#MissionBeforeMoney

2025 CISSP Mentor Program

CHAPTERS 8 & 10

Christophe Foulon

Founder CPF Coaching & vCISO

CISSP® MENTOR PROGRAM – SESSION FIVE

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

CISSP® MENTOR PROGRAM – SESSION FIVE

INTRODUCTION

Agenda –

- Welcome
- Introduction
- Principles of Security Models, Design and Capabilities
- Physical Security Requirements

CISSP® MENTOR PROGRAM – LEAD MENTOR INTRO

WHOAMI

Christophe Foulon

Founder CPF Coaching & vCISO

https://www.linkedin.com/in/christophefoulon/

https://substack.cpf-coaching.com/

CISSP® MENTOR PROGRAM – SESSION FIVE

WHO I AM?

I love Baby Yoda

Outside of being a security practitioner focused on helping businesses tackle their cybersecurity risks while minimizing friction resulting in increased resiliency and helping to secure people and processes with a solid understanding of the technology involved.

I am a dad, dog dad and career coach. I love helping other to achieve their best. Through this channel, I help veterans with their transitions and others via non-profits like Whole Cyber Human Initiative, Boots2Books and others.

I give back by producing a podcast focused on helping people who are "Breaking into Cybersecurity" by sharing the stories of those who have done it in the past 5 years to inspire those looking to do it now.

Co-authored:
"Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level"
"Hack the Cybersecurity Interview: A complete interview preparation guide for jumpstarting your cybersecurity career"
And advised on "Understand, Manage, and Measure Cyber Risk"

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Discord Channels
- Exercise or get fresh air in between study sessions

Let's get going!

QUESTIONS.

The most common questions have been about:

- **About the Discord channel**
- Live session links.
- Instructor slide deck.

Because of the way Discord works and normal communications challenges, the Discord invite you received may have “expired”. Email the FRSecure CISSP Mentor List (**cisspmentor@frsecure.com**) for a new invite.

QUESTIONS.

The most common questions have been about:

- About the Discord channel
- **Live session links.**
- Instructor slide deck.

All LIVE session links will be sent by email on the same day as the LIVE session. If you have not received the live session link it's usually because the email went to your "Junk" folder (or similar).

QUESTIONS.

The most common questions have been about:

- About the Discord channel
- Live session links.
- **Instructor slide deck.**

The instructor slide decks will be sent as soon as FRSecure receives them from the instructors. Sometimes the decks are not available until they teach. Whenever possible, we will try to send you the slide decks before each class.

Secure Design Principles

Definitions - Let's Jump In

Subjects

•The active entat that requests access to a resource

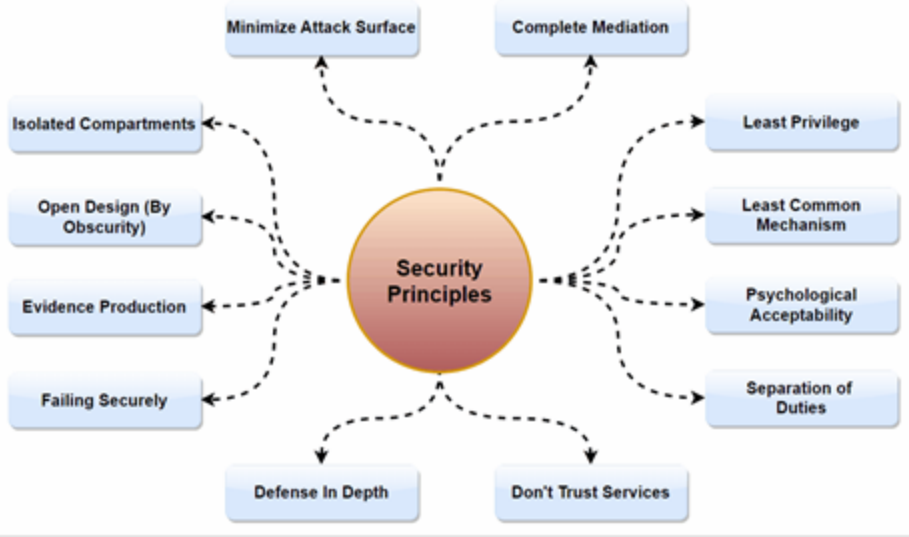
Most commonly a user, also can be process, program, computer or organization

Objects

• A passive entity which they subject wants access to

most commonly a resources, such as a file, printer

but could also be a process, program, computer or organization



Secure Design Principles

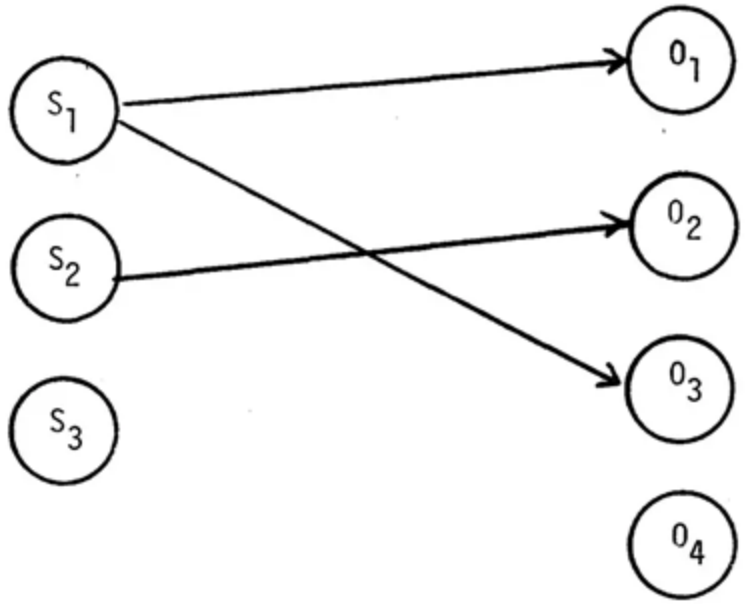


Figure 1. Subjects Accessing Objects

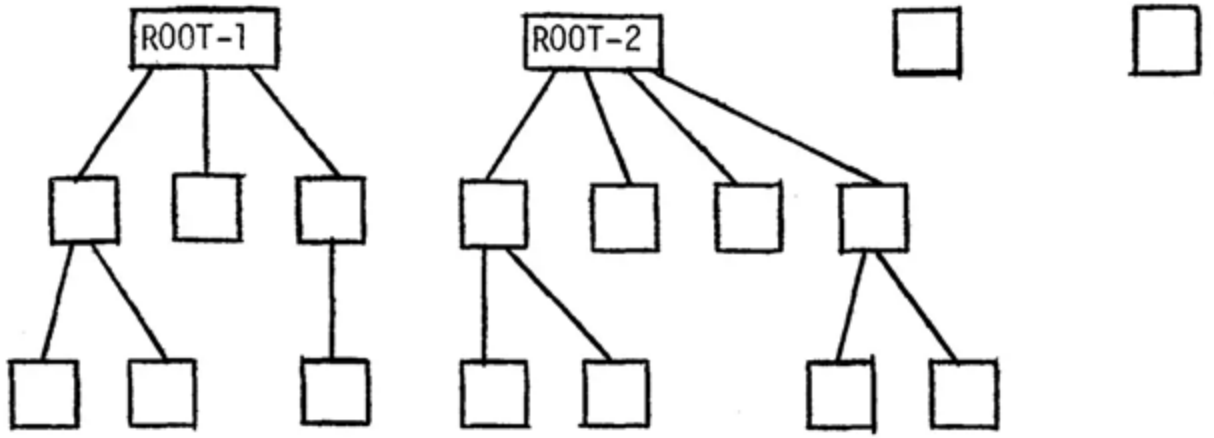


Figure 2. The Desired Object Structure

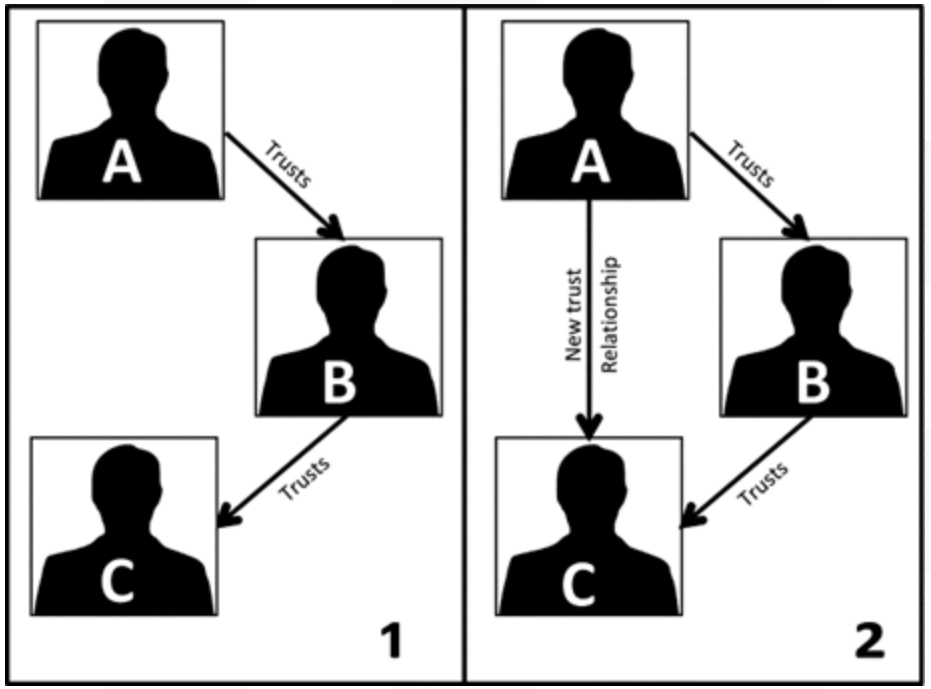
Secure Design Principles

Transitive Trusts

- Transitive trust refers to the phenomenon where if user A trusts user B and user B trusts user C, then user A will also trust user C based on the trust relationship

Security Concerns

- Based on this trust relationships, security controls which might have prevented A and C from interactions from the two subjects



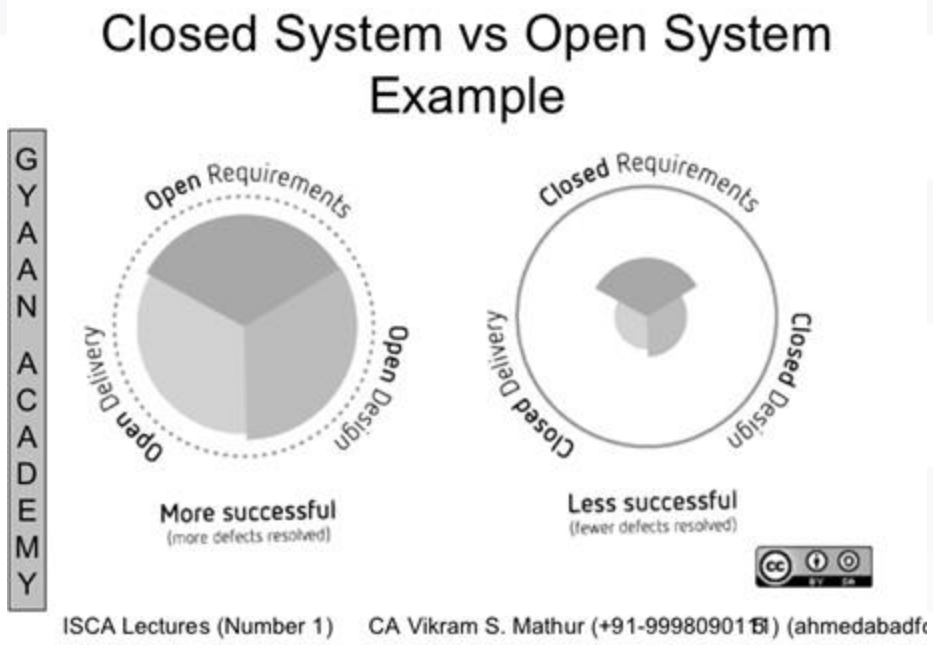
Secure Design Principles

Open Systems

- Designed to work together with agreed-on industry standards

Closed Systems

- Designed to work well with a narrow range of systems



Secure Design Principles

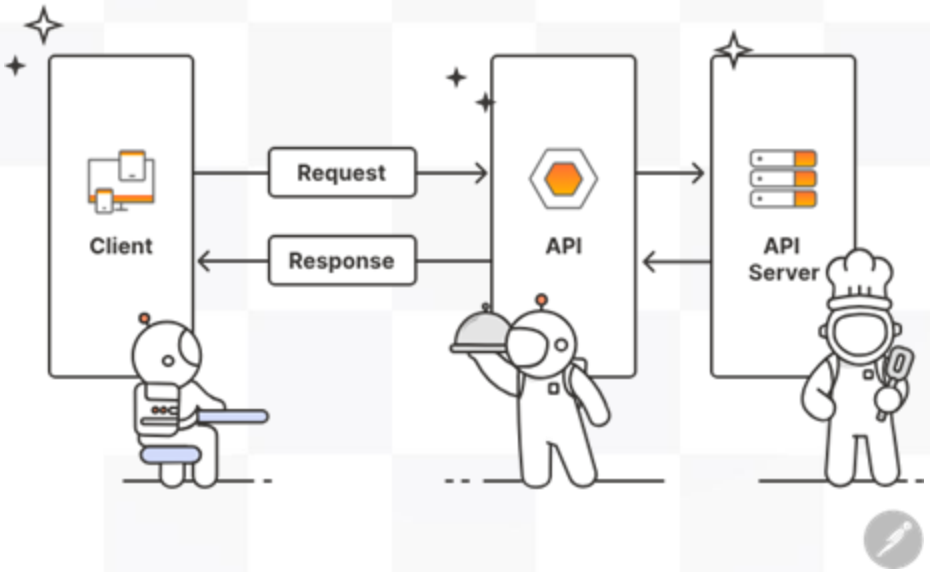
Application Programming Interfaces (APIs)

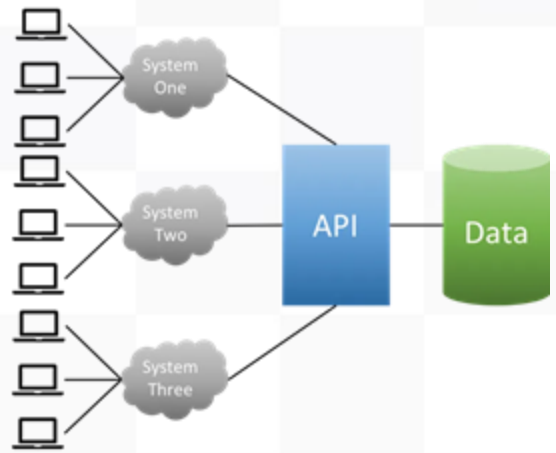
- There provide a defined set of interactions which would be allowed by computing elements

- Make the interoperability between different computing elements possible.

