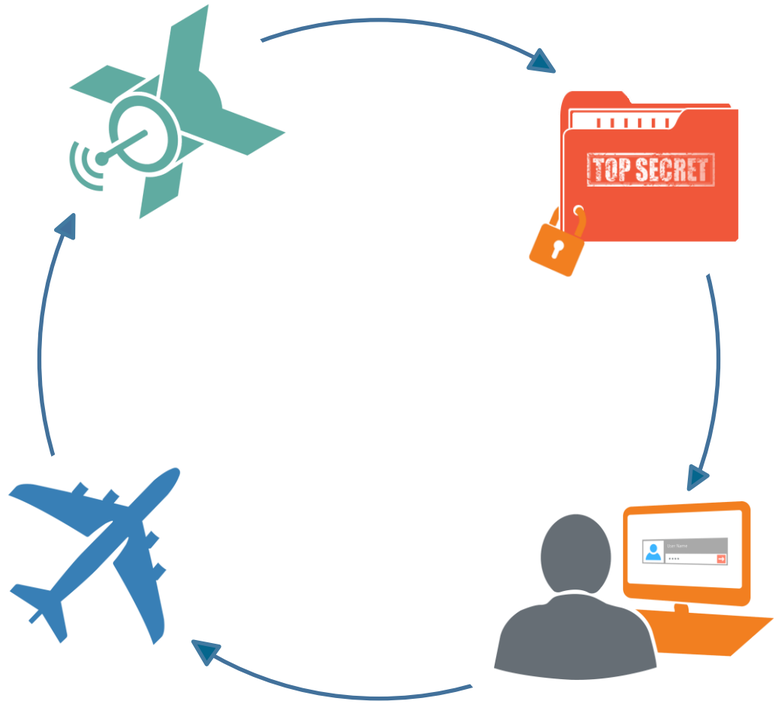


State Machine Model Characteristics

Multilevel Lattice Models

- Multilevel security models describe strict layers of subjects and objects.
- They are often described using 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 documents at confidential and secret levels, however, not at a top-secret level.



Access Control Matrix

An access control matrix 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

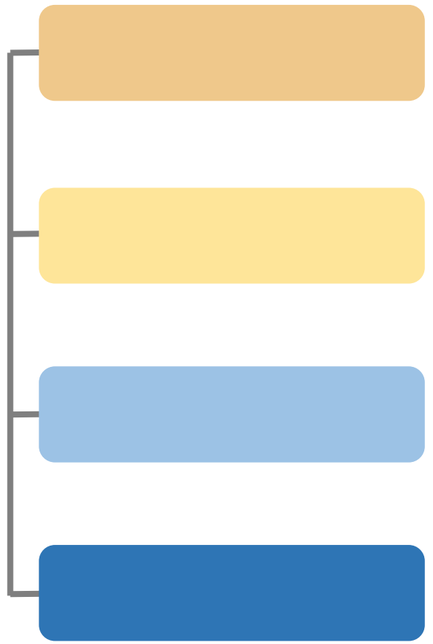
Table 8.1 An access control matrix

Noninterference Model

- The goal of a **noninterference** model is to ensure that high-level actions do not determine what low-level users can see.
- The term non-interference means that activities performed by a user with high clearance will not interfere with any activities performed by a user with low clearance.
- It addresses two attacks:
  - Covert channel attacks
  - Inference attack

Non – Interference Model

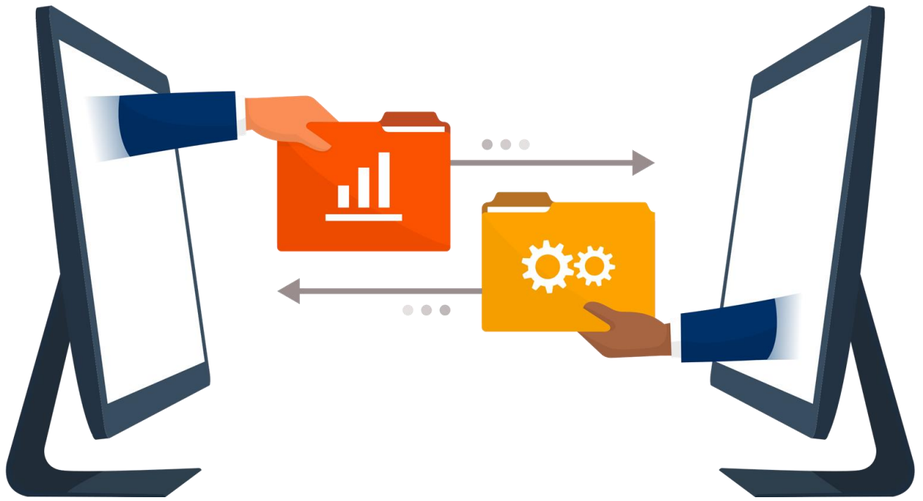
Ensures that actions at one security level has no effect on objects on another security level



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

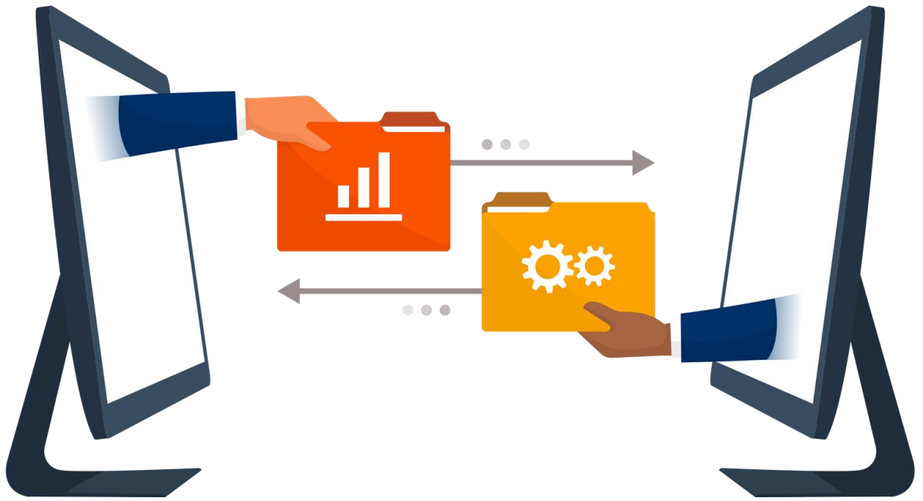
Information Flow Model

- The information flow model focuses on the flow of information rather than on access control.
- The model is based on a state machine.
- It doesn't necessarily deal with only the direction of the information flow.
- It can also address the type of flow.

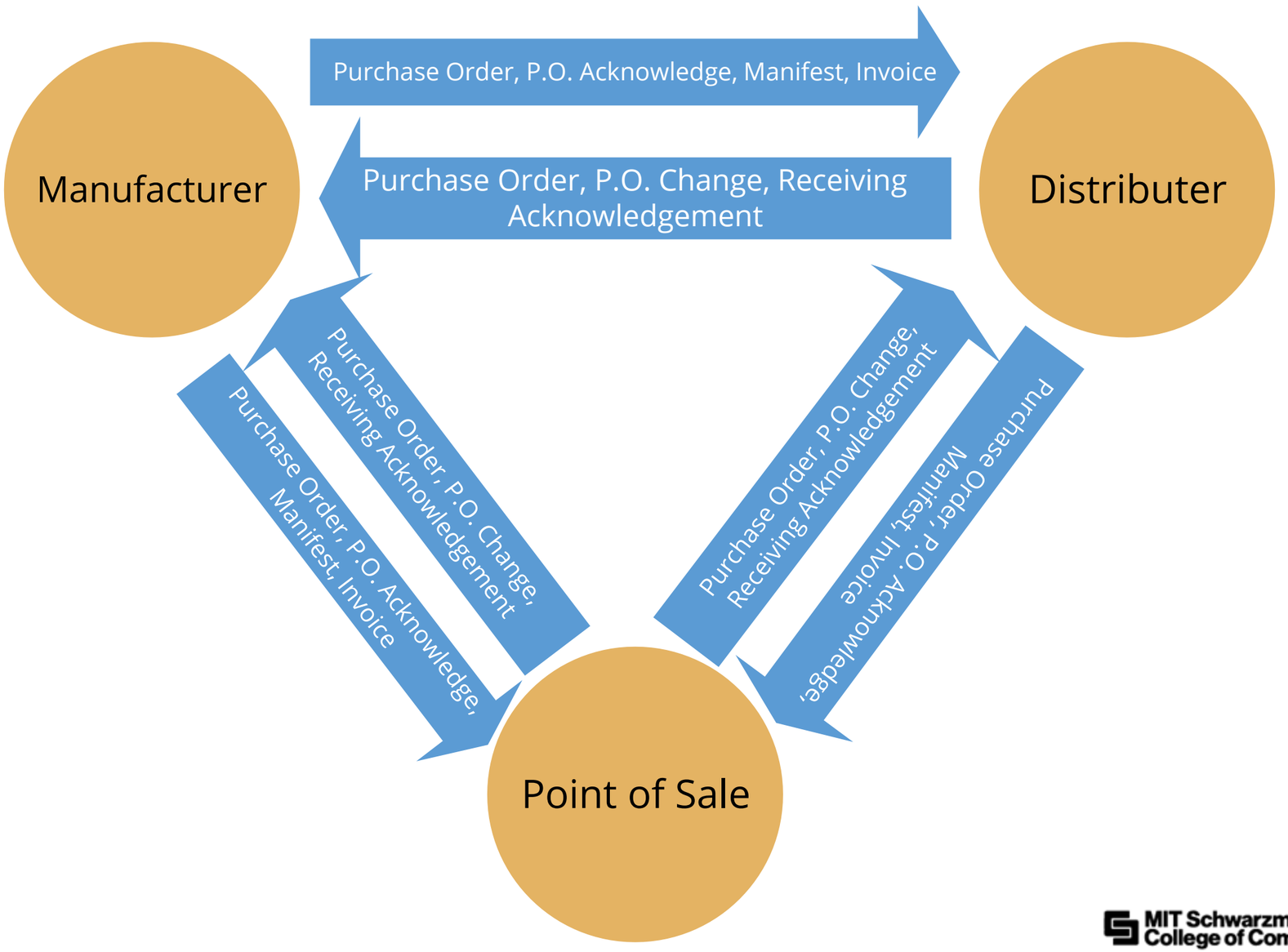


Information Flow Model

- The models are designed to prevent unauthorized, insecure, or restricted information flow, often between different levels of security.
- These are often referred to as a multilevel models.
- Information flow can be between subjects and objects at the same classification level as well as between subjects and objects at different classification levels.



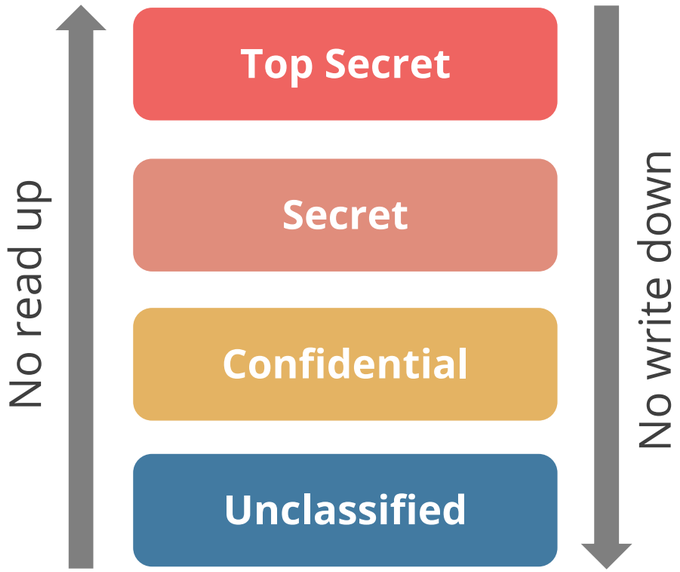
Information Flow Model



Examples of Security Models: Bell–LaPadula Confidentiality Model

Bell–LaPadula

- It focuses on maintaining the confidentiality of objects.
- It is the first mathematical model of a multilevel security policy that defines a secure state of the system.
- It's a framework for computer systems that store and process sensitive information.
- Matrix and security levels are used to determine if a subject can access an object.
- It uses subjects, objects, access operations, and security labels.



Examples of Security Models: 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.

Examples of Security Models: BIBA Integrity Model

The BIBA Integrity Model 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:

The Simple Integrity Axiom

- It states that a subject cannot read data at a lower integrity level
- It means that a subject cannot read documents below its level. This is called a no read down, or NRD.

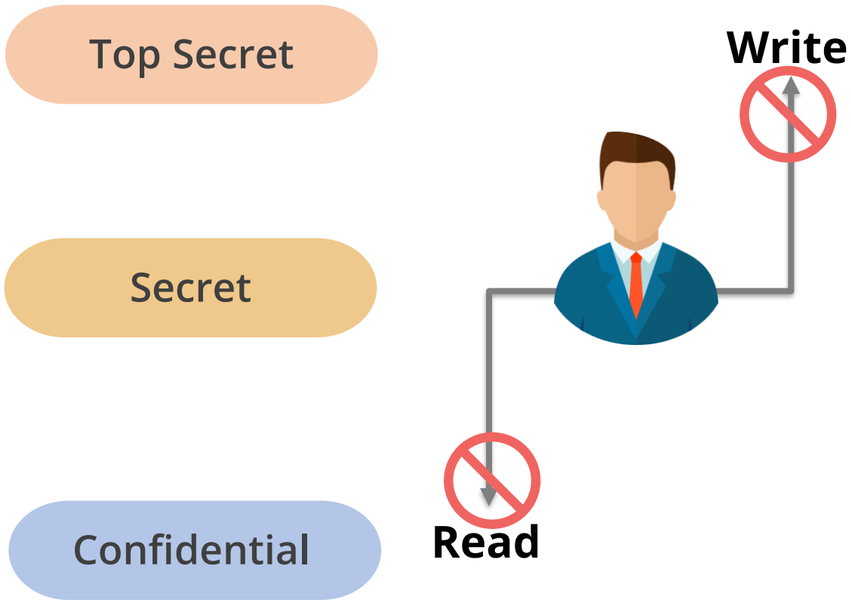
The Star Integrity Axiom

- It states that a subject cannot modify an object in a higher integrity level.
- This is called no write-up, or NWU.

Examples of Security Models: BIBA Integrity Model

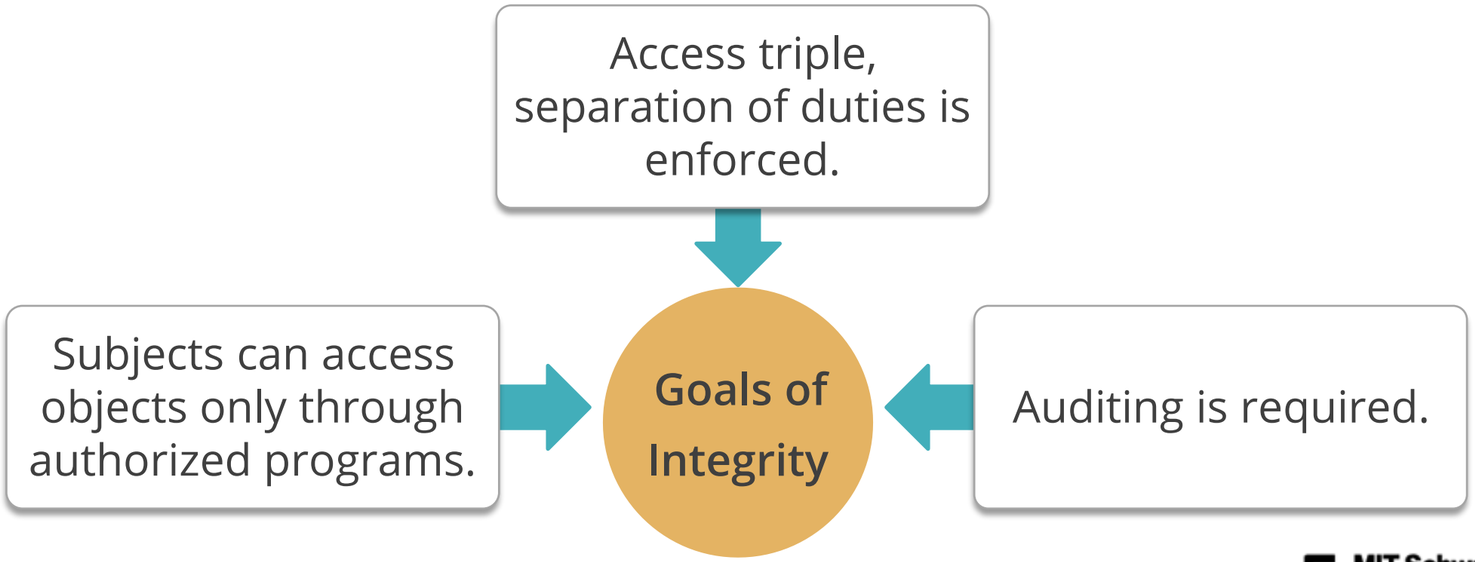
Drawbacks:

- It addresses only integrity, not confidentiality or availability.
- It focuses on protecting objects from external threats; it assumes that internal threats are handled programmatically.
- It does not prevent covert channels.



Examples of Security Models: Clark–Wilson Integrity Model

- It is an integrity model developed after the BIBA model.
- It is used commercially.
- It addresses all the goals of the integrity model:
  - Prevents unauthorized users from making modifications (BIBA model)
  - Prevents authorized users from making improper modifications
  - Maintains internal and external consistency



Examples of Security Models: Clark–Wilson Integrity Model

It focuses on well-formed transactions and separation of duties.

Well-formed Transaction

A series of operations that transform a data item from one consistent state to another is a well-formed transaction.

Access Triple

The model uses a three-part relationship of a subject, program, or object (where a program is interchangeable with a transaction), known as a triple or an access control triple.

Clark–Wilson Integrity Model

Clark-Wilson 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 that is not controlled by the security model. Any input or output that hasn't been validated would be considered an unconstrained data item.

Clark–Wilson Integrity Model

Integrity verification procedure (IVP)

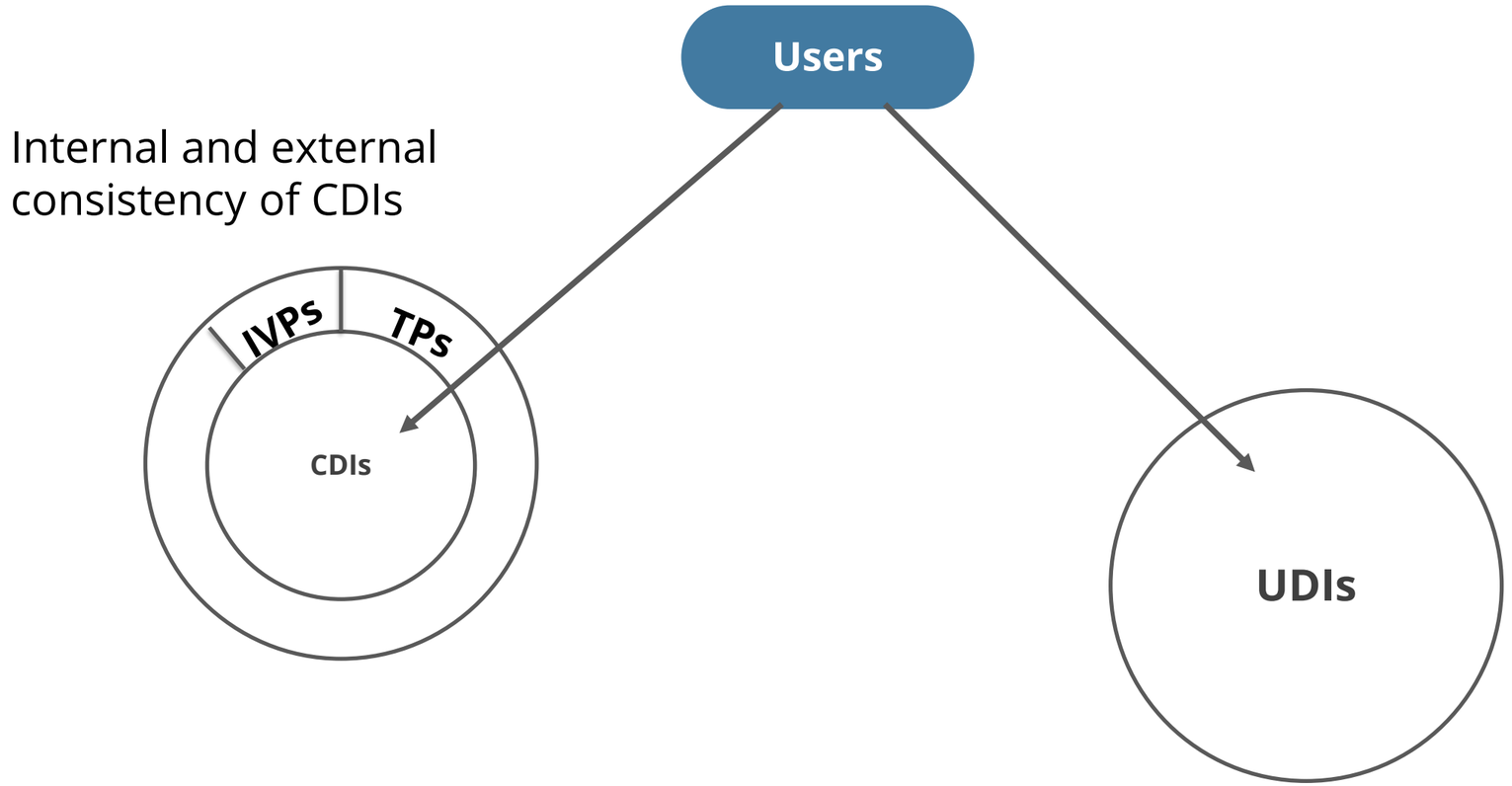
It is a procedure that scans data items and confirms their integrity.

Transformation procedures (TPs)

- They are the only procedures that are allowed to modify a CDI.
- The limited access to CDIs through TPs forms the backbone of the Clark Wilson Integrity model.

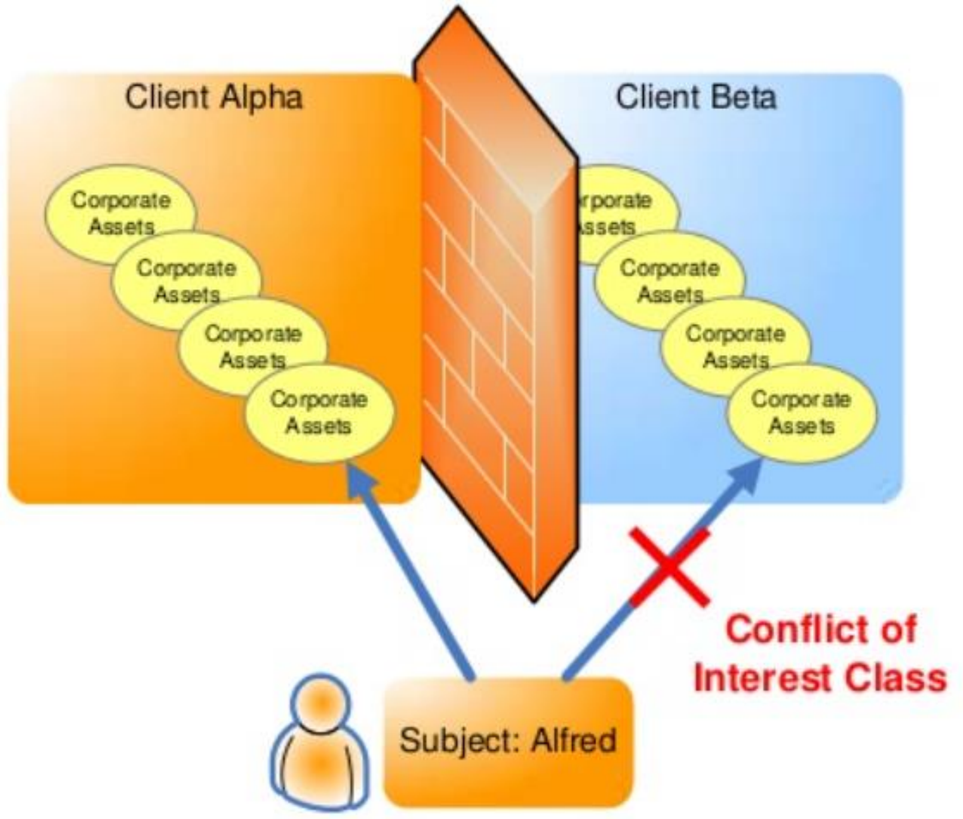
Clark–Wilson Integrity Model

Clark Wilson model is illustrated below:



Brewer and Nash Model

- It is also called the Chinese wall model.
- Information flow model provides access control mechanism that can change dynamically depending on a user's authorization.
- Previous actions are designed to provide 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

- 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.
- The model is based on the Access Control Matrix model.

Graham Denning Model

It has eight protection rights that detail how the functionalities should take place securely:

- 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

Employs a direct graph to dictate how rights can be passed from one subject to another subject or an object

Take Rule

Allows the subject to take rights over an object

Grant Rule

Allows the subject to grant rights to an object

Create Rule

Allows the subject to create new rights

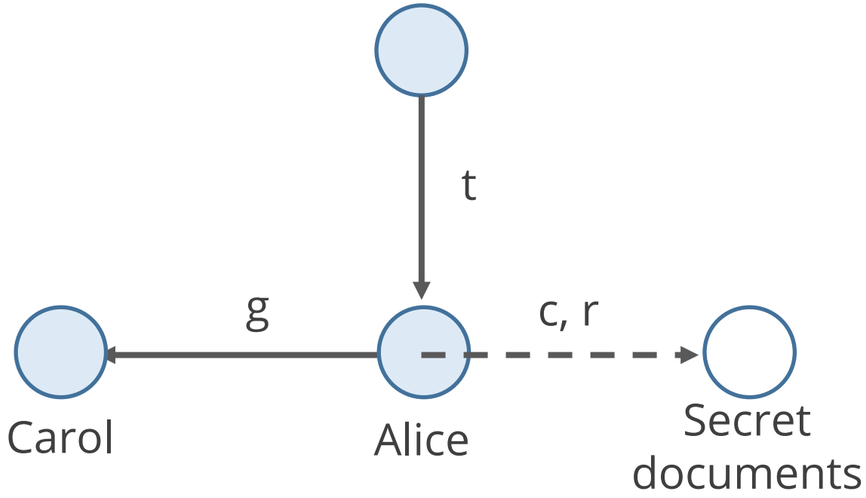
Remove Rule

Allows the subject to remove the rights it has

Take Grant Model

Example for the Take Grant model:

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



Composition Theories

- Systems are usually built by combining smaller systems.
- Security of components must be considered when these components are combined into larger systems.
- This is based on the notion of how inputs and outputs between multiple systems relate to one another
    - It follows how information flows between systems rather than within an individual system.

Composition Theories

Types of composition theories:

Cascading:

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

A B C

Feedback:

One system provides input to another system, which reciprocates by reversing those roles (so that system A first provides input for system B and then system B provides input to system A).

A B

B A

Hookup:

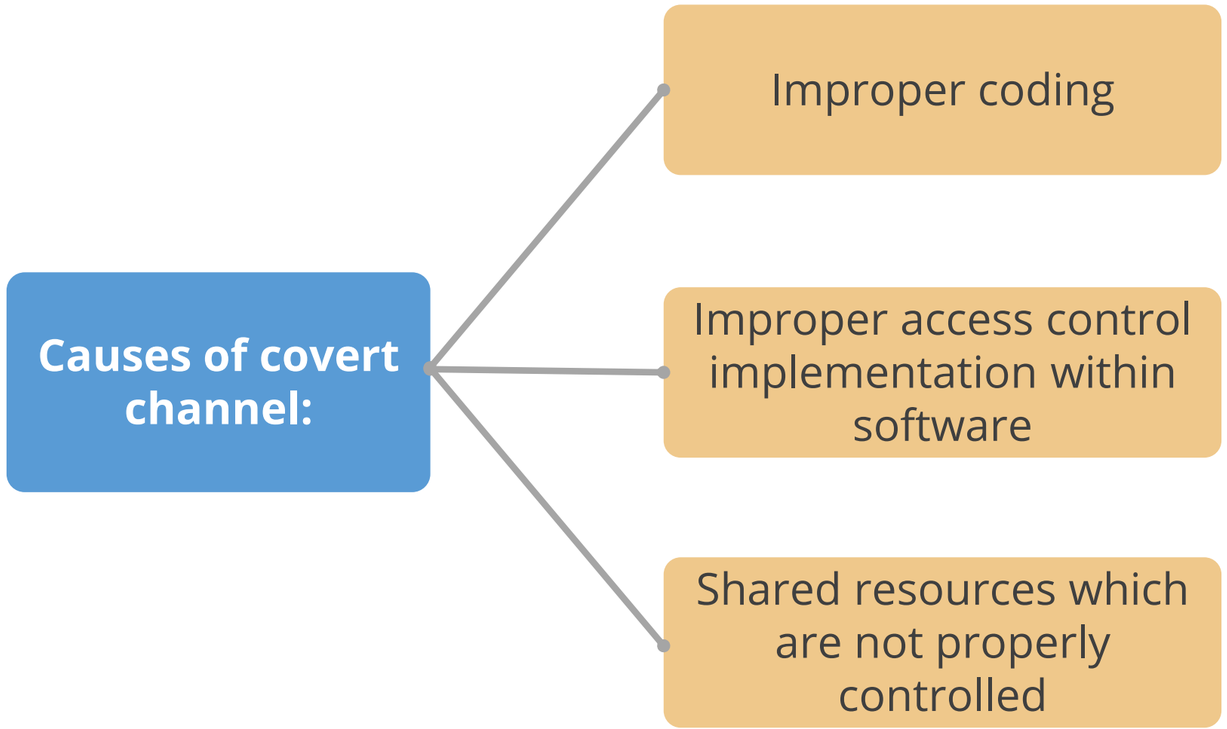
One system sends input to another system but also sends input to external entities.

A B

A C

Covert Channel

Covert channel is a type of attack that creates a capability to transfer information objects between processes that are not allowed to communicate by the computer security policy.



Covert Channel

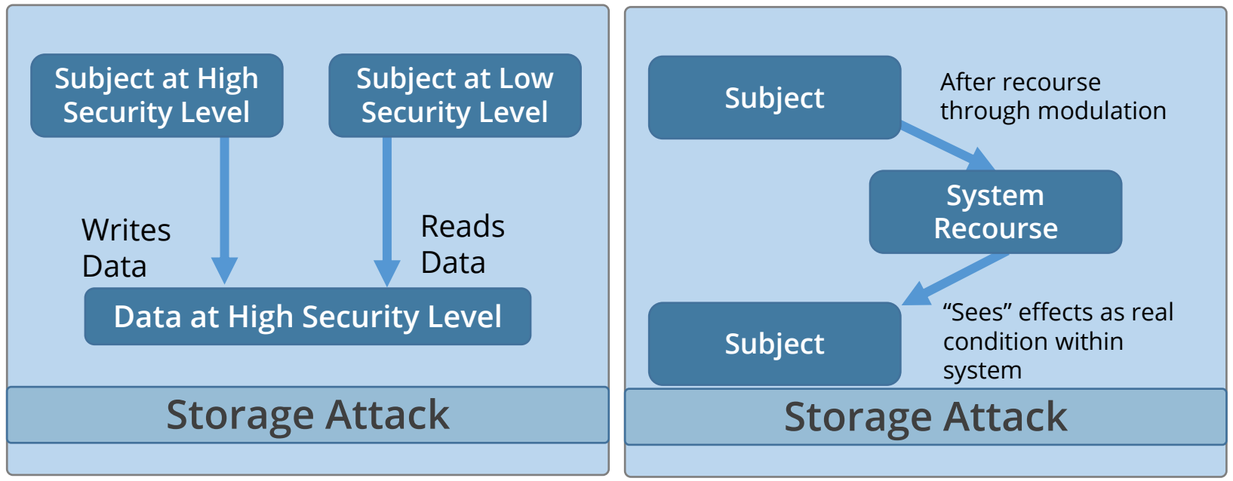
The two types of covert channels are covert storage channel and covert timing channel.

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

An attack where communication is transmitted over a channel that was not intended for communication



Covert Channel

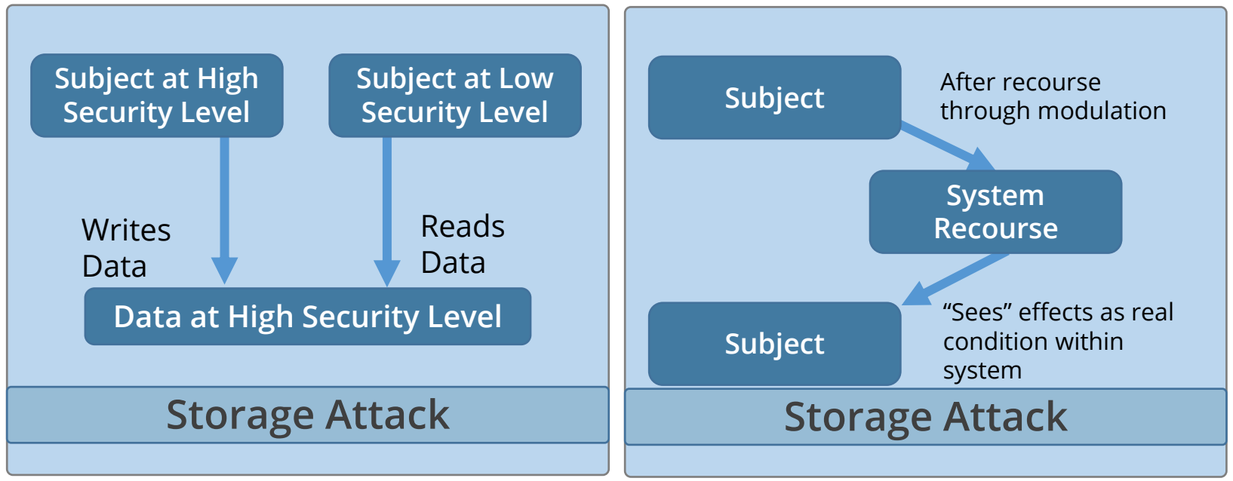
The two types of covert channels are covert storage channel and covert timing channel.

Covert timing channel

- It performs operations that affect the real response time observed by the receiver
- Methods:
  - Knowing when data is transmitted between parties
  - Monitoring the timing of operations

Example: Monitoring cryptographic functions

An attack where communication is transmitted over a channel that was not intended for communication



Open and Closed Systems

Closed System

- This solution is the one where the source code and other internal logic are hidden from the public.
- It is designed to work well with a narrow range of other systems, generally all from the same manufacturer.
- It is harder to integrate with unlike systems, but it can be more secure.
- It is more dependent on the vendor and programmer to revise the product over time.

Open System

- It is the one where the source code and other internal logic are exposed to the public.
- It is designed using agreed-upon industry standards.
- It is easier to integrate an open system with systems from different manufacturers that support the same standards.
- It often depends on public inspection and review to improve the product over time.
- It can provide interoperability.

Business Scenario

Kevin Butler, the security administrator at Nutri Worldwide Inc., wants to set up different accesses to a set of folders on a network.

The access should be such that some of his colleagues will have read and write access, while others are allowed read-only access to the files in the folder. Kevin starts the process of selecting a security model.

Question: Which security model should Kevin Butler implement in the given scenario?

Business Scenario

Kevin Butler, the security administrator at Nutri Worldwide Inc., wants to set up different accesses to a set of folders on a network.

The access should be such that some of his colleagues will have read and write access, while others are allowed read-only access to the files in the folder. Kevin starts the process of selecting a security model.

Question: Which security model should Kevin Butler implement in the given scenario?

Answer: The one-to-one relationship among subjects and objects is the focus of a matrix-based model. Kevin should choose the matrix-based model.

Select Controls Based on System Security Requirements

Privacy Frameworks

The three privacy frameworks:

- OECD Privacy Principles
- The General Data Protection Regulation (GDPR)
- Privacy Management Framework (PMF)

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

Cybersecurity Frameworks

The four cybersecurity frameworks:

- ISO/IEC 270xx
- Risk Management Framework (RMF)
- HITRUST Common Security Framework (CSF)
- Cloud Security Alliance (CSA); Security, Trust, Assurance, and Risk Registry (STAR)

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

Risk Frameworks

The four risk frameworks:

- ISO 31000
- Committee of Sponsoring Organizations (COSO)
- ISACA Risk IT
- NIST Special Publication (SP) 800-37

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

Understand Security Capabilities of Information Systems

Architecture

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

It provides a representation of the concerns of each stakeholder.

Architecture

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

Example: In a house architecture, house plan, electricity plan, or plumbing plan for the kitchen is the highest or first level in the development process.

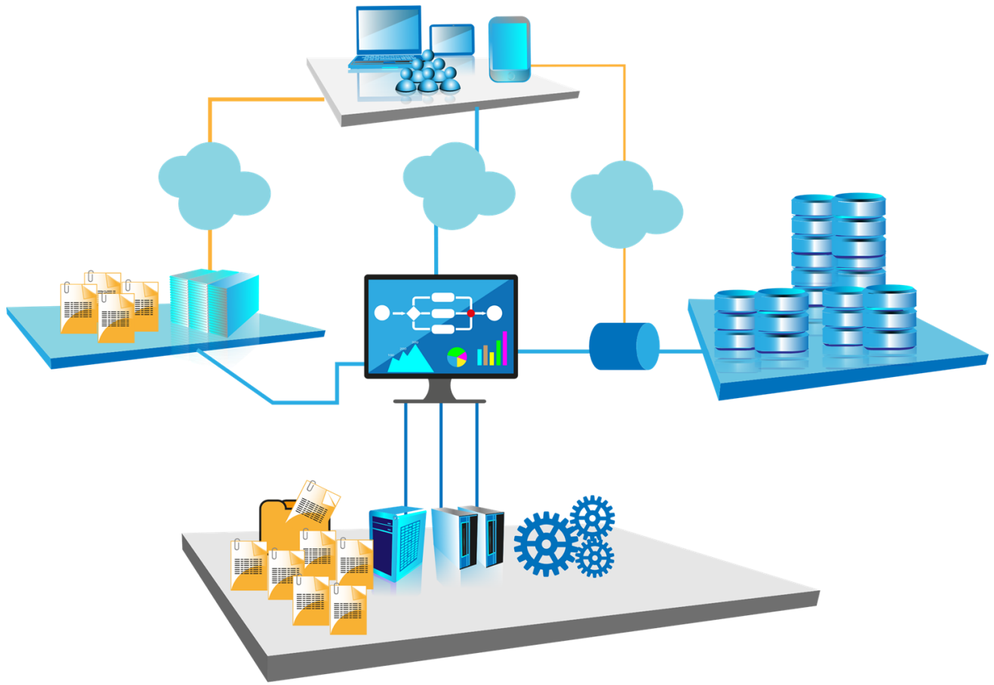
Architecture

- Architecture description is a formal description and representation of the system.
- It describes the relationships, interactions, and dependencies between components.