Common way for open systems to communicate with each other.

Closed Systems - Harder to integrate with, but this “feature” could make them more secure.





Secure Design Principles

Open-Source Soultions

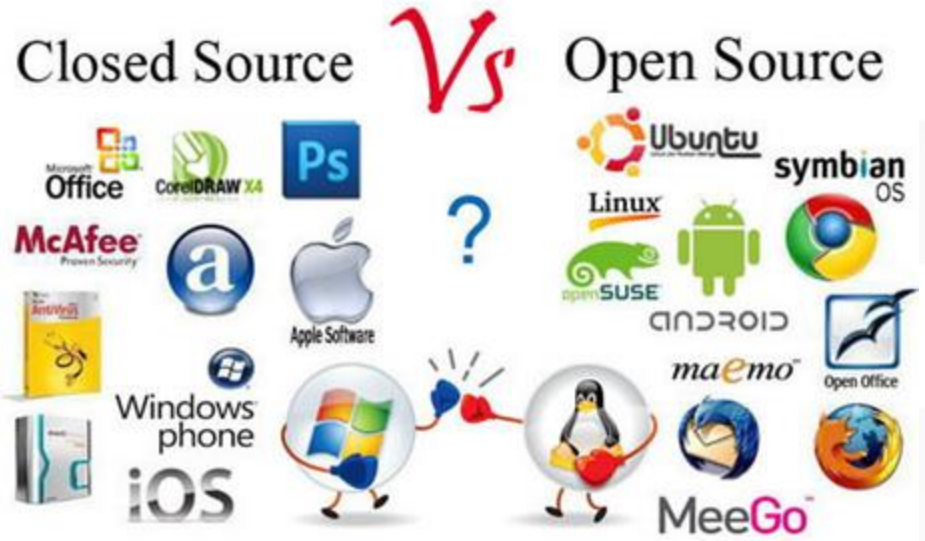
•The source code, and other internal logic is exposed to the public

- Open inspection can improve the product over time

Closed Systems

• The source code and other internal logic is hidden from the public

- Dependant on the vendor or programmer for improvements



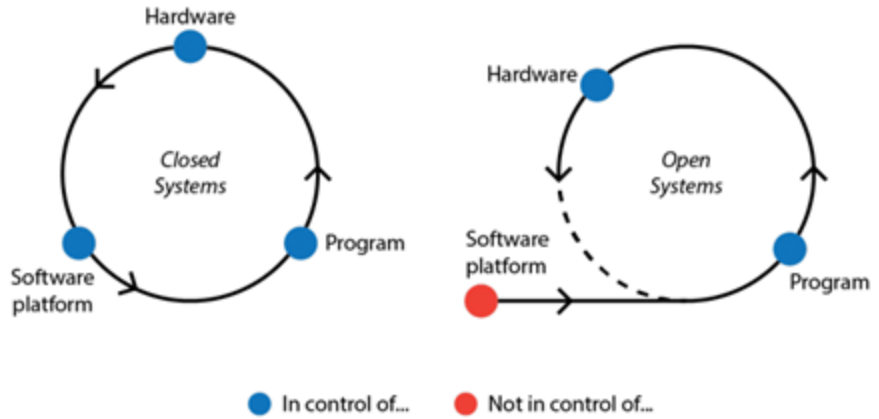
Secure Design Principles

Open-Source programs / Systems

- While a programs can be open sourced, they can operate in either open or closed systems

Closed Sources programs / Systems

- Same goes for closed sourced orgrams



Secure Design Principles

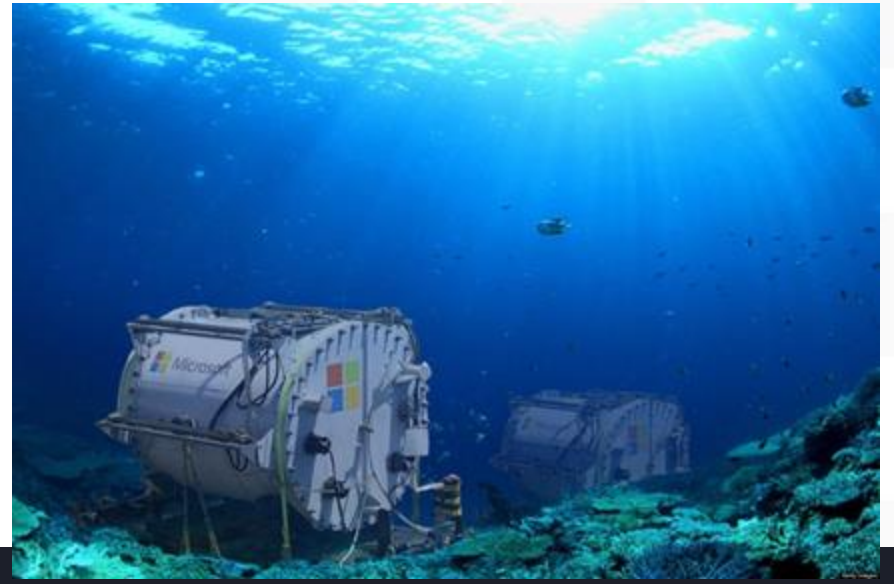
Secure Defaults

- The concept that you build in secure options, or configurations into systems by design

Minimize User Friction

- The concept you want users to be able to easily use applications or systems from the first time the use it

Secure Design Principles



Secure Design Principles

Secure Defaults

- The continuous battle of locking things down to prevent accidents, while continuing to make systems “just work”

Restrictive Defaults

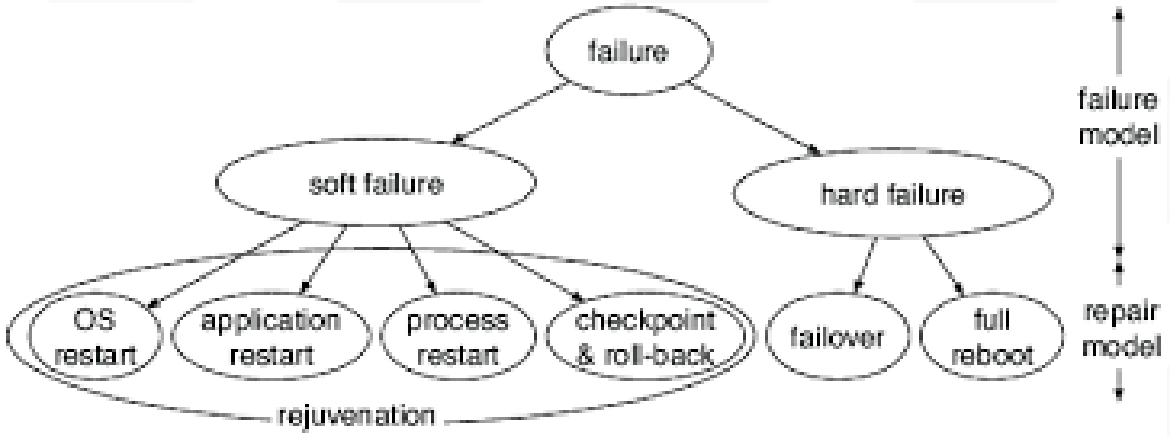
- The practice or policy of setting defaults to be intentionally limiting or restrictive to enhance security, privacy or compliance

Secure Design Principles

Failure Securely

•Things fail, plan ahead and think through how should the system react during failure.

- Some doors fail open or fail closed depending on the security considerations.
- Fail-soft, Fail-secure, Fail-safe, Fail-open, Fail-clouse



Fail-soft

• This allows a system to continue to function even when one or more of its components fails

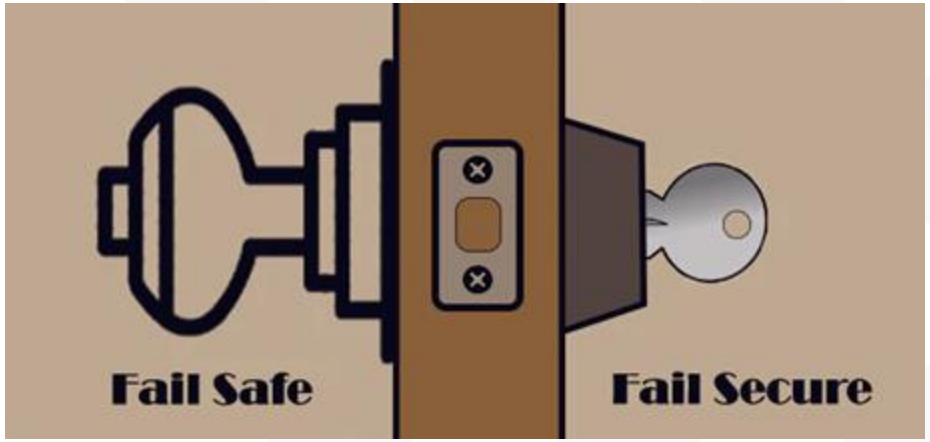
Secure Design Principles

Fail-safe

- The considerations of system failures which are designed to protect human lives, even in failure modes

Fail-secure

- The practice or policy of setting defaults to be intentionally limiting or restrictive to enhance security, privacy or compliance



Secure Design Principles

Failure Modes

- When considering failure modes, consider which component or components of the CIA model are of primary concern for the system.

Considerations for whether the system is protecting a human, physical or digital asset.

KISS - Keep it simple and small.

Complexity brings more considerations for failure.

Physical	State	Digital
Protect People	Fail-Open	Protect Availability
Protect People	Fail-Safe	Protect Confidentiality and Integrity
Protect Assets	Fail-Closed	Protect Confidentiality and Integrity
Protect Assets	Fail-Secure	Protect Confidentiality and Integrity

Secure Design Principles

Don’t Repeat Yourself (DRY)

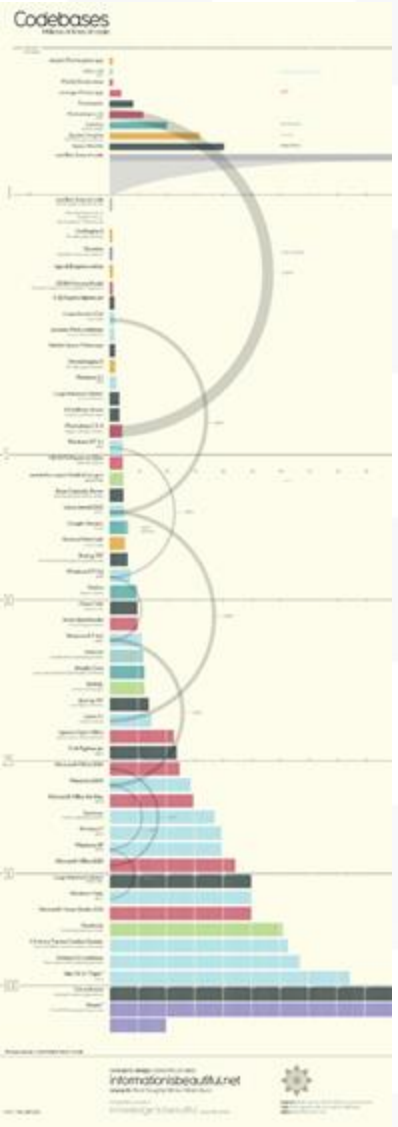
- The idea is to remove redundancy in software by not repeating the same code in multiple places (more places to go back and change later ;-).

Computing Minimalism

- Crafting code to use the least necessary hardware or software possible

Rule of Least power

- Use the least powerful programming language for the needed solution



Link to image comparing the size of the number of lines of code.