System Architecture

System architecture describes the major components of a system and how they interact with each other, users, and other systems.

- A disciplined approach to system architecture helps in:
  - Quality
  - Interoperability
  - Portability
  - Security
  - Extensibility
- Security goals have to be defined before the architecture of a system is created (**baked-in** concept).



System Architecture

- Security being addressed late in the development phase is called **baked-on** concept.
- ISO/IEC 42010 is the systems and software engineering architecture description.
- It is important to understand the scope of the target system before you can develop, architect, or evaluate it.

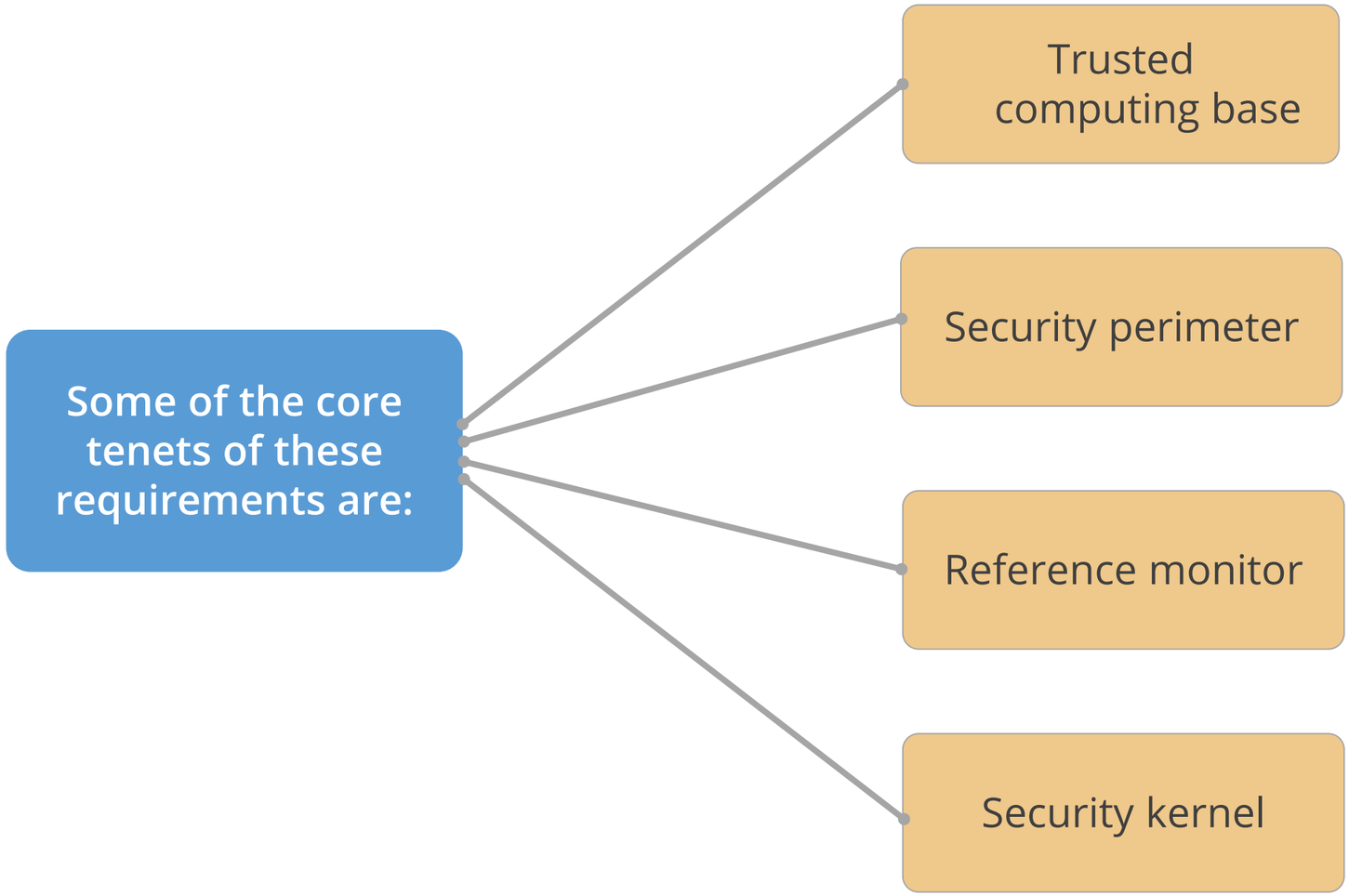
Security Architecture Requirement

- The government and the industry needed to ensure that all the systems that they were purchasing and implementing were protecting its secrets.
- They needed to come up with a way to instruct vendors on how to build computer systems to meet their security needs.
- In order to find a way to test the products, the architecture is developed based on the same security needs.

Security Architecture Requirement

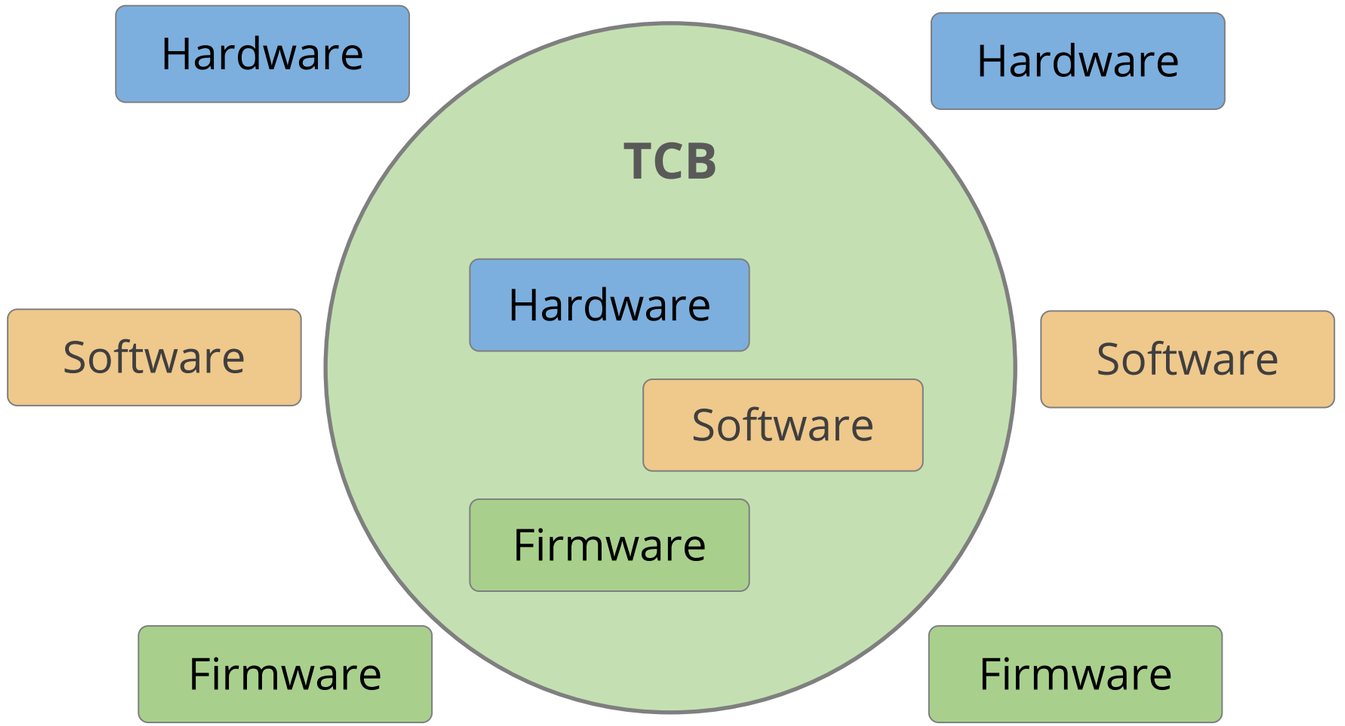
- In 1972, the U.S. government released a report (Computer Security Technology Planning Study) that outlined basic and foundational security requirements of computer systems that it would deem acceptable for purchase and deployment.
- These requirements shaped the security architecture of almost all of the systems in use today.

Security Architecture Requirement



Trusted Computing Base

It is the collection of all the hardware, software, and firmware components within the system that provides security control and enforces the system security policy.



Trusted Computing Base

The TCB does not only address operating system components, but it also addresses hardware, software, and firmware components as they can also affect the system negatively or positively.

Trusted Computing Base

The components that make up the TCB provide extra layers of protection around these mechanisms to help ensure they are not compromised, so the system will always run safely and predictably.

Trusted Computing Base

If TCB is enabled, then the system has:

A trusted path

The communication path between the user or program and the TCB is secure.

A trusted shell

Actions within the interpreter or shell cannot be exposed out and other processes cannot intrude.

System Components: Trusted Platform Module (TPM)

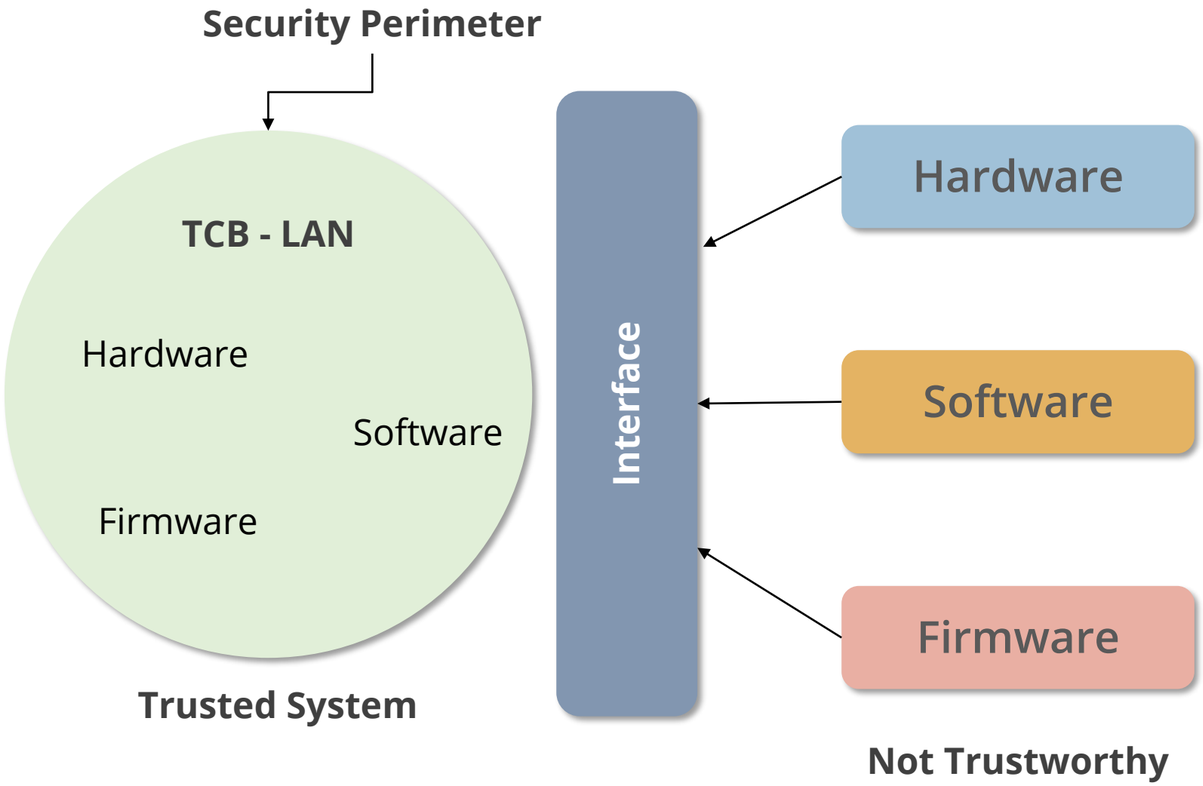
TPM is the implementation of a secure crypto- processor.

- 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 Vista, Windows 7, and Windows 8. Windows Server 2008 uses the disk encryption software named BitLocker.

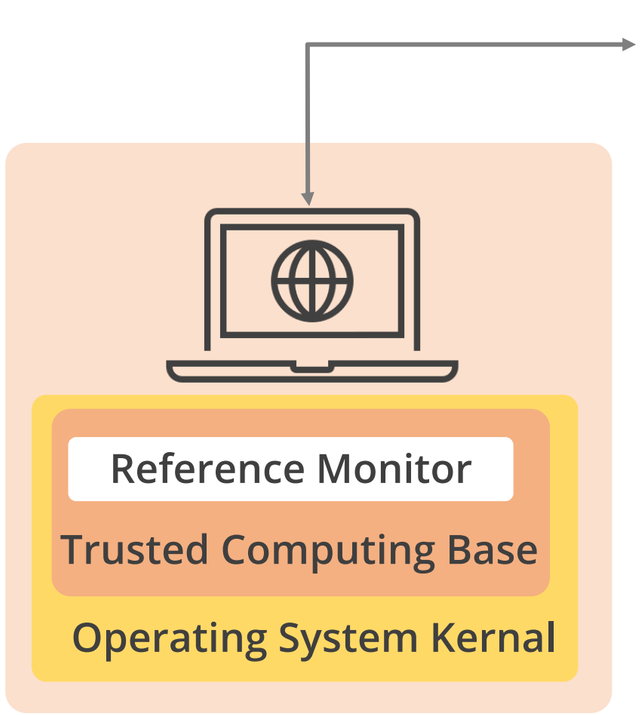
Security Architecture: Security Perimeter

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



Security Architecture: Reference Monitor

- It’s an abstract machine that mediates all access that subjects must object.
- It is an access control concept and is also referred to as **reference monitor concept** or **abstract machine.**
- A fully secure system will require subjects to be fully authorized before access is provisioned to the objects.
- It provides direction on how all access control decisions are made.
- All-access decisions should be made by a core-trusted, tamper-proof component of the OS that works at the system kernel.

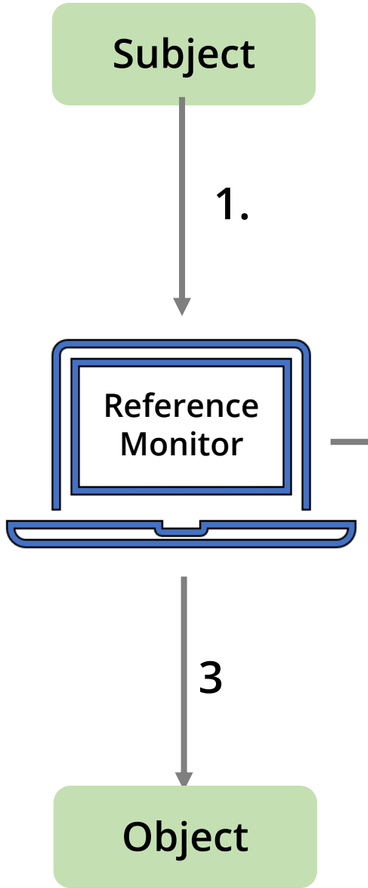


All System calls go through the refence monitor for security checking

Security Architecture: Security Kernel

Security Kernel: Components in system that enforce and implement the rules of the reference monitor

- It is made up of hardware, software, and firmware components within the TCB.
- It implements and enforces the reference monitor concept.
- It is the core of TCB.

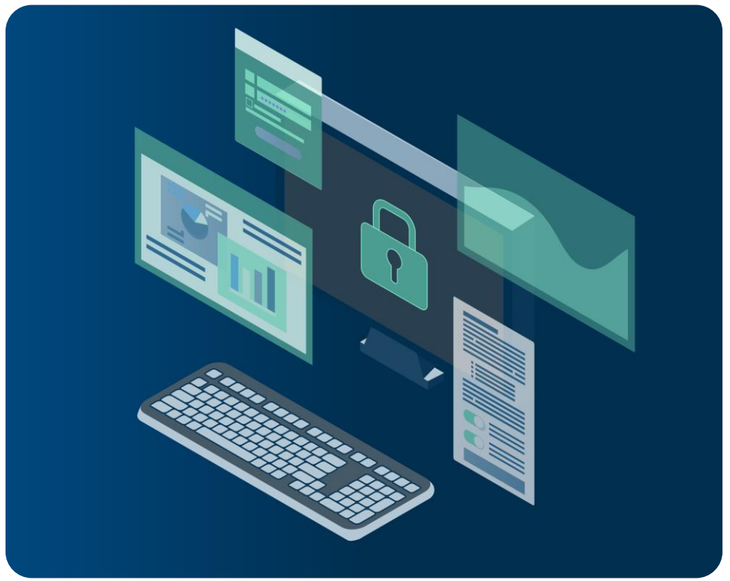


John	Full control
Bob	No Access
David	Read
Marge	Full control
George	Write
Sean	No Access
John	Full control
Bob	No Access

Security Architecture: Security Kernel Requirements

Security kernel has three main requirements:

Must provide isolation for the processes carrying out reference monitor concept



Must be invoked for every access attempt and should be tamperproof

Must be small enough to be tested and verified in a complete and comprehensive manner

Confinement, Bounds, and Isolation

Confinement

- It allows a process to read from and write to only certain memory locations and resources.
- If a process attempts to initiate an action beyond its granted authority, that action will be denied and logged.

Bounds

- Bounds are the limits of memory a process cannot exceed when reading or writing.
- The bounds of a process consist of limits set on the memory addresses and resources it can access.

Isolation

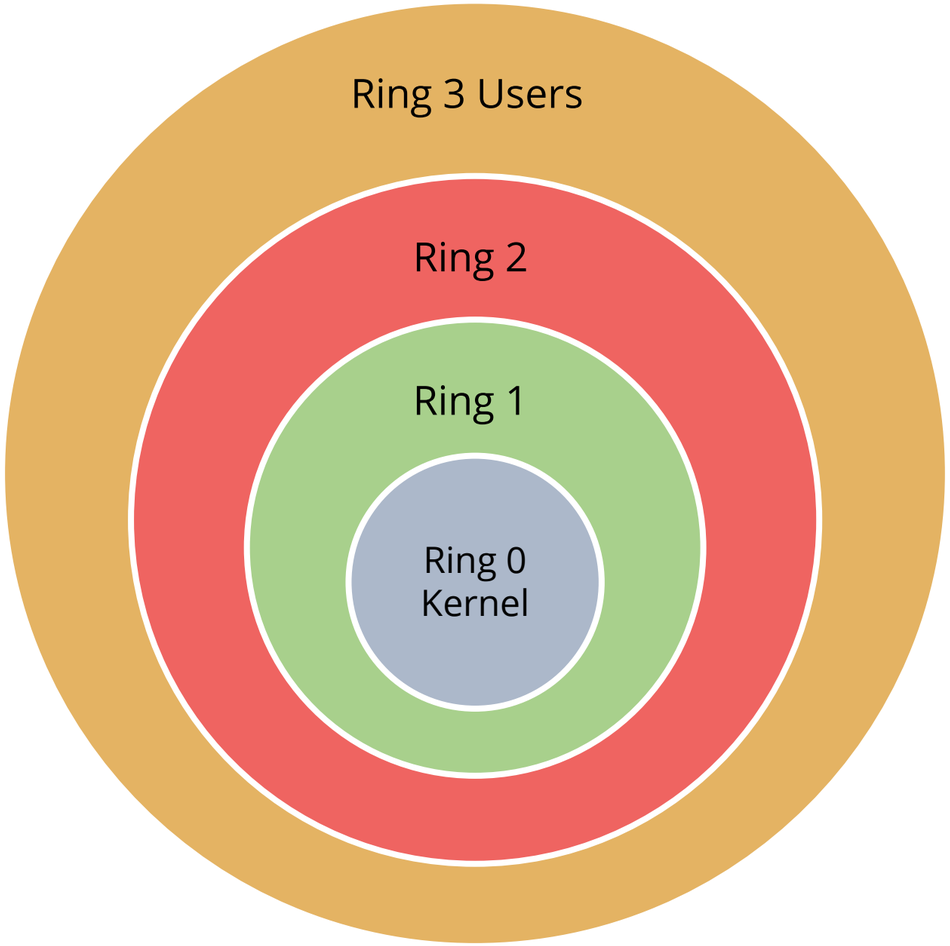
- It is the mode a process runs in when it is confined using memory bounds.
- Process isolation ensures that any behavior will affect only the memory and resources associated with the isolated process.

Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

CPU Architecture: Ring Model

Ring model 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.
- Processes communicate between rings via system calls.

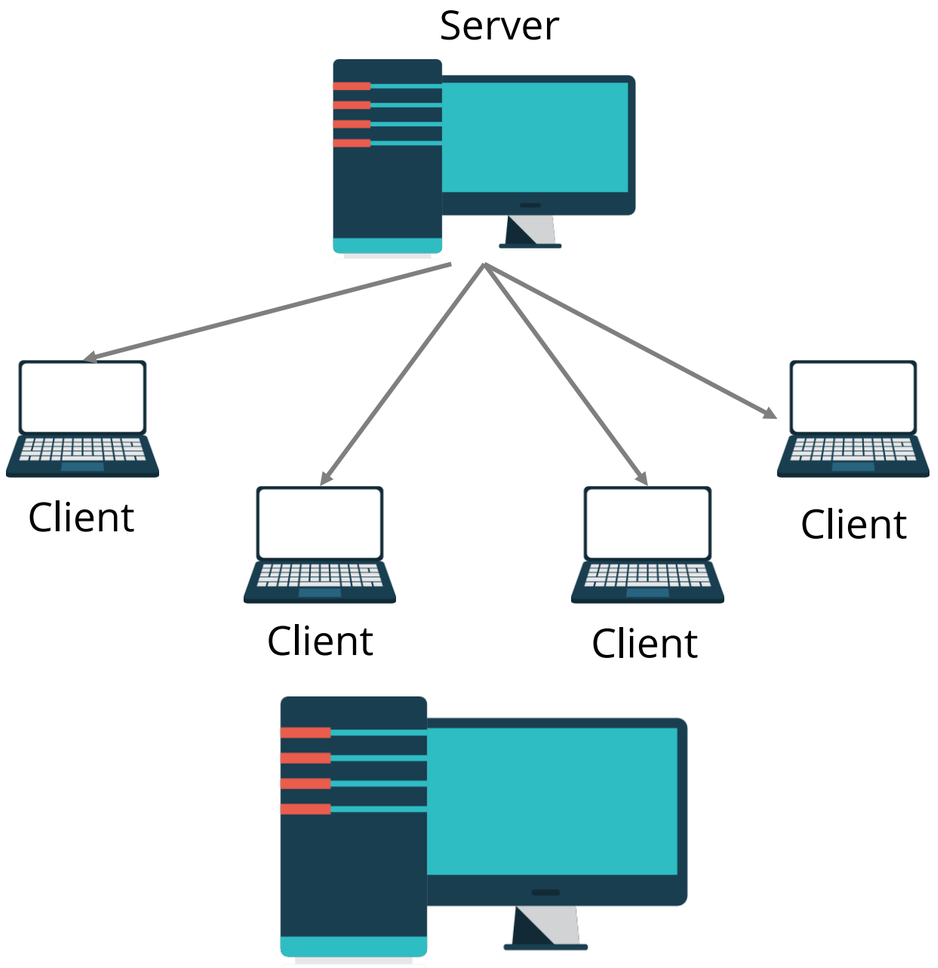


Ring 0 : kernel
Ring 1 : Other OS Components
Ring 2 : Device Drives
Ring 3 : User Applications

Client-Server Systems and Local Environment

Client-server systems enable an application system to be divided across multiple platforms.

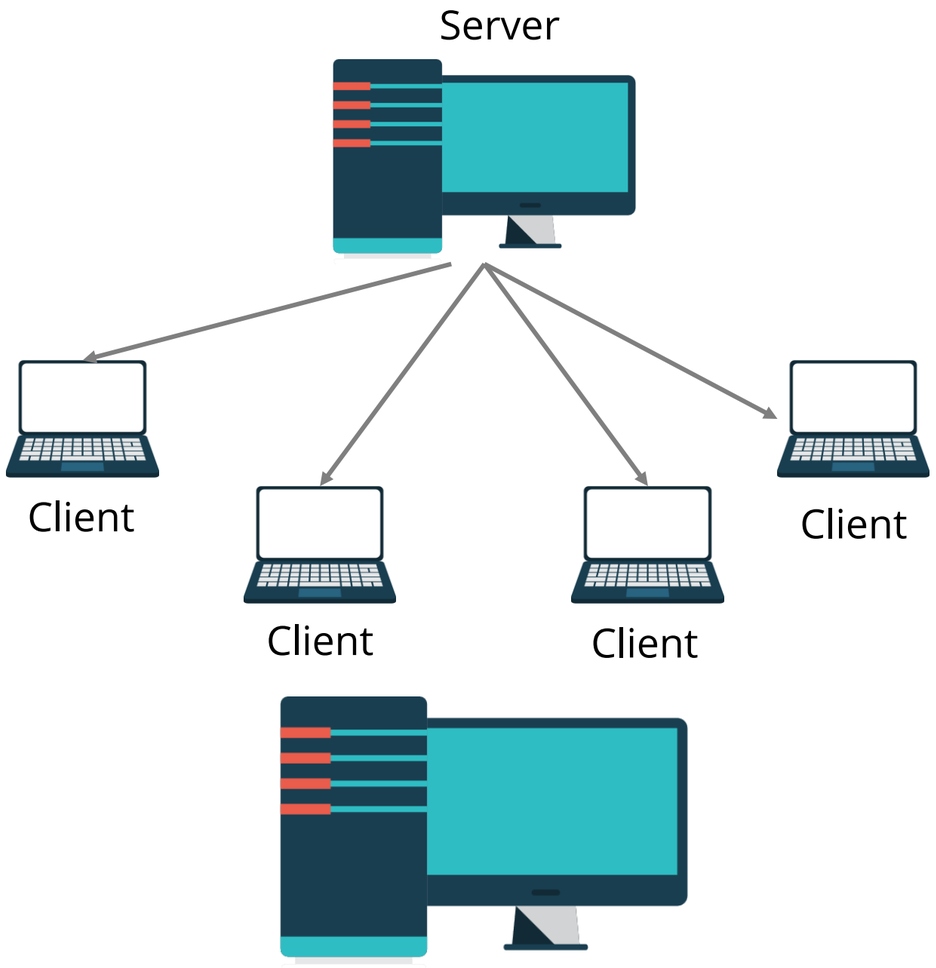
- The client requests services and the server fulfills these requests.
- The client is the front-end portion of an application.
- The server is the back-end portion of an application.



Client-Server Systems and Local Environment

Local environment is a type of environment in which:

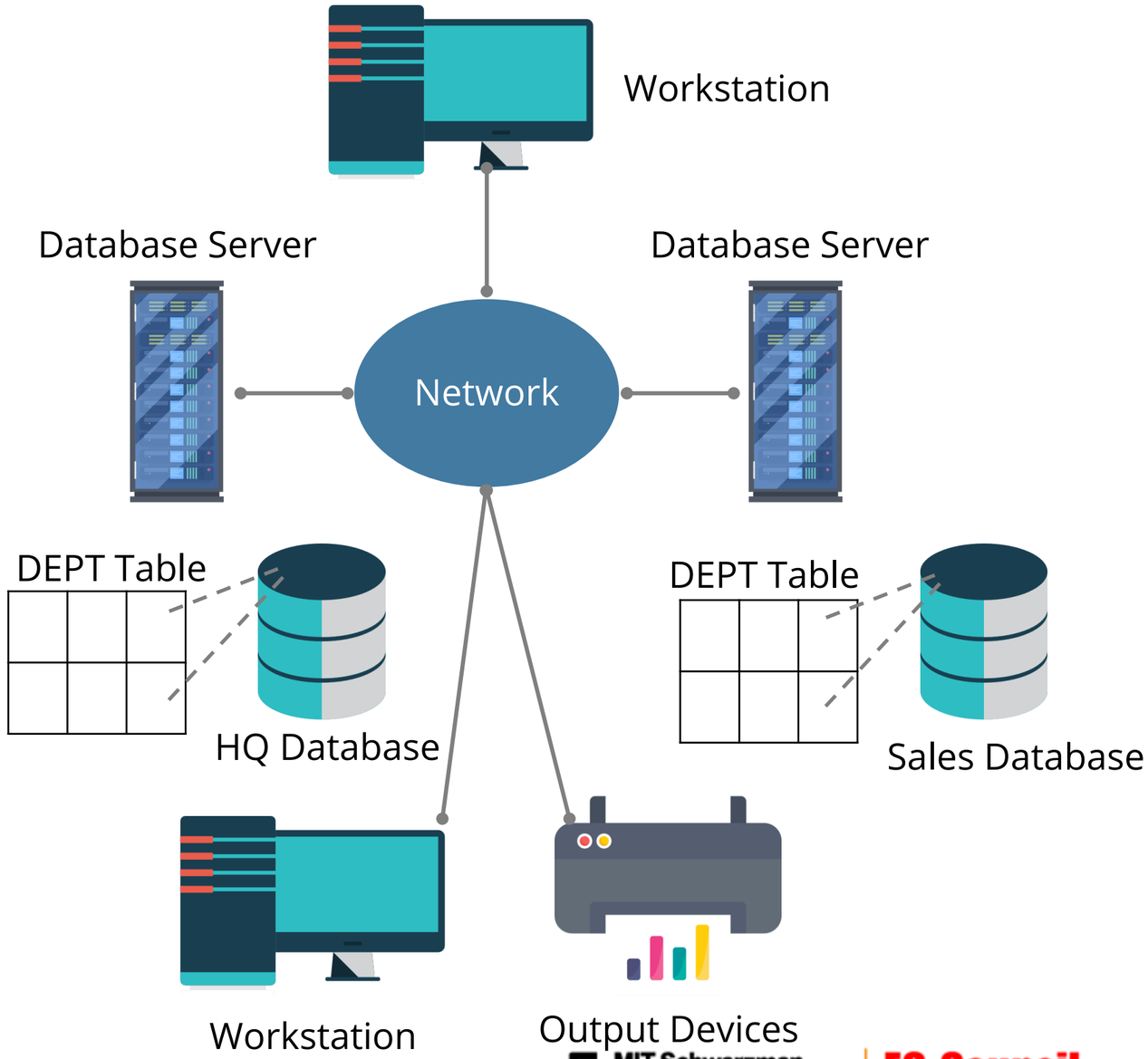
- Applications are located on only one system
- No communication links exist with other systems



Distributed Environment

Distributed environment is a type of system architecture, which integrates the management of:

- Application software
- Application platform
- Technology interface
- Information
- Communications



Industrial Control System (ICS)

> Industrial Control System (ICS) 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

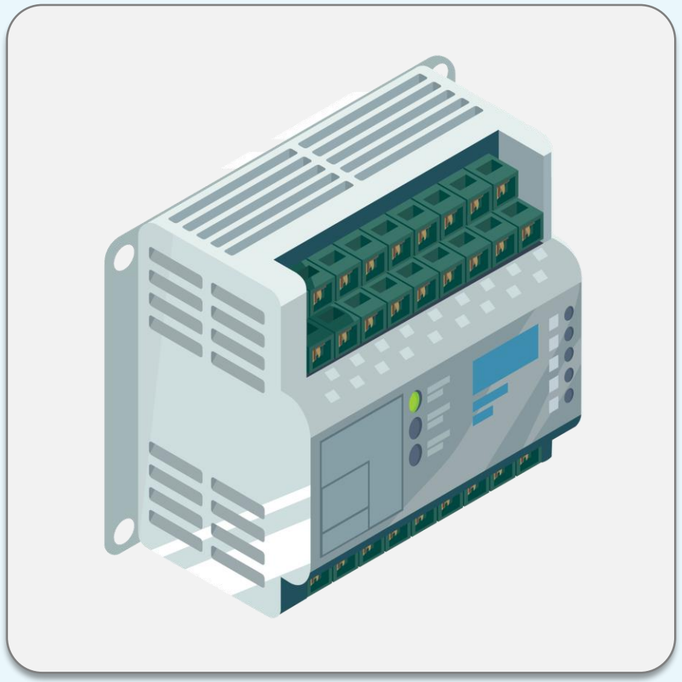
Programmable Logic Controllers (PLC)

Distributed Control Systems (DCS)

Supervisory Control and Data Acquisition (SCADA)

Programmable Logic Controller (PLC)

- A programmable logic controller (PLC) is a small industrial computer originally designed for factory automation and industrial process control.
- A PLC can be programmed as per the process that needs to be controlled.
- PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCS.
- PLCs are also used as the primary controller in smaller system configurations.
- PLCs are used extensively in almost all industrial processes.



Distributed Control Systems (DCS)

A distributed control system (DCS) is a specially designed automated control system used to monitor and control distributed equipment in process plants and industrial processes.

Unlike PLCs, which are generally standalone and perform a particular task, DCS 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.

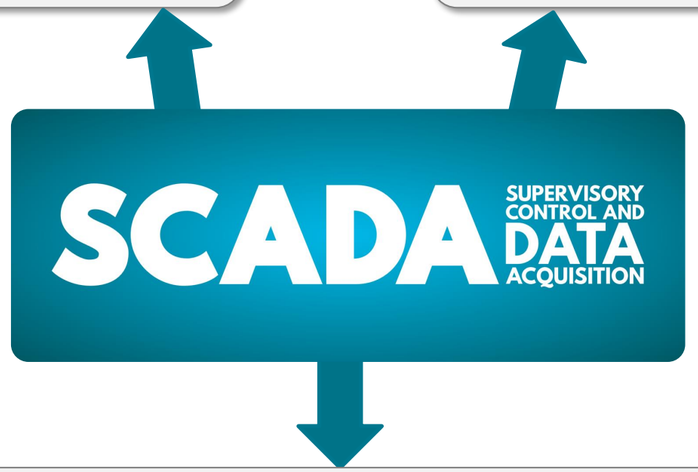
Supervisory Control and Data Acquisition (SCADA)

SCADA (Supervisory Control and Data Acquisition) systems are used to monitor and control a plant or equipment in industries such as telecommunications, water, waste control, energy, oil and gas refining, and other public transportation systems (airport, traffic control, and rails).

Supervisory Control and Data Acquisition (SCADA)

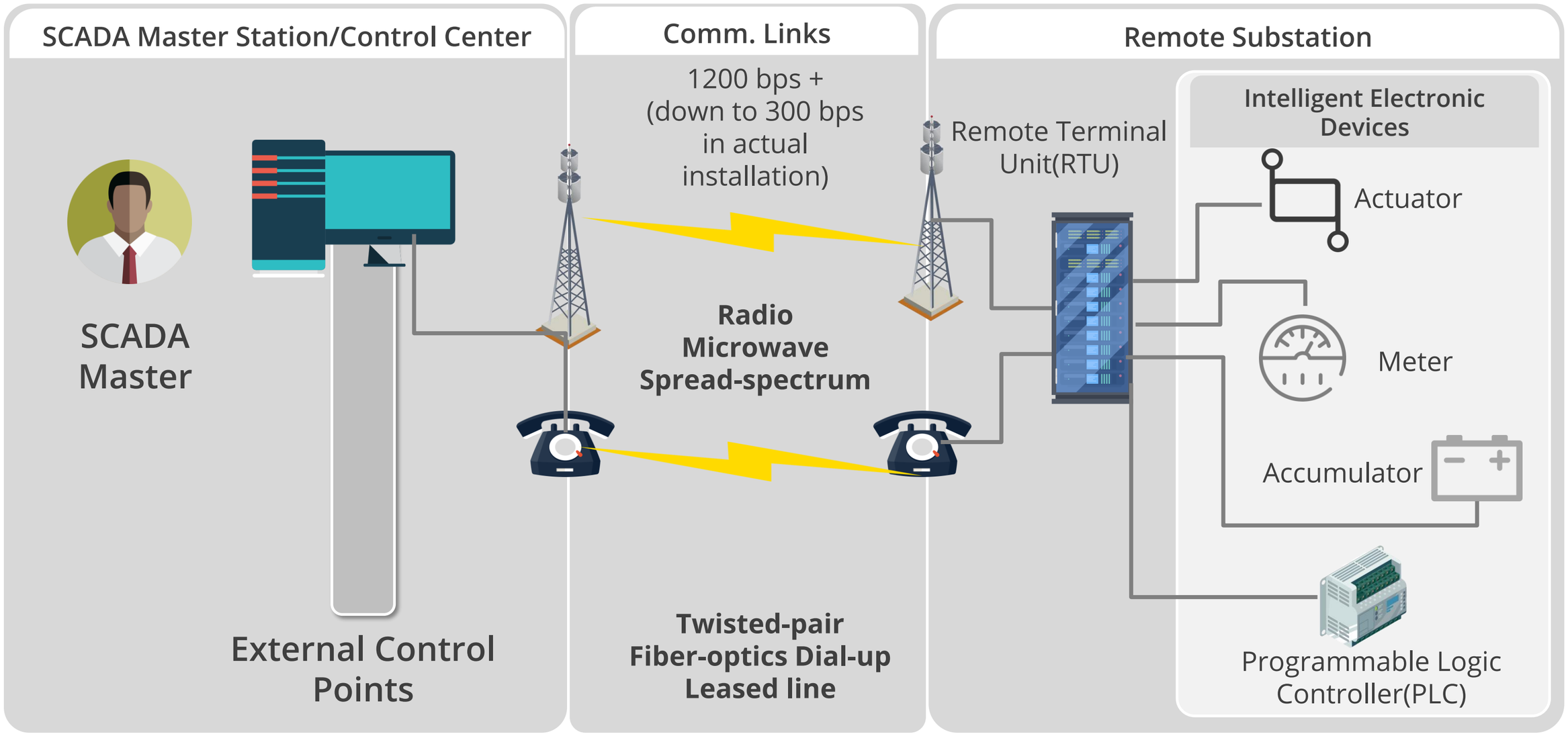
SCADA consists of many remote terminal units spread geographically across for the collection of data and is connected to the master station for centralized data acquisition via any communication system.

SCADA provides management with real-time data on production, improves plant and personnel safety, and reduces costs of operation.



SCADA systems have increasingly adopted Internet of things technology to significantly improve interoperability, reduce infrastructure costs, and increase ease of maintenance and integration.

Supervisory Control and Data Acquisition (SCADA)



Difference between PLC, DCS, and SCADA

	PLC	DCS	SCADA
Usage	Used for controlling the medium or large-scale applications	Used for controlling the entire plant	Used for supervising and acquiring data from remote plants
Location	Local	Local	Geographically dispersed
Communication	LAN	LAN	Any communication system
Performance	High	Medium	Slow

Security Concerns with ICS

Industrial Control System (ICS) poses the following security concerns:

- Control systems protocols with little or no security
- Migration to TCP/IP networks with its inherent vulnerabilities
- Interconnection with enterprise networks
- Old operating systems and applications with poor patching practices
- Little monitoring of control systems to detect and prevent attacks
- Poor security practices followed by vendors resulting in insecure products
- Increased risk of insider attacks by outsourced IT services
- Increased attacks on ICS by terrorists and foreign governments

Business Scenario

First uncovered by Kaspersky Lab in 2010, the Stuxnet Worm targeted SCADA systems and was responsible for causing substantial damage to Iran's nuclear program.