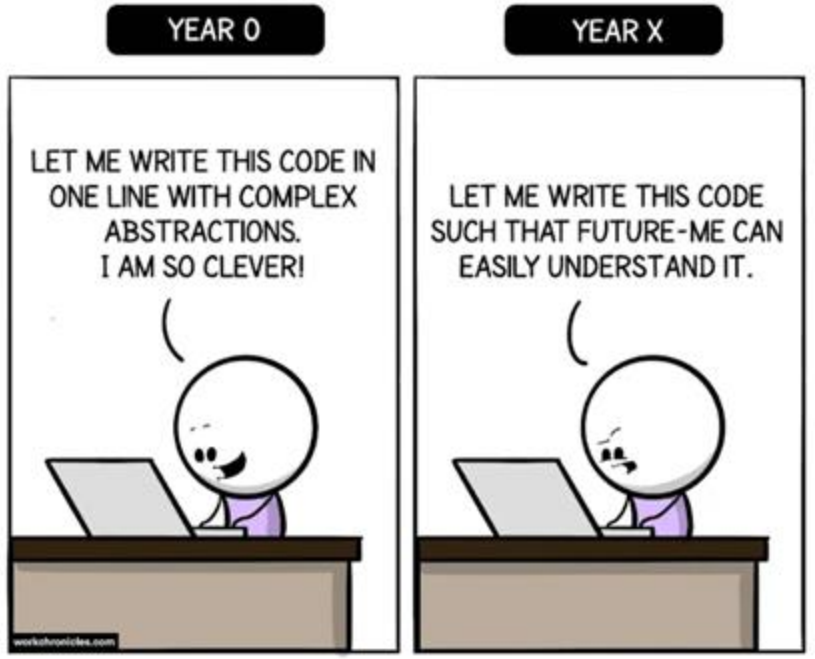
Secure Design Principles

“Worse is better”

- The quality of software does not necessarily increase with increased capabilities and function
  - there is often a worse software state with fewer functions which might offer a more secure option

You Aren’t Gonna Need It (YAGANI)

- The practice that programmers should not write capabilities and functions until they are necessary
  - only create them when you need them



Work Chronicles! I love their comics. (Source)

CISSP® MENTOR PROGRAM – SESSION FIVE

Secure Design Principles

Zero Trust Maturity Model

CISA

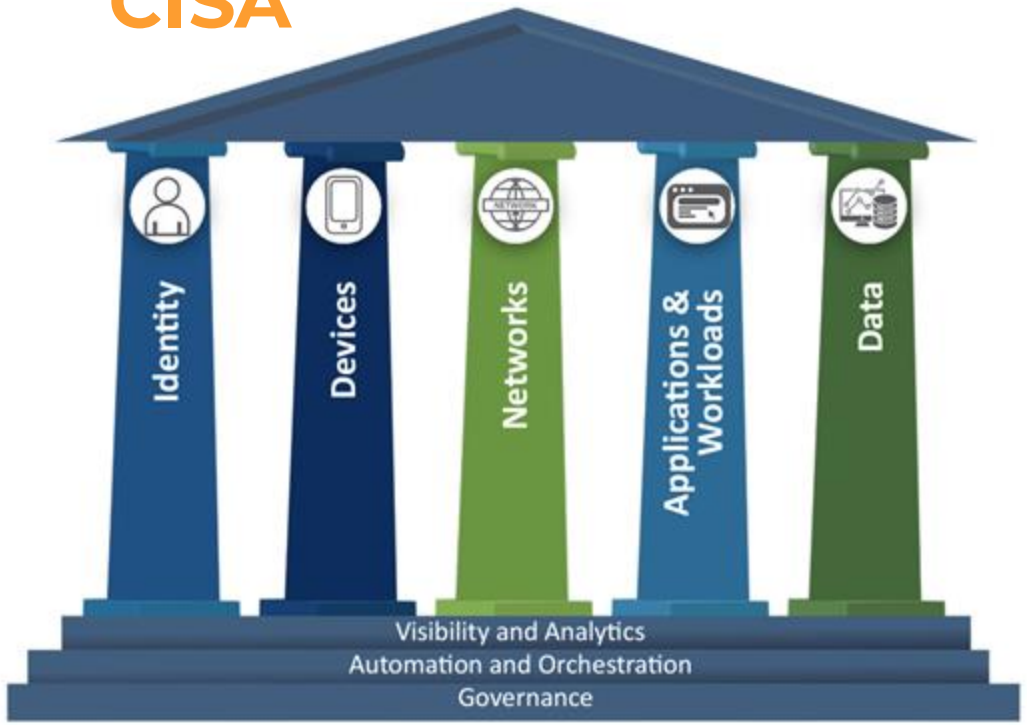
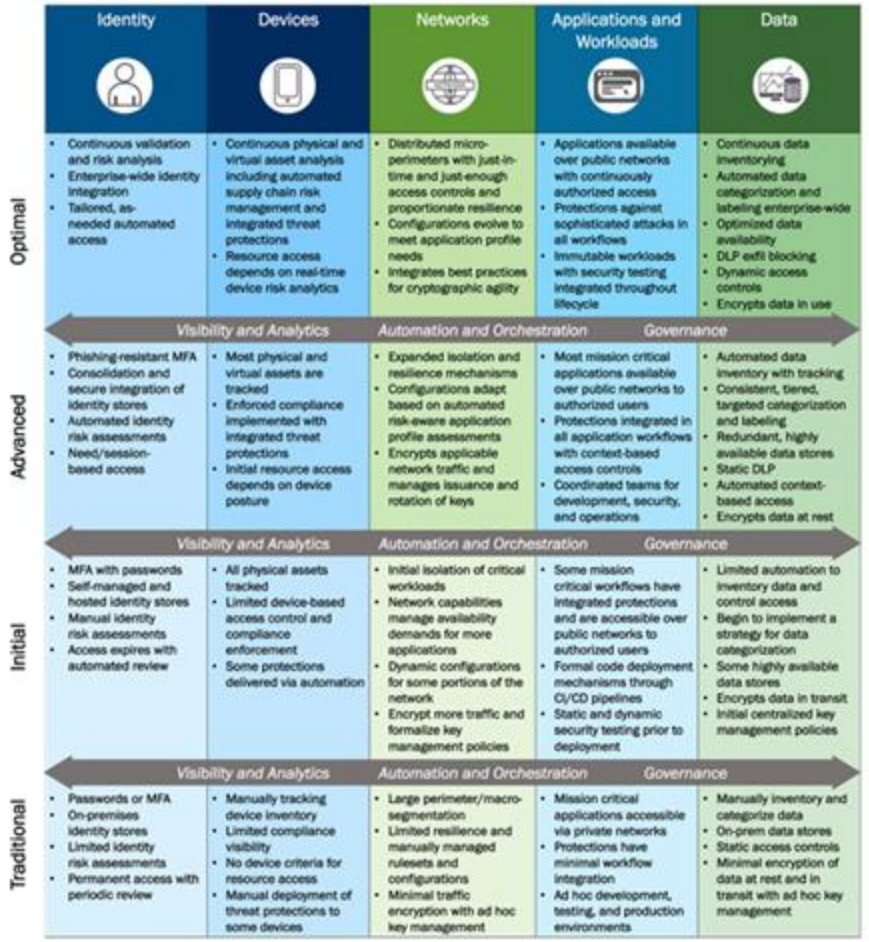


Figure 1: Zero Trust Maturity Model Pillars[8]

CISA's ZTMM is one of many paths to support the transition to zero trust.



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics	Automation and Orchestration	Governance		
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics	Automation and Orchestration	Governance		
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics	Automation and Orchestration	Governance		
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

CISA Zero Trust Maturity Model v.2.0 https://www.cisa.gov/zero-trust-maturity-model

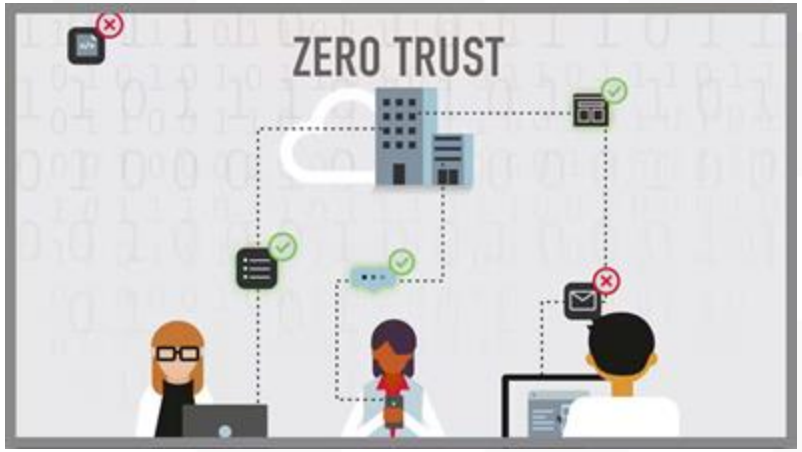
Secure Design Principles

Zero Trust

- The security concept where nothing and no person inside the organization is automatically trusted.

No more castle walls and motes

- While it was it was a long belief that everything inside the organization is trusted and everything outside in trusted, this was a fallacy from the beginning