A key differential with Stuxnet was that, unlike most viruses, the worm targeted systems that are air-gapped and not connected to the internet for security reasons, via USB keys.

Business Scenario

- It exploited four zero-day security vulnerabilities found in Windows OS and then propagated across the network, exploiting security holes on computers running Siemens Step7 software that controls the PLCs.
- The operations were designed to provide the hackers with sensitive information on Iranian industrial infrastructure and even cause the fast-spinning centrifuges to tear themselves apart while masking the changes in rotational speed from monitoring systems.
- Its complexity indicated that only nation-state actors could have been involved in its development and deployment.

Question: What is a zero-day vulnerability?

Business Scenario

- It exploited four zero-day security vulnerabilities found in Windows OS and then propagated across the network, exploiting security holes on computers running Siemens Step7 software that controls the PLCs.
- The operations were designed to provide the hackers with sensitive information on Iranian industrial infrastructure and even cause the fast-spinning centrifuges to tear themselves apart while masking the changes in rotational speed from monitoring systems.
- Its complexity indicated that only nation-state actors could have been involved in its development and deployment.

Question: What is a zero-day vulnerability?

Answer: A zero-day exploit is an attack that exploits a previously unknown security vulnerability.

Case Study

ICS Malware Targets European Energy Company:

The SFG malware, discovered in June 2016 on the networks of a European energy company, created a backdoor on targeted industrial control systems.

The backdoor delivered a payload that was **used to extract data from or potentially shut down the energy grid**, according to security researchers at endpoint security firm SentinelOne Labs.

Case Study

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

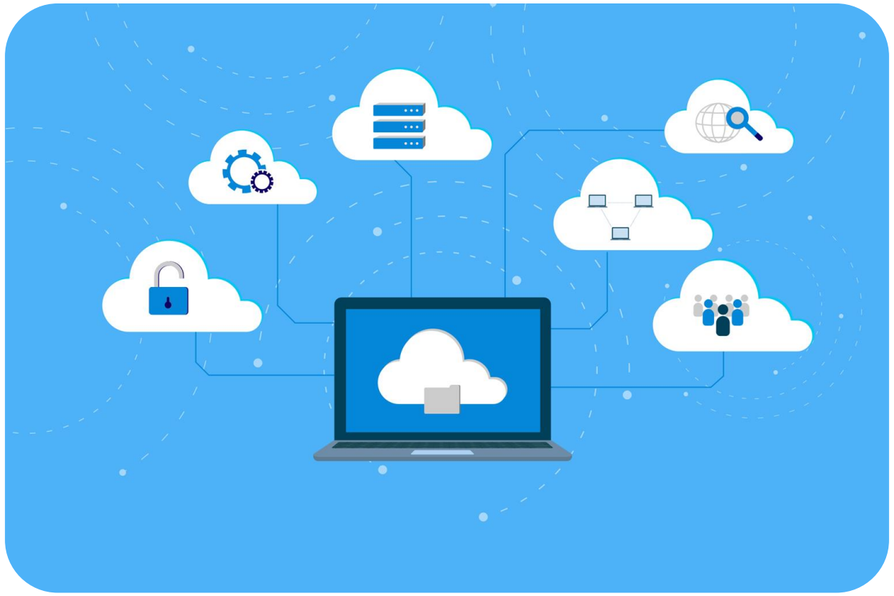
Case Study

Cyber-criminals are shifting their focus to industrial facilities as a lucrative target, where they can blackmail facilities through techniques such as ransomware.

For nation-states, identifying weaknesses in critical infrastructures of adversaries can be used strategically in case of conflicts, where cyber-attacks can be launched to paralyze a nation's key sectors, such as power, water, and transportation.

Cloud Computing

Cloud computing 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 your data rather than your local server or local computer.

Cloud Computing Models

Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Essential Characteristics

Resource Pooling

Software as a Service (SaaS)

Platform as a Service (Paas)

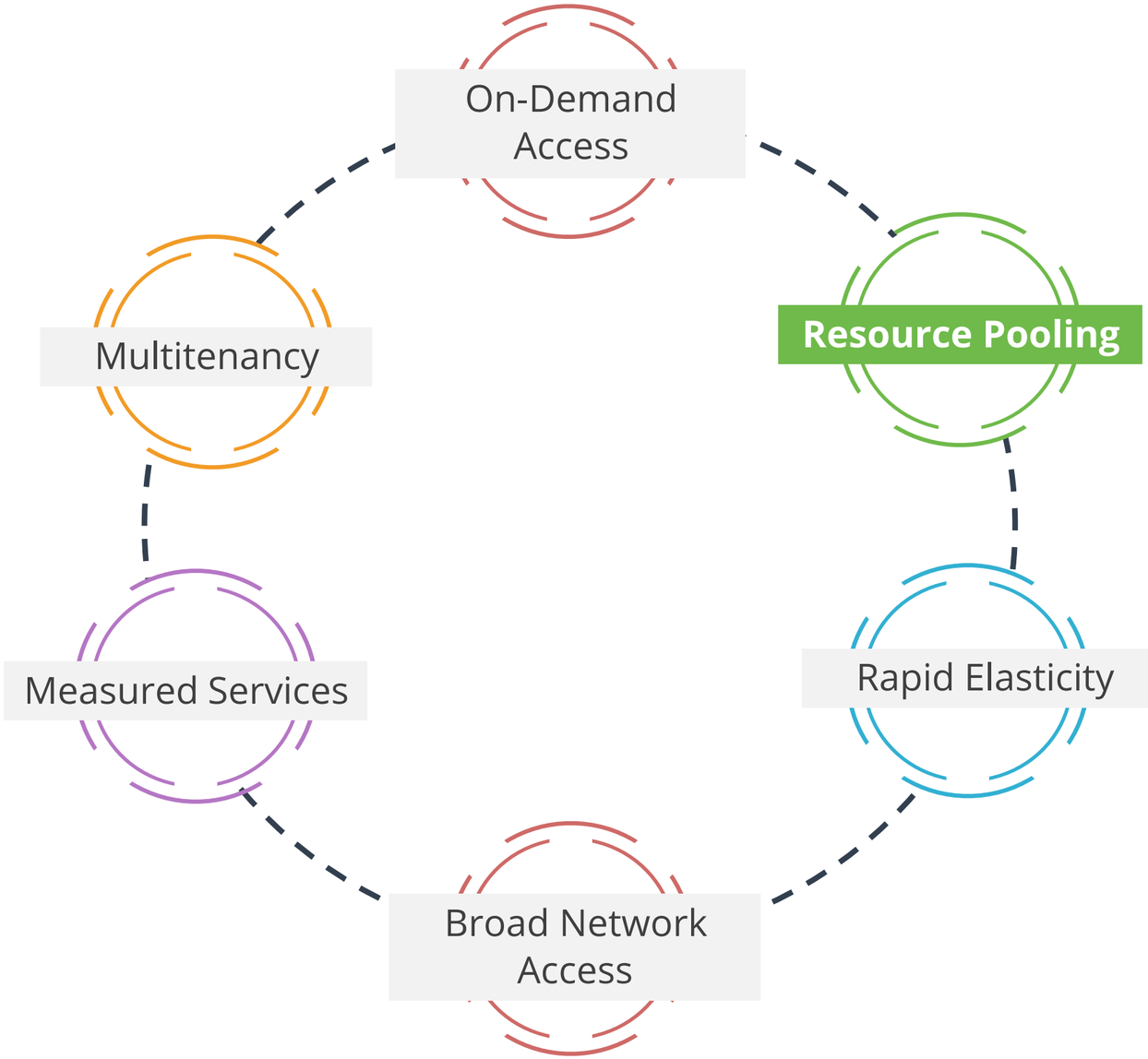
Infrastructure as a service (IaaS)

Delivery Models

Deployment Models

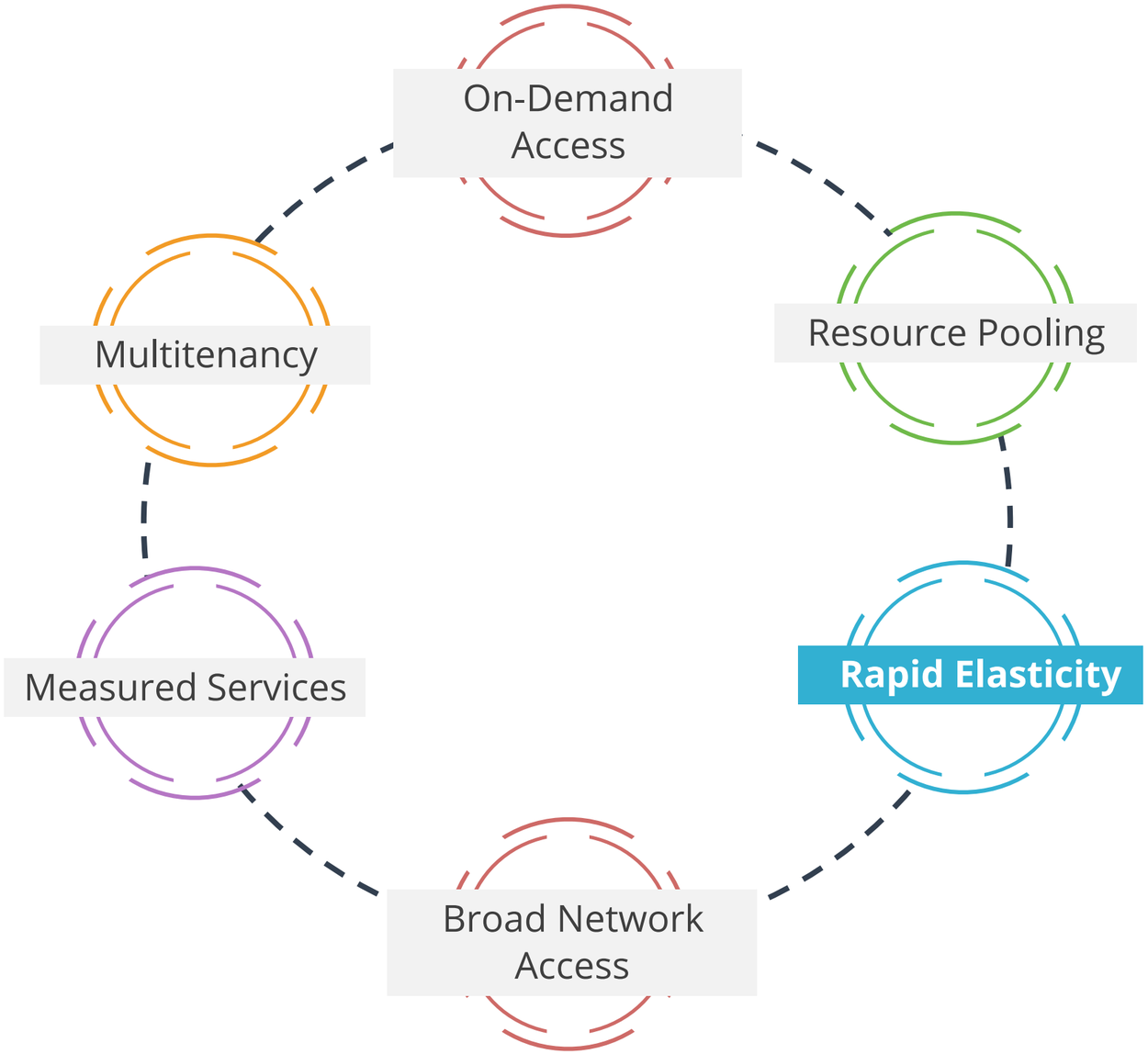
Cloud Computing Characteristics

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



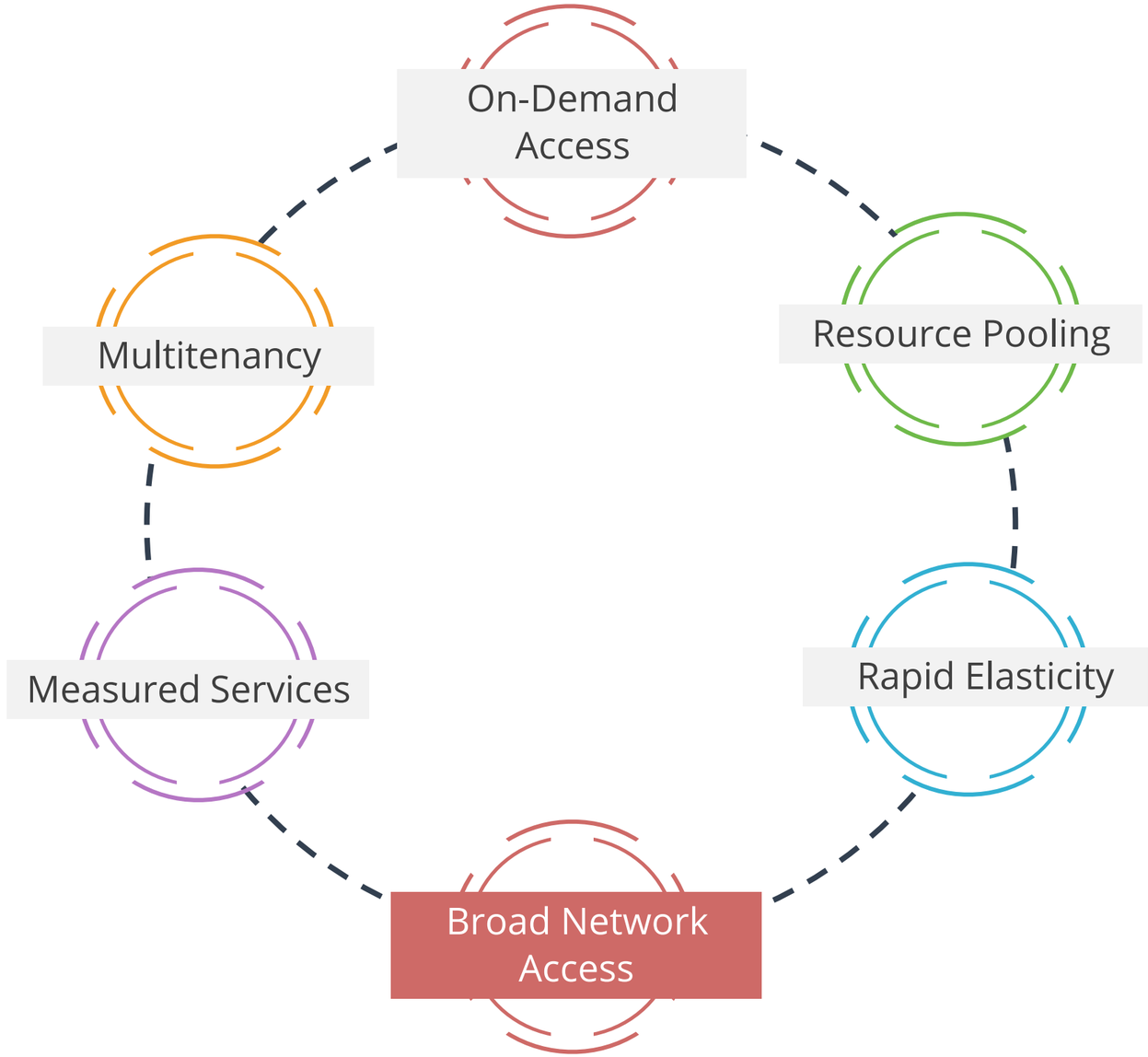
Cloud Computing Characteristics

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



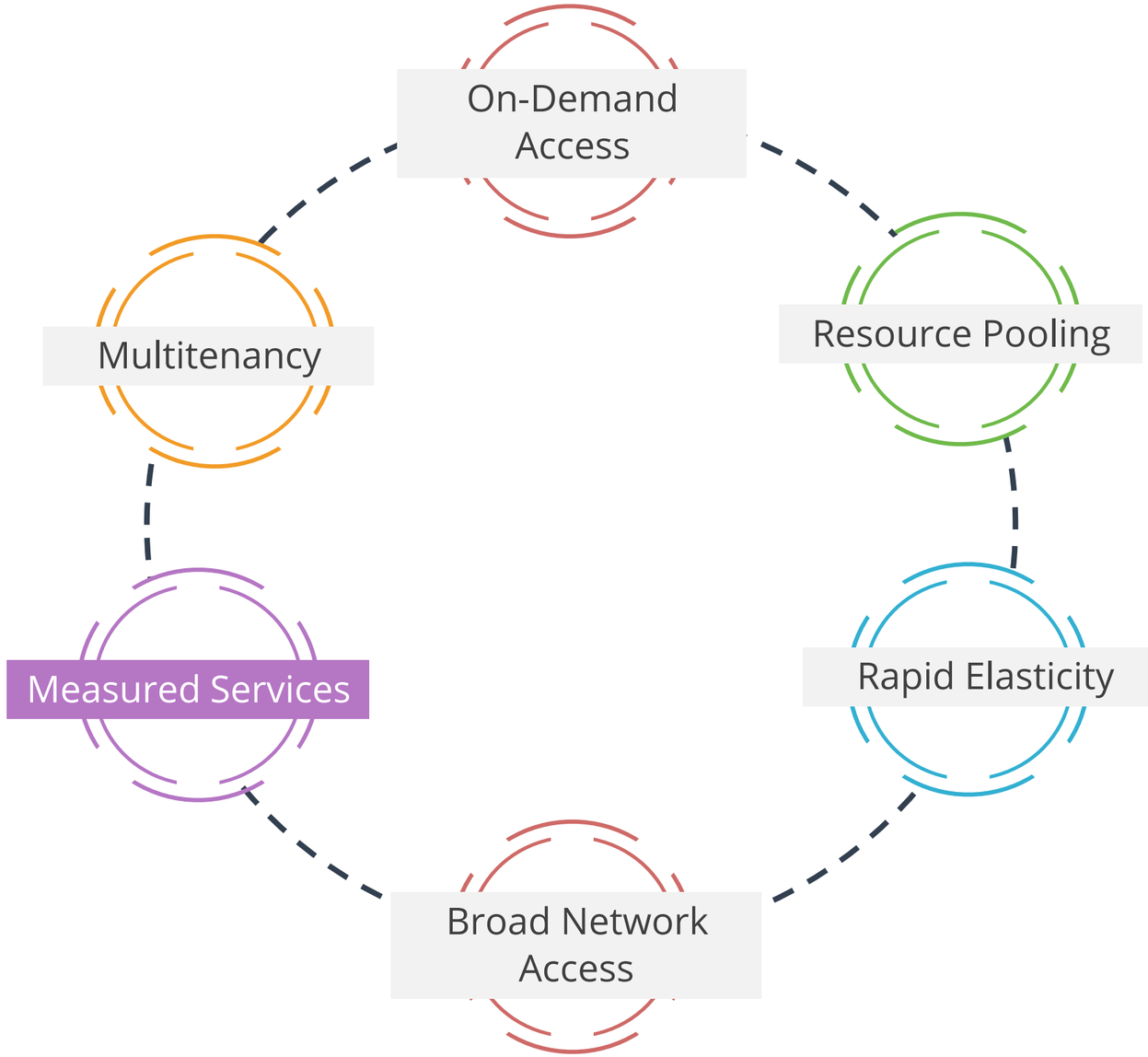
Cloud Computing Characteristics

In broad network access, all resources are available over a network, without any need for direct physical access.



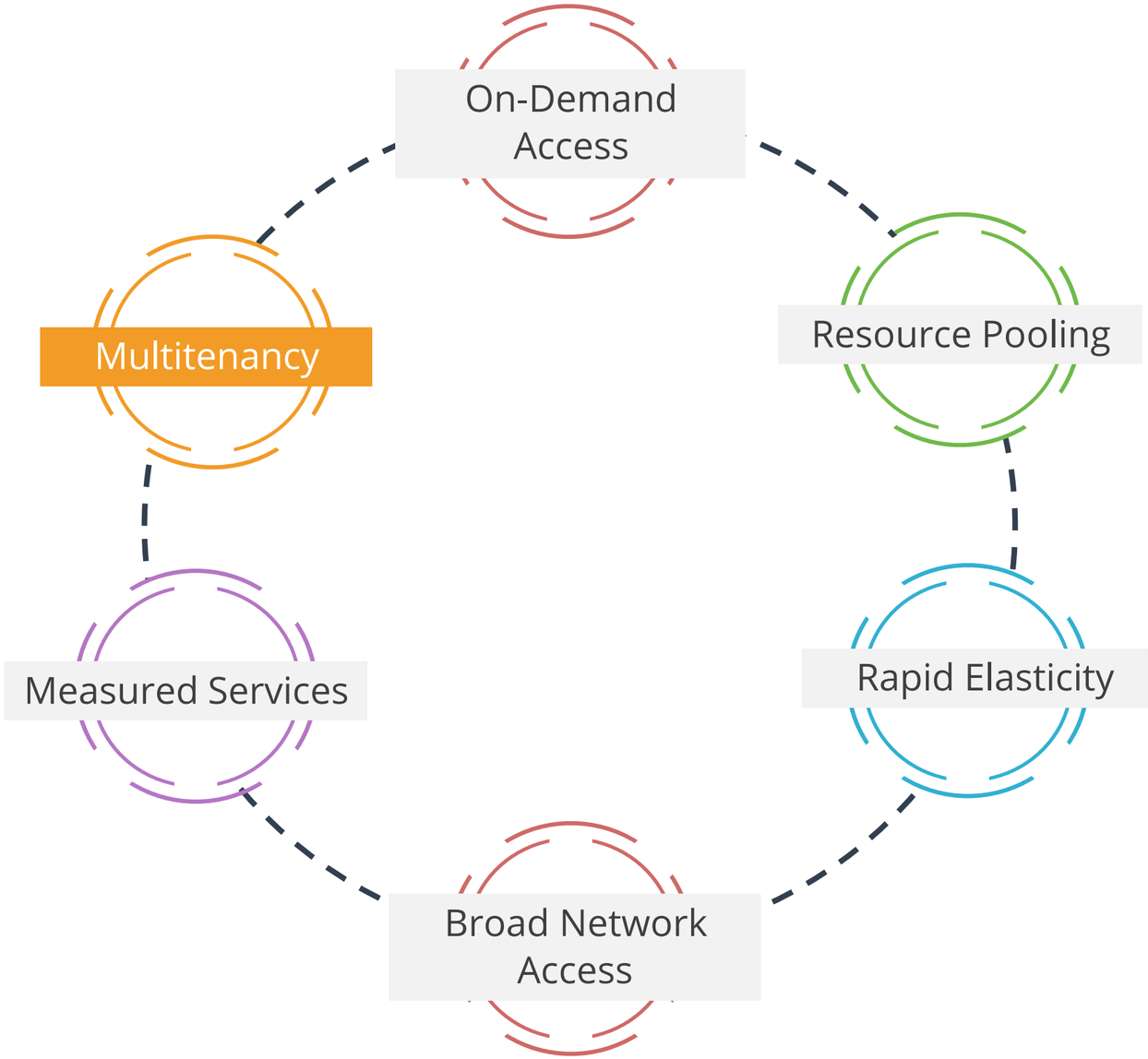
Cloud Computing Characteristics

In measured services, customers are charged for what they are using or consuming.



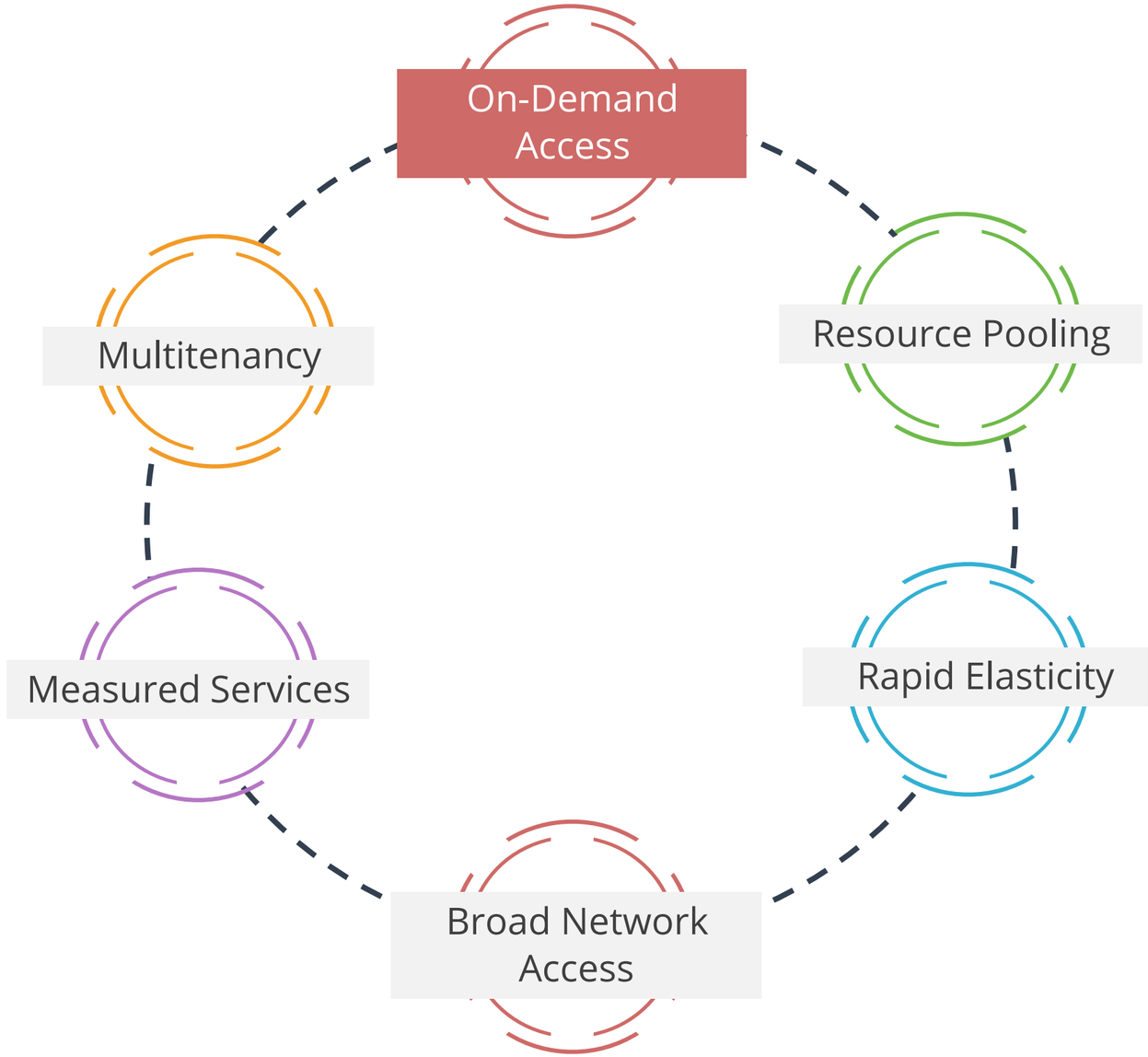
Cloud Computing Characteristics

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



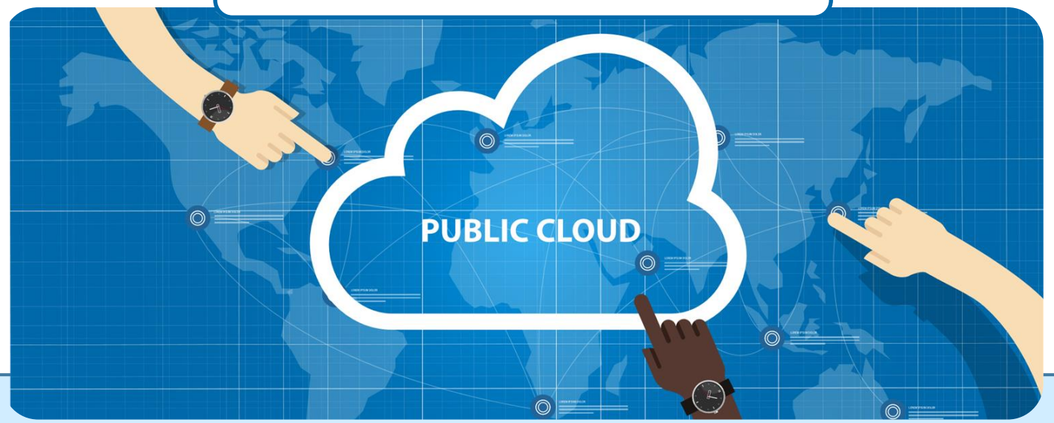
Cloud Computing Characteristics

- In on-demand access, 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.



Categorization of Cloud: Deployment Categories

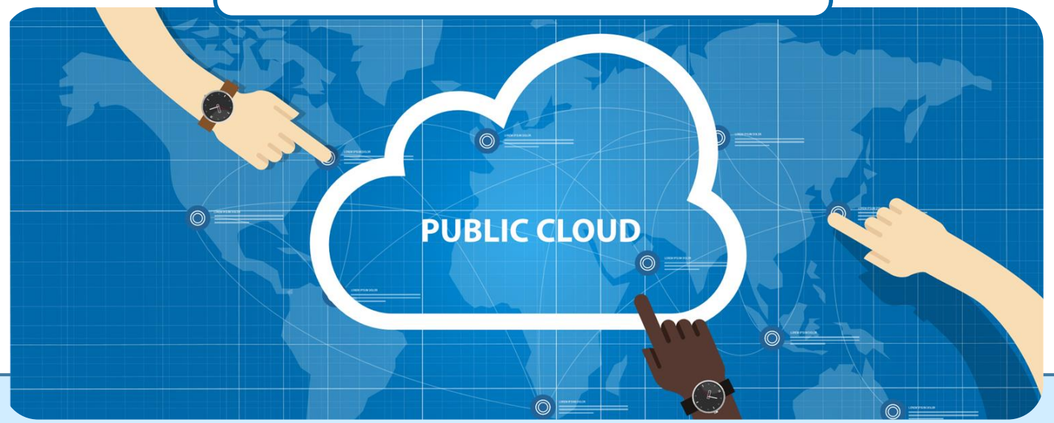
Public Cloud



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

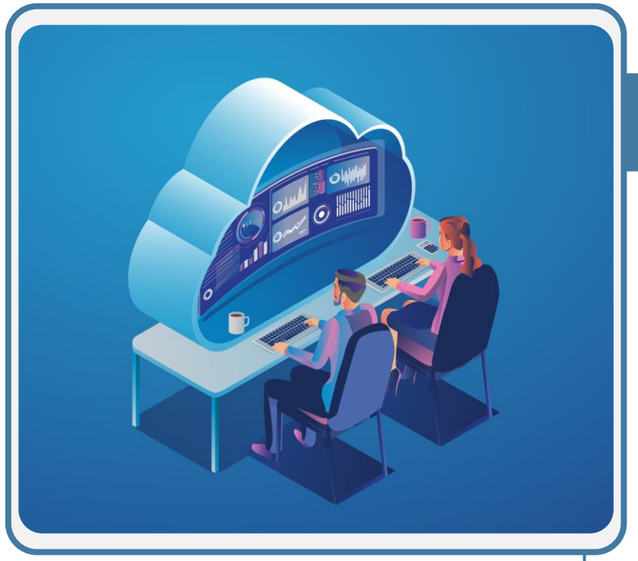
Categorization of Cloud: Deployment Categories

Private Cloud



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

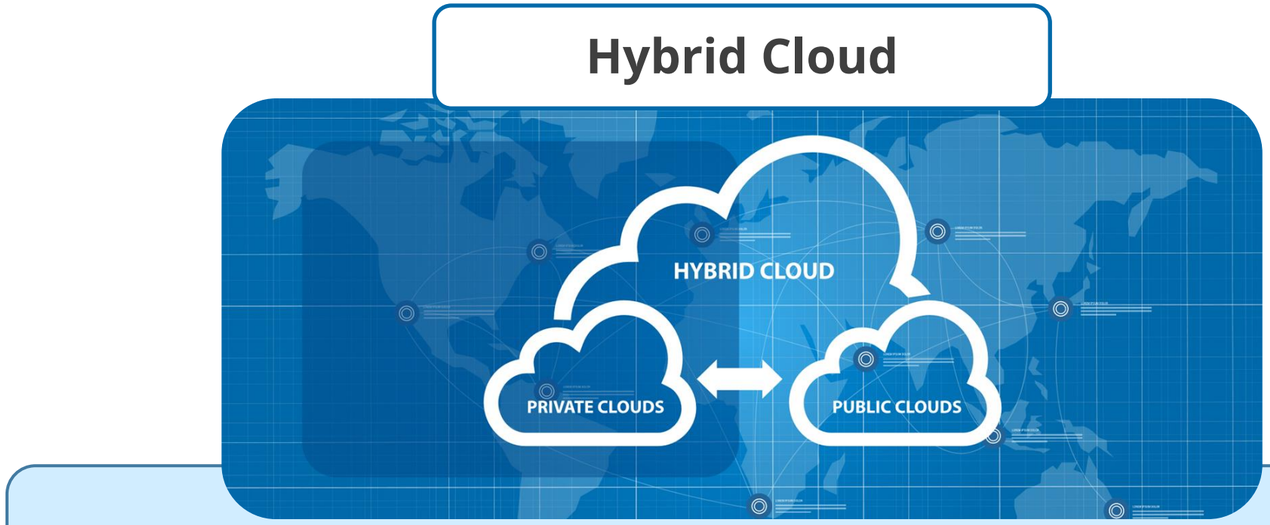
Categorization of Cloud: Deployment Categories



Community Cloud

- Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, or compliance considerations)
- Might be managed by the organizations or by a third party
- Might be located on-premises or off-premises

Categorization of Cloud: Deployment Categories

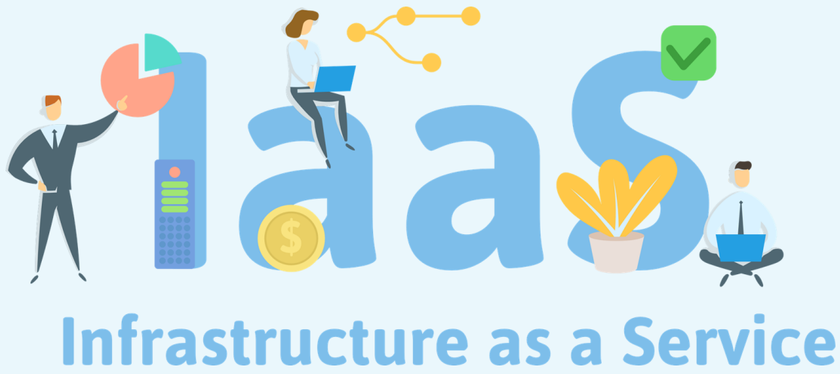


Cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities.

Categorization of 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.
- These are also called the SPI tiers.
- Examples: Amazon EC2, Google Compute Engine, and HP Cloud



Categorization of Cloud: Service Categories

Platform as a Service (PaaS)

- It is a category of cloud computing services that provides 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 app.
- Examples: Google App Engine, Windows Azure Cloud Services

Categorization of 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 app, or a lightweight client app.
- Examples: Google Apps, Microsoft Office 365

Categorization of Cloud: Service Categories

Security as a Service (SaaS)

- It is the outsourcing of security functions to a vendor that can offer advantages in scale, costs, and speed.
- Security is a complex, wide-ranging cornucopia of technical specialties, all working together to provide appropriate risk reductions in today's enterprise.