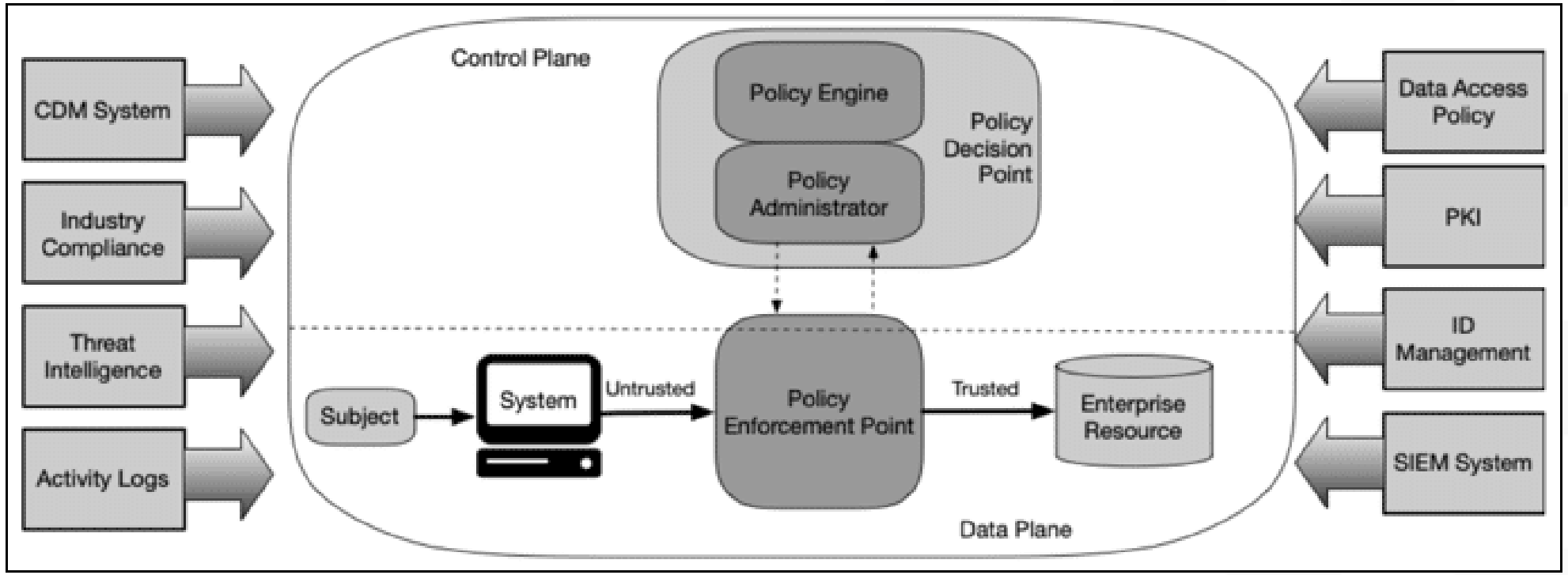


CISSP® MENTOR PROGRAM – SESSION FIVE

Secure Design Principles

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

Zero Trust - NIST



NIST Zero Trust Architecture, SP800-207

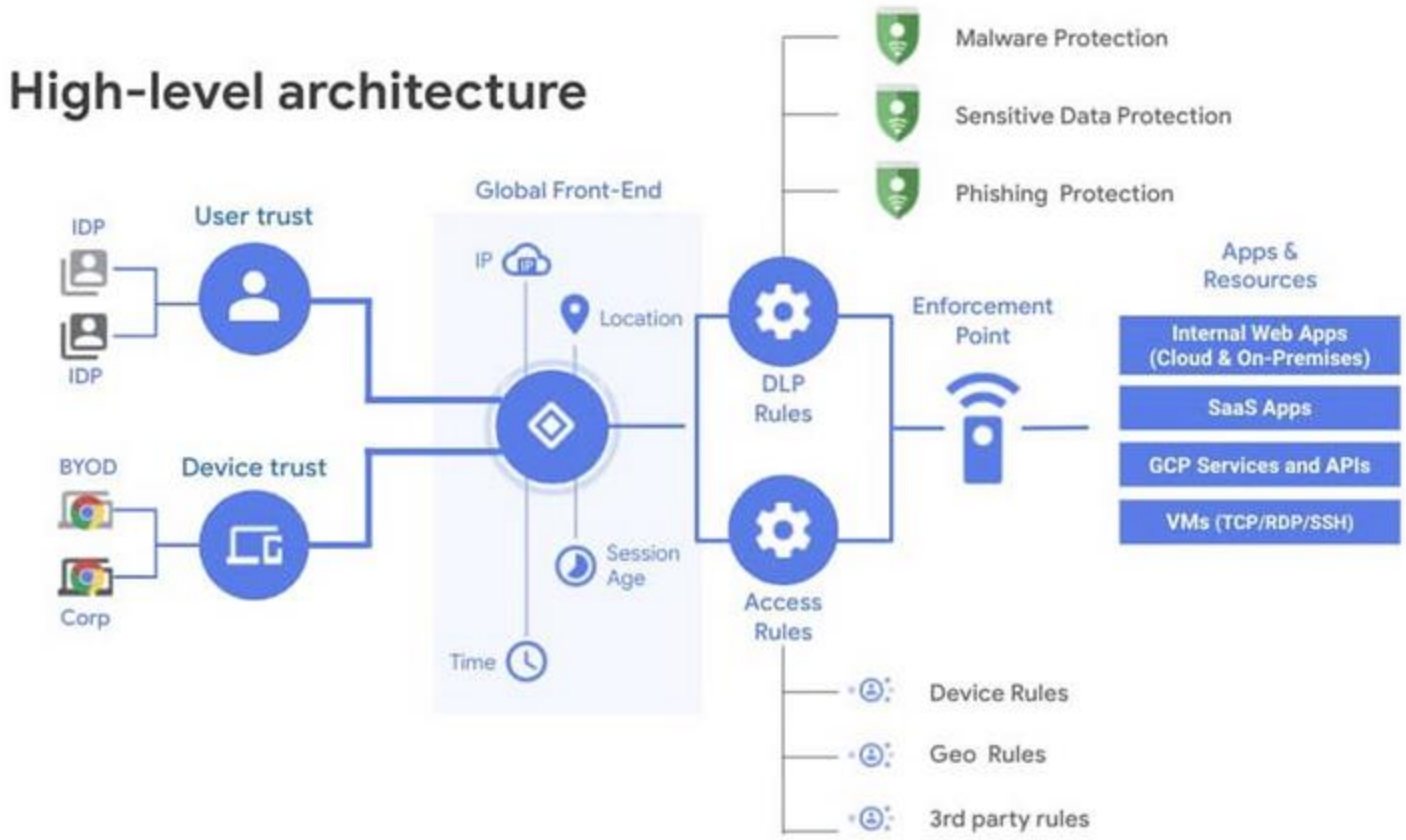
https://www.nist.gov/publications/zero-trust-architecture

CISSP® MENTOR PROGRAM – SESSION FIVE

Secure Design Principles

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

Zero Trust



Secure Design Principles

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

Defense in Depth (layered security)

- Concept of applying multiple, distinct layers of security technologies and strategies to achieve greater overall protection.
- By using combinations of security controls, the impact from the failure of any single control can be reduced if not eliminated.
- Layering is another method of separating system components: security controls are placed between the layers, preventing an attacker who has compromised one layer from accessing other layers.
- Having overlapping security controls such that the failure or compromise of one does not by itself result in an exposure or compromise
- Related to the concept of assumption of breach, which means managing security on the assumption that one or more security controls have already been compromised.

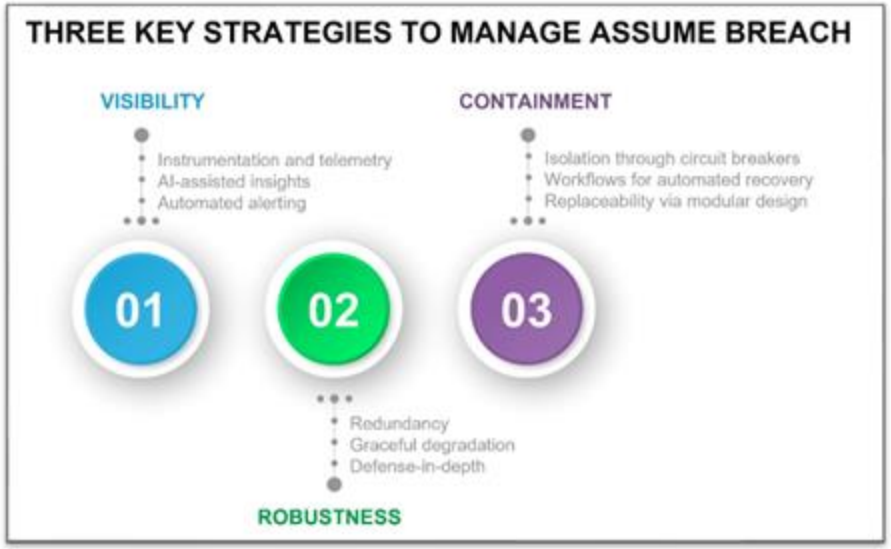
Secure Design Principles

Never Trust, Always Verify

- Since you are not sure if a subject is malicious or not, you don't automatically trust it.
  - Verify its actions before they are allowed to occur

Assume Breach

- The running assumption that you are operating in an environment that whoever or whatever is making the request is malicious.

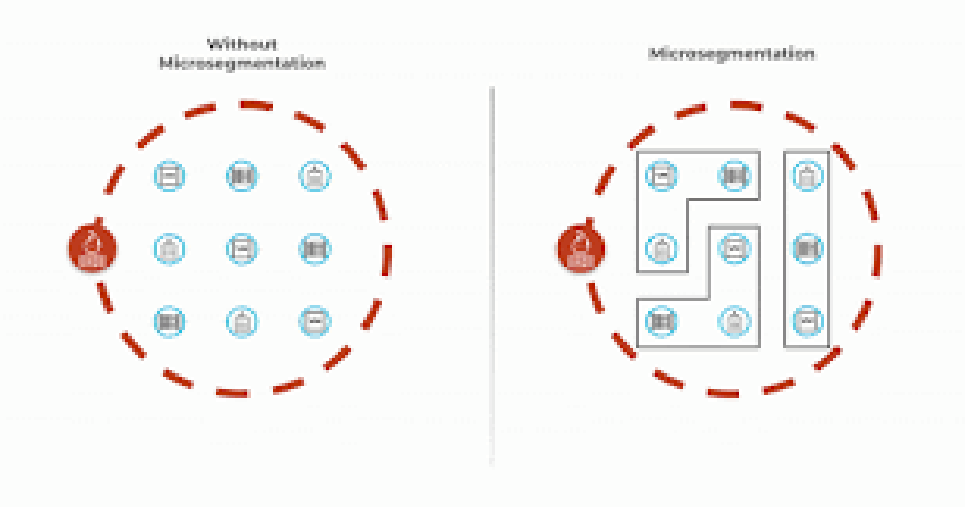


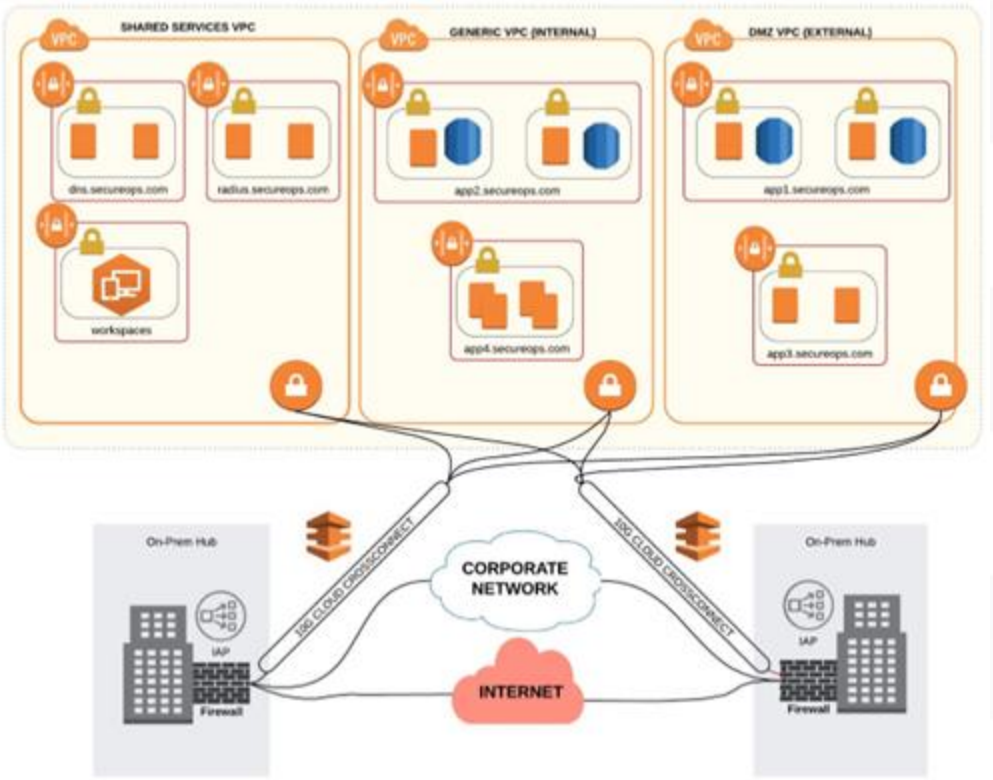
Secure Design Principles

Microsegmation

•Dividing up an internal network into numerous subzones, just enough for the application, system or device to function.

- uses the concept of least privilege
  - Only get access to what you need to know or use

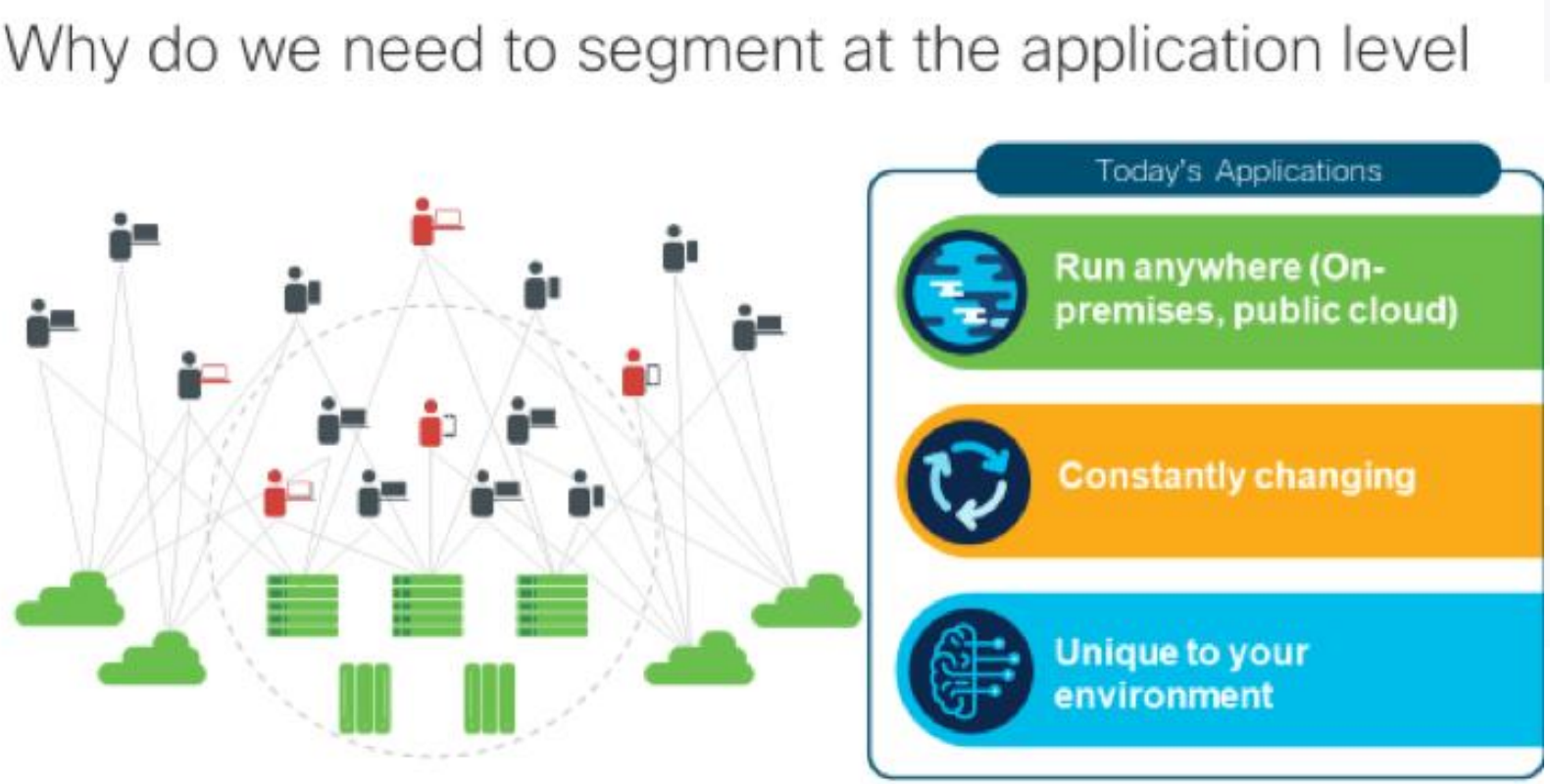




Secure Design Principles

Microsegmation

- Allow applications to run anywhere
- Keep up with changing environments
- Customize to your security needs



Secure Design Principles

Never Trust, Always Verify

- Reduces the impact of insider threats
- Limits lateral movement in the environment

Privacy by Design (PbD)

• A guideline to integrate privacy protections into products during the early design states rather than at the end of the development lifecycle.

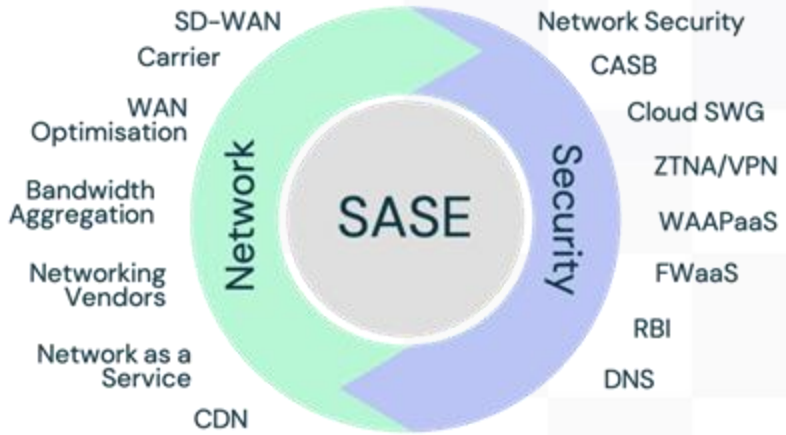
- Proactive, not reactive; preventive not remedial
- Privacy as the default
- Privacy Embedded into the design
- Full Functionality
- End-to-end life cycle protection
- Visibility and Transparency
- Respect for User Privacy

Secure Design Principles

Secure Access Service Edge (SASE)

- is framework that combine network security functions with wide area network capabilities

- Dynamic and secure
- Cloud-native architecture
- Identity-centric security
  - prioritizing the identity of the user and devices over traditional security models
- ZeroTrust Network Access (ZTNA)
- Edge Computing
- Delivered as a Services
- Designed to scale

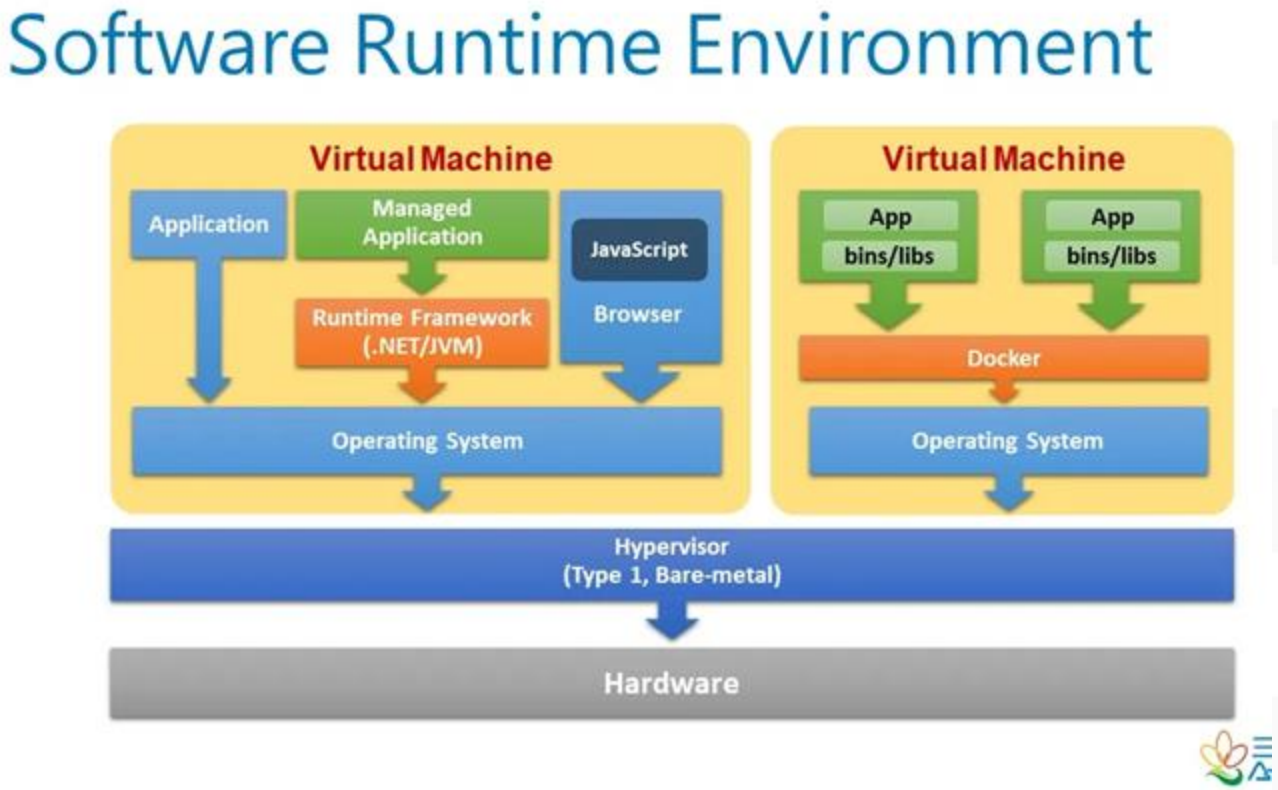


Secure Design Principles

Techniques for Ensuring CIA

• Different system design and development techniques used to ensure CIA principles

- **Confinement**: limiting the access to resources. aka Sandboxing
- **Bounds**: each process rungs at its own authority level (user or kernel in in simple systems.
  - Authority level tells the Operating system how to set the bounds for the process
- **Isolation**: when a process is confined through enforcing access bounds.
  - Used to protect the operating environment



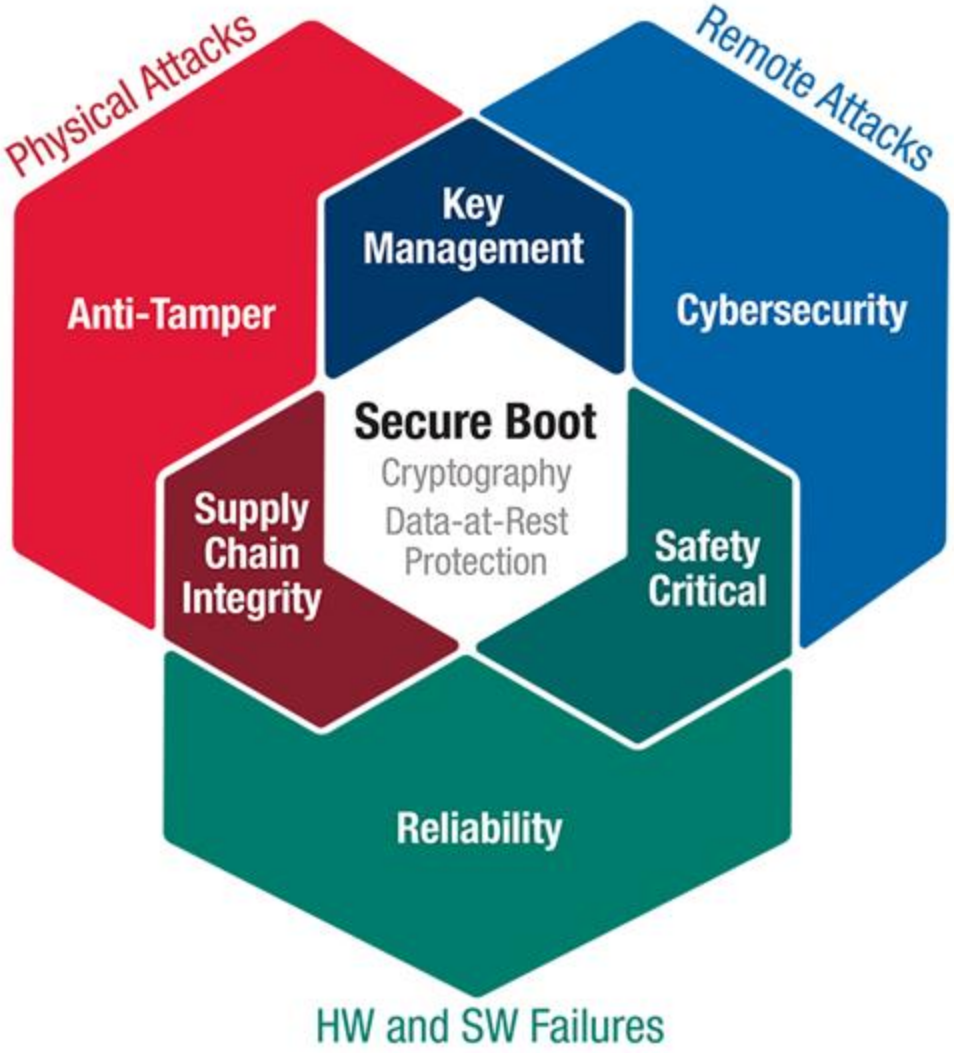
Secure Design Principles

Access Controls

- To ensure the security of the system, only allow subject access only authorized objects
  - Access controls lim the access of a subject to an object
  - Access rules state which objects are valid for each subject

Trust and Assurance

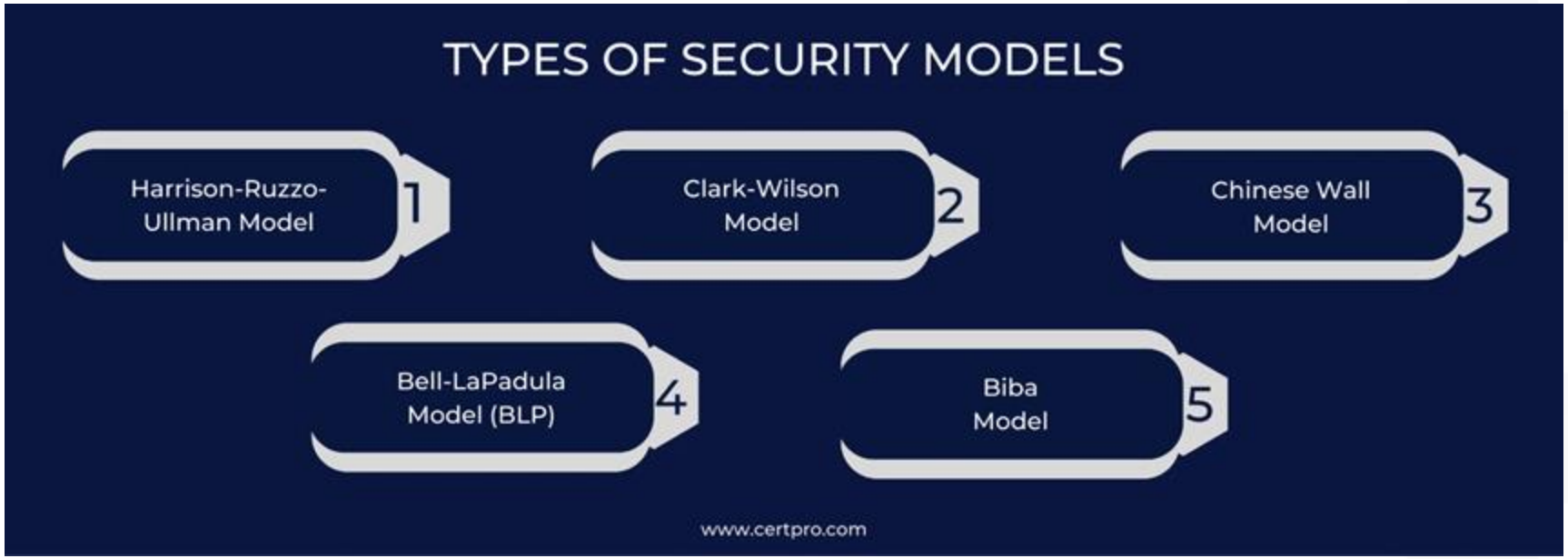
- A trusted system is one which all the protection mechanisms work together to process sensitive data for many different types of users, while remaining stable and secure
  - Assurance the degree of confidence in the satisfaction of the security needs



Security Models

Security Models

- provides a way to designers to map abstract statements into a security policy that tells it what algorithms and data structures are needed to build hardware and software