Security as a Service (SaaS): Services, Benefits, and Concerns

Services

- Proxy services
- Identity management
- SIEM
- IDS and IPS
- Web application firewall

Benefits

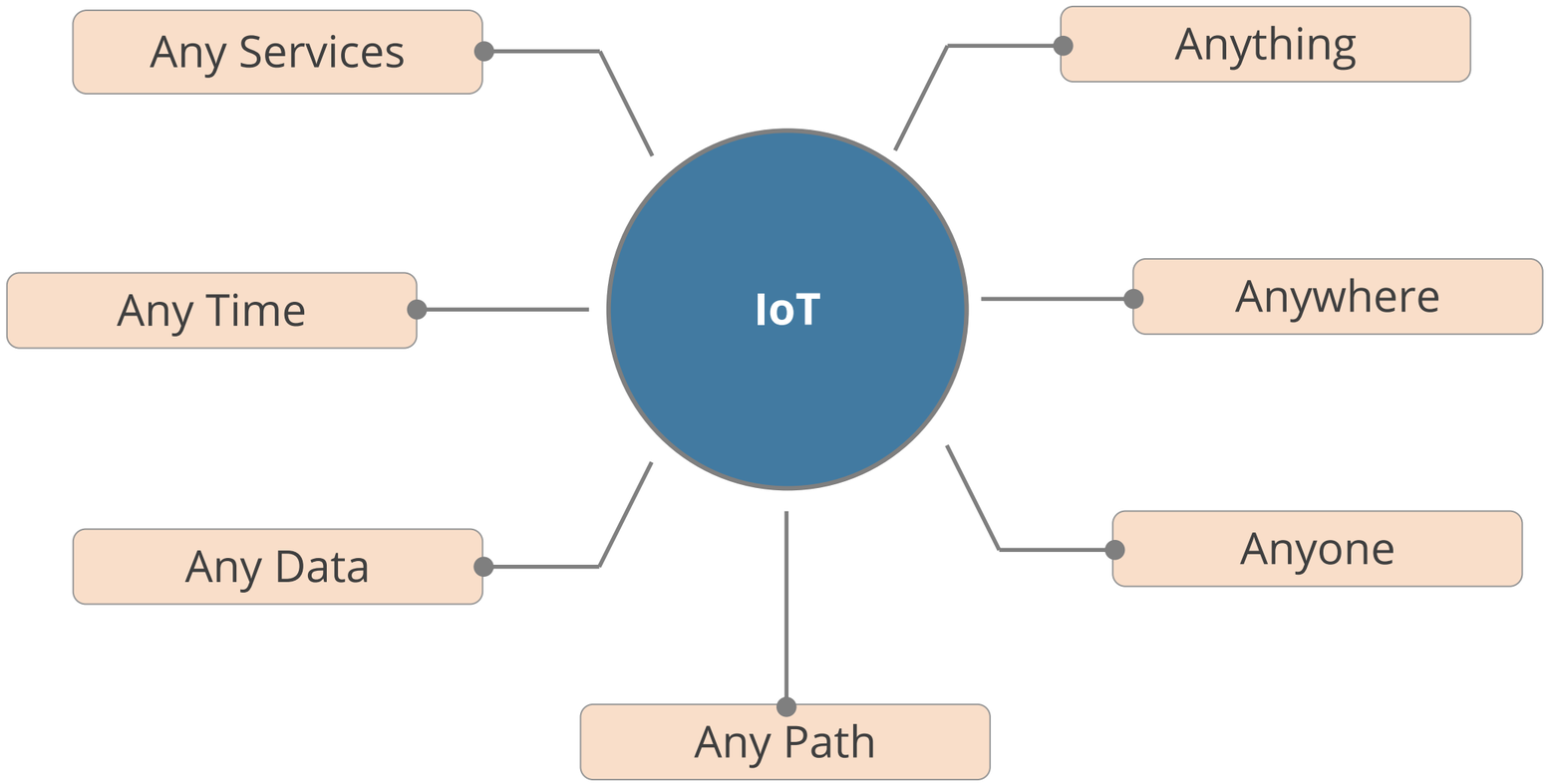
- Cloud-computing benefits
- Staffing and expertise
- Intelligence-sharing
- Deployment flexibility
- Scaling and cost

Concerns

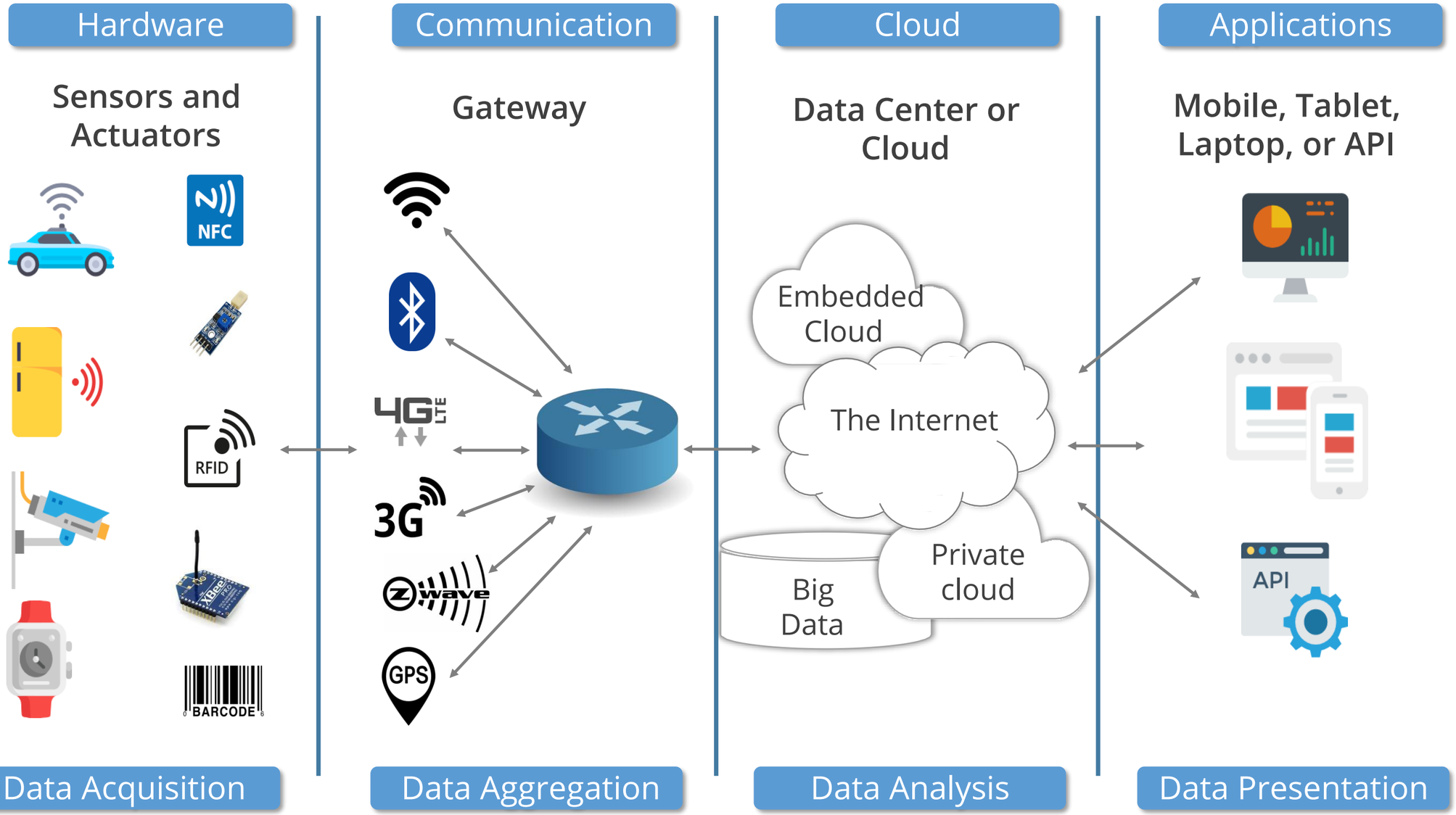
- Lack of visibility
- Regulation differences
- Handling of regulated data
- Changing providers
- Data leakage

Internet of Things (IoT)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity that enables these objects to connect and exchange data.



IoT Architecture



Top 10 IoT Vulnerabilities of OWASP

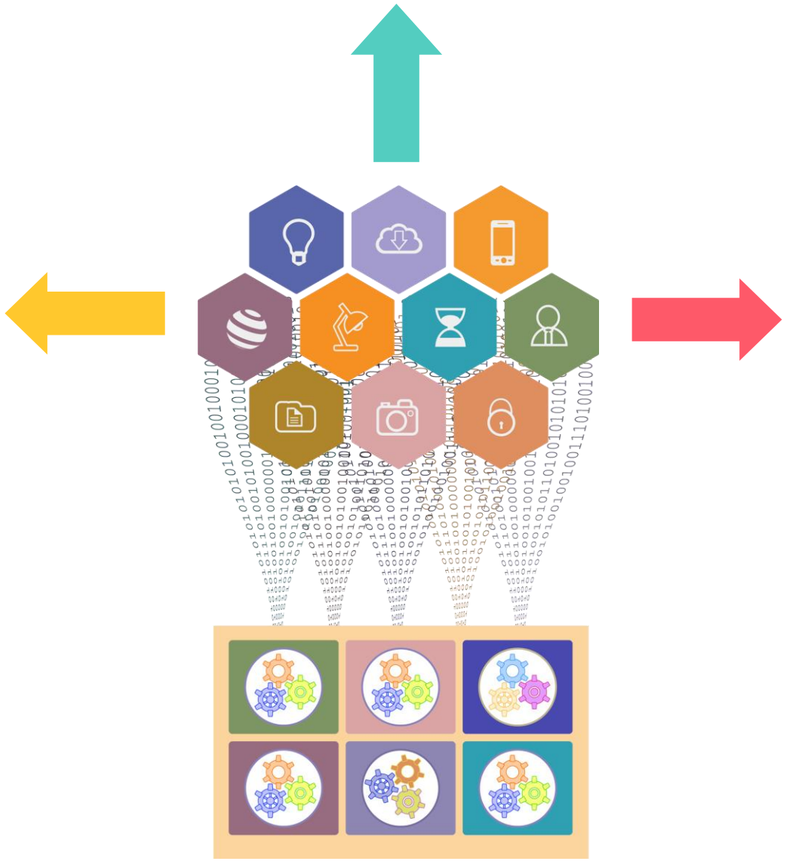
1. Weak, guessable, or hard coded passwords
2. Insecure network services
3. Lack of secure update mechanism
4. Insecure ecosystem interfaces
5. Insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Lack of physical hardening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

Source: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Microservices Architecture

Microservices architecture is an approach in which a single application is composed of many loosely coupled and independent services.

Microservices can be thought of as a variant of **service-oriented architecture (SOA)** wherein applications are built as a collection of different smaller services rather than one whole app.



Microservices follow Ken Thompson's Unix philosophy: **Do one thing and do it well.**

Microservices

Benefits

- Code can be updated more easily
- Components can be scaled independently of one another
- Better fault isolation
- Code for different components can be written in different languages

Disadvantages

- More complex than monolithic applications
- Can present security threats
- Testing can become complicated and tedious

Source: https://www.tiempodev.com/blog/disadvantages-of-a-microservices-architecture/

Uber: Case Study

- Like most startups, Uber built their application with a monolithic architecture.
- However, as Uber started expanding worldwide they started facing several issues related to scalability, performance, and stability of its application.
- Monolithic architecture is a very popular single-tiered software application in which all components are combined into a single program.
- Those components include the client-side user interface, server-side business logic, the data access layer, and integrations.

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

Uber: Case Study

- These components are interconnected and interdependent, meaning when one component needs to be updated, you have to make changes to the entire application.
- Failure of one component can bring down the entire system.
- When the number of services increases, integration and managing whole products can become complicated.
- To avoid such problems Uber decided to break its monolithic architecture into multiple applications to form a microservice architecture.

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

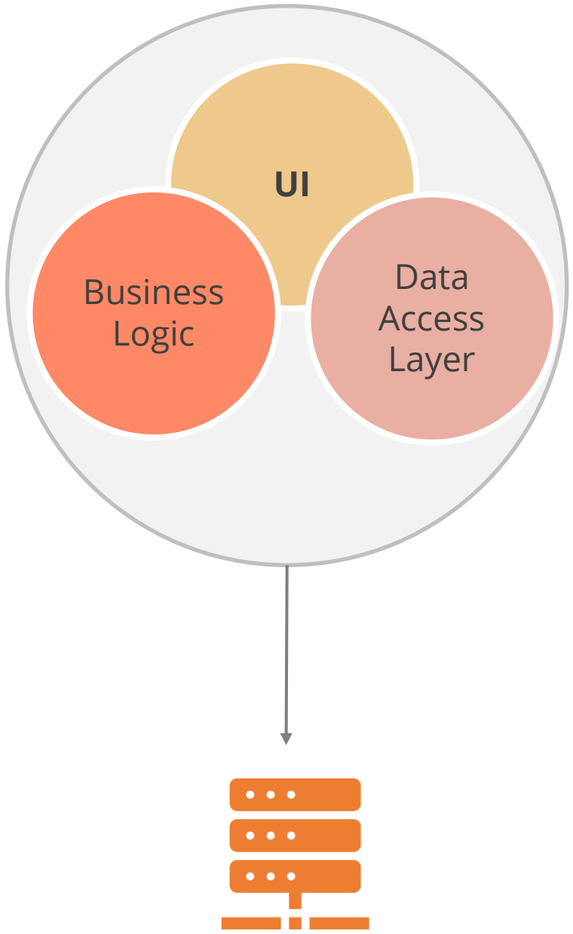
Uber: Case Study

- Microservices divide and distribute the application workload, providing stable, seamless, and scalable services by interacting with each other.
- Compared to traditional data storage models used by monolithic applications, microservices decentralize the data storage by managing their own data stores.
- Uber was now able to manage each microservice individually as the dependency between each and every feature was removed.
- In this way, Uber benefited by shifting its architecture from monolithic to microservices.

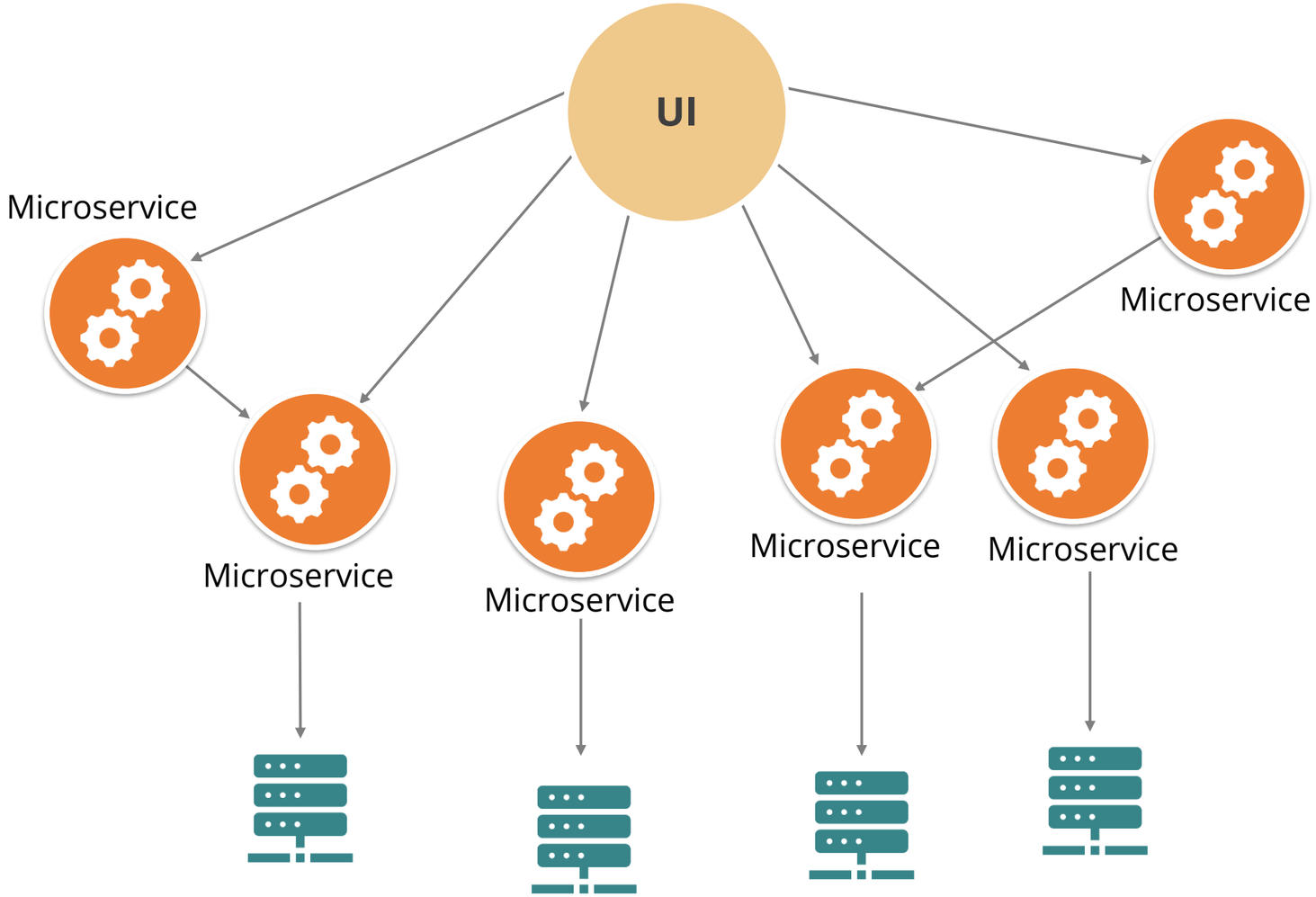
Source: https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d
And
https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

Microservices

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



Monolithic Architecture

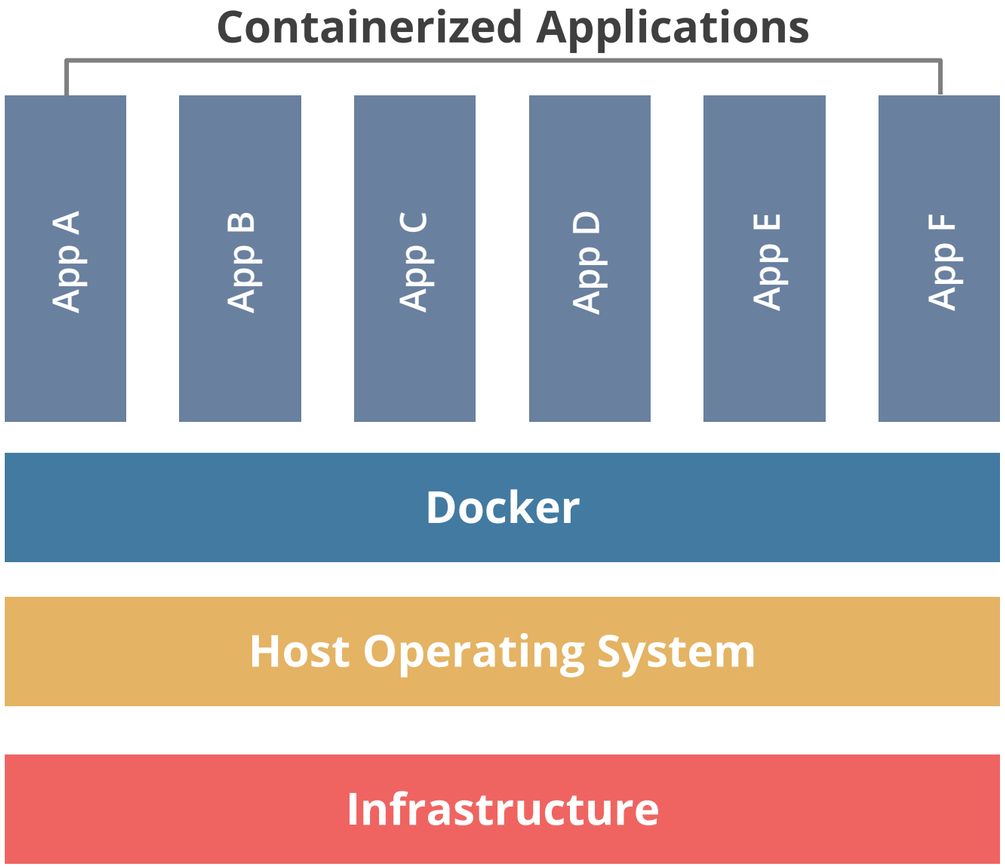


Microservice Architecture

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

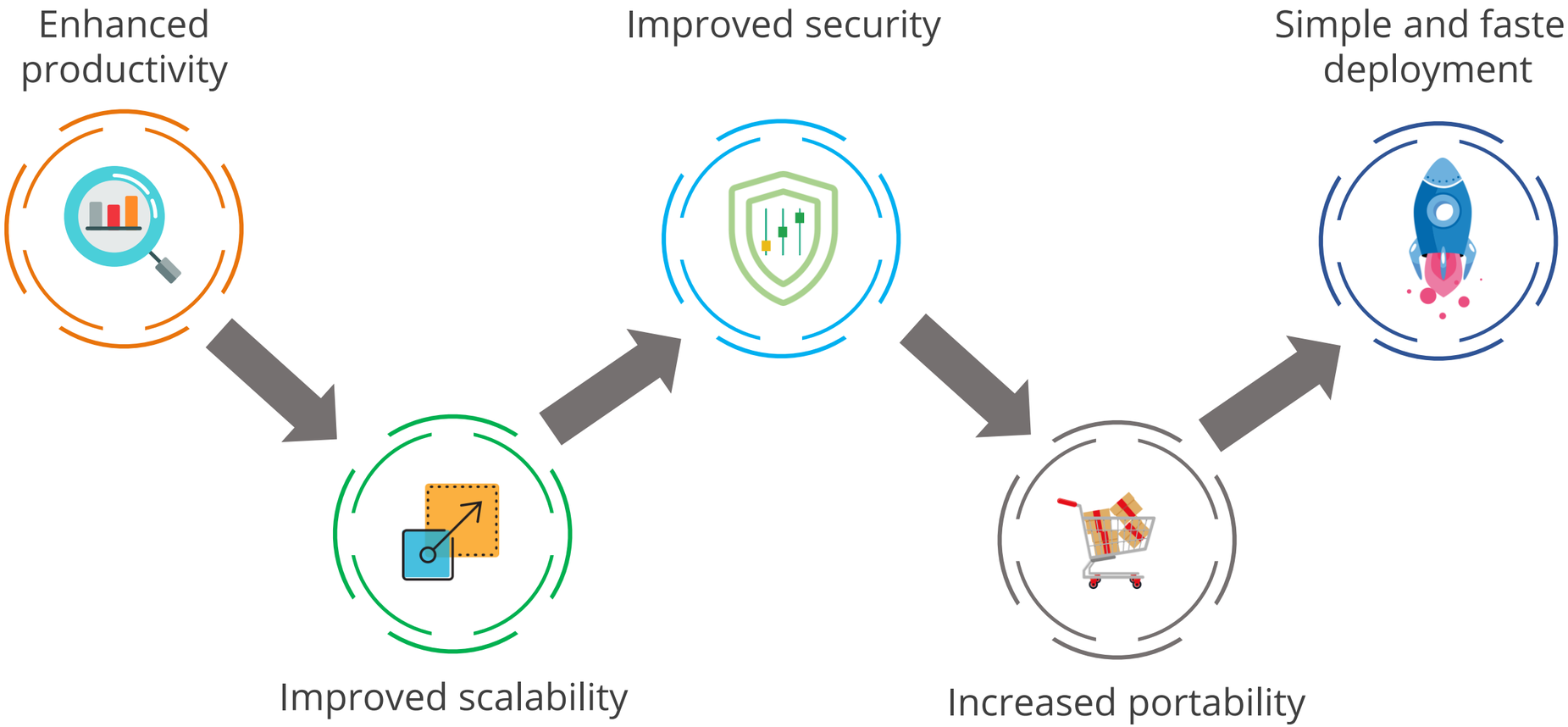
Containerization

Containerization is the process of packaging an application with all its related configuration files, libraries, and dependencies required for it to run in an efficient and bug-free way across different computing environments.



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

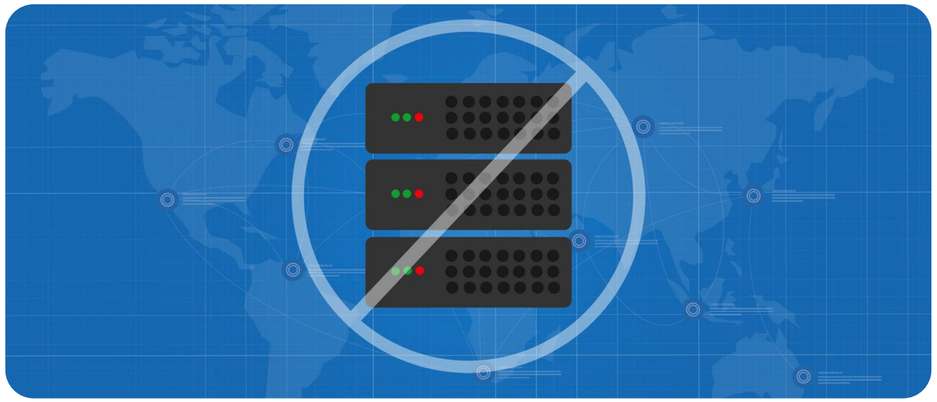
Containerization: Benefits



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

Serverless

Serverless computing is a cloud architecture that enables the execution of code on-demand.

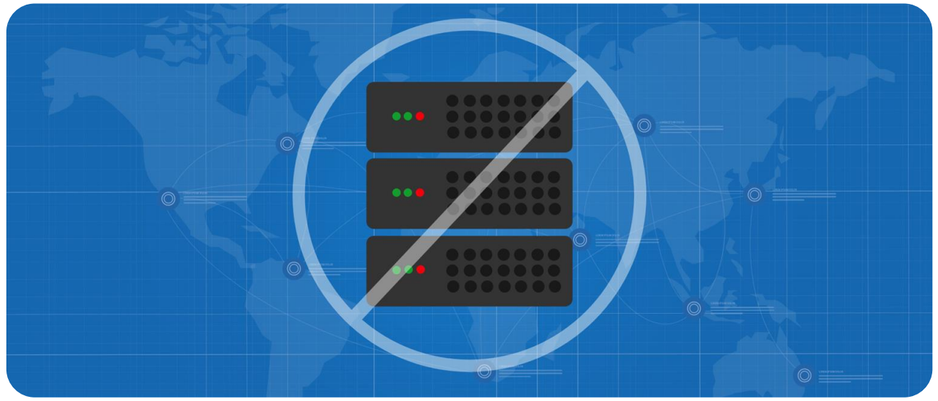


The cloud service provider automatically provisions, manages, and scales the resources required to run the code.

Serverless

Benefits

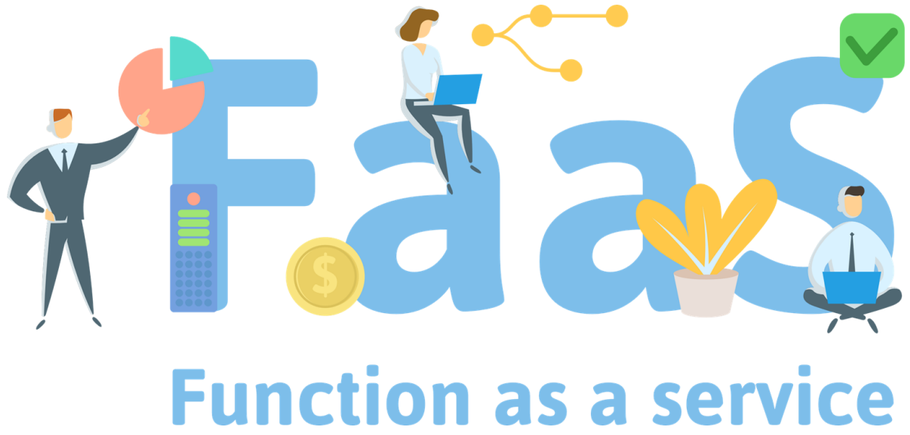
- Build applications faster
- Pay only for resources used
- Scale up or down automatically



Function-as-a-Service (FaaS)

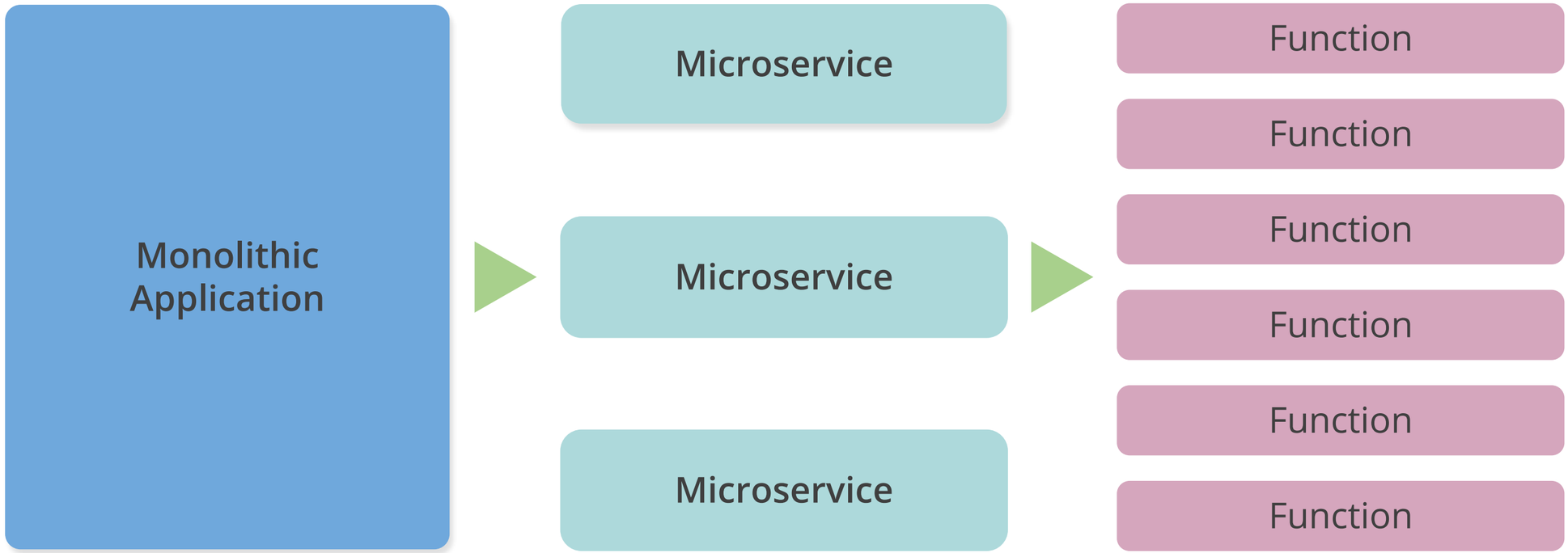
Function-as-a-Service (FaaS) is a type of cloud-computing service that enables the execution of code in response to events without the complexity of building and maintaining the infrastructure.

- Subset of serverless
- Server-side logic runs in stateless containers



Serverless

The following diagram illustrates a serverless architecture:

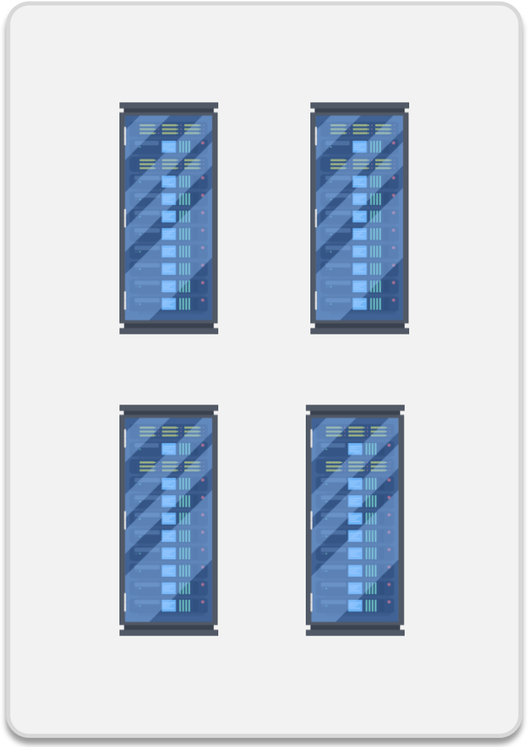


Source: https://www.cloudflare.com/en-in/learning/serverless/glossary/function-as-a-service-faas/

High-Performance Computing (HPC) Systems

High-performance computing (HPC) is the use of parallel processing for running computationally intensive operations across multiple resources. High-performance computing consists of computing, network, and storage.

User/Scheduler



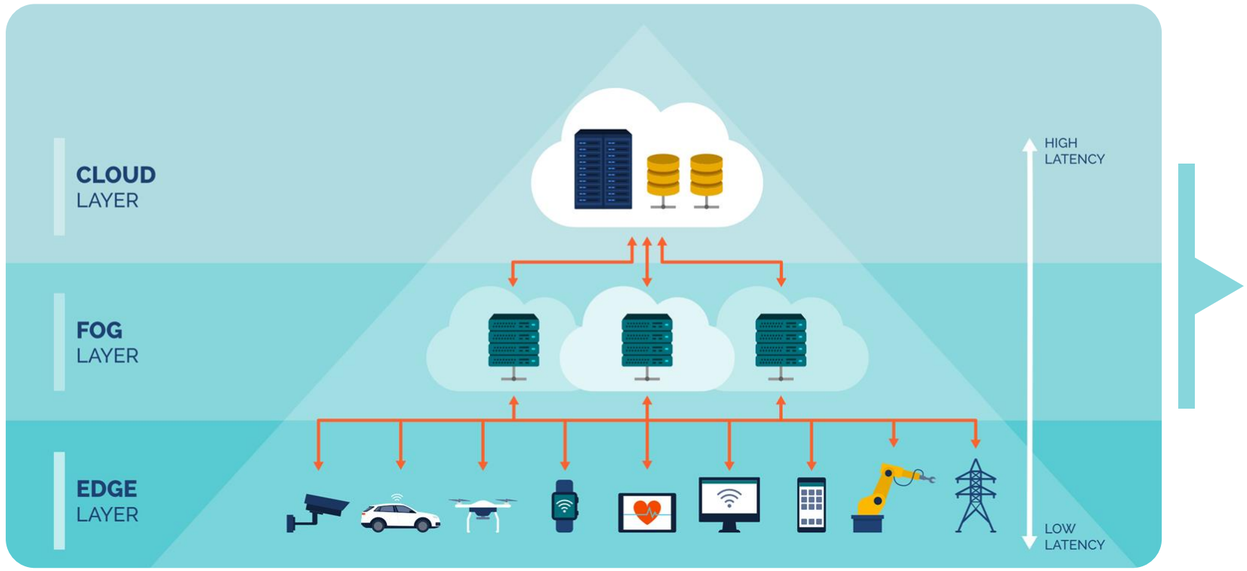
Computer Cluster

Data Storage

Edge and Fog Computing

Fog computing is a standard that defines the way edge computing should work, and it 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

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

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

Benefits:

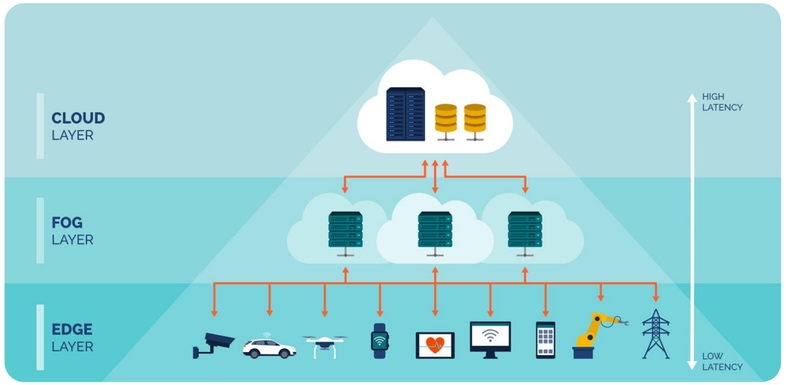
- Real-time data analysis
- Improved response time
- Lower bandwidth consumption

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

Edge and Fog Computing: Vulnerabilities and Mitigations

Vulnerabilities

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



Mitigations

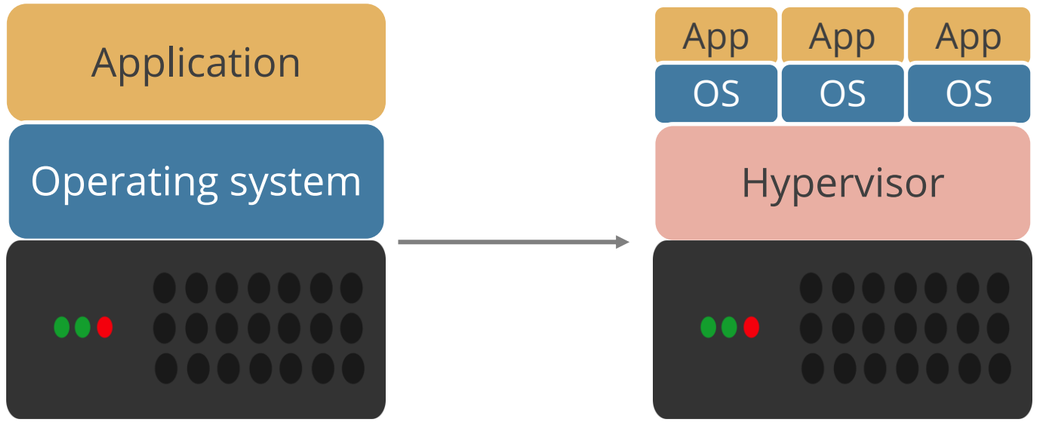
- Employ **security by design**
- Increase network monitoring

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

Virtualization

Virtualization 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's benefits include efficiency, higher availability, and lower costs.

Hypervisor

A hypervisor is a software that is installed to virtualize a given computer.

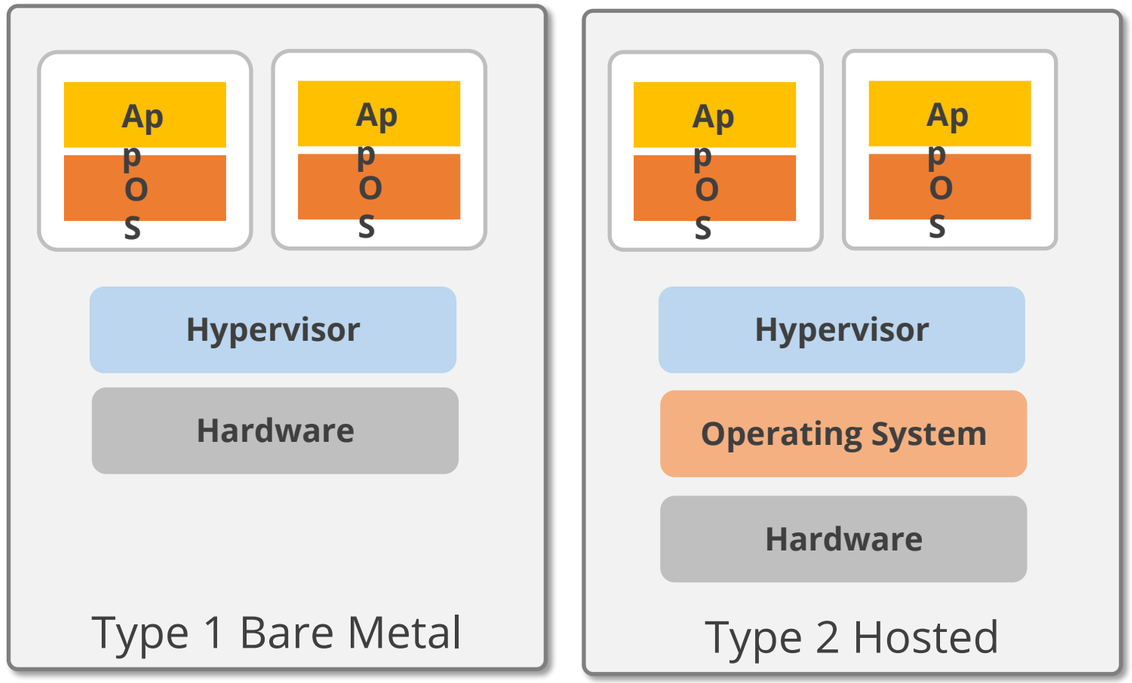
- **Host machine:** A computer on which a hypervisor is installed
- **Guest machine:** Every virtual machine

Type 1 hypervisors run directly on the host machine's hardware

- Example: Microsoft Hyper-V hypervisor, VMware ESX/ESXi

Type 2 hypervisors run within an existing operating system environment

- Example: VMware Workstation, Virtual Box



Business Scenario

During the 2017 Pwn2Own, an annual hacking contest in Vancouver, a hacker compromised Microsoft's heavily fortified Edge browser in a way that escapes a VMware Workstation virtual machine it runs in, which fetched a prize of $105,000.

- The hacker used a JavaScript engine bug within Microsoft Edge to achieve the code execution inside the Edge sandbox, and he used a Windows 10 kernel bug to escape from it and fully compromise the guest machine.
- Then he exploited a hardware simulation bug within VMware to escape from the guest operating system to the host one.
- This sets up a scenario in which malicious websites can not only compromise a visitor's virtual machine, but also the much more valuable host machine the VM runs on.
- VMware patched the vulnerabilities within 2 weeks.

Question: What is the risk of breakout from a hypervisor isolation?

Business Scenario

During the 2017 Pwn2Own, an annual hacking contest in Vancouver, a hacker compromised Microsoft's heavily fortified Edge browser in a way that escapes a VMware Workstation virtual machine it runs in, which fetched a prize of $105,000.

- The hacker used a JavaScript engine bug within Microsoft Edge to achieve the code execution inside the Edge sandbox, and he used a Windows 10 kernel bug to escape from it and fully compromise the guest machine.
- Then he exploited a hardware simulation bug within VMware to escape from the guest operating system to the host one.
- This sets up a scenario in which malicious websites can not only compromise a visitor's virtual machine, but also the much more valuable host machine the VM runs on.
- VMware patched the vulnerabilities within 2 weeks.

Question: What is the risk of breakout from a hypervisor isolation?