Security Models

Token

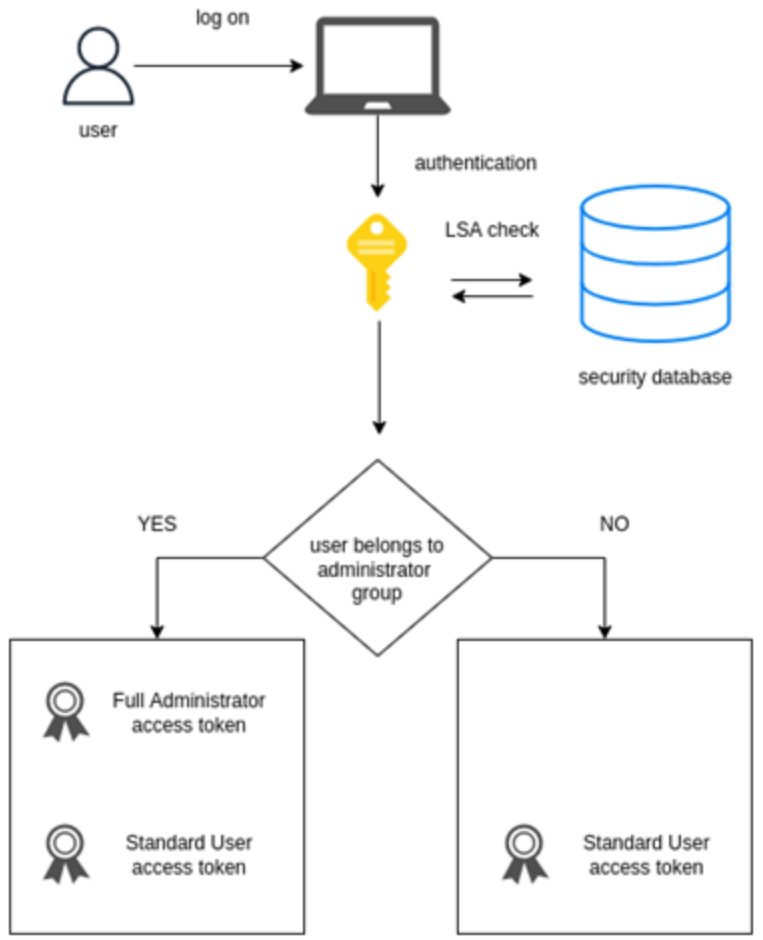
•is a separate object that is associated with a resource and describes the security attribute

Capabilities

• offers a list of security attributes for each controlled object

Labels

• a permanent part of an object attribute
  - does not change
  - can not be altered
  - safeguards against tampering



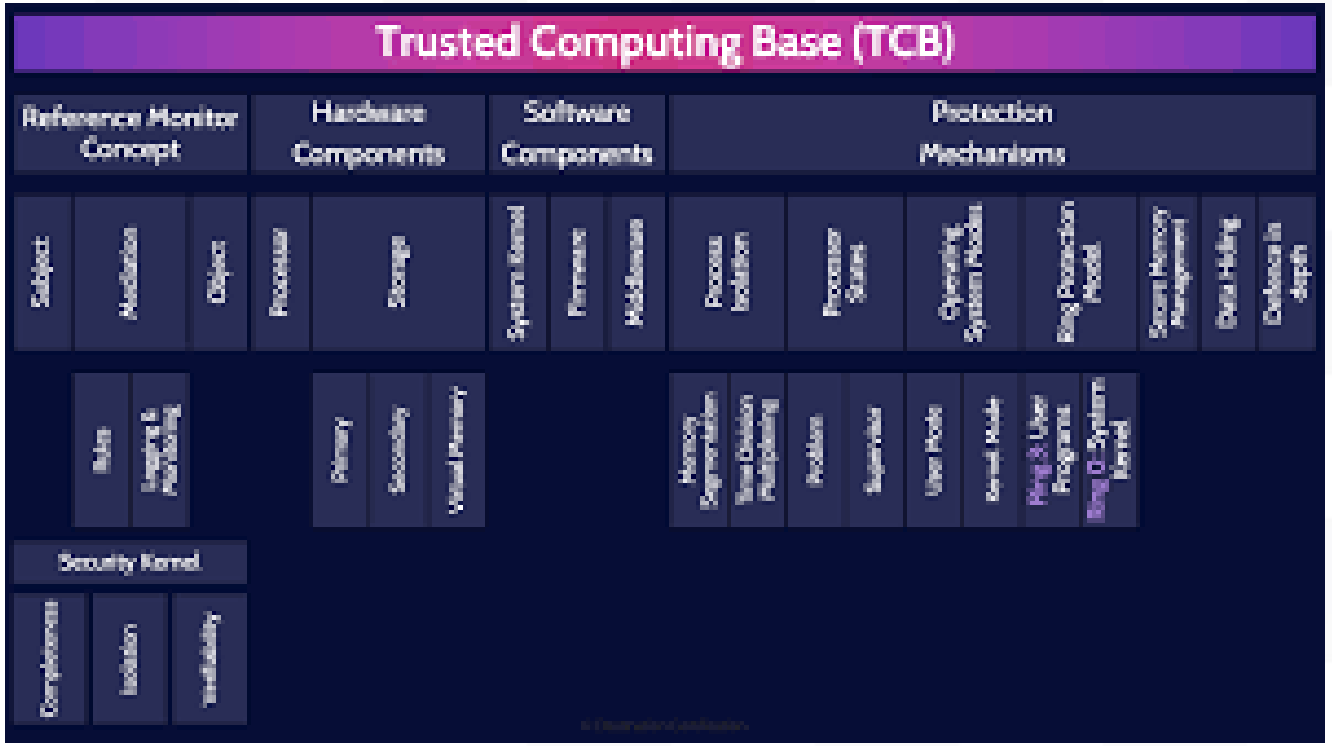
Security Models

Trusted Computing Base (TCB)

- is a design principle that the combination of hardware, software, and controls work together for form a TCB to enforce your security policy

Security Perimeter

- the imaginary boundary that separates the TCB from the rest of the system



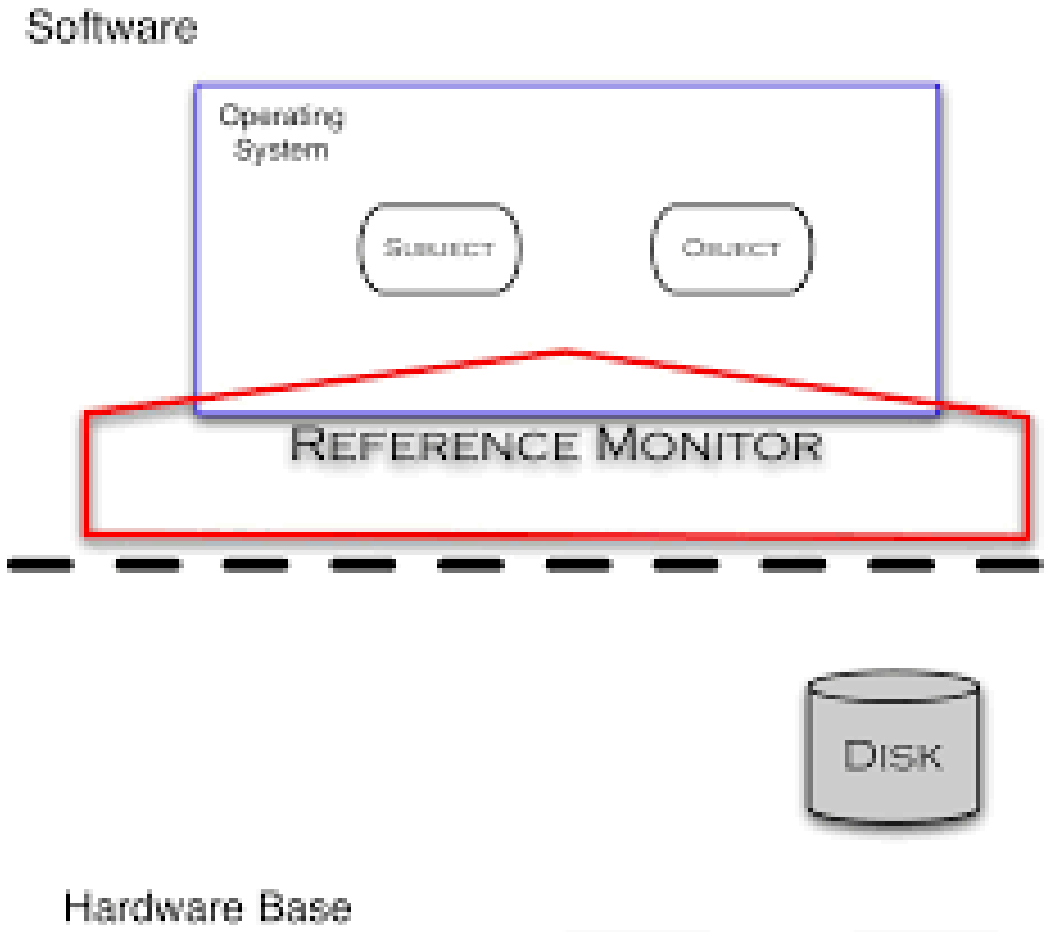
Security Models

Reference Monitors

- is a part of the TCB that validated access to every resources prior to granting access

Security Kernel

- the collection of components in the TCB that work together to implement the reference monitor functions



Security Models

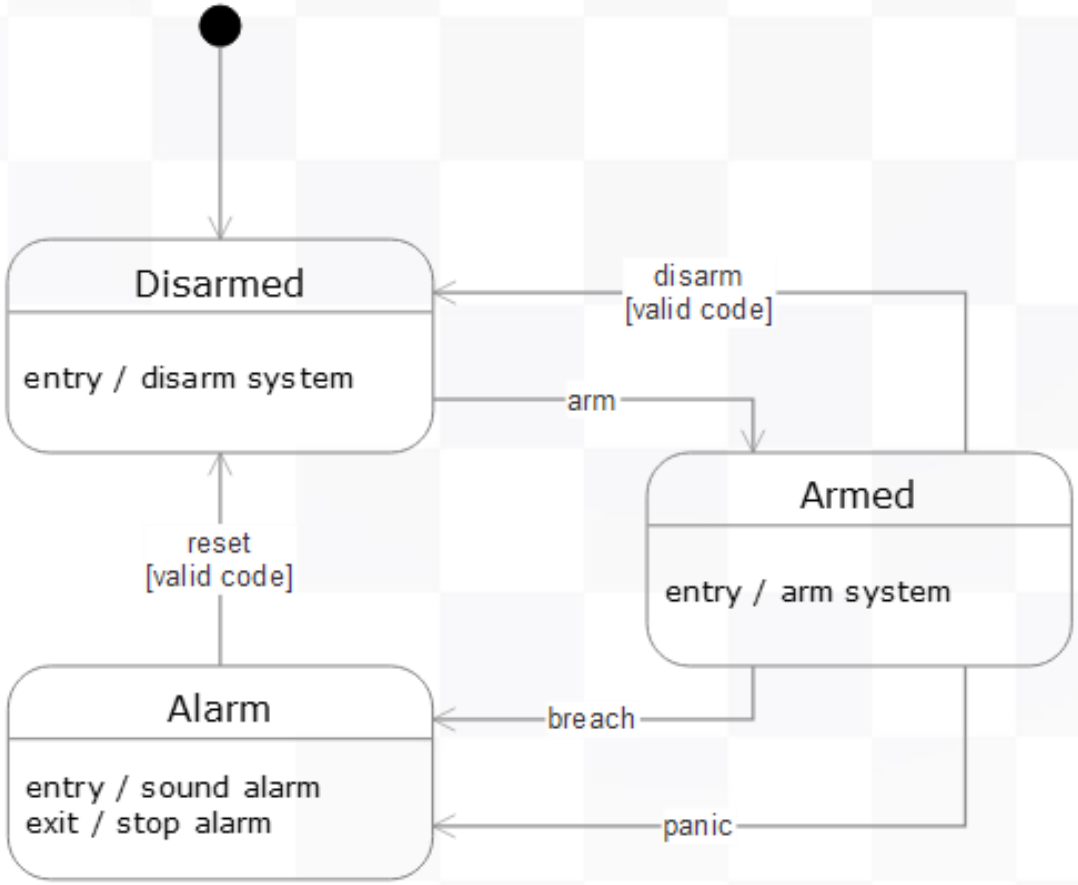
Secure Machine Model

•is a system that is alway secure no matter what state it is in. Based on finite state machine (FSM)

Finite State Machine

• Combines external inputs with and internal machine state to model all kinds of complex systems, including parsers, decoders and interpreters.

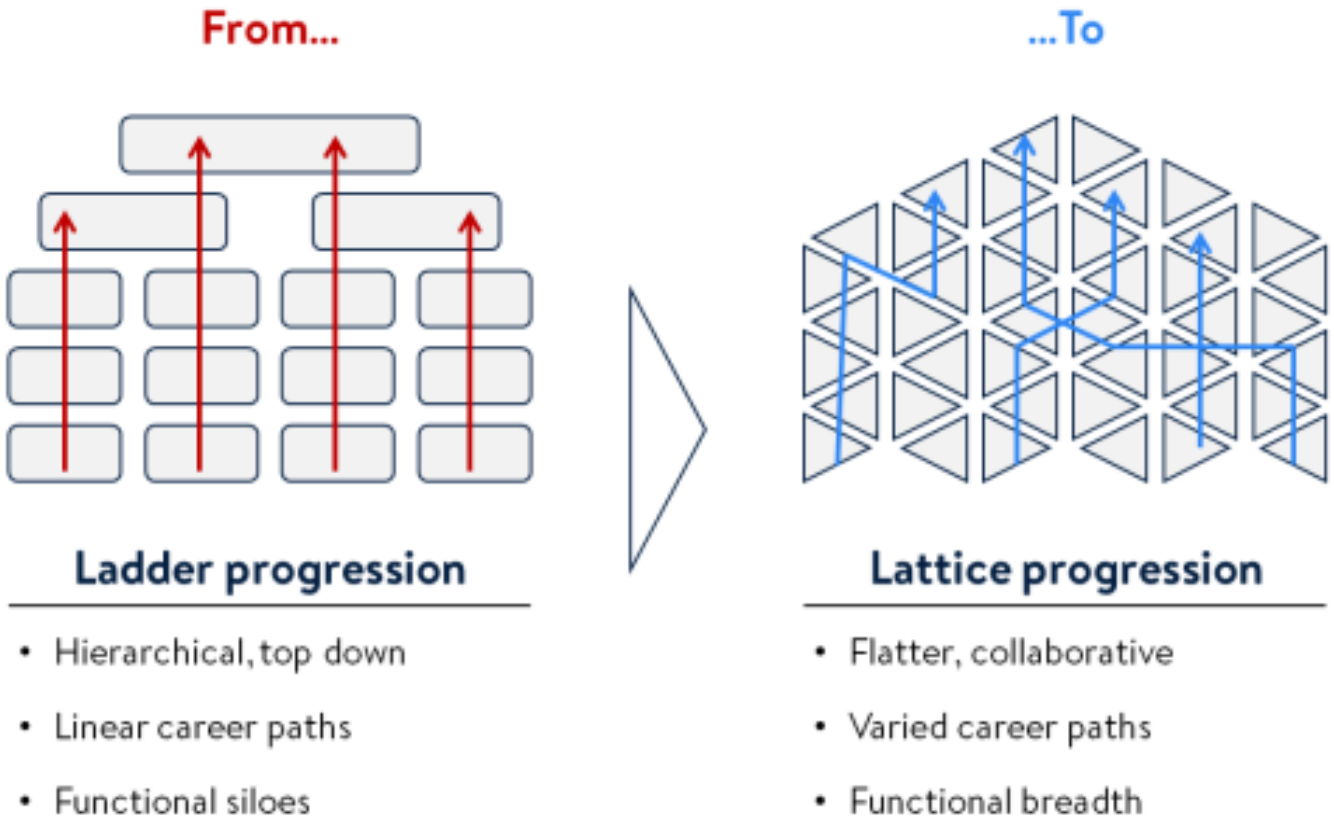
- Input + current state = Function of the current state
- Output = F(input,current state)



Security Models

Lattice Model

- A lattice is a finite set with a partial ordering - partial ordering is a binary relation that is reflexive, anti-symmetric, and transitive.
  - Reflexive means that each item in the set is comparable to itself.
  - Anti-symmetric means that no two different elements precede each other.
  - Transitive means that if a yields b, and b yields c, then a yields c.



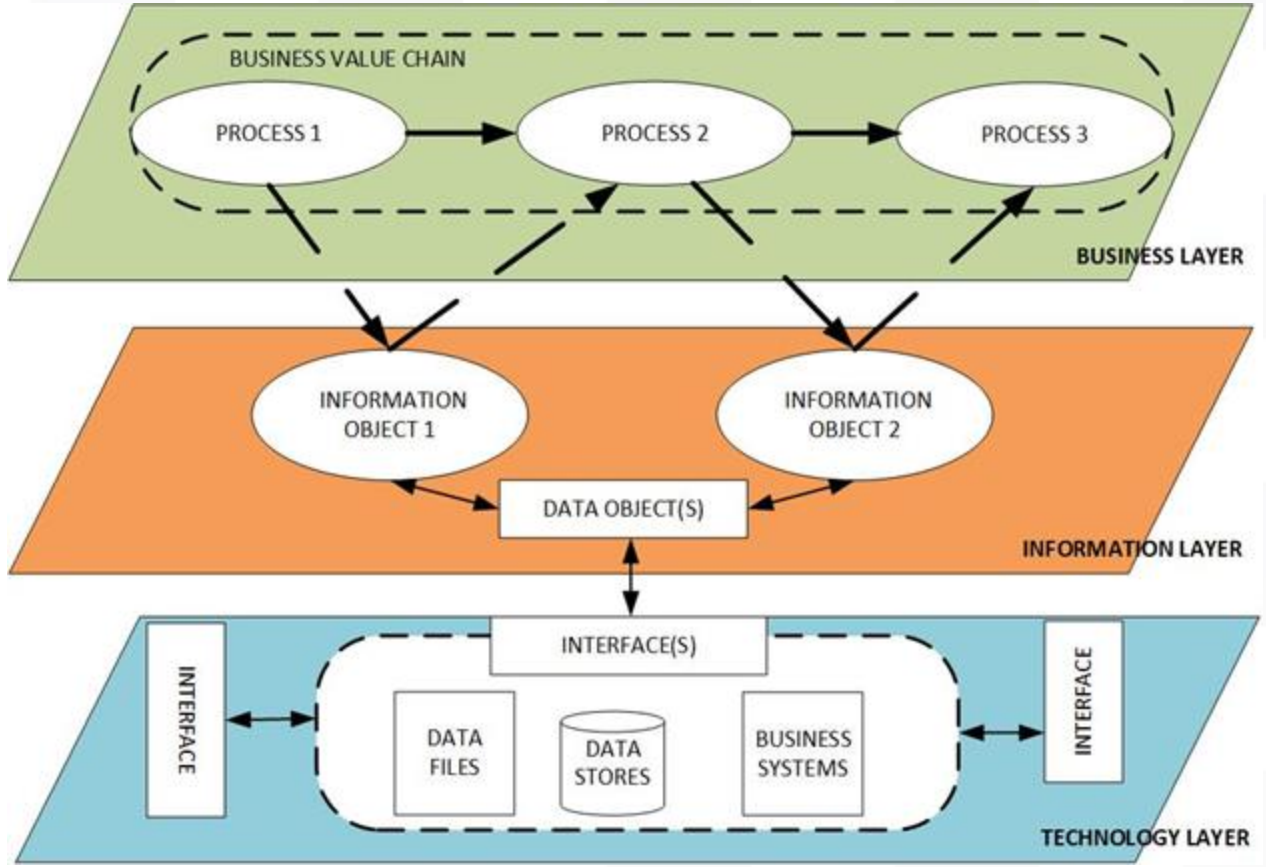
Security Models

Information Flow Model

•is a system that focusing on the flow of information.

- designed to prevent unauthorized, insecure or restricted information flow between different levels of security

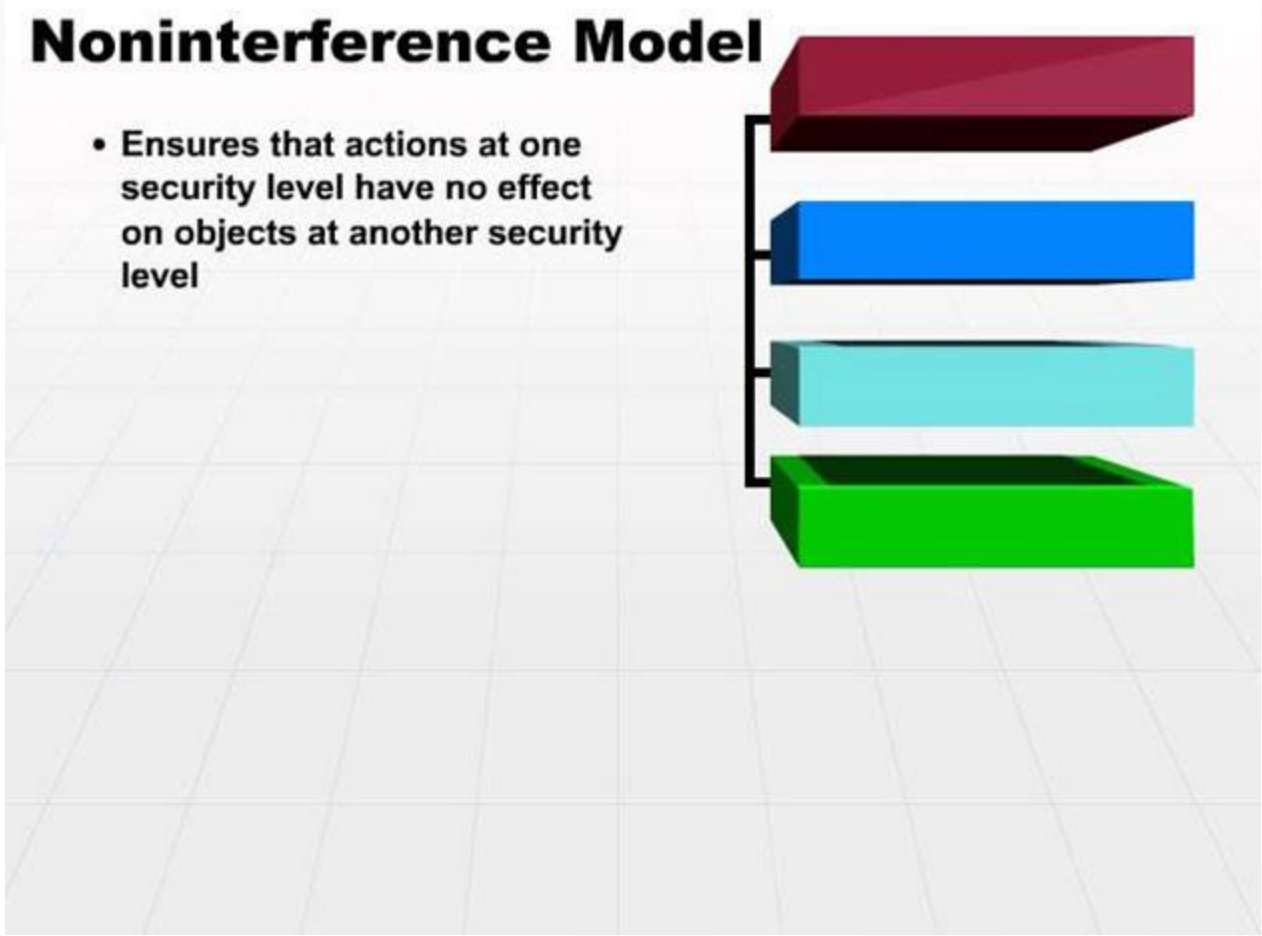
- differentiate between subjects and objects at the same or different classification levels



Security Models

Noninterference Model

- loosely based on the information flow model,
  - focused on the actions of a subject at a higher security level affecting the system or state of a subject at a lower security level

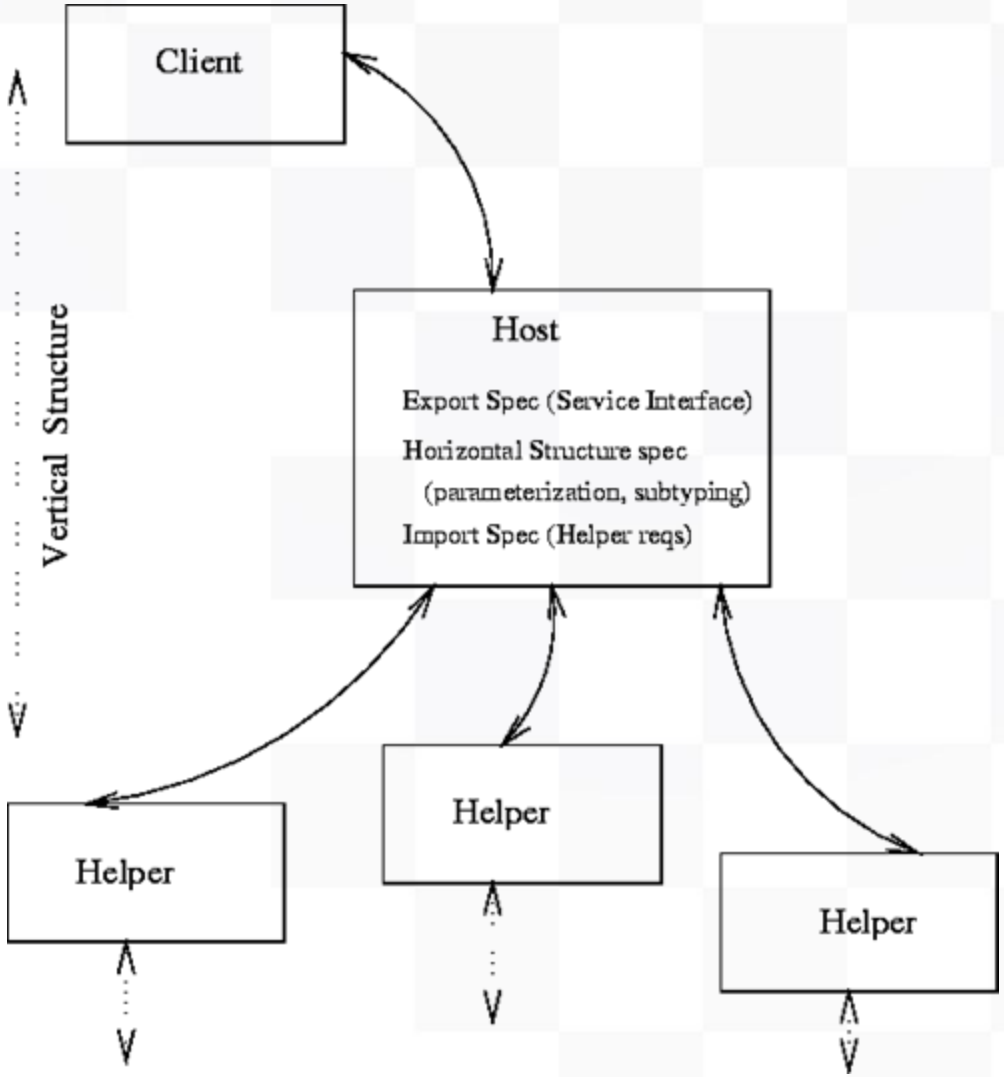


Security Models

Composition Theories

• explains how the outputs from on system relates to the inputs to another system