Answer: If the hypervisor is compromised, all VMs residing on the hypervisor can be compromised

Select and Determine Cryptographic Solutions

Cryptography

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

It enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Basic Definitions

Cryptography	Science of secret writing that enables an entity to store and transmit data in a form that is available only to the intended individuals
Cryptosystem	Hardware or software implementation of cryptography that contains all the necessary software, protocols, algorithms, and keys
Cryptology	The study of both cryptography and cryptanalysis
Algorithm (Cipher)	Set of mathematical and logical rules used in cryptographic functions
Kerckhoff's principle	The concept that an algorithm should be known and only the keys should be kept secret

Conventional Encryption

Conventional encryption is illustrated below:

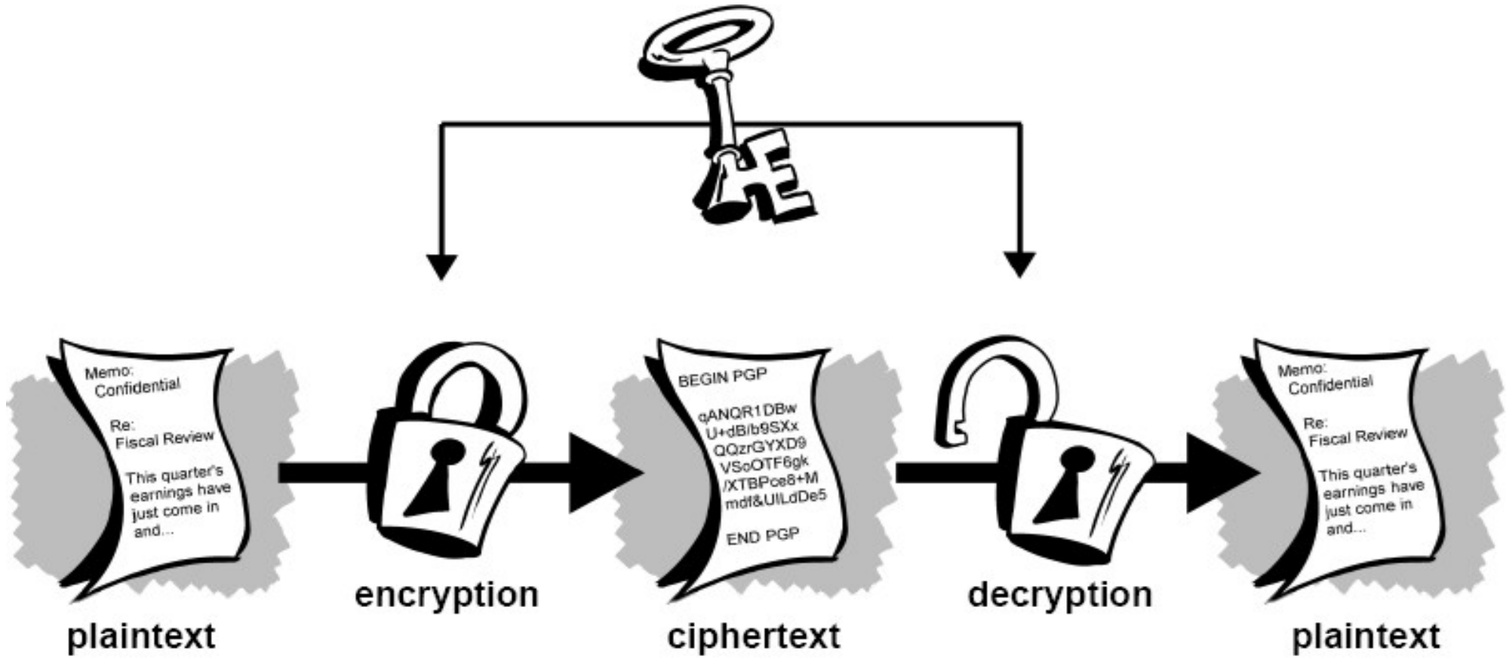
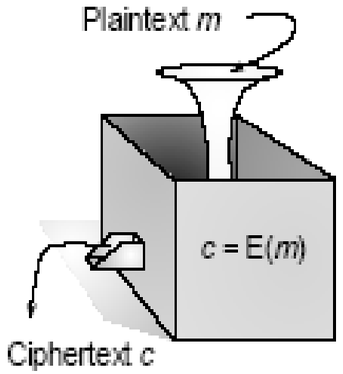


Figure 1-2. Conventional encryption

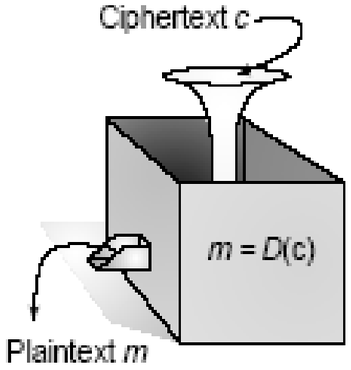
Encryption and Decryption

Encryption



The conversion of a original message, referred to as *plaintext* or *cleartext*, into a different message known as *ciphertext* (the word cipher comes from an old Arabic word meaning empty or zero), or *cryptogram*.

Decryption



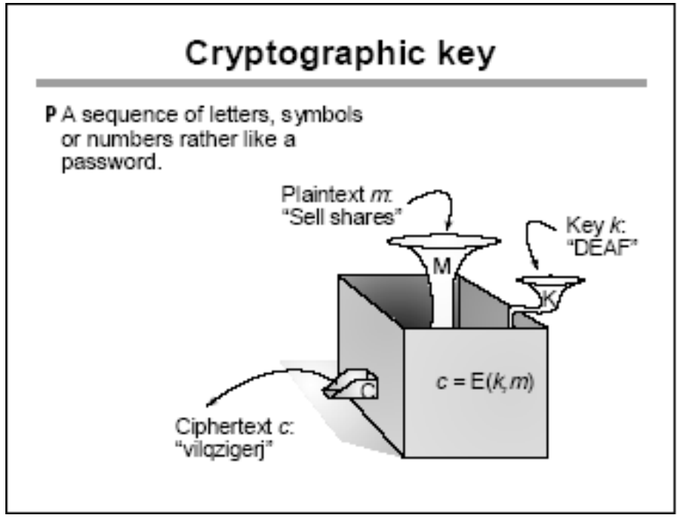
The extraction process by which the intended receiver extracts the plaintext from the ciphertext

Cryptographic Key

A **key** 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.

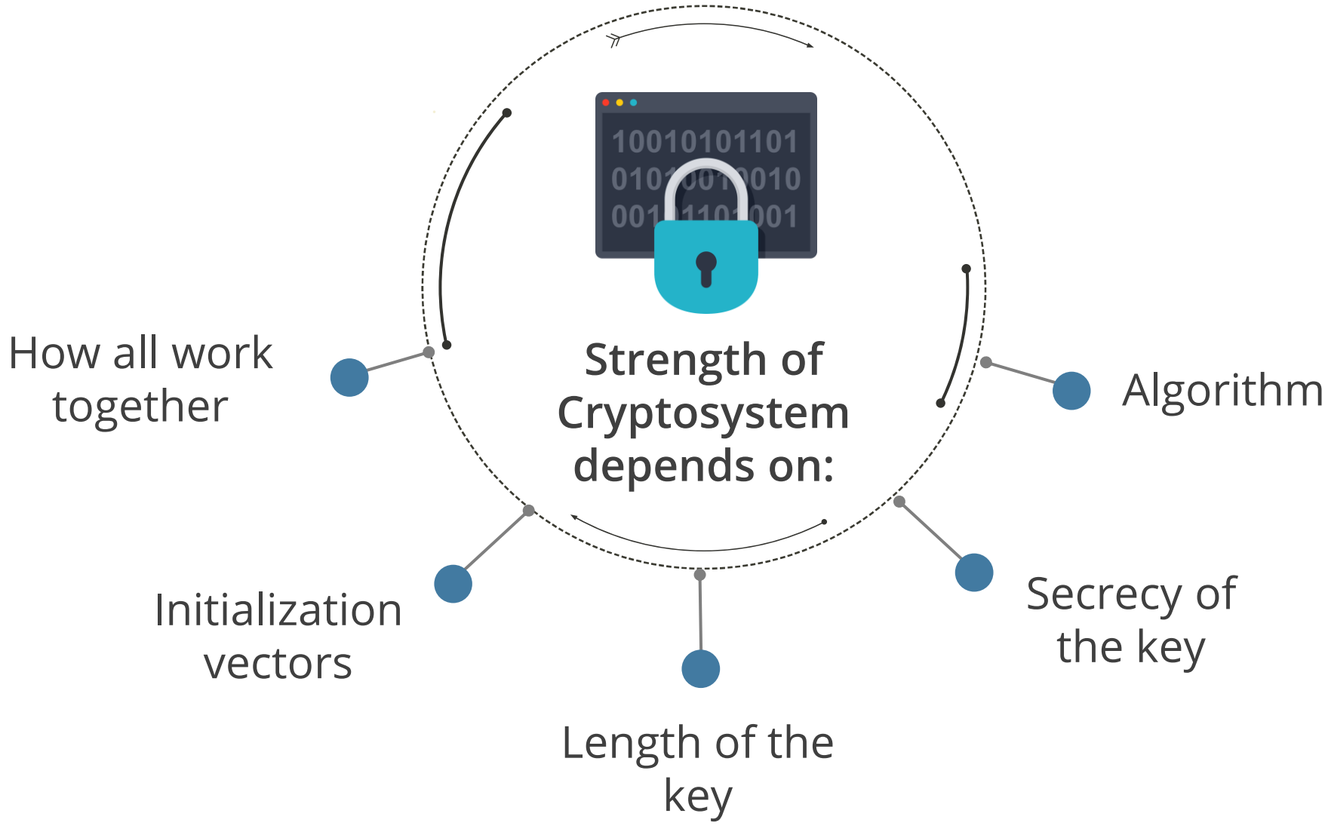


Strength of Cryptosystem

Work factor is an estimate of the effort and resources it would take an attacker to penetrate a cryptosystem.

- A good cryptosystem should be cost-efficient and less time-consuming.
- A brute force attack is used to break a cryptosystem.

Strength of Cryptosystem



Cryptosystem Elements

- Use an algorithm without flaws
- Use a large key size
- Use all possible values within the key space as randomly as possible
- Protect the actual key

Cryptosystem Services

Cryptosystem services ensure:

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

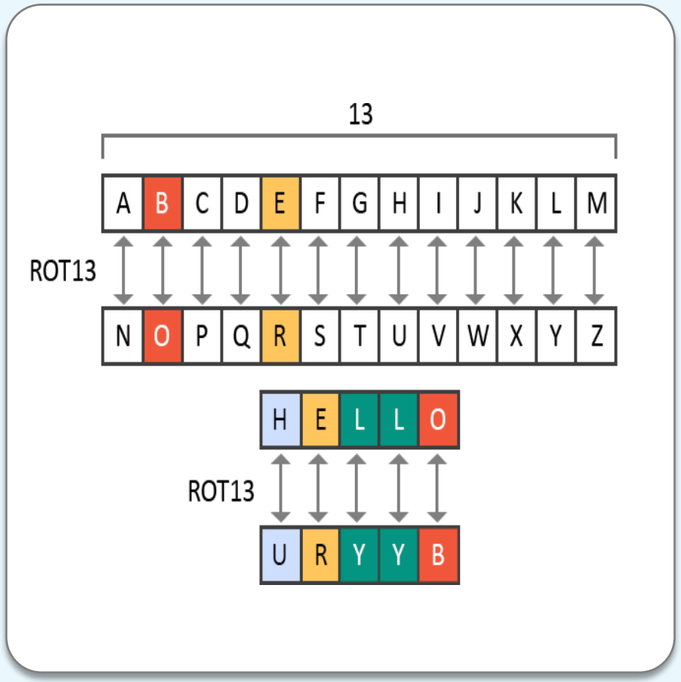
Verifies the identity of the user or the system that created the information

Nonrepudiation

Ensures that the sender cannot deny sending the message

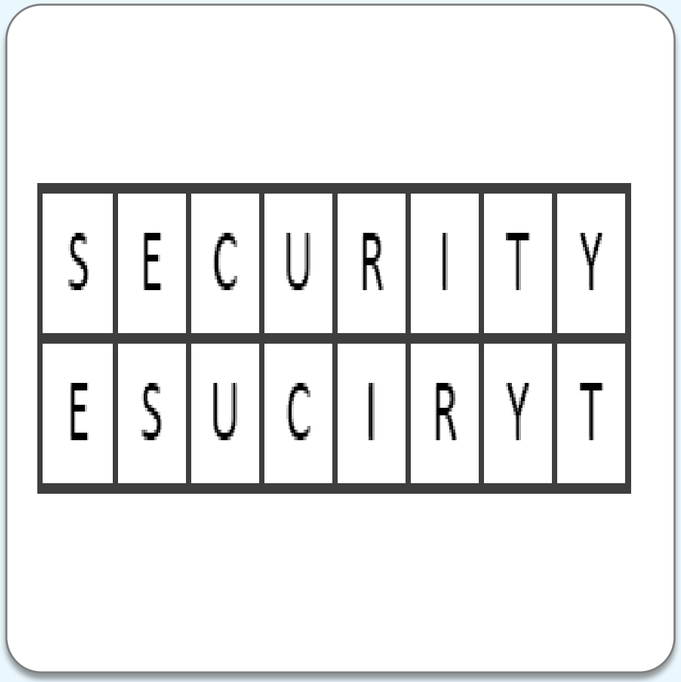
Cryptography Methods: Substitution Cipher

- It works by substituting one letter for another letter based on a key.
- Example: Caesar cipher or ROT13 in which the alphabet is rotated by 13 steps.
- The message **HELLO** becomes **URYYB** after ROT13 substitution.
- Substitution Cipher is generally used on blogs to filter certain words and in combination with other ciphers.



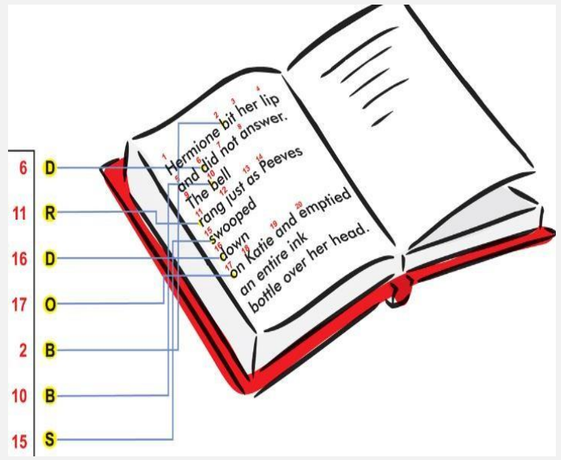
Cryptography Methods: Transposition Cipher

- Transposes the original text with long sequences of complex substitutions and permutations
- Uses a key to determine positions the characters are moved to
- Is used in combination with substitution cipher in standard ciphers



Cryptography Methods: Running Key Cipher

- It could use a key that does not require an electronic algorithm and bit alterations, but cleverly uses components in the physical world around you.
- For instance, the algorithm could be a set of books agreed upon by the sender and receiver. The key in this type of cipher could be a book page, line number, or column count.

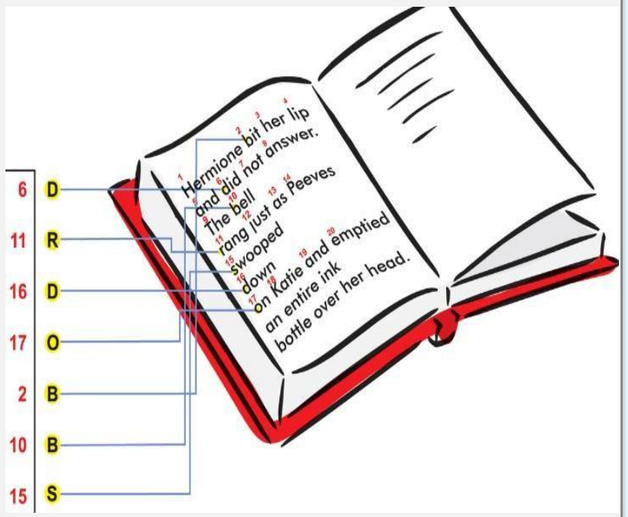


Cryptography Methods: Running Key Cipher

- For example, you get a message from your super-secret spy buddy and the message reads **CRYPTOGRAPHY 149l6c7.299l3c7.911l5c8**.
- This could mean for you to look at the 1st book in your predetermined series of books, the 49th page, the 6th line down the page, and the 7th column.

Cryptography Methods: Concealment or Null Cipher

- A concealment cipher is a message within a message. If your other super-secret spy buddy and you decide the key value is every third word, then when you get a message from him, you will pick out every third word and write it down.
- Example: Suppose he sends you a message that reads, **The saying, "The time is right" is not cow language, so is now a dead subject**.
- Because your key is every third word, you produce **The right cow is dead**.



Steganography

Steganography is the art of hiding the existence of a message.

- It is used to insert digital watermarks on images to identify illegal copies.
- It is used to send secret messages through emails.
- It involves concealing the very existence of data by hiding it in some other media such as a picture, audio, and video file.

XOR Function

XOR function 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

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

Mod Function

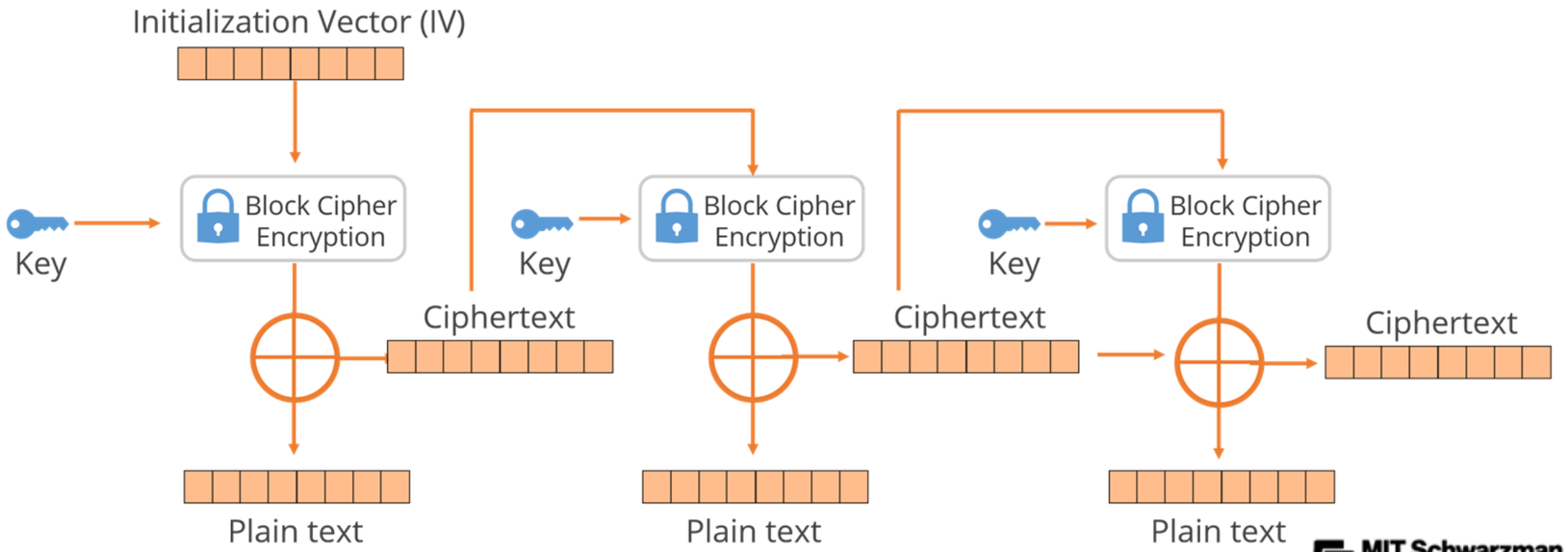
The modulo function is quite simply the remainder value left over after a division operation is performed.

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

The modulo function is just as important to cryptography as logical operations.

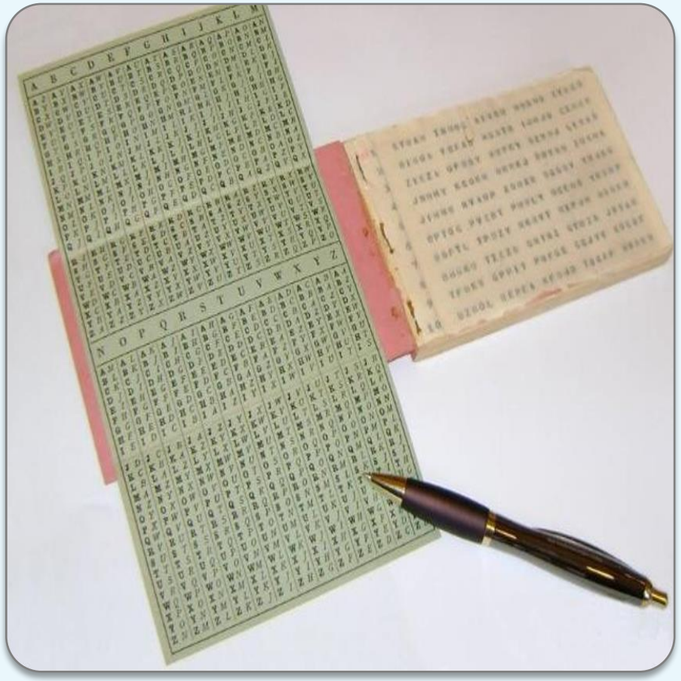
Initialization Vector(IV)

- Random values are used with algorithms to ensure patterns are not created during the encryption process.
- They are used with keys and need to be encrypted when being sent to the destination.
- If IVs are not used, then two identical plaintext values that are encrypted with the same key will create the same ciphertext.
- The IV and the key are both used by the algorithm to provide more randomness to the encryption process.



One-Time Pad

- Also known as Vernam Cipher
- Perfect encryption scheme
- Considered unbreakable if implemented properly
- Two copies of the pad (also known as the key) required to use a one-time pad
- A block of truly random data, which is at least as long as the message you wish to encode



One-Time Pad

This encryption process uses a binary mathematical function called Exclusive OR or XOR Secure Implementation:

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

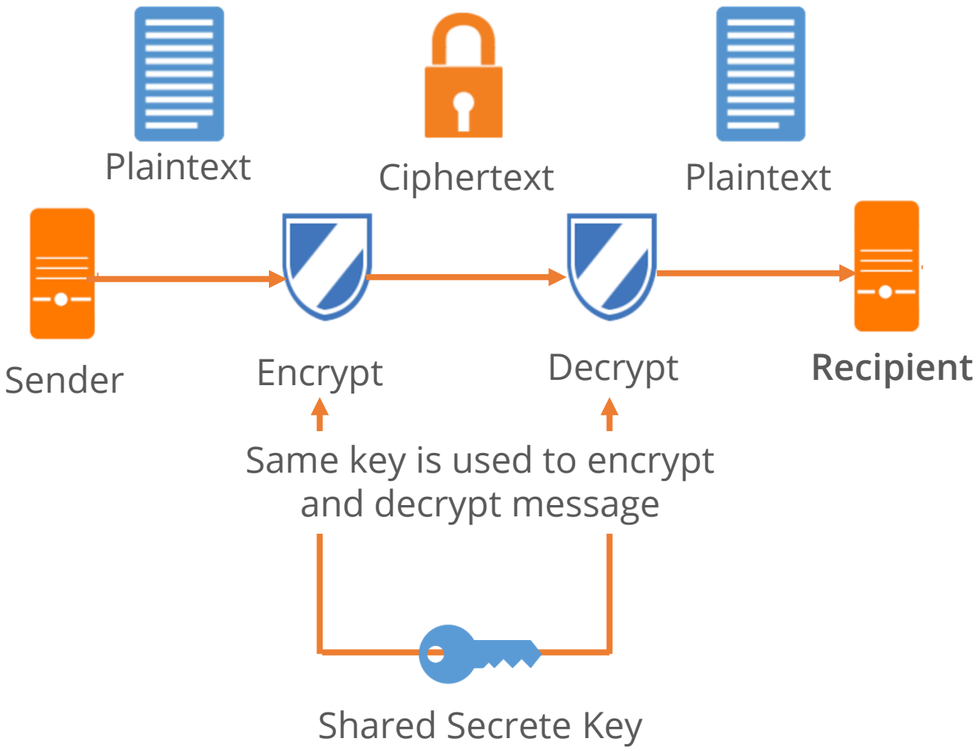
Encryption Methods

Symmetric Key Algorithm

Asymmetric Key Algorithm

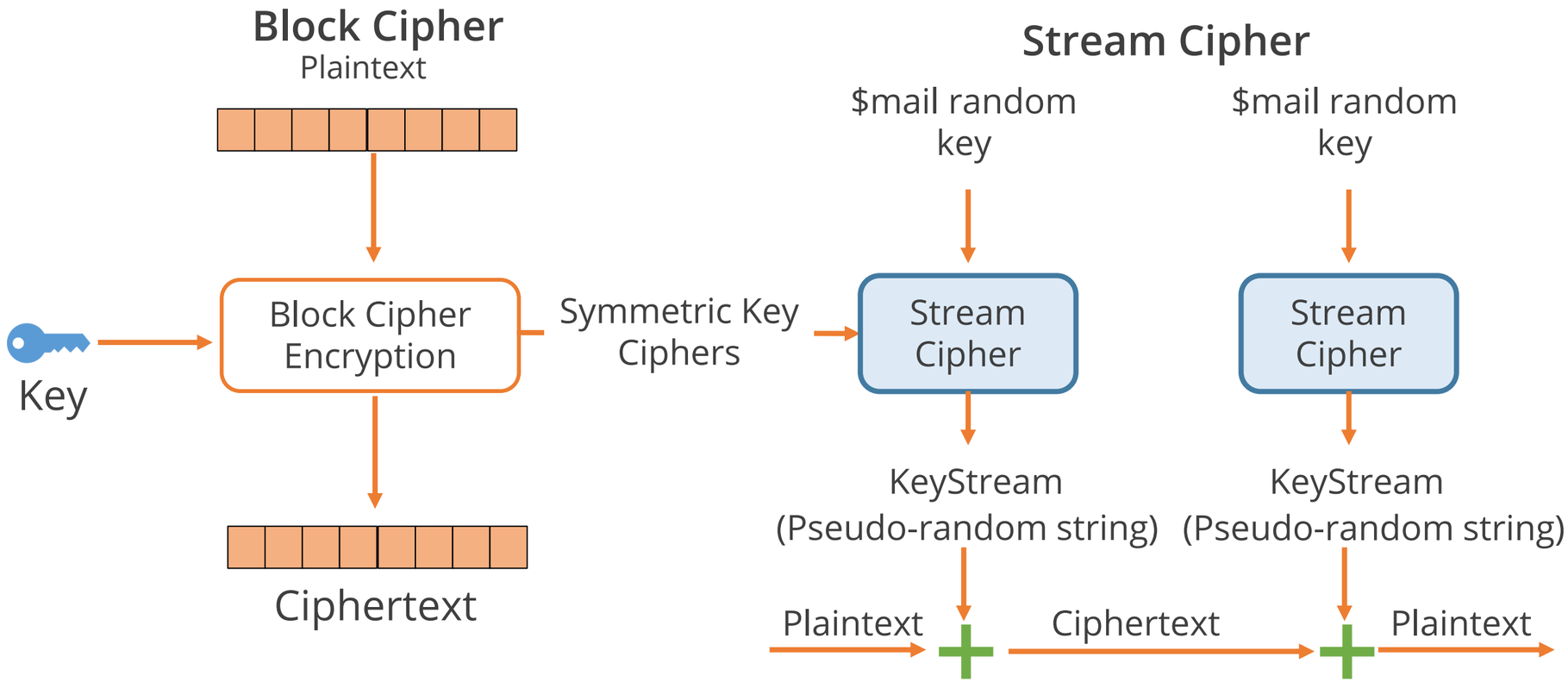
Introduction to Symmetric Cryptography

- Both encryption and decryption of a message performed using only a single cryptographic key
- Each pair of communicating users must have a copy of the key
- Can provide confidentiality because of the same key, but not authenticity or non-repudiation
- Used to send secret messages where confidentiality is the main criterion
- Used in wired and wireless networks
- Number of keys = n(n-1)/2
- Keys must be securely shared between communicating parties
- Examples: Blowfish, AES, IDEA, RC4, RC5, RC6, DES, and 3DES.



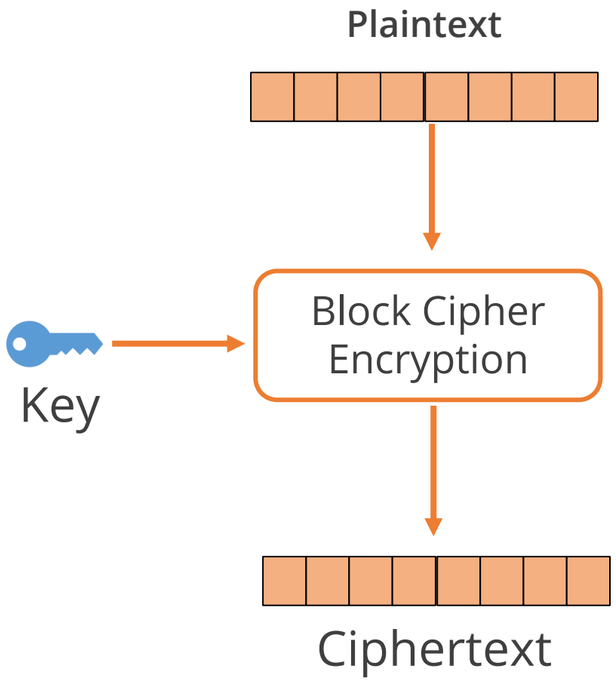
Symmetric Key Ciphers

The two primary types of symmetric key ciphers are:



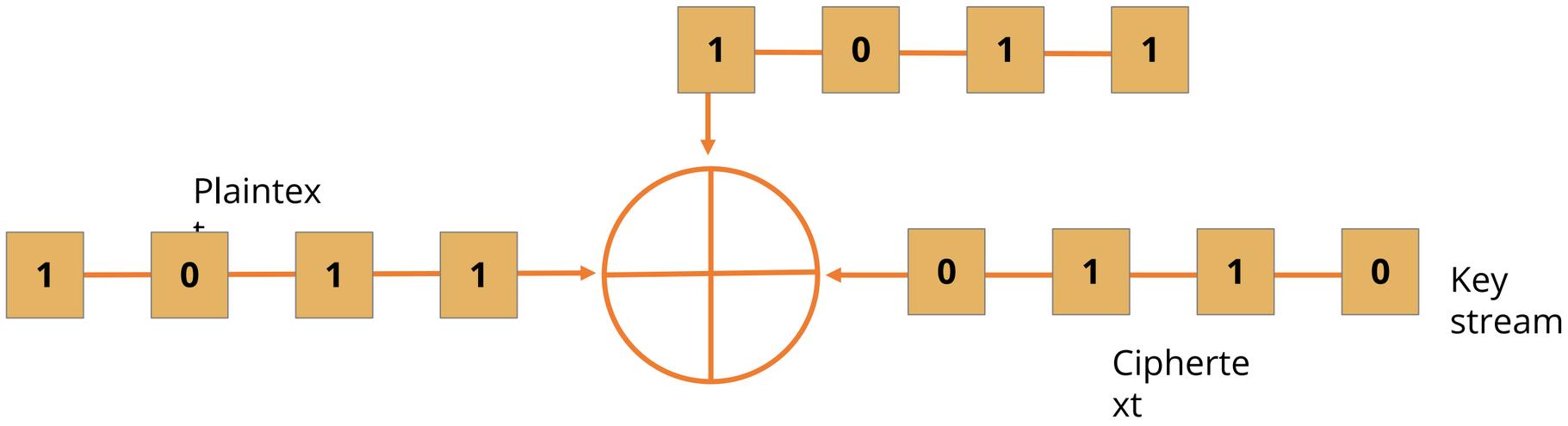
Block Cipher

- Converts a fixed-length block of plaintext data to a block of ciphertext data of the same length
- Text is operated on preset blocks (64,128,192 bits, etc.)
- A combination of substitution and transposition is used
- Although stronger than stream-based ciphers, it is more expensive and computationally more exhaustive
- Mainly implemented in software
- Used in ciphers like DES and AES



Stream Cipher

- A stream of ciphertext data is generated by combining the keystream (sequence of bits) with plaintext data bit by bit using XOR operations
- To ensure security, keystream must have a non-repeating pattern of bits
- Mainly implemented in hardware
- Most common in voice or video



Stream Cipher

- Can encrypt and decrypt more quickly
- Can scale better within increased bandwidth requirements
- Used when real-time applications, such as VoIP or multimedia, are encrypted
- Considered less secure than block ciphers
- Requires a lot of randomness and encrypts individual bits at times
- Requires more processing power than block ciphers
- Difficult to generate a truly random and unbiased keystream

Stream Cipher vs. Block Cipher

Stream Cipher

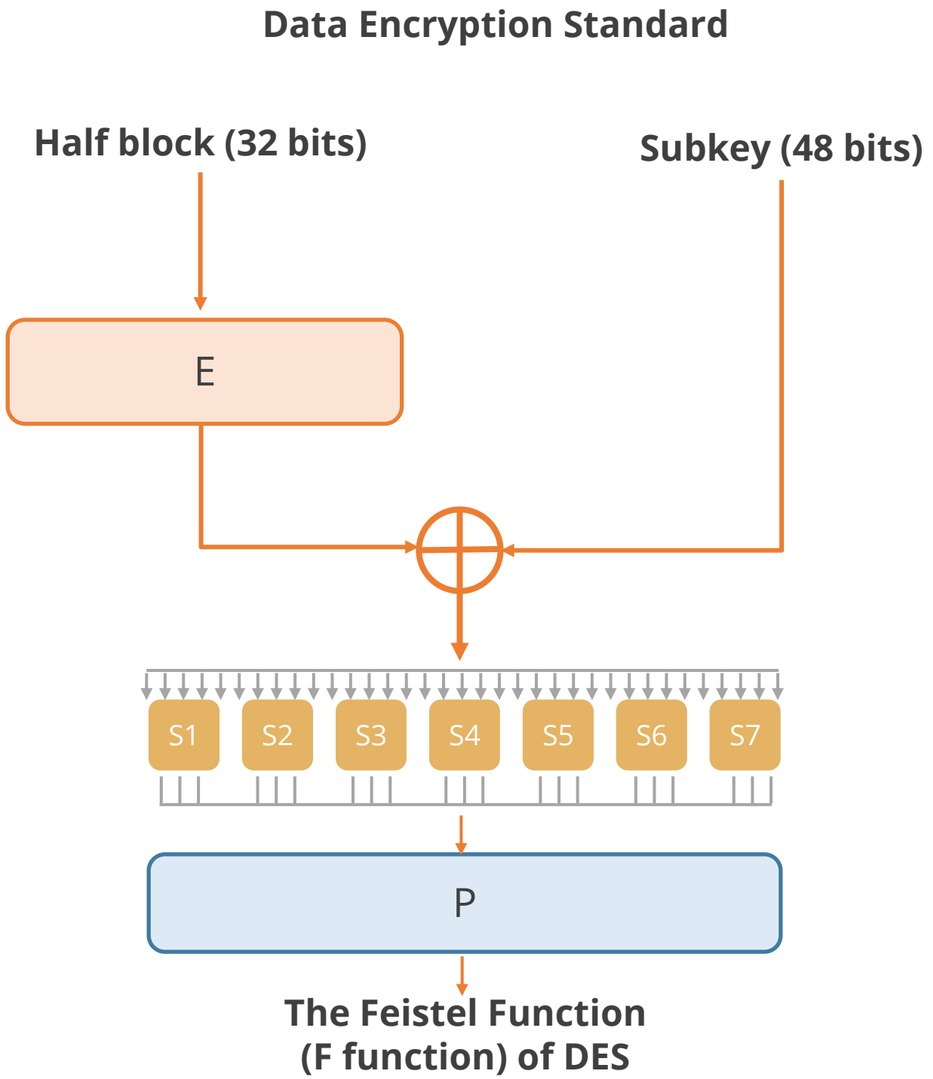
- Faster than block cipher
- Processes the input element continuously producing output, one element at a time
- Requires less code
- With steam cipher, keys can be used only one time
- Application: SSL (Secure connection on Web)
- Easier to implement in hardware

Block Cipher

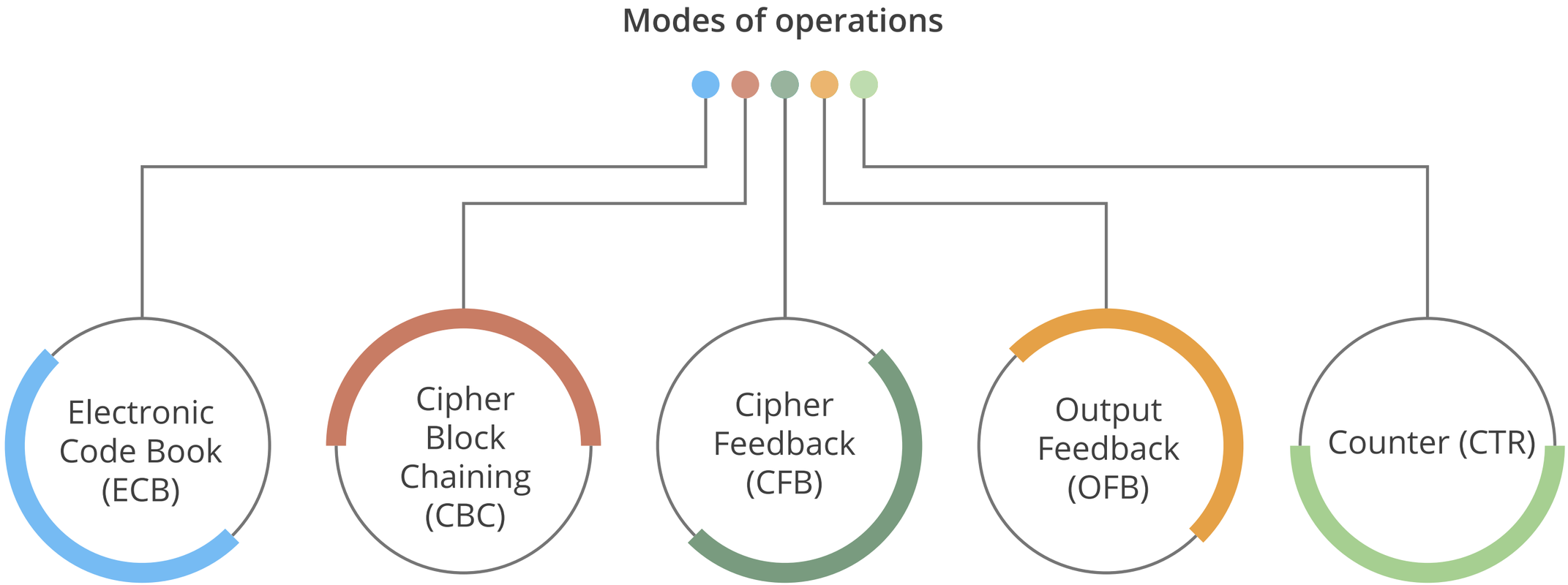
- Operates on larger block of data
- Slower than stream cipher
- Processes one block at a time, producing output for each input block
- Requires more code
- Reuse of key is possible
- Example: DES encryption
- Application: Database, file encryption
- Easier to implement in software

Data Encryption Standard (DES)

- Based on symmetric-key cryptosystem
- Is a block encryption algorithm with fixed sized 64-bit blocks
- Uses a 56-bits key (plus 8-bits of parity)
- Uses 16 rounds of transposition and substitution
- No longer considered strong enough

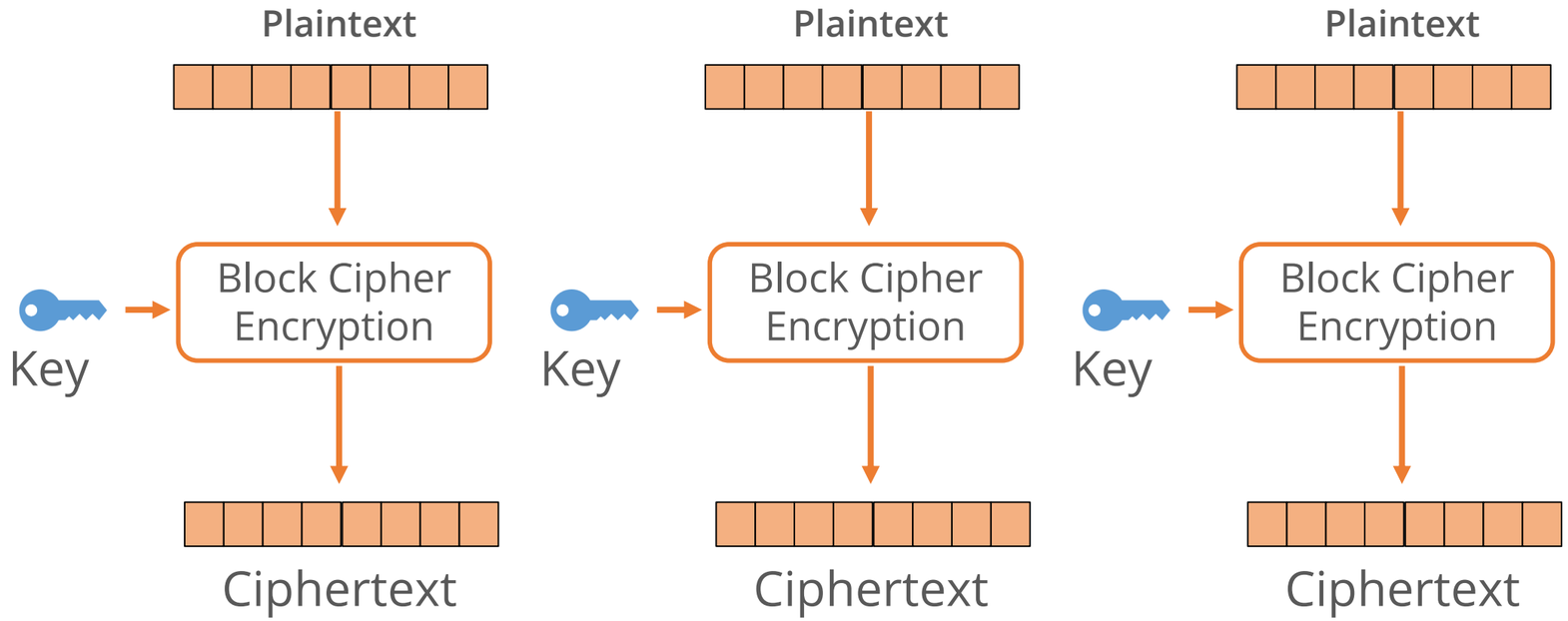


Data Encryption Standard (DES) Modes



DES Operation Modes: Electronic Code Book

- Simplest and the weakest form of DES
- Message is broken into independent (64-bit) blocks which are encrypted
- Each block is encoded independently of the other blocks (No Chaining)
- Operations can be run in parallel, which decreases processing time
- Errors are contained
- Useable only for shorter messages



DES Operation Modes: Electronic Code Book

Cannot carry out preprocessing functions before receiving plain text

Involves generation of identical ciphertext by identical plaintexts and keys

Susceptible to known plaintext attacks

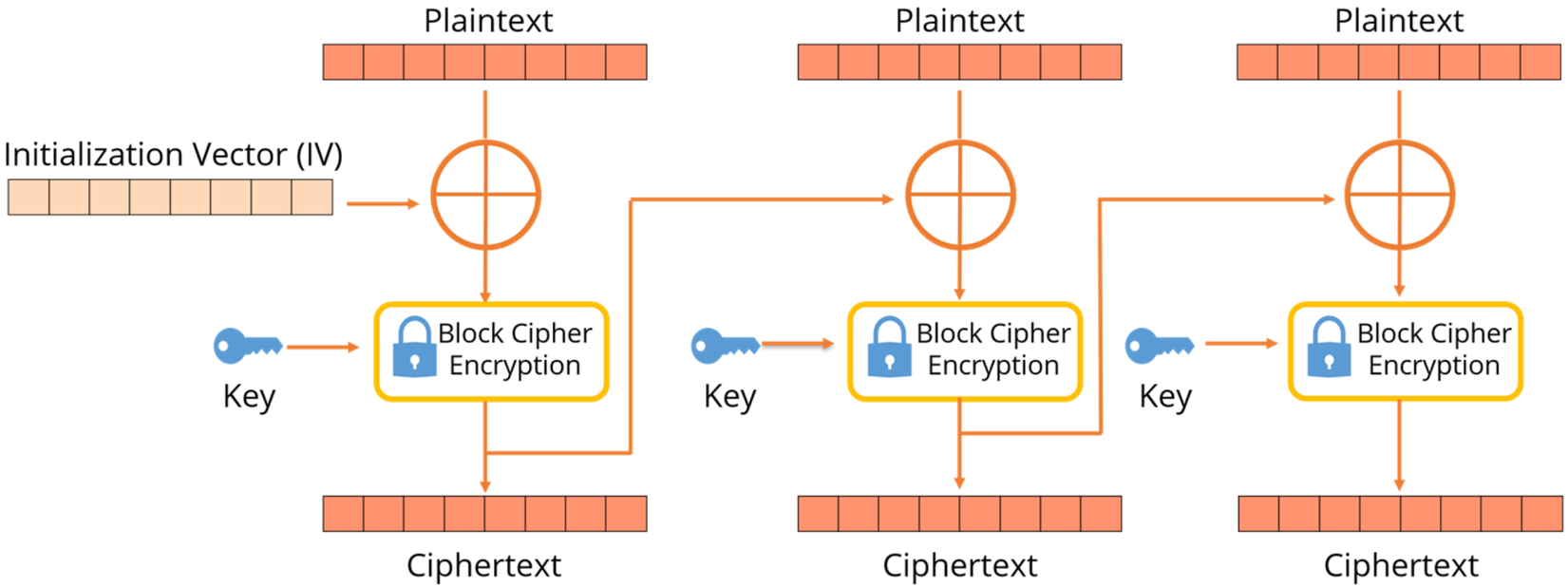
Fast and easy

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 is the same

DES Operation Modes: Cipher Block Chaining

- Stronger than ECB and solves security deficiencies in ECB
- Uses an IV (initialization vector) to add some randomness to encryption
- Previous ciphertext becomes IV for the next block using a chaining function
- Uses 64-bit plaintext blocks which are XORed with 64-bit IV



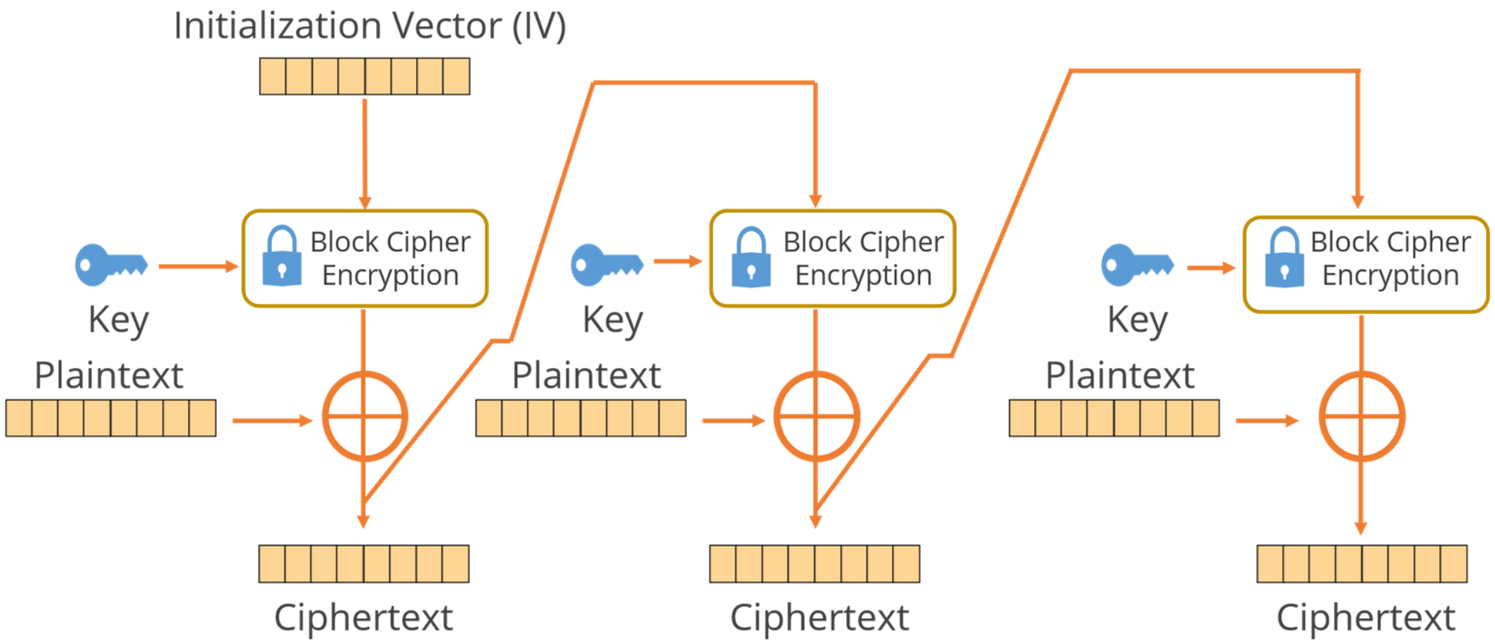
Cipher Block Chaining (CBC) mode encryption

DES Operation Modes: Cipher Block Chaining

- Repeats same plaintext block result in different ciphertext block
- Each previous cipher block should be chained to be in input with the current plaintext block
- Repeated plaintext blocks are encrypted differently since the encryption of a block depends on the current and all blocks before it
- Uses bulk encryption

DES Operation Modes: Cipher Feedback

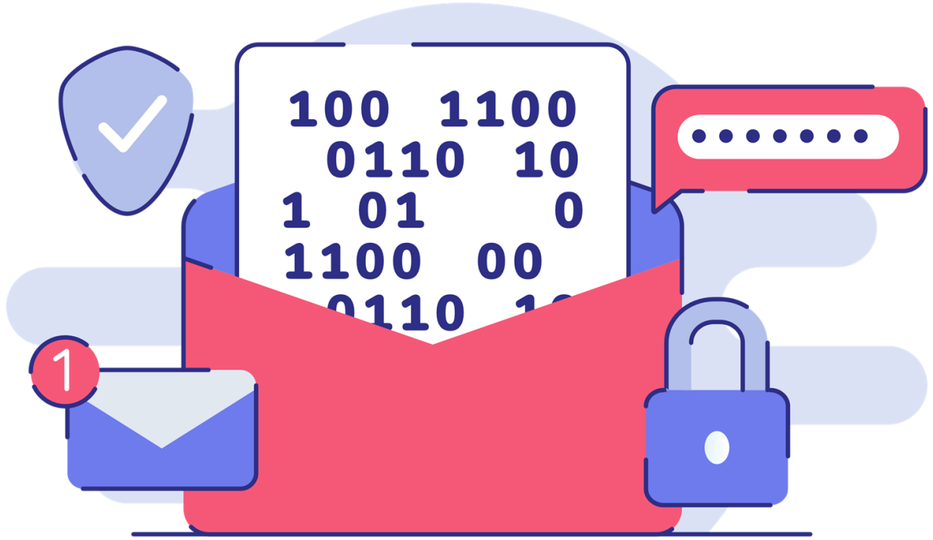
- The plaintext is divided into 1, 8, 64, or 128-bit segments (the four sub-modes of CFB).
- Block cipher is used as a stream cipher.
  - Can encrypt any number of bits. For example, single bits or single characters (bytes)
  - S=1: bitstream cipher
  - S=8: character stream cipher



Cipher Feedback (CFB) mode encryption

DES Operation Modes: 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 uses stream data encryption and authentication.

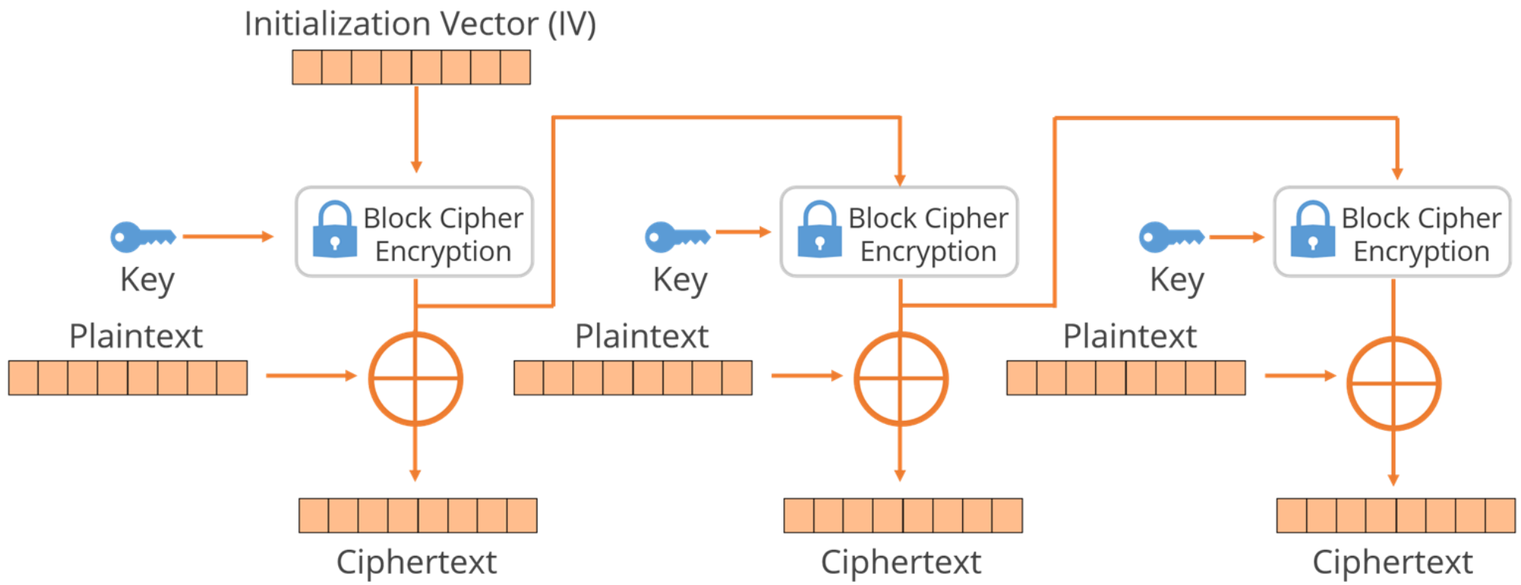


DES Operation Modes: Output Feedback

- Encrypted keystream of the previous block is fed to the next block to create the next portion of the keystream.
- It is very similar to CFB.
- The block cipher is used as a stream cipher.
- OFB is appropriate when data arrives in bits or bytes and when error propagation is not accepted.
- The keystream needs to be of the same size as the block of plaintext.

DES Operation Modes: Output Feedback

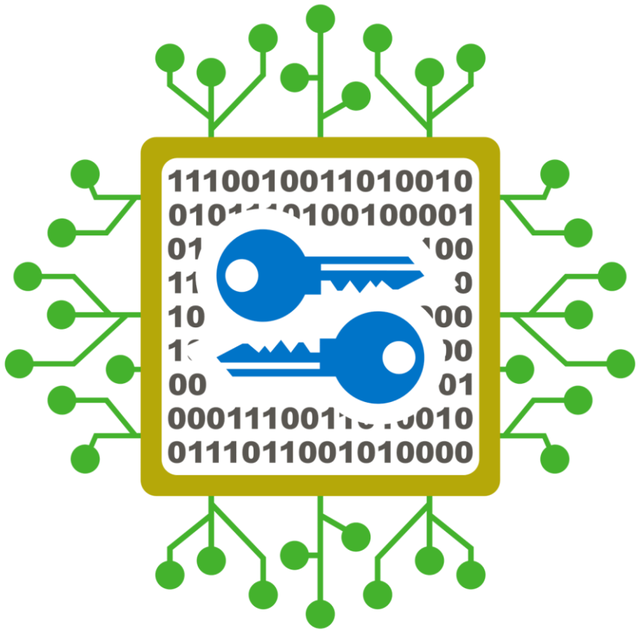
- **Advantages**:
  - More resistant to transmission errors; a bit error in a ciphertext segment affects only the decryption of that segment
  - IV should be generated randomly each time and sent with the ciphertext
- **Uses**:
  - Stream encryption over noisy channels (digital video and audio signals)



Output Feedback (OFB) mode encryption

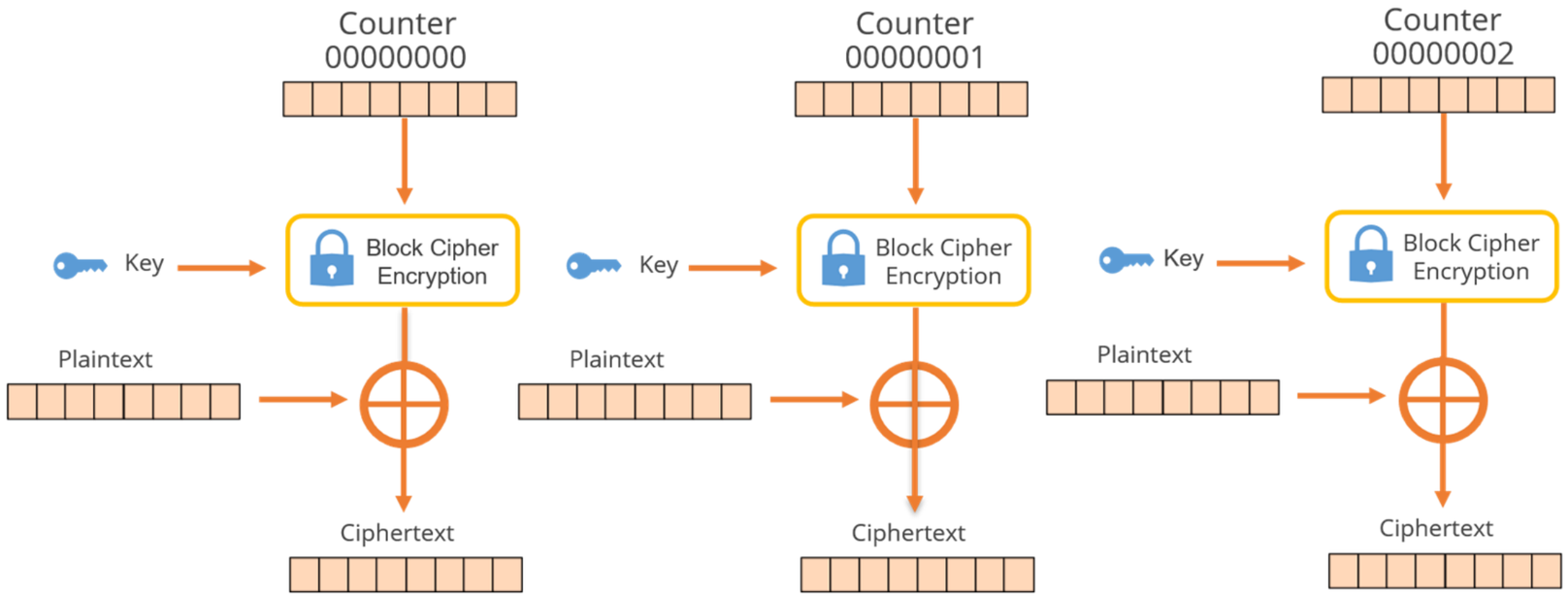
DES Operation Modes: Counter

- Counter 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.
- Counter for each plaintext will be different.
- IV and key are encrypted; the quantity is then XORed with each plaintext block or ciphertext block.
- Like stream cipher, the encrypted CTR values generate a keystream, which is then XORed with the message stream.
- The counter must be unknown and unpredictable.
- The counter can be any function that produces a sequence that is guaranteed not to repeat for a long time.



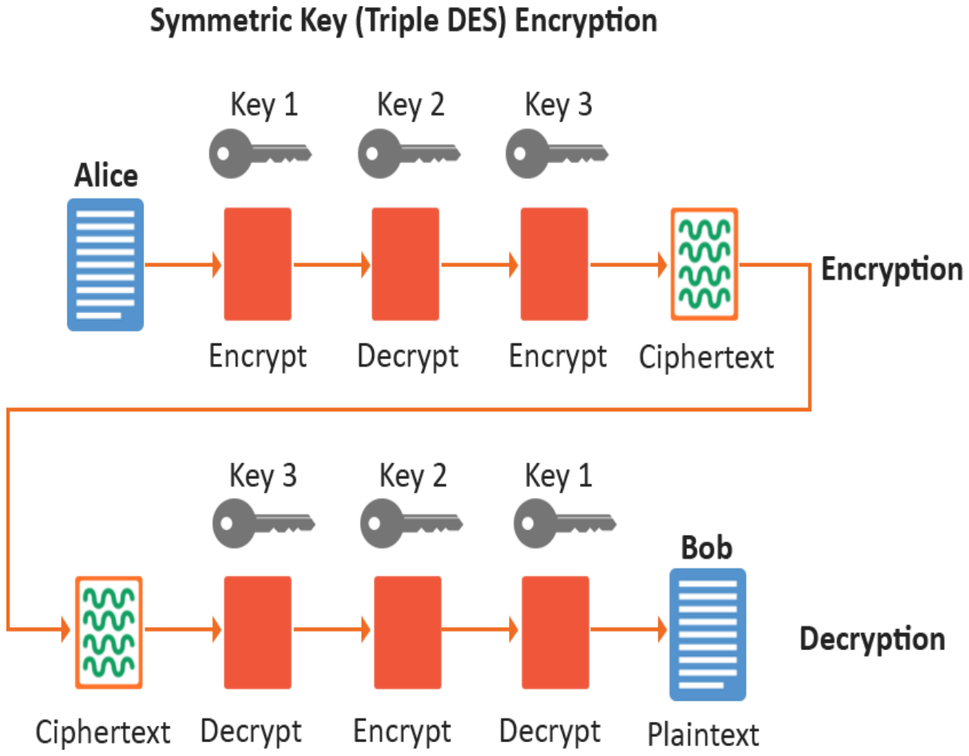
DES Operation Modes: Counter

- **Strengths**:
  - Needs only the encryption algorithm
  - Random access to encrypted data blocks
  - Blocks can be processed (encrypted or decrypted) in parallel
  - Simple and fast encryption or decryption
- **Uses**: High-speed network encryptions, encrypting ATM cells, IPSec, and Wireless 802.11i



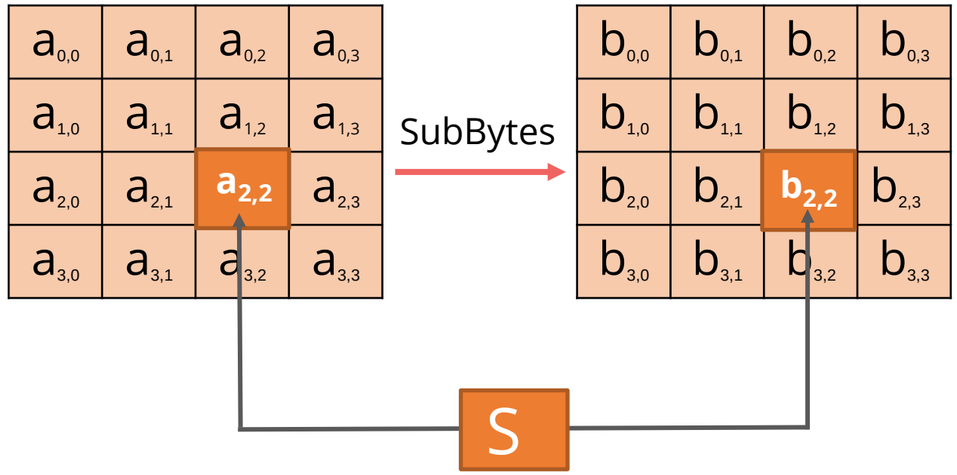
Triple DES

- Uses three 56-bit keys instead of one and uses 48 rounds of transposition and substitution (instead of 16)
- Approximately 256 times stronger than DES
- Used in secure electronic transmission of data
- Can be configured for use in VPN connectivity (example: IPsec)



Advanced Encryption Standard (AES)

- Advanced Encryption Standard (AES) is a symmetric block cipher.
- AES is the current U.S. standard.
- For encryption it uses:
  - 128-bit keys (10 rounds of encryption)
  - 192-bit keys (12 rounds of encryption) or
  - 256-bit keys (14 rounds of encryption)
- AES 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

- Stands for International Data Encryption Algorithm
- Uses 64-bit blocks, 128-bit key, and 8 rounds of computation
- Used in e-mail encryption software, pretty good privacy (PGP)

Blowfish

- Uses 64-bit block size
  - 32 – 448 bits (in steps of 8 bits) key size and 16 rounds of computation
- Optimized for 32-bit micro-processors

Twofish

- Is a modification of Blowfish using 128-bit blocks
- Uses variable key length up to 256 bits

Other Symmetric Systems

RC5

- Uses block sizes of 32, 64, or 128-bits, with key length up to 2040-bits
- Created as a candidate algorithm for AES

RC6

- Uses key size of 128, 192, and 256-bits and has a block size of-128 bits
- 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	• 8 rounds transposition and substitution • Used in PGP
CAST	64 bit	40 to 128 bits	
SAFER	64 to 128 bit	64 to 128 bit	A version 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	

Business Scenario

Hilda Jacobs who is the general manager, IT Security, assigned Kevin Butler the task of selecting a good encryption system to secure the confidentiality of the company's data. She had asked for a symmetric block cipher system that can encrypt using a 128-bit encryption key.

Kevin started gathering information about the existing encryption standards. Based on the current and the future requirements, he had to choose between DES, 3DES, and AES.

Question: Which encryption standard should Kevin select, the DES, the 3DES, or the AES?

Business Scenario

Hilda Jacobs who is the general manager, IT Security, assigned Kevin Butler the task of selecting a good encryption system to secure the confidentiality of the company's data. She had asked for a symmetric block cipher system that can encrypt using a 128-bit encryption key.

Kevin started gathering information about the existing encryption standards. Based on the current and the future requirements, he had to choose between DES, 3DES, and AES.

Question: Which encryption standard should Kevin select, the DES, the 3DES, or the AES?

Answer: With the given requirement, AES is the best choice as it supports a 128-bit key.

Introduction to Asymmetric Cryptography

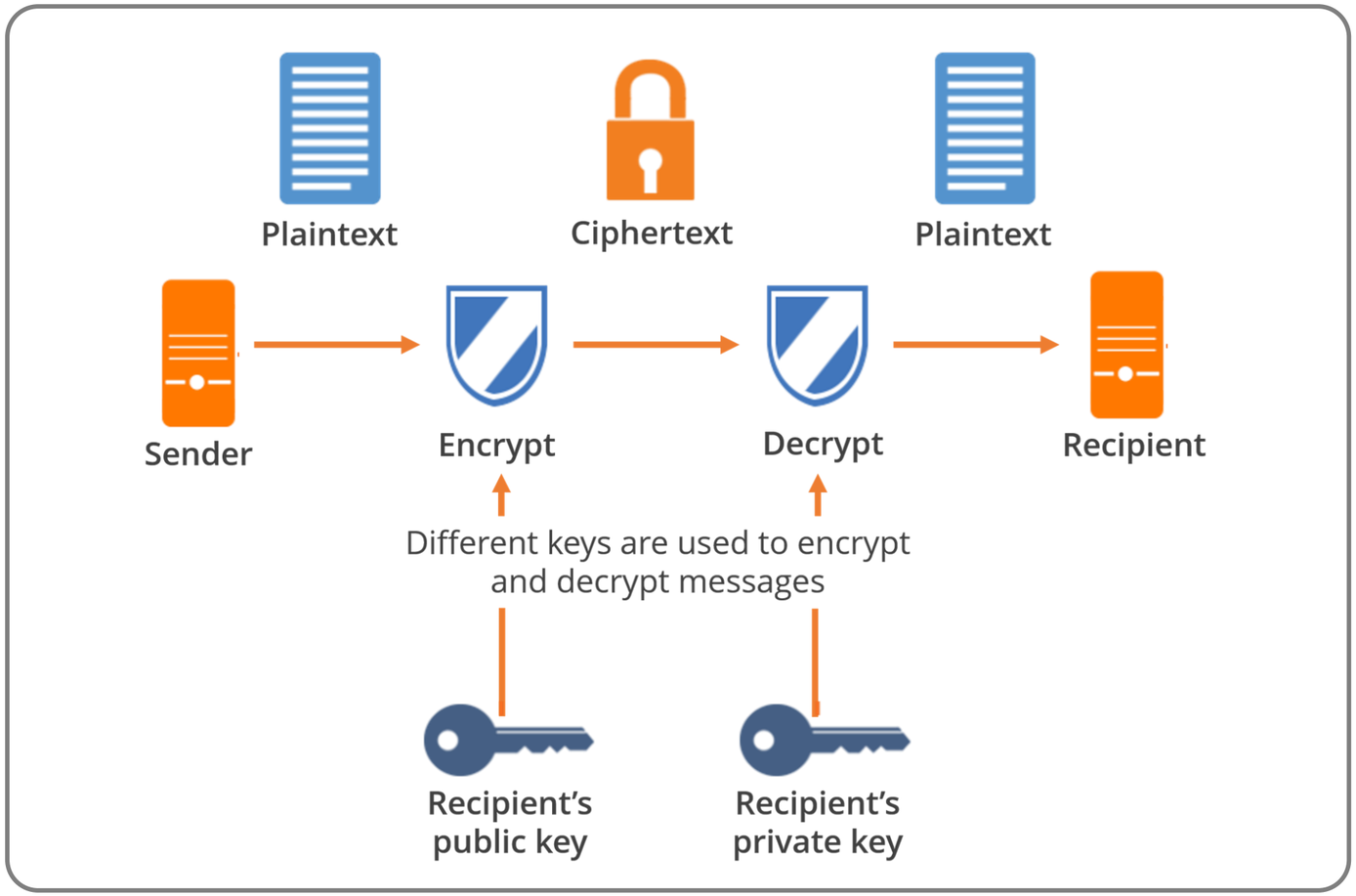
In asymmetric cryptography, two keys are used that are linked mathematically but are mutually exclusive. One key is for encryption, and the other is for decryption.

Introduction to Asymmetric Cryptography

- Asymmetric cryptography is also called public-key encryption as one key is made public.
- A pair of keys is required for encryption or decryption.
- The keys are mathematically related.
- Each key is used to encrypt or decrypt.
- You cannot encrypt or decrypt with only one key.
- The public key is usually shared, while the private key is secured by the owner.
- **Secure Message format:** The message is encrypted with the receiver's public key (confidentiality).
- **Open Message format:** The message is encrypted with the sender’s private key (authenticity).
  - This provides authenticity, integrity, and non-repudiation.
  - Examples: RSA, Diffie-Hellman, Elliptic curve cryptosystem (ECC), El Gamal, and Digital signature algorithm (DSA).

Introduction to Asymmetric Cryptography

Working of asymmetric cryptography is illustrated below:



Introduction to RSA Algorithm

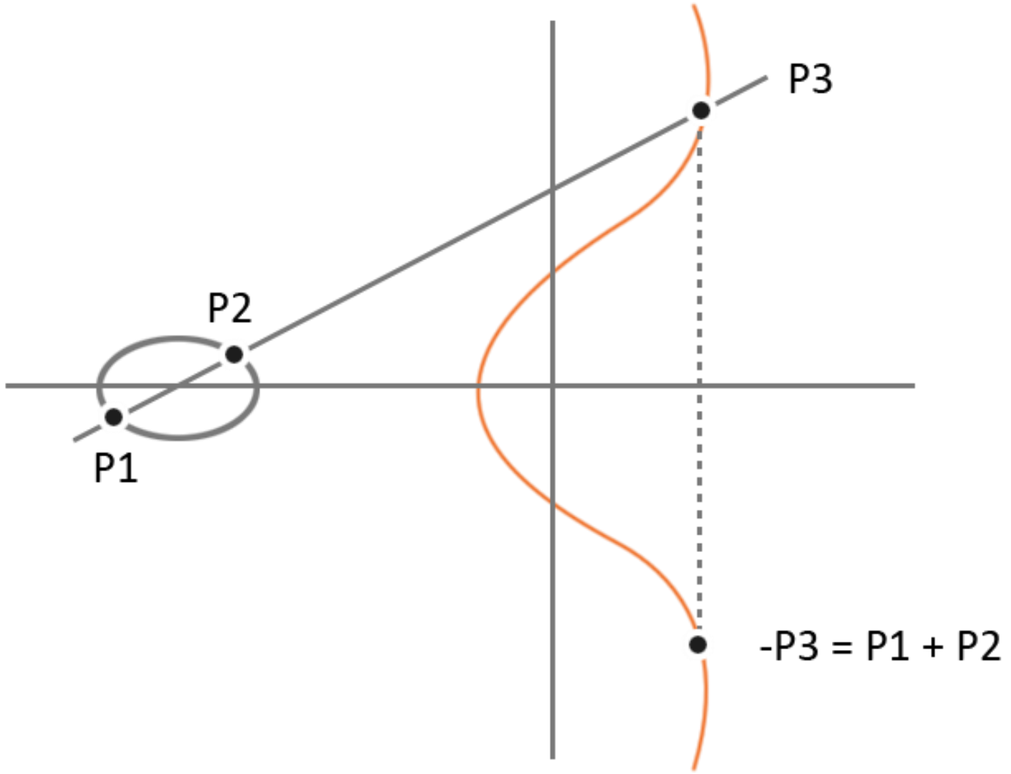
RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of this algorithm.

RSA:

- Is a worldwide de facto standard
- Provides digital signatures, encryption, and secret key distribution
- Is based on the fact that factoring the two large prime numbers' (up to 200 digits long) product forms is difficult; hence, difficult to crack the cryptosystem
- Used in web browsers with SSL, systems that use public-key cryptosystems

Other Types of Asymmetric Cryptography: Elliptic Curve Cryptosystems

- Instead of generating keys as the product of very large prime numbers, ECC generates keys through the properties of the elliptic curve equation.
- An ECC key of 160 bits provides the same protection as a 1024-bit RSA key.
- ECC 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



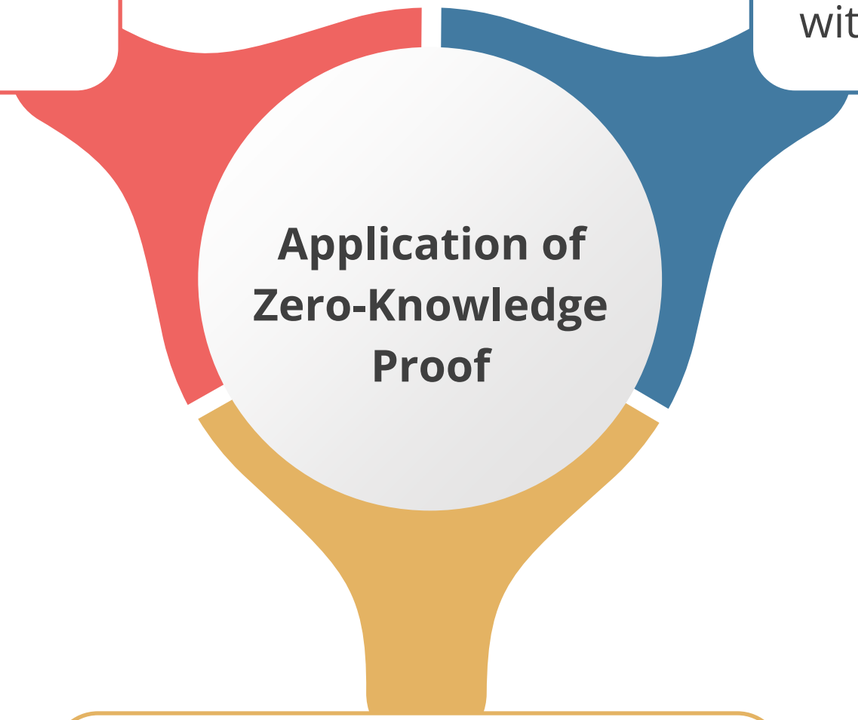
Zero-Knowledge Proof

- Zero-knowledge proof is applicable in public-key cryptography.
- It means someone can tell you something that you can trust without telling you more information that you need.
- For example, you trust 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

Ownership:
Proves that you own a private key

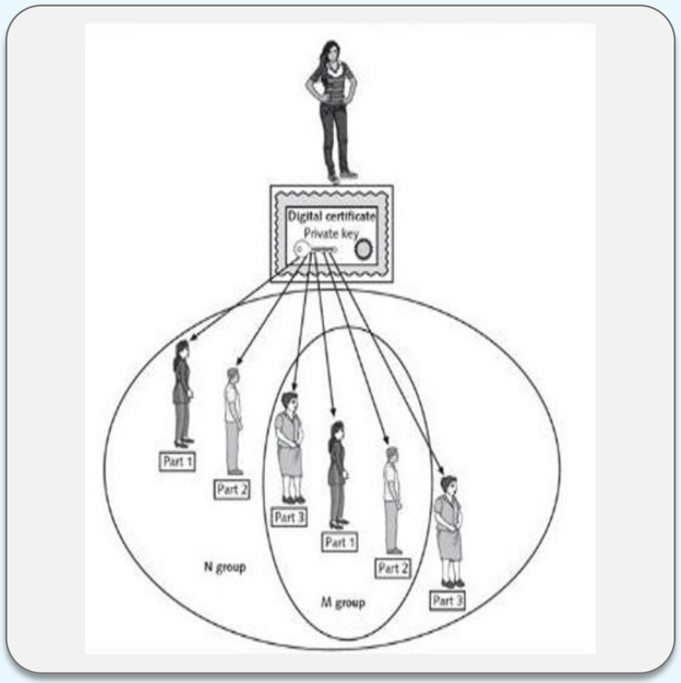
Membership:
Proves you are part of a group, without revealing your identity



Sealed Bid Auction:
Proves who won, without revealing bid

M of N Control

- M of N control requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks.
- This is a backup process of public and private key material over multiple systems or devices.



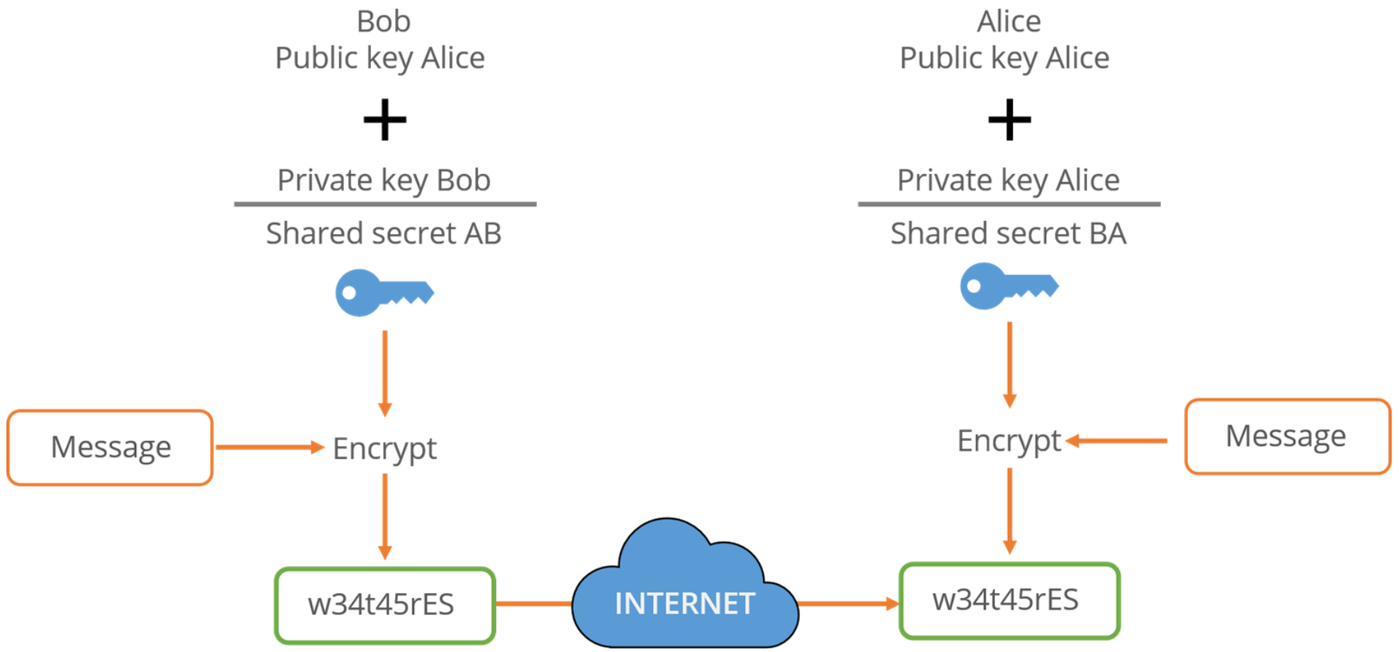
Source: https://slideplayer.com/slide/12293221/

M of N Control

- It’s a tool that prevents the recreation of private and public key material from the backup.
- The key materials are backed up and then mathematically distributed across several systems or devices.
- Implementing three of eight controls would require three people out of the eight with the assigned work task of key escrow recovery agent to work together to pull a single key out of the key escrow database (thereby also illustrating that M is always less than or equal to N).

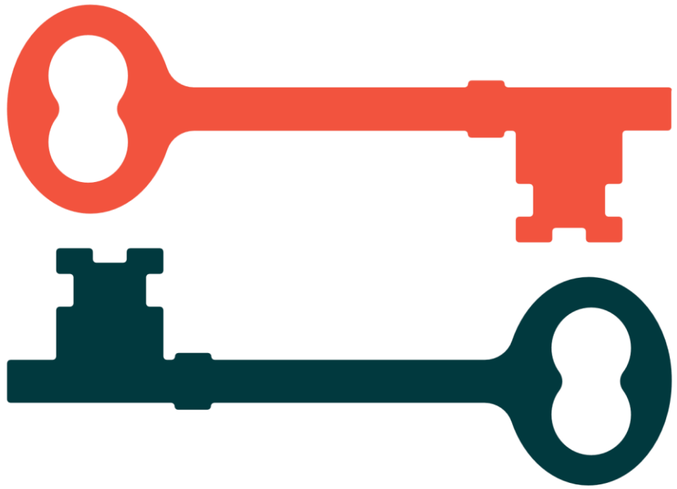
Other Types of Asymmetric Cryptography: Diffie-Hellman Key Exchange

- A key distribution asymmetric algorithm
  - A protocol whereby two or more parties can agree on a key in such a way that both influence the outcome
- Allows two users to exchange a secret key
- Requires no prior secrets
- Does not provide for encryption or digital signature functions



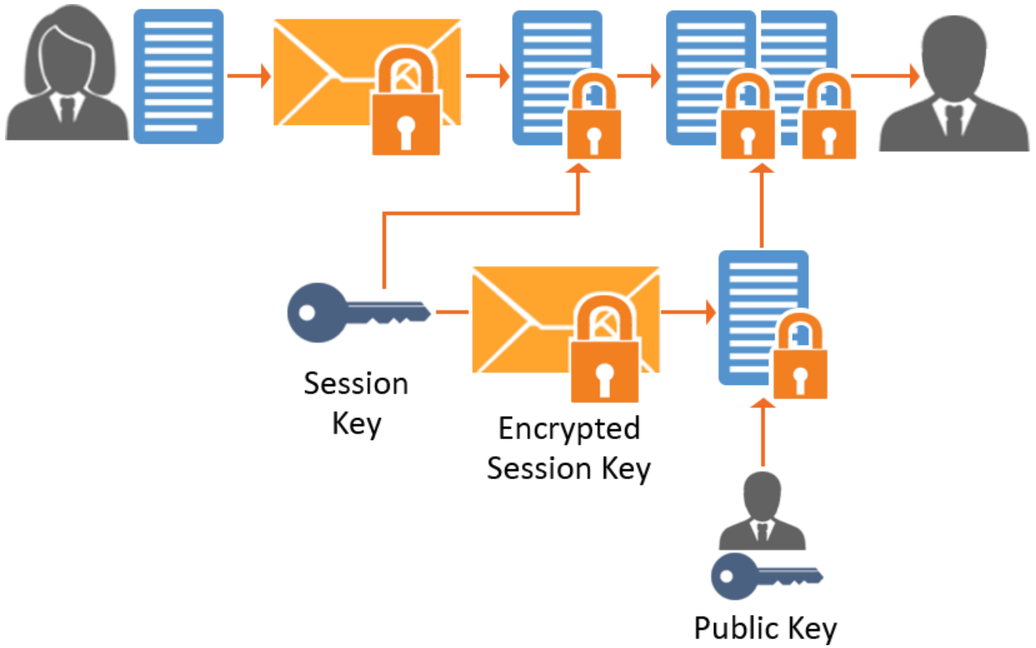
Other Types of Asymmetric Cryptography: Diffie-Hellman Key Exchange

- Vulnerable to man-in-the-middle attack
- Based on the difficulty of calculating discrete logarithms in a finite field
- 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 or Digital Envelope

- It is a hybrid system that combines the symmetric and asymmetric methods.
- The more efficient symmetric algorithm 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 or Digital Envelope

- The recipient uses his 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

- A single-use symmetric key is used to encrypt or decrypt communication between two users for a single session.
- It’s more secure than static symmetric keys.
- Here, peers decide on the session key and continue to use it till the session is over.
- Here, eavesdropping is difficult and breaking the keys will prove to be futile.

Symmetric vs. Asymmetric Cryptography

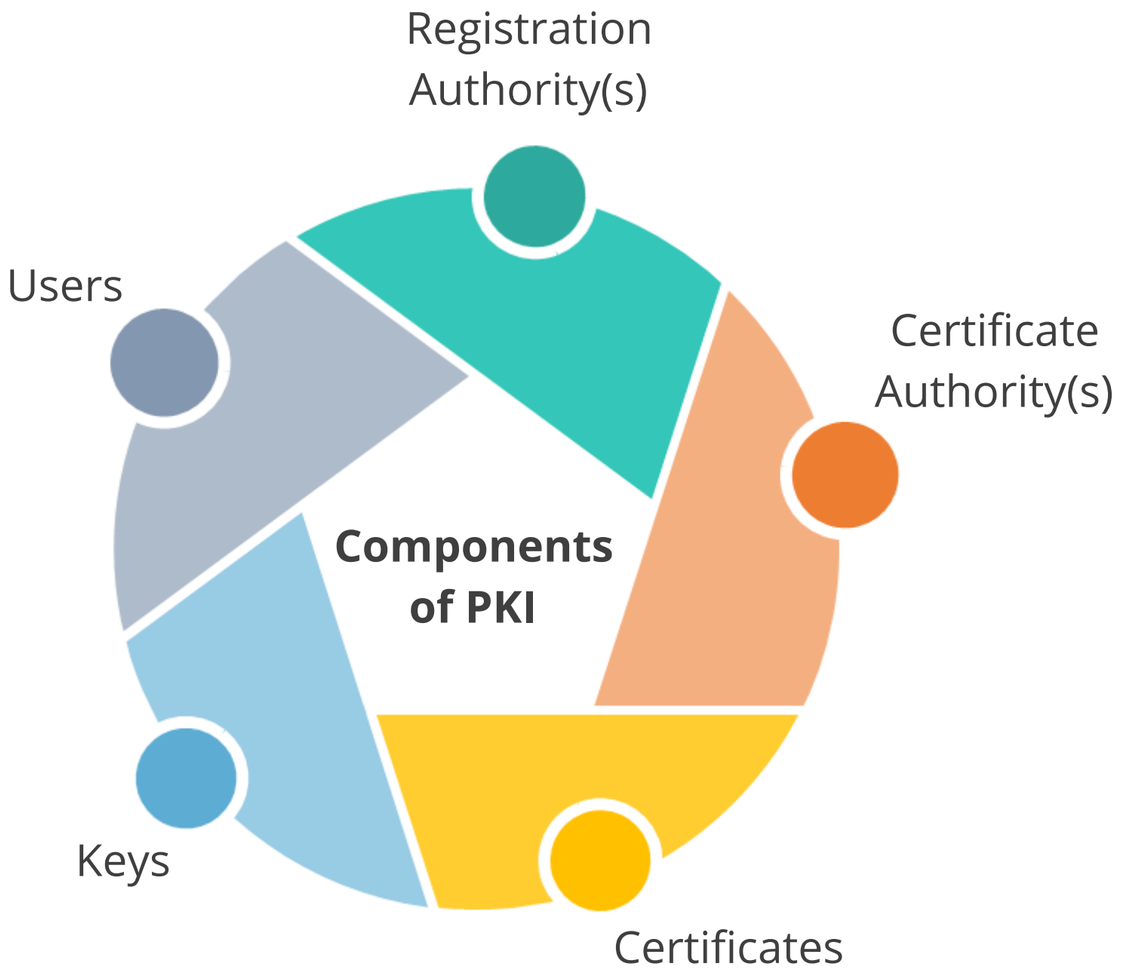
Symmetric Cryptography	Asymmetric Cryptography
Same key for encryption and decryption	A pair of keys, one for encryption and the other for decryption
Consumes less computing power	Consumes more computing power
Is much faster	Used to distribute the symmetric key as they are slower
Symmetric key is synonymous with secret key or session key	• Encryption key is called public key • Decryption key is called private or secret key • The asymmetric key refers to the public key or private 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	Provides: • Better key distribution than symmetric systems • Better scalability due to ease of key distribution • Authenticity and nonrepudiation, in addition to confidentiality and integrity	• Much slower operation than symmetric systems • Vulnerable to man-in-the-middle attacks

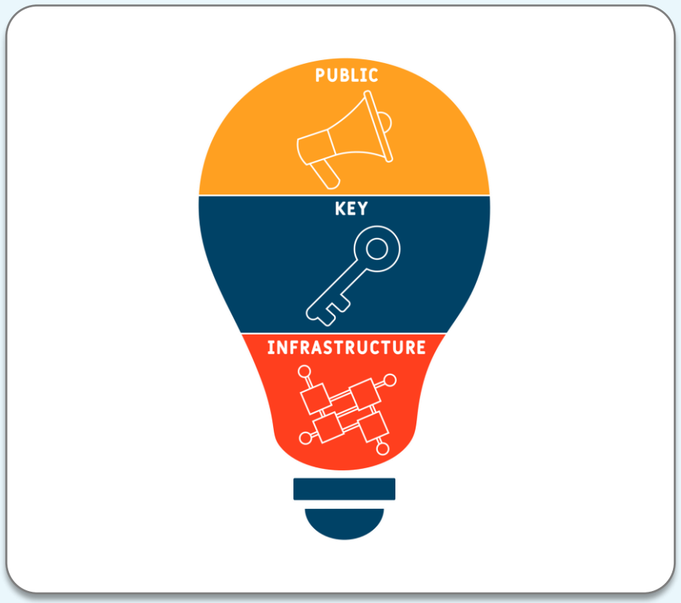
Introduction to Public Key Infrastructure

> "A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates."



Introduction to Public Key Infrastructure

- The public key infrastructure provides CIA and nonrepudiation.
- PKI 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 in a PKI, which contains a particular participant's public key and other identifying information.
- This is signed by a trusted certificate authority and the authenticity of the public key is the liability of the CA.
- PKI is used in online banking and e-commerce.



Certificate Authority and Registration Authority

- CA is a trusted third party responsible for the issuance and maintenance of digital certificates.
- It can also be internal to an organization.
- CA also handles the revocation of certificates.
- The revoked certificates are stored in the Certificate Revocation List (CRL) which is updated and maintained by the CA.

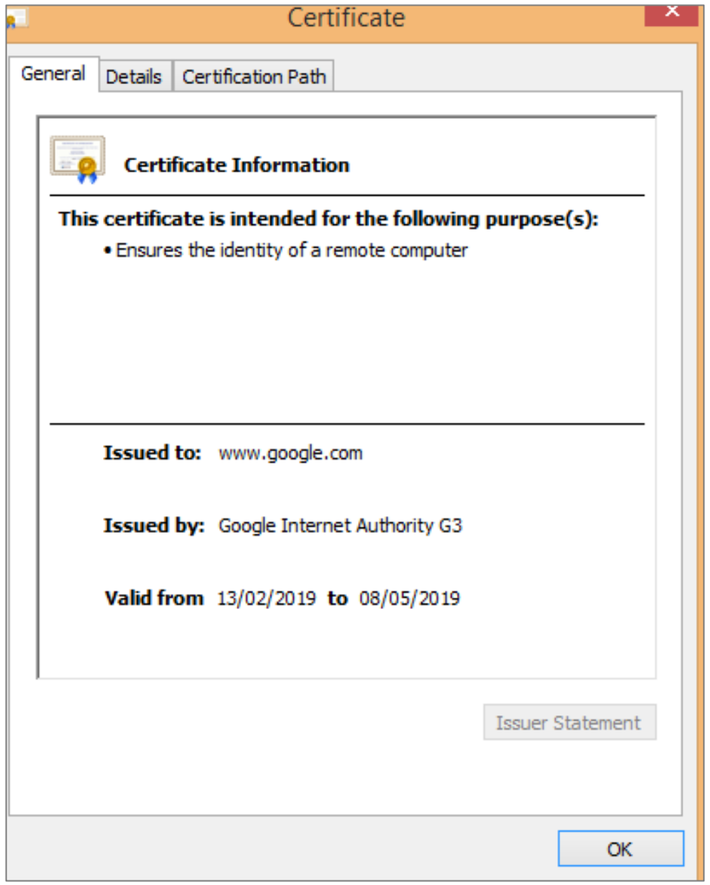
Certificate Authority and Registration Authority

- The RA performs the registration duties.
- It establishes and confirms the identity of the individual, initiates the registration process with CA, and performs certificate lifecycle management.
- The RA verifies all the necessary information before allowing a request to go to CA.
- The RA cannot issue certificates.

Registration Authority

PKI Certificate

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



Digital certificates are for sharing public keys to be used for encryption and authentication.

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

PKI Certificate

- Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate, and a digital signature of the public key created by the issuer of the certificate.
- X.509 is the standard that dictates the fields that are used in the certificate and the valid values that can be populated in the fields.

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

Enrollment Process

When a user wants to obtain a digital certificate, the user must first prove his identity to the CA in some manner. This process is called enrollment.

Enrollment Process

Steps of Enrollment Process:

Step 1

The user needs to prove his identity to obtain a digital certificate.

Step 2

The user seeking the certificate needs to provide its 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 he wishes to communicate, he must verify if:

The digital signature of the CA is authentic

The CA is trusted by the user

The certificate contains the data you trust

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 of the certificate changed

The security association changed

Certificate Revocation Lists (CRLs)

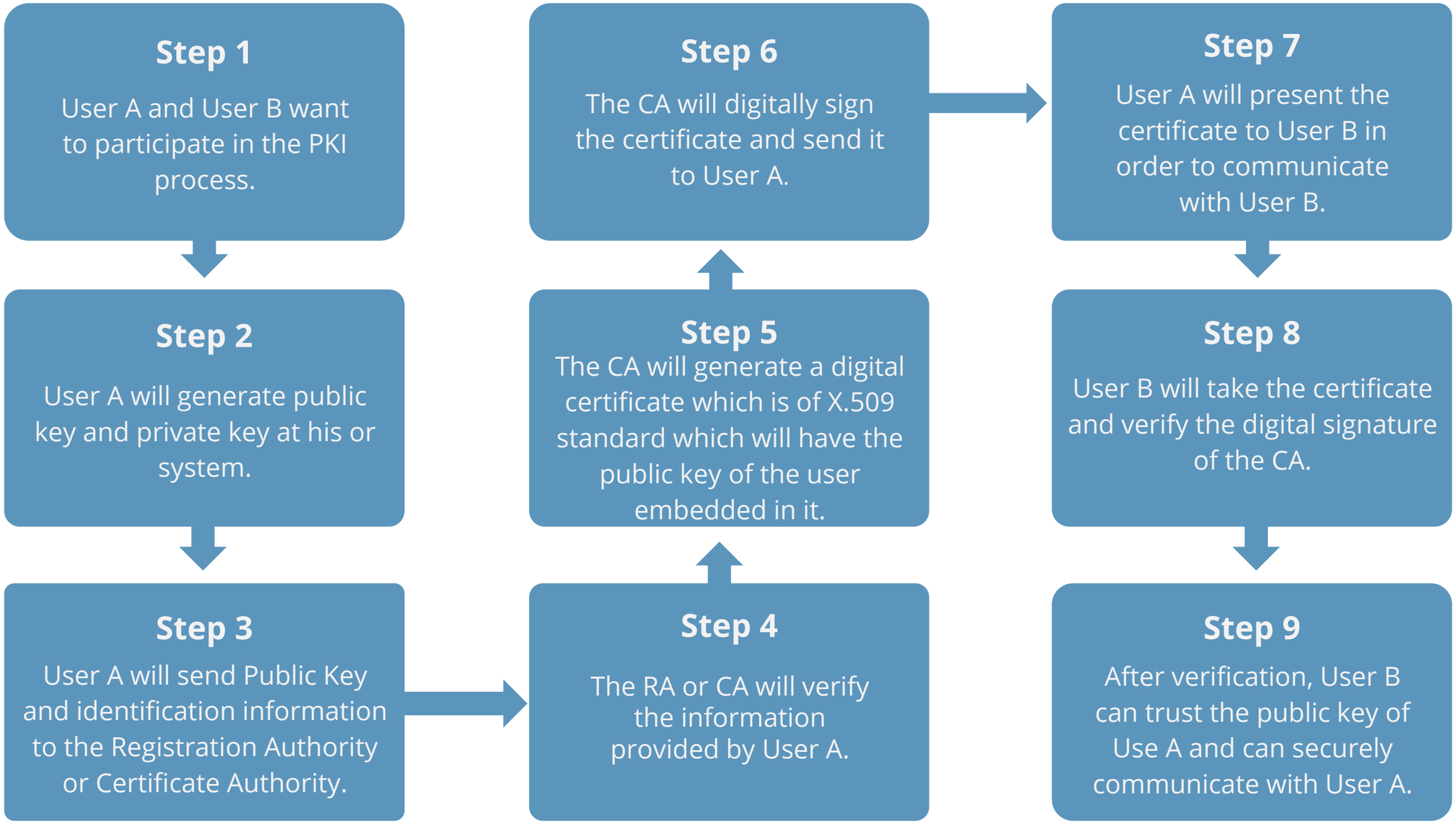
Certificate Revocation Lists

- Certificate revocation lists (CRLs) are maintained by various certificate authorities.
- They contain the serial numbers of certificates that have been issued by a CA and have been revoked along with the date and time the revocation went into effect.

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.

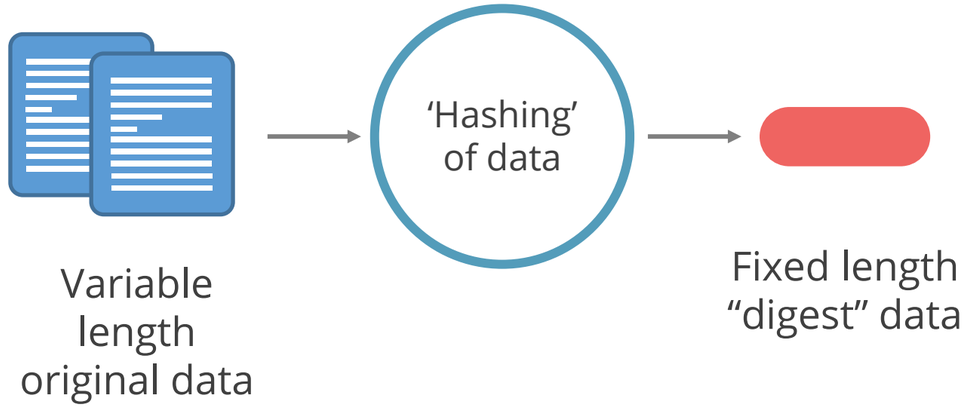
PKI Process


Step 1
User A and User B want to participate in the PKI process.
Step 2
User A will generate public key and private key at his or system.
Step 3
User A will send Public Key and identification information to the Registration Authority or Certificate Authority.
Step 4
The RA or CA will verify the information provided by User A.
Step 5
The CA will generate a digital certificate which is of X.509 standard which will have the public key of the user embedded in it.
Step 6
The CA will digitally sign the certificate and send it to User A.
Step 7
User A will present the certificate to User B in order to communicate with User B.
Step 8
User B will take the certificate and verify the digital signature of the CA.
Step 9
After verification, User B can trust the public key of Use A and can securely communicate with User A.

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.
- When the plaintext changes, its hash value also changes. Thus, for providing integrity, hash functions are used.
- Hash is used to guarantee the integrity of data.
- It can be applied to data block of any size.
- It produces fixed-length output.



One-Way Hash

Characteristics:

- Hash should be computed over the entire message.
- Hash should be a one-way function.
- Given a message and hash value, computing another message with the same hash value should be 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:

- Most widely used of the MD (Message-Digest Algorithm) family of hash algorithms
- Harder to break; for input of any length, it creates a 128-bit hash value

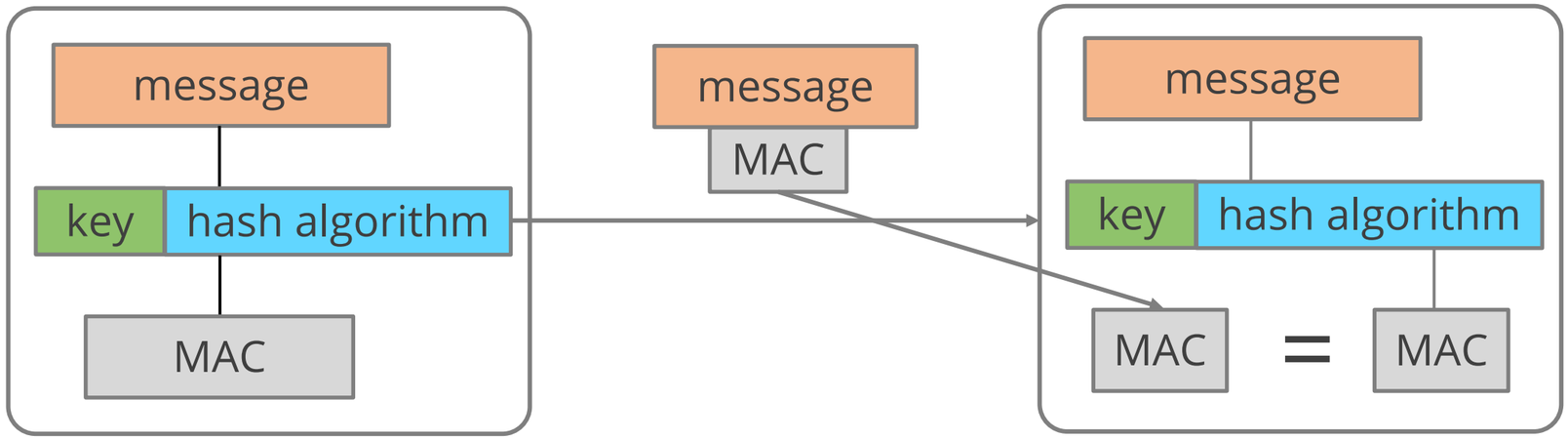
SHA-1:

- Belongs to the Secure hash algorithm (SHA) family
- 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

Message Authentication Code

- A Message Authentication Code (MAC), also known as a tag, is a short piece of information used to authenticate a message to confirm that the message came from the stated sender (its authenticity) and has not been changed.

- 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.

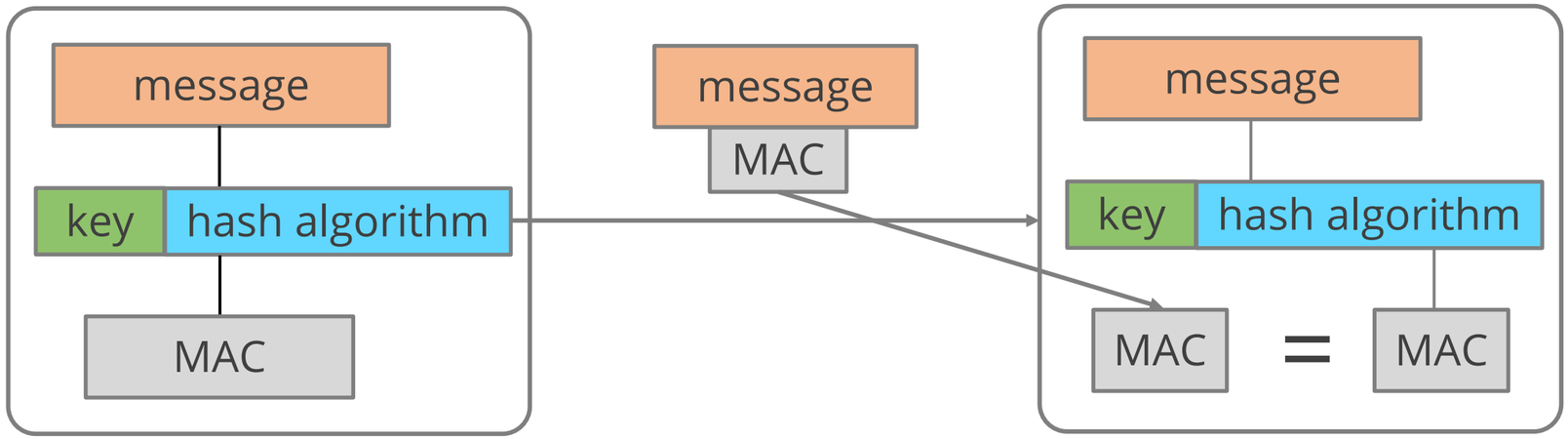


Sender sends mac with the message

Client computers the mac and Compares with the mac send

Message Authentication Code

- It is an authentication scheme derived by applying a secret key, in some form, to a message.
- The receiver performs the same computation on the message and checks if it matches the MAC.



Sender sends mac with the message

Client computers the mac and Compares with the mac send

Birthday Attack

Birthday Attack

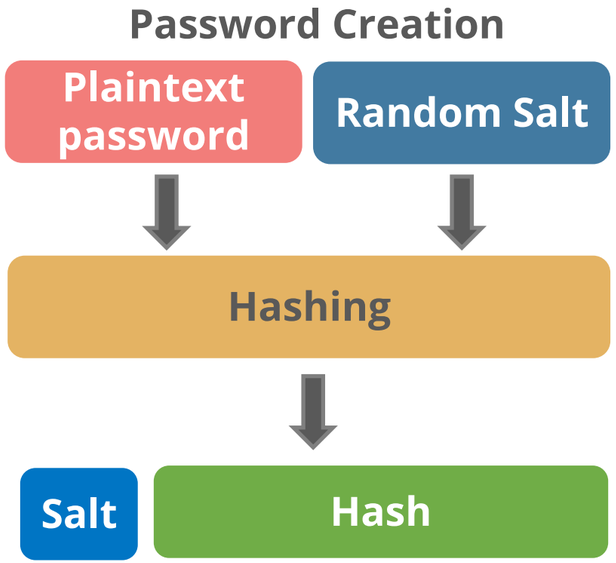
- If the algorithm does produce the same value for two distinctly different messages, it is called a hash collision.
- The birthday attack attempts to exploit the probability of two messages producing the same message digest by using the same hash function.
- It is based on the statistical probability that with 23 people in a room, there is more than 50% probability that two people have the same birthday.
- SHA-1 (160 bits) may require approximately 280 computations to find a hash collision.
- A hashing algorithm that has a larger bit output, such as a birthday attack, is less vulnerable to brute force attacks.

Salting

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

Salting

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



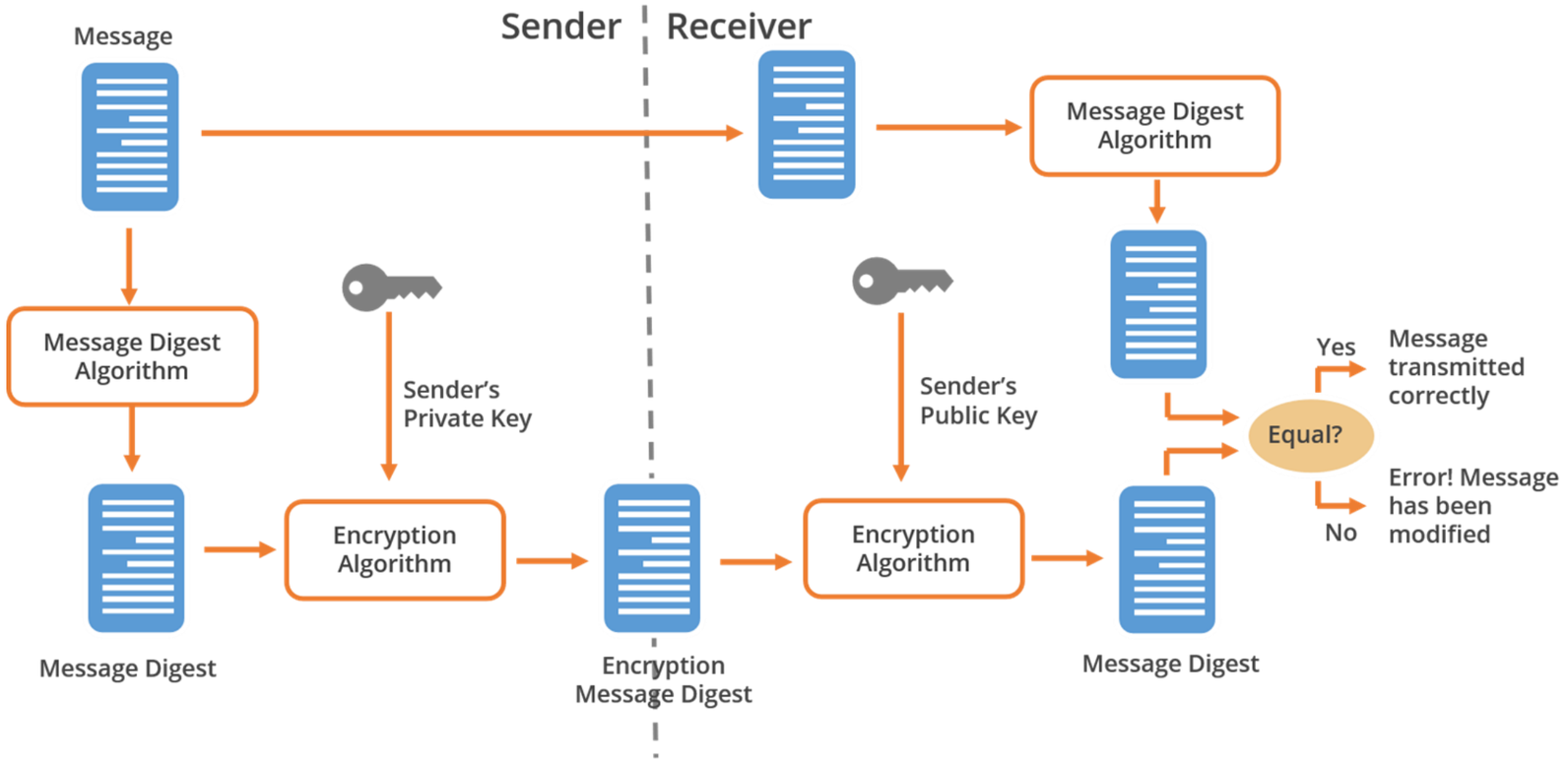
Digital Signatures

Digital signatures:

- 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 non-repudiation
- Involve encrypting the hash value of a message with a private key

Digital Signatures

The working of digital signatures is illustrated below:



Key Management

Key Management

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

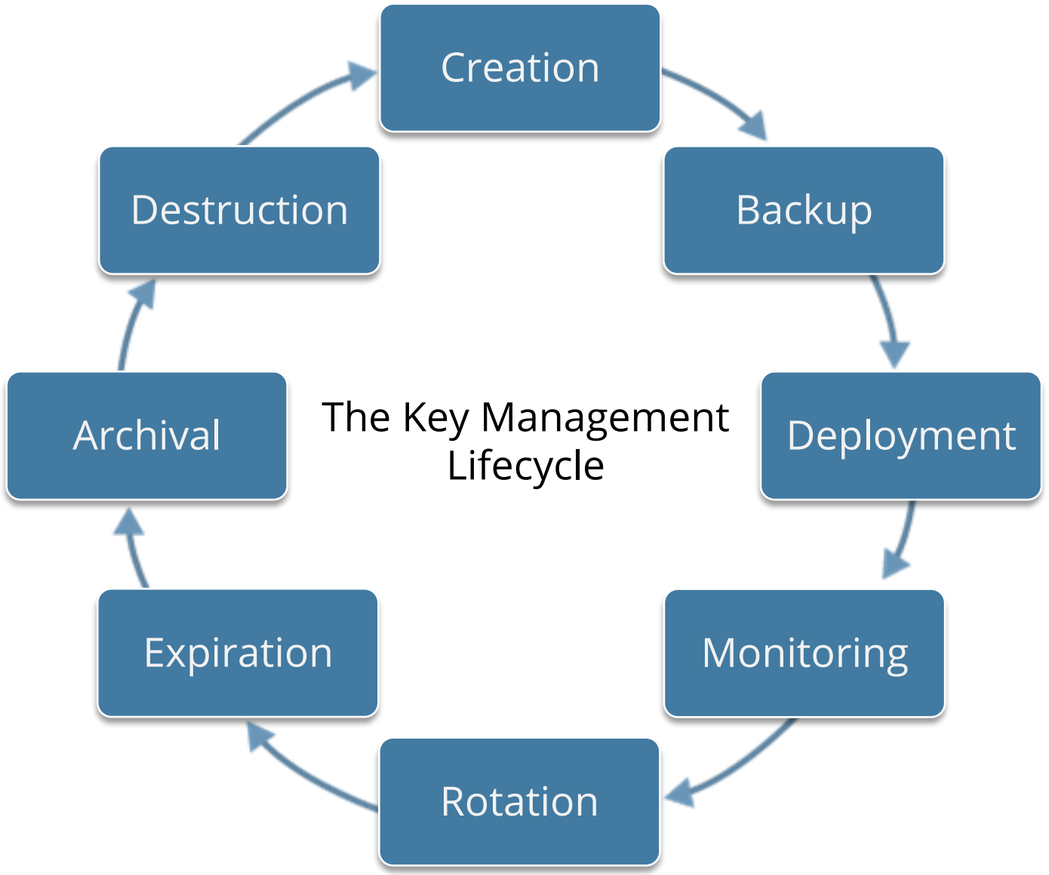
- Key management includes:
  - Generating, destroying, and recovering keys
  - Protection of keys against capturing, modification, corruption, or disclosure to unauthorized individuals
  - Regular update of keys and distribution to the right entities
- Key distribution protocols (asymmetric) include:
  - RSA
  - Diffie-Hellman
- The Kerberos Key Distribution Center (KDC) is an example of automated key management.

Key Management Principles

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

Keys Management Rules

- Keys should be:
  - Stored and transmitted by secure means
  - Random
  - Properly destroyed at the end of their lifetime
  - Long enough to provide the necessary level of protection
- The key's lifetime should correspond with the sensitivity of the data it is protecting.



Business Scenario

Important points on key management:

- The value of information encrypted with a key should correspond to the level of effort taken to protect an encryption key.
- The ciphertext can be compromised if the encryption key is compromised.
- The level of protection required for a key should be the same as that required for the original unencrypted data.
- The automatic key management is more accurate and secure.
- Keys must be updated continuously and distributed to the right entities.
- Keys need to be generated, recovered, and destroyed properly.

Question: What should be the relationship between key's lifetime and sensitivity of data?

Business Scenario

Important points on key management:

- The value of information encrypted with a key should correspond to the level of effort taken to protect an encryption key.
- The ciphertext can be compromised if the encryption key is compromised.
- The level of protection required for a key should be the same as that required for the original unencrypted data.
- The automatic key management is more accurate and secure.
- Keys must be updated continuously and distributed to the right entities.
- Keys need to be generated, recovered, and destroyed properly.

Question: What should be the relationship between key's lifetime and sensitivity of data?

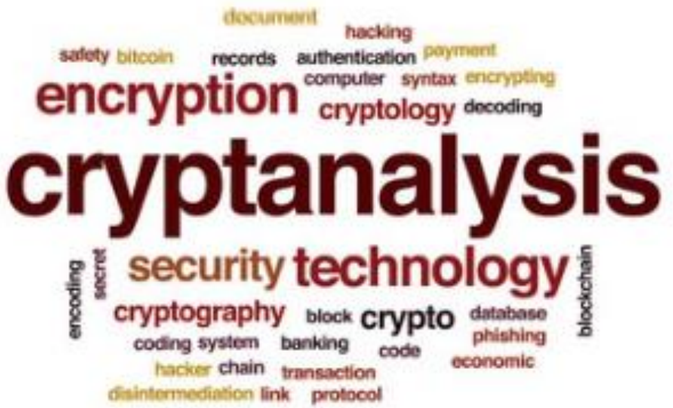
Answer: Shorter key lifetime is for more sensitive data and longer key lifetime is for less sensitive data.

Understand Methods of Cryptanalytic Attacks

Cryptanalysis

Cryptanalysis

- Cryptanalysis is the study of ciphertext, ciphers, and cryptosystems to understand how they work and find improving techniques for defeating or weakening them.
- Cryptanalysis is used to breach cryptographic security systems and decipher the contents of encrypted messages, even without knowing the cryptographic key.



Brute Force

- The attacker attempts to break the key by systematically checking all possible combinations of characters until the correct one is found.
- It is always successful if the time for the attack is not limited.

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

Ciphertext Only

- The attacker has the ciphertext of several messages.
- Each of the messages has been encrypted using the same encryption algorithm.
- The goal is to discover the key used in the encryption process.
- It is the hardest attack to be successful at because the attacker has very little information about the encryption process.

Known-Plaintext

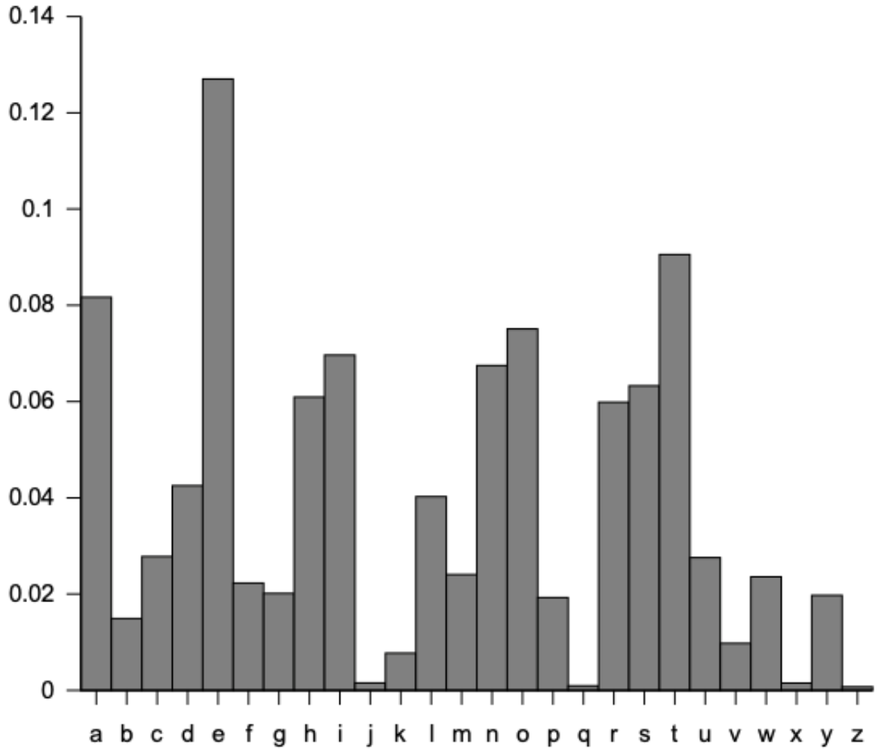
The attacker has the plaintext and the corresponding ciphertext of one or more messages.

The attacker can analyze the relationship between the plaintext and the ciphertext.

The goal is to discover the key used to encrypt the messages.

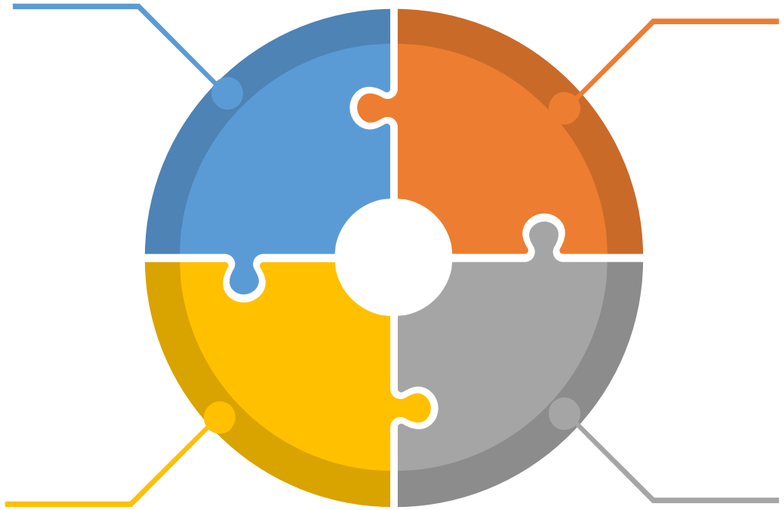
Frequency Analysis

- Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext.
- Frequency analysis 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

The attacker knows the algorithm used for encryption.



The attacker runs samples of plaintext to obtain the corresponding ciphertexts.

An Adaptive Chosen-Plaintext attack is where the attacker can modify the chosen plaintext based on the resulting ciphertext.

The attacker can compare ciphertexts to possibly discover the encryption key.

Chosen-Ciphertext

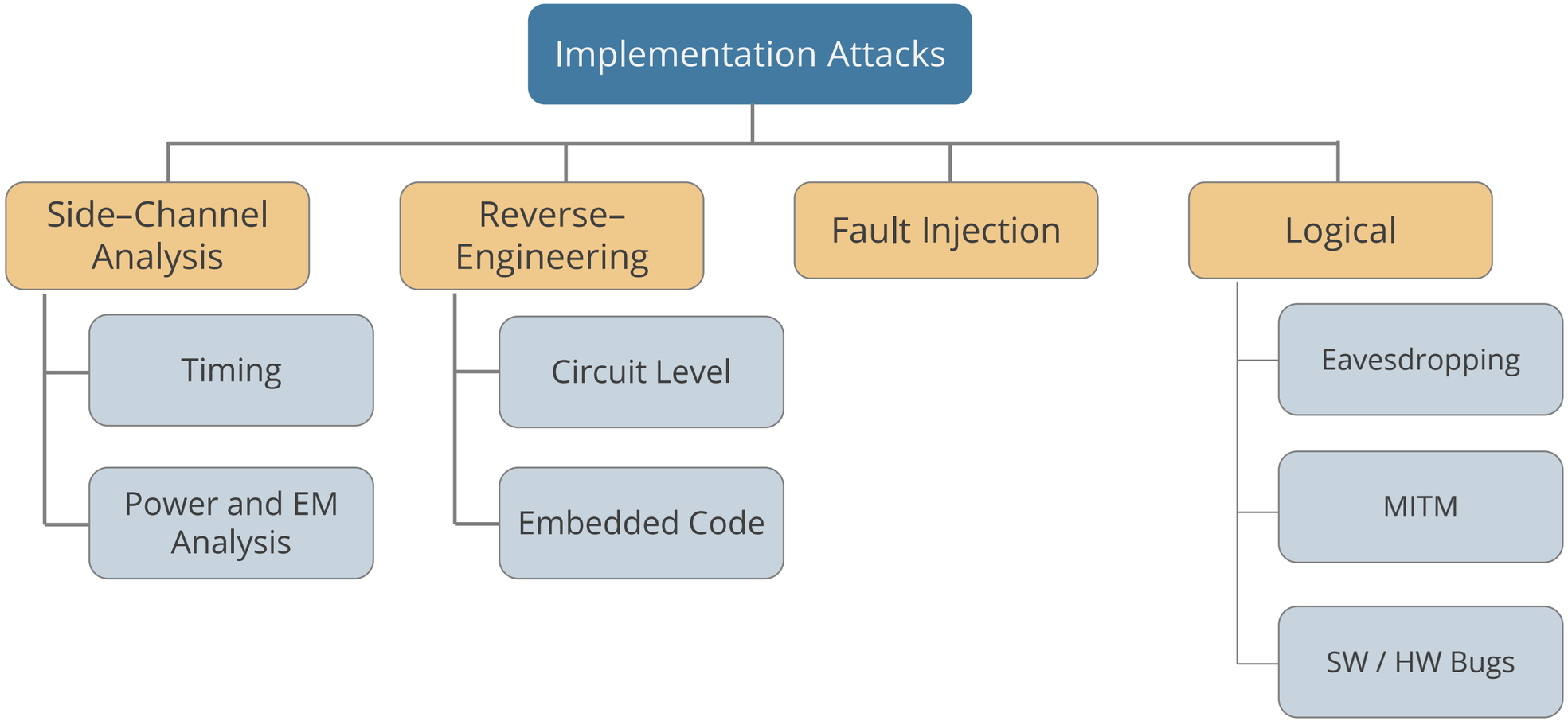
The attacker has access to the system used for decryption.

The attacker can choose the ciphertext to be decrypted and have access to the resulting decrypted plaintext.

The attacker gains access to an unattended decryption system through **lunchtime**, **midnight** attacks. The goal is to figure out the encryption key.

Implementation Attacks

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



Side-channel Attacks

The attacker analyzes the information retrieved from the encryption device.

Power consumption statistics

Radiation emissions

Error information

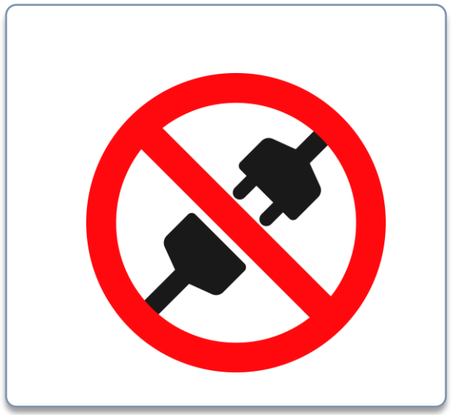
Time taken for encryption and decryption

Sound

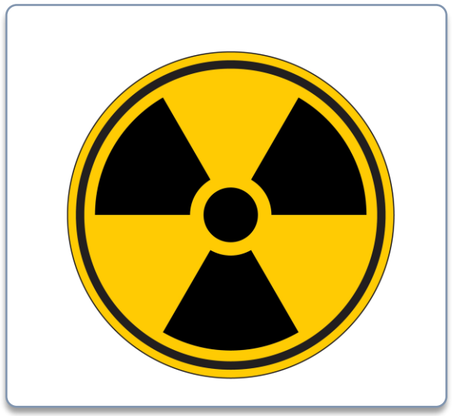
Fault Injection

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

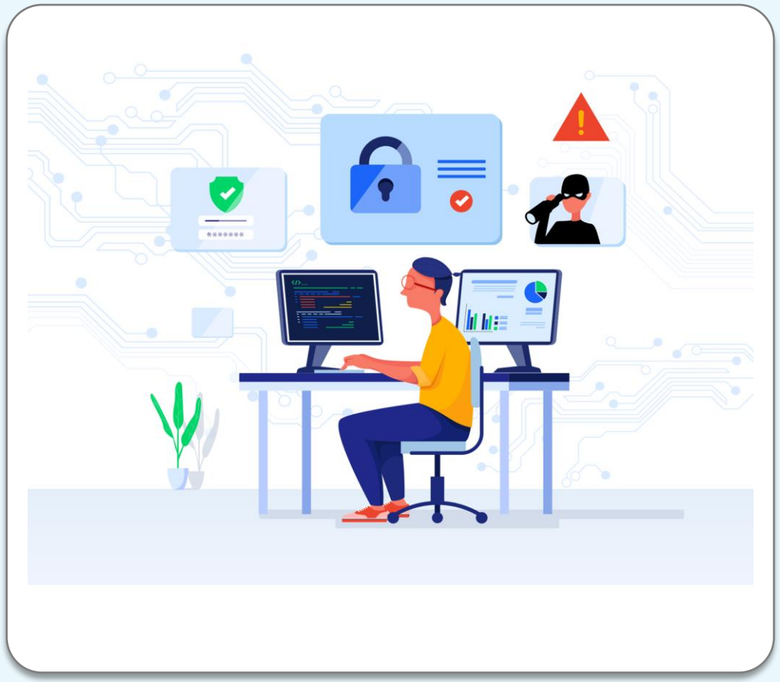


Radiation-based fault injections

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

Man-in-the-Middle (MITM)

- It's a type of side-channel attack.
- The attacker tries to break the ciphertext by analyzing the time taken to execute the encryption and decryption algorithms for various inputs.
- The goal is to discover the key used to encrypt the messages.

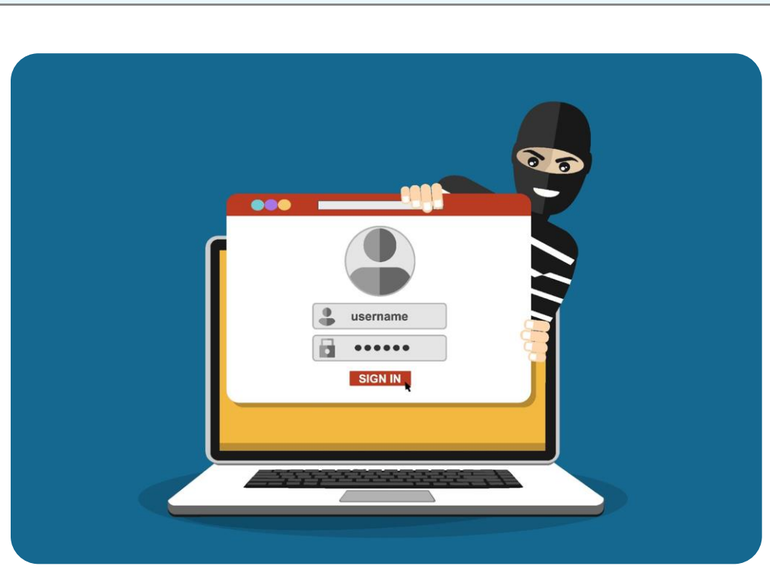


Man-in-the-Middle (MITM)

- It is a communication eavesdropping attack.
- The attacker intercepts and relays messages between two targets.
- The client and the server believe they are directly communicating with each other.

Pass-the-Hash

- 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 plain text password.
- This technique can be performed against any system which accepts NTLM authentication.



Ransomware

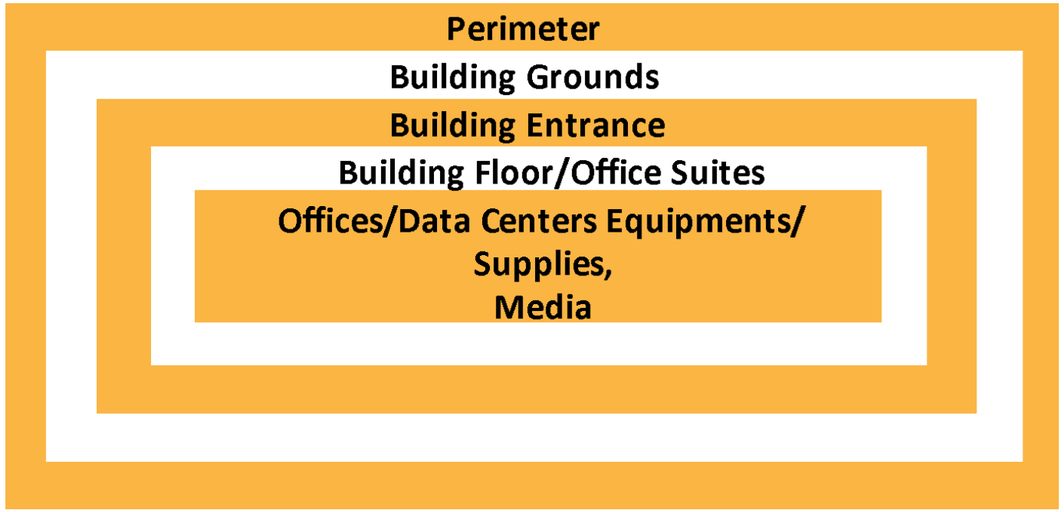
It is a form of malware that encrypts a victim's data and important files.

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.

Apply Security Principles to Site and Facility Design

Site and Facility Design Criteria



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.

It is a standard operational procedure for a security professional to review all aspects of construction.

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

Information Protection Environment

Factors considered by a security professional:

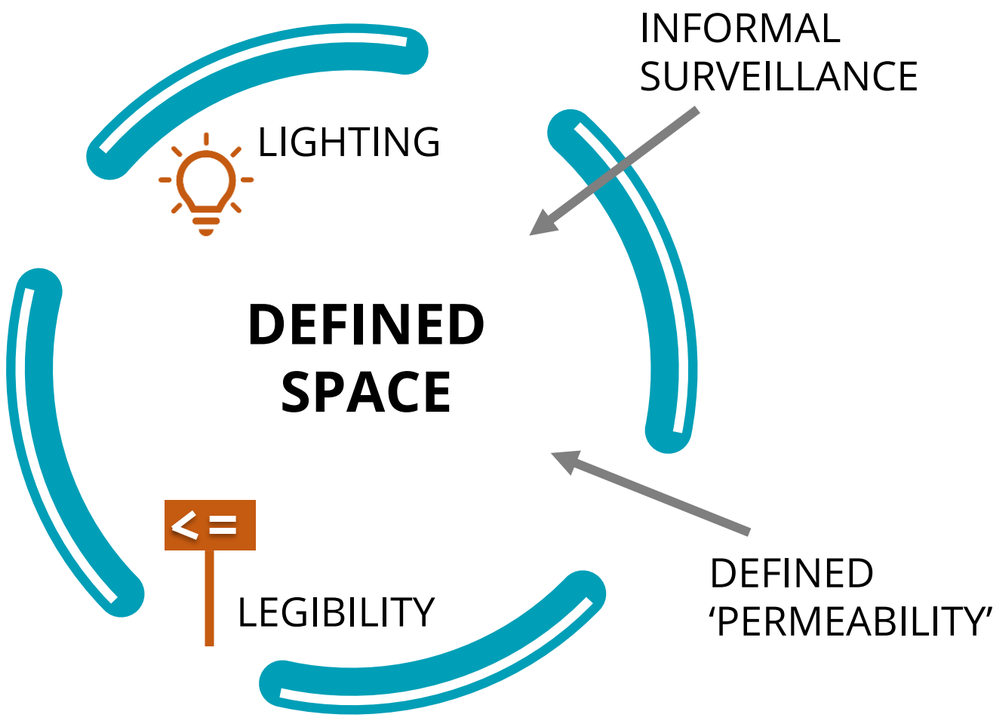
Protection of life, property, and operations

Minimize 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)

CPTED is a crime reduction technique.
Examples: Streets, parks, museums, government buildings, houses, and commercial complexes.



The three environmental strategies of CPTED are:

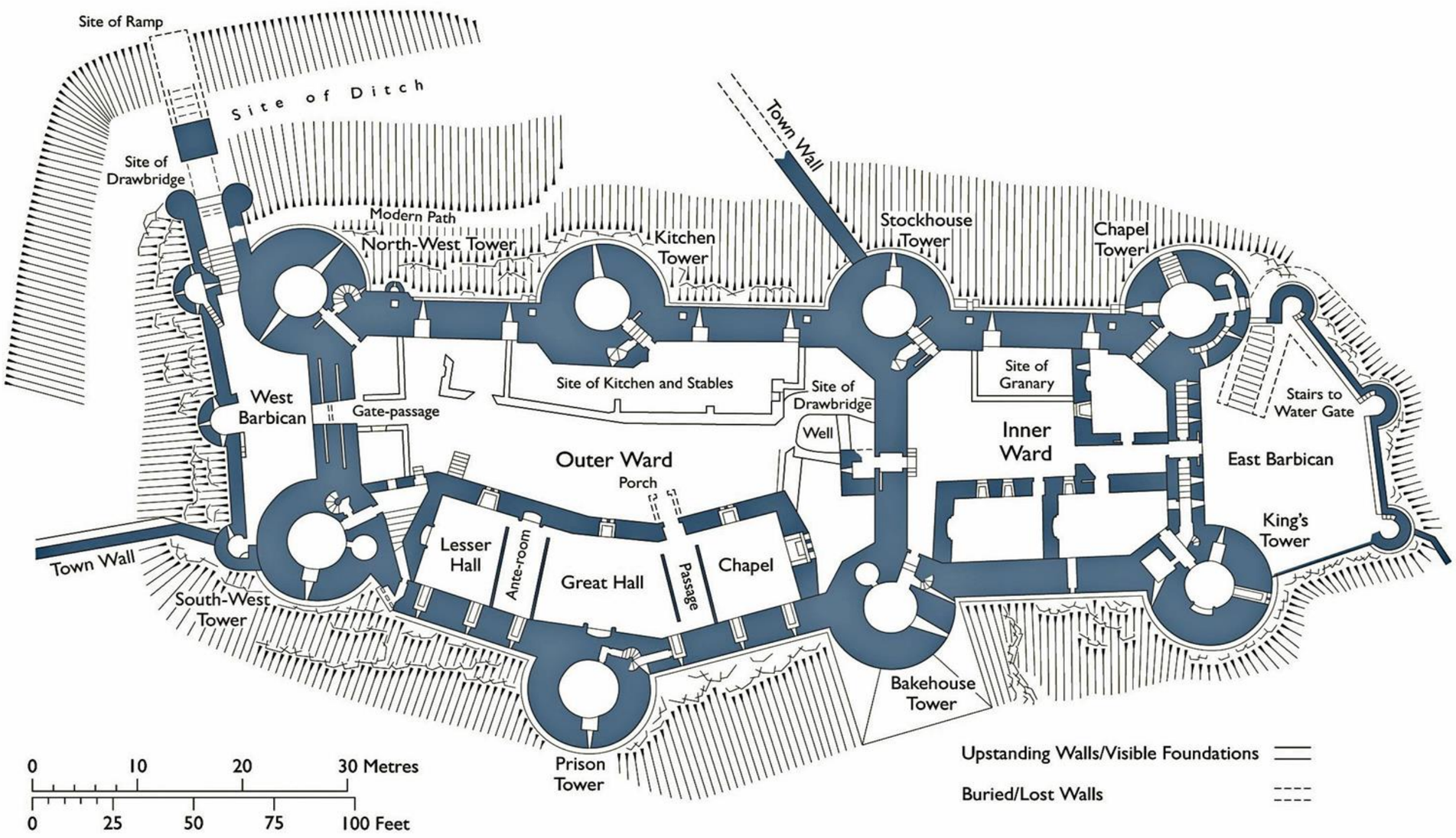
- Territoriality: These make users feel safe and make the potential offender aware of a substantial risk of apprehension.
- Surveillance: It creates the perception that people can be seen.
- Access Control: It limits the opportunities for crime.

Discussion

Discussion

Review the blueprint of Conwy Castle (in the next slide) and determine if it demonstrates the use of CPTED principles.

Discussion



Source: https://www.pinterest.com/pin/342203271683079513/

Business Scenario

Hilda Jacobs, General Manager, IT Security at Nutri Worldwide Inc. was planning the physical security controls of the new site along with Kevin. Hilda asked Kevin to assist her in this project since she is handling the planning all by herself.

- Hilda Jacobs decided to use the existing landscape to deter threats.
- Use of fences, vehicle barriers, warning signs, access point restriction, proper lighting, and a CCTV system were planned.

Question: Which concept of physical security are Hilda and Kevin trying to implement here?

Business Scenario

Hilda Jacobs, General Manager, IT Security at Nutri Worldwide Inc. was planning the physical security controls of the new site along with Kevin. Hilda asked Kevin to assist her in this project since she is handling the planning all by herself.

- Hilda Jacobs decided to use the existing landscape to deter threats.
- Use of fences, vehicle barriers, warning signs, access point restriction, proper lighting, and a CCTV system were planned.

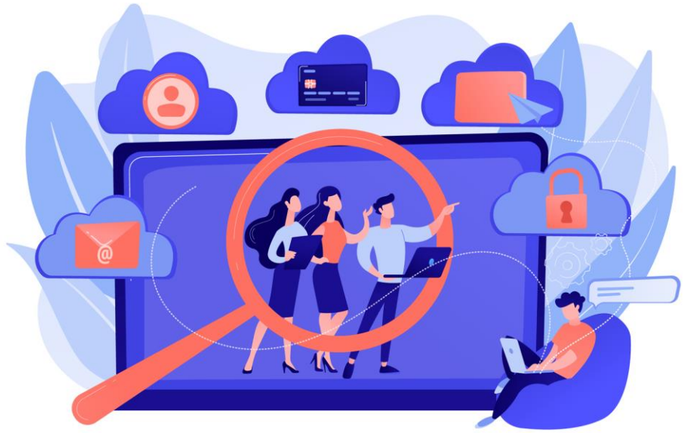
Question: Which concept of physical security are Hilda and Kevin trying to implement here?

Answer: Crime Prevention through Environmental Design (CPTED)

Site Location

The site location of the facility is also a concern during the initial planning.

- Existing Boundary Protection
- Location and Access
- Stable Power Supply
- Local Crime
- Joint Tenants
- Visibility
- Wind and Surface Traffic
- Emergency Access
- Natural Hazards



Construction

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

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

Business Scenario

Nutri Worldwide Inc. is a rapidly growing company with offices in different parts of the world. Recently, the company thought of opening an office in India. Hilda Jacobs, General Manager, IT Security at Nutri Worldwide Inc. was reviewing the physical and environmental security of the proposed office.

- She assigned the task of listing out various threats from natural and environmental factors, man-made factors, and political factors based on the location of the proposed office to Kevin.

Question: What is the first thing Kevin should consider when designing good physical and environmental security?

Business Scenario

Nutri Worldwide Inc. is a rapidly growing company with offices in different parts of the world. Recently, the company thought of opening an office in India. Hilda Jacobs, General Manager, IT Security at Nutri Worldwide Inc. was reviewing the physical and environmental security of the proposed office.

- She assigned the task of listing out various threats from natural and environmental factors, man-made factors, and political factors based on the location of the proposed office to Kevin.

Question: What is the first thing Kevin should consider when designing good physical and environmental security?
Answer: Life safety is the most important and first factor Kevin needs to consider for designing good physical and environmental security.

Design Site and Facility Security Controls

Support Facilities

The factors involved are:

HVAC	**(**Heating, Ventilation, Air Conditioning) IT managers should know who is responsible for HVAC.
Water	Turn off all electrical power to the equipment, allow water to drain out, place all affected equipment or media in an air-conditioned area, and wipe with water displacement spray.
Electricity	Recommended practices are installing user surge protectors, uninterruptible power supply (UPS), installing backup source for critical systems, and anti-static carpet.
Earthquakes	Keep computers away from glass windows and high surfaces, place components on shock absorbers and anchors, and ensure other objects do not fall on computers.
Lightning	Best practice is to switch off the systems, unplug them, and store the backup tapes away from the building's steel support.

Data Center Security: Guidelines

Data Centers, 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. This helps 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. No contaminants can be sucked into the room. Water detectors should be placed under raised floors and on dropped ceilings.

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

Personnel Access Control

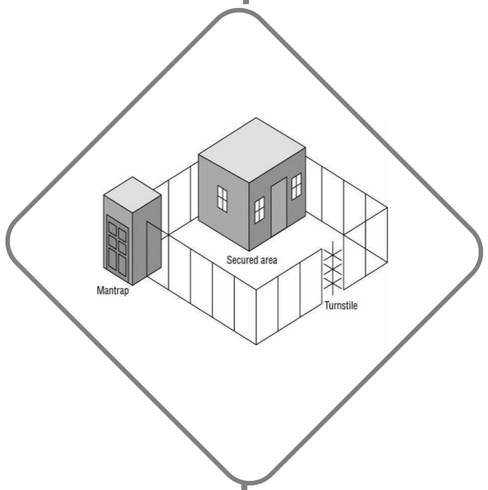
Piggybacking

Piggybacking is when another person follows through a door with the permission of the person who has received access.

Tailgating

Tailgating is when another 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

- A turnstile 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 and can trap individuals at the discretion of security personnel.

Access Control

Smart card

- Security ID with an embedded magnetic strip, bar code, or integrated circuit chip
- Can process information or store a reasonable amount of data in memory
- Can be used in multifactor authentication to improve security
- Vulnerable to physical security attacks

Memory card

- Machine readable ID cards with memory sticks
- Can hold a small amount of data in memory but cannot process it
- Are easy to copy or duplicate

Proximity reader

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

Media Storage Security: Safe

- Safes are commonly 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.
- 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	Embedded into the floor and easily hidden
Chests	Stand-alone safe
Depositories	Safes with slots; allow valuables to be slipped in
Vaults	Safes that are large enough to allow walk-in

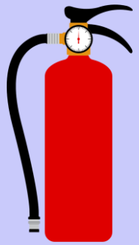
Fire Prevention, Detection, and Suppression

Fire Prevention

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

Fire Detection

Placing fire detectors at strategic points to detect smoke or fire



Fire Suppression Systems

Using a suppression agent to put out a fire

Stages of Fire

The earlier the fire is detected, the easier it is to be extinguished.

Stage 1: Incipient stage	Stage 2: Smoke stage	Stage 3: Flame stage	Stage 4: Heat stage
Initial stage, only air ionization, no smoke	Smoke is visible from the point of ignition	Flame can be seen with naked eye	Fire is considerably higher

Fire Detection Devices

Smoke Activated

- Good early warning devices
- Photoelectric device
  - Detects a variation in light intensity and produces a beam of light and if the light is obstructed, an alarm is produced.

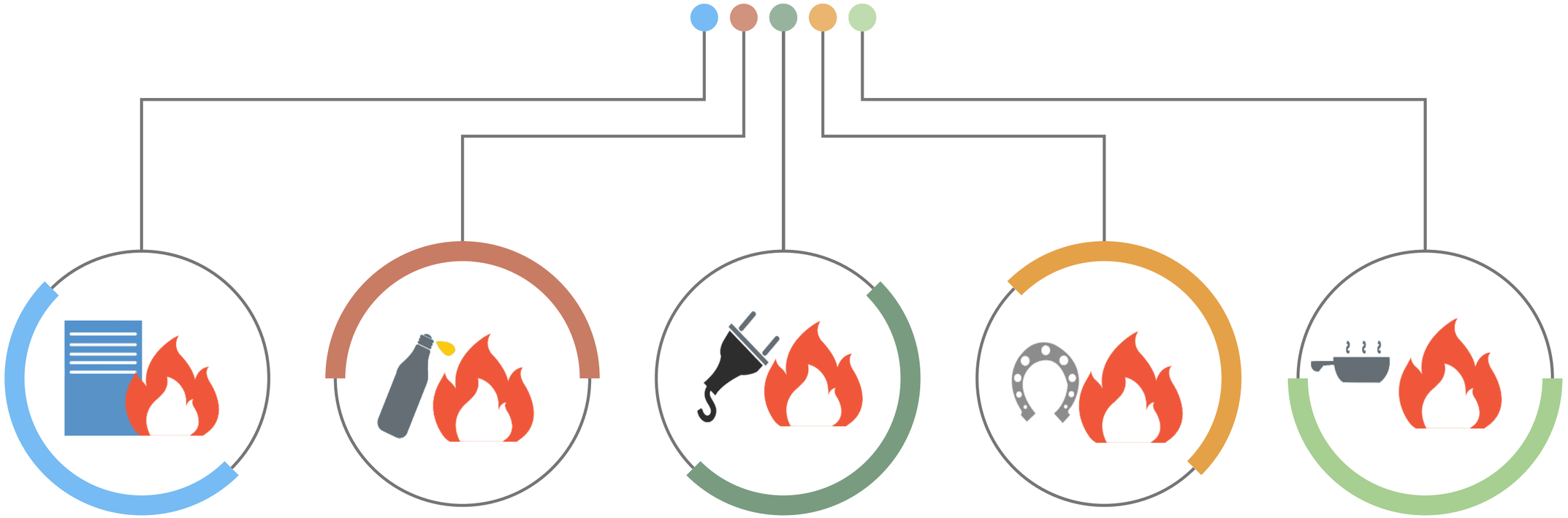
Fire Detection Devices

Heat Activated

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

Environmental Controls: Fire

The following are the classes of fires:



Environmental Controls: 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: Most important step: Turn off electricity first!)
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

Wet Pipe	• Always full of water, usually discharged by temperature control sensors. • Also called closed head systems
Dry Pipe	• Water is not stored in the pipe, instead contains compressed air. • Opening the water valve causes water to fill the pipes and discharge.
Preaction	• Combination of wet and dry pipe • Water is not held in the pipes until the fire is detected. • Released only after the sprinkler head activation triggers are melted by sufficient heat.
Deluge	• Another form of dry pipe system that uses larger pipes and can deliver a significantly larger volume of water.

Gas Suppression

Gas Suppression

- It is more effective than water suppression systems.
- Gas discharge systems remove oxygen from the air and should not be used in environments where people are located.
- Halon is an effective gas suppression system, but as it degrades the environment, it is banned.
- Effective replacements for Halon are:
  - FM200
  - NAF-S-III
  - Argon
  - Inergen

Motion Detectors

Infrared

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

Heat-based

Monitors 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

Monitors the changes in the electrical or magnetic field surrounding a monitored object.

Photoelectric

Monitors visible light levels in a monitored area.

Passive Audio

Listens for abnormal sounds in a monitored area.

Alarm Types

Deterrent

- Alarms that trigger deterrent actions
- The goal is to make intrusion attempts more difficult.

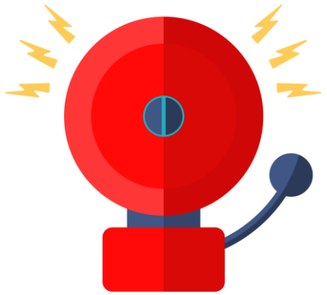
Repellent

- Alarms that trigger sound or light
- The goal is to discourage intruders.

Notification

- Alarms that trigger notifications to security analyst
- Silent from an attacker's perspective, but it gives warning signals to the security team.

Alarm Categories



Local Alarm System

- Must broadcast an audible alarm signal that can be heard within 400 feet.
- Security guards should be stationed nearby.

Central Station

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

Auxiliary system

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

Emanation Security: Electronic Emanation

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:

Faraday Cage

A closed enclosure with external metal mesh that fully surrounds the enclosure, absorbing EM signals.

White Noise

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

Control Zone

- Implementation of zones so that the emanations are controlled within the environment.
- Can use faraday cage or white noise in those zones

Business Scenario

Kevin Butler is studying the importance of security for data centers. He reads about the recent unauthorized intrusion in data centers caused by a faulty design. He studied some of the countermeasures for the same. He understands that for dropped ceilings, the walls should extend above the ceiling to the true ceiling.

- Similarly, for the raised floors, the walls should extend below the false floor.
- Even the air ducts should be small enough to prevent an intruder from crawling through them.
- Kevin identified, apart from the above-mentioned considerations, the need to have strong access control for the data center and made his suggestions to Hilda.

Question: What suggestion did Kevin include in his report to ensure strong access control for the data center?

Business Scenario

Kevin Butler is studying the importance of security for data centers. He reads about the recent unauthorized intrusion in data centers caused by a faulty design. He studied some of the countermeasures for the same. He understands that for dropped ceilings, the walls should extend above the ceiling to the true ceiling.

- Similarly, for the raised floors, the walls should extend below the false floor.
- Even the air ducts should be small enough to prevent an intruder from crawling through them.
- Kevin identified, apart from the above-mentioned considerations, the need to have strong access control for the data center and made his suggestions to Hilda.

Question: What suggestion did Kevin include in his report to ensure strong access control for the data center?

Answer: The use of three-factor authentication for access control.

HVAC

Heating, Ventilation, and Air-Conditioning (HVAC)

- Temperature and humidity are maintained within reasonable limits.
- Positive pressure and drainage are employed.
- Recommended humidity levels are 40 to 55%.
- Low humidity causes static electricity.
- High humidity may cause corrosion.
- Recommended **set point** temperature range for a data center is 68 to 77°F (20–25°C).

Power Supply

A 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:** Prolonged, complete loss of electric power
- **Fault:** Momentary power outage

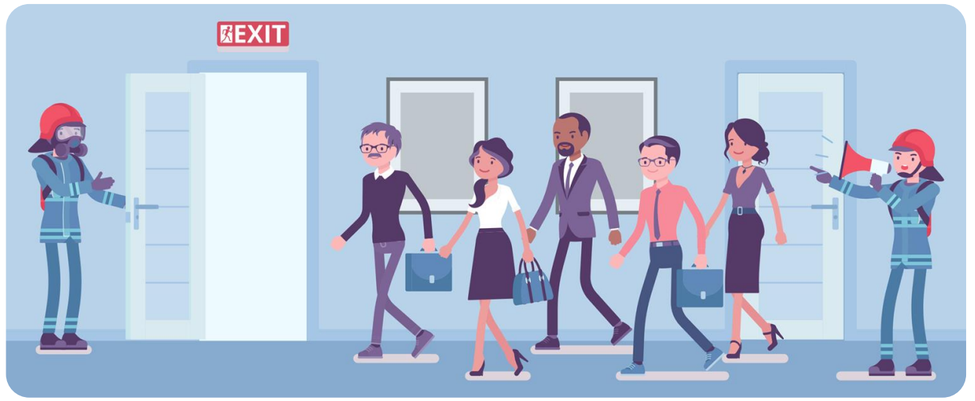
Power Degradation

- **Brownout:** Prolonged reduction in voltage
- **Sag or dip:** Momentary reduction in voltage

Training and Awareness

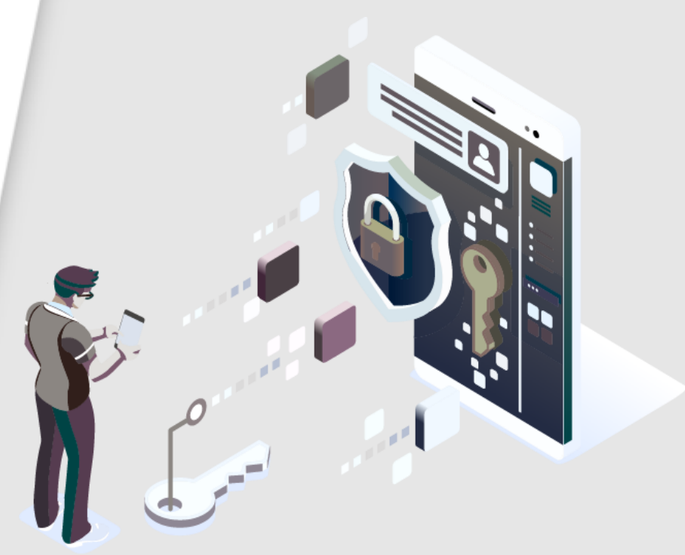
Physical security awareness and training are very critical. It should include:

- Training on operating emergency power systems
- Training on operating fire extinguishers
- Evacuation routes should be prominently displayed
- Fire drills



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 standard.
- System security architecture is focused on designing security services within individual computing systems.
- The various types of distributed systems are virtualization, hypervisor, cloud computing, grid computing, and peer-to-peer.



This concludes **Security Architecture and Engineering.**

The next domain is **Communications and Network Security**.