- **cascading** - the input for one come from the output of another
- **feedback** - one system provides input to another system which reciprocates by reversing the roles
- **hookup** - one system sends inputs to another system but also send inputs to external entities

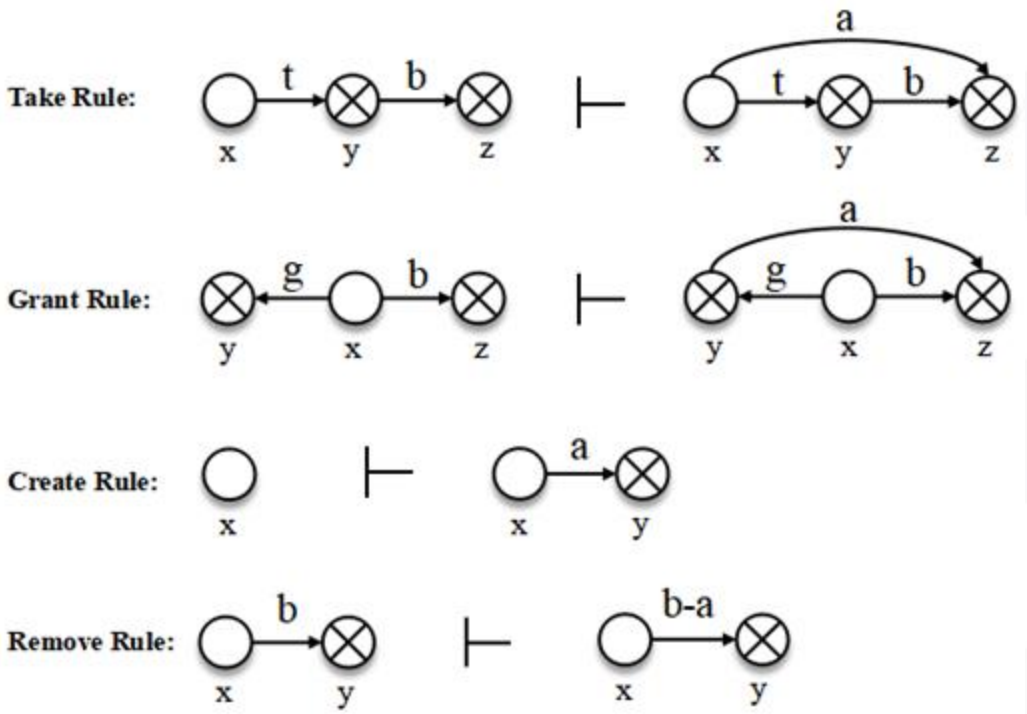


Security Models

Take-Grant Model

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

- **take rule** - allows a subject to take rights over from another object
- **grant rule** - allows a subject to grant rights to an object
- **create rule** - allows an object to create new rights
- **remove rule** - allows a subject to remove rights it has

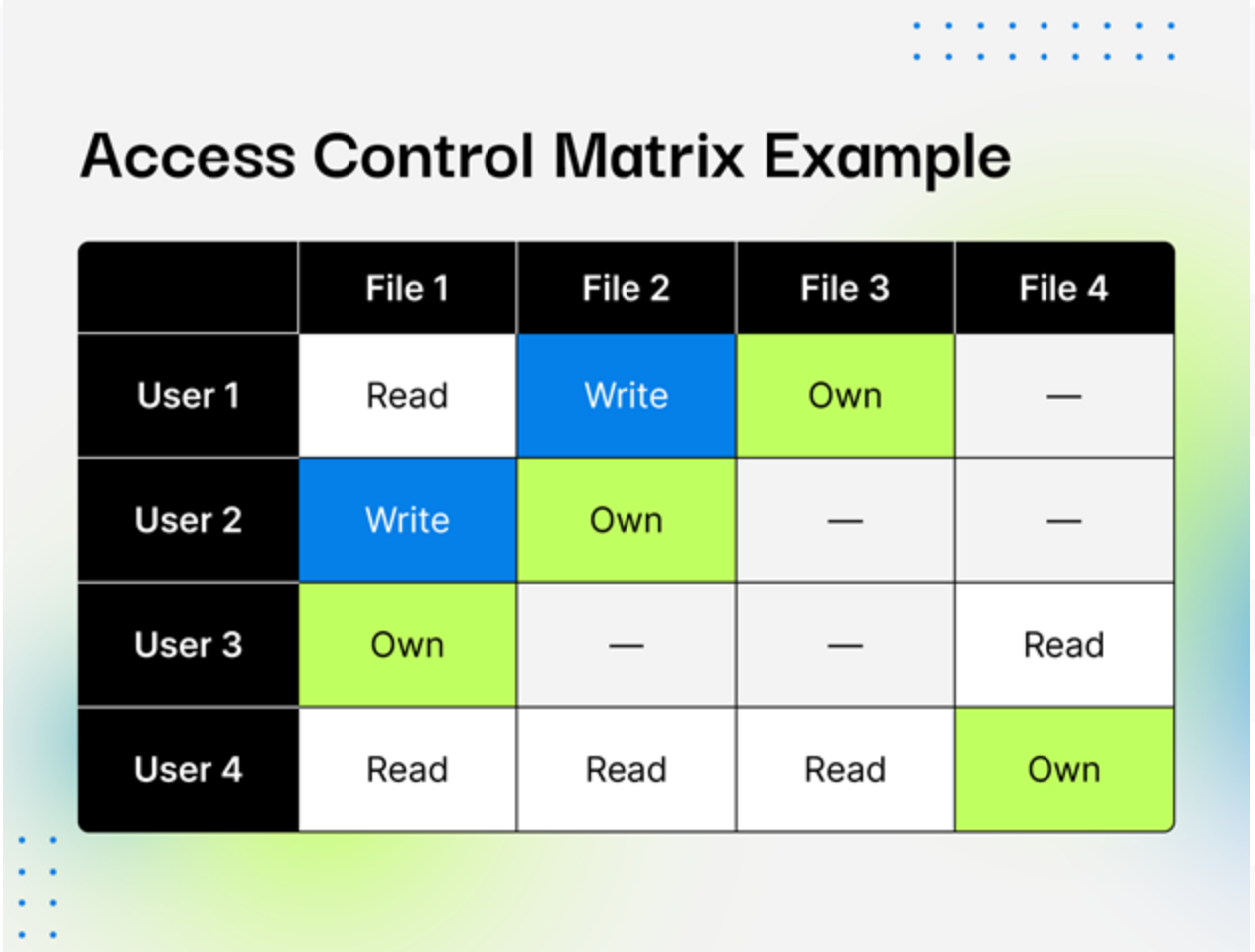


Security Models

Access Control Matrix

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

- each column is an Access Control List (ACL) pulled from an object.
- An ACL is tied to an object and validates the actions each subject can perform



CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Confidentiality Model

Bell-LaPadula Model (3 rules)

Simple Security Property (ss property) - **No read up**, this rule prevents a subject from reading an object at a higher security level.

Star Property (* property) - **No write down**, this rule prevents a subject from writing to an object at a lower security level.

Discretionary-Security Property - Subject can perform an operation on an object if **permitted by the access matrix**

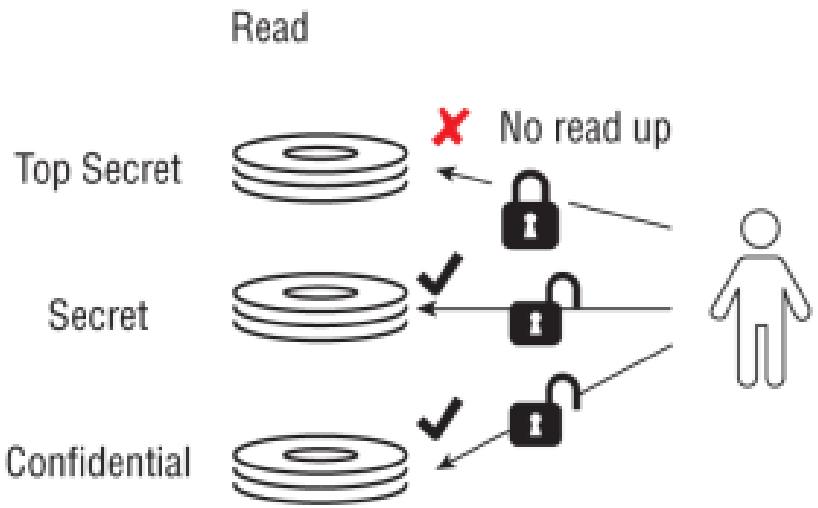
CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

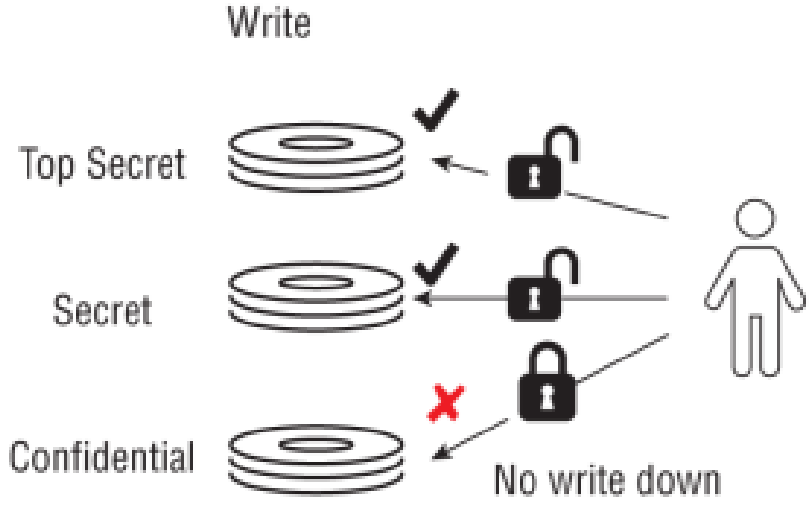
Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Bell-LaPadula Model (3 rules)



Simple Security Property



The Star Property

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Bell-LaPadula Model (3 rules)

Issues not well addressed by the Bell-LaPadula Model

- It does not consider risks to the *integrity* of information. Protecting the integrity of objects means preventing the unauthorized, possibly malicious, modification of an object.
- Does not deal with covert channels or the possibility of performing permitted operations in a manner that reveals confidential information through side channels

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Biba *Integrity* Model

- Simple Integrity Property - **No read down**, this rule prevents compromising the integrity of more secure information from a less secure source. In other words, higher integrity processes could produce untrustworthy results if they read and use data from lower integrity sources.

- Star Integrity Property (* integrity property) - **No write up**, this rule prevents the corruption of more secure information by a less privileged subject.

- Invocation Property states that a process from below **cannot request higher access (read nor write)**; only with subjects at an equal or below

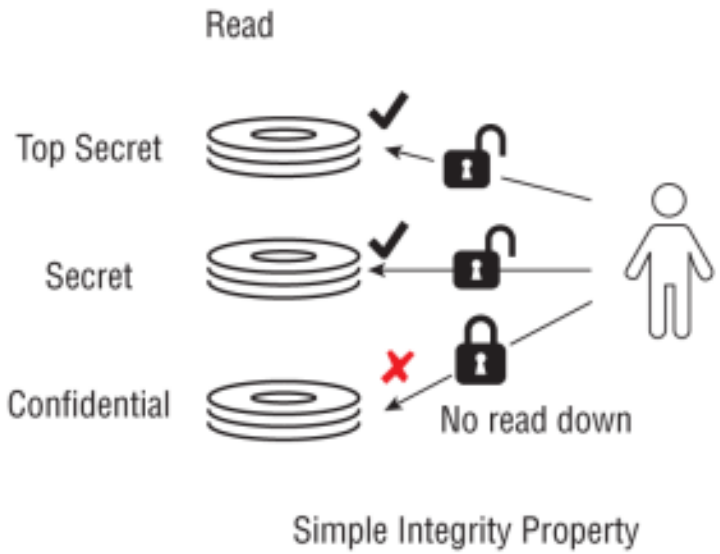
CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Biba Integrity Model



Simple Integrity Property

Star Integrity Property

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Clark-Wilson Model (2 concepts)

- **Well-formed transactions -** Well-formed transaction is that subjects are constrained to make only those changes that maintain the integrity of the data.
- **Separation of duties -** Aims to make sure that the certifier of a transaction is a different party from the initiator or implementer of the transaction.

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Clark-Wilson Model -

- uses security labels to grant access to objects, but only through transformation procedures and a restricted interface model, which uses classification-based restrictions to offer only subject specific authorized information and functions.
- **Constrained data item (CDI)** - This is the key data type in the Clark– Wilson model, and it refers to data whose integrity must be preserved.
- **Unconstrained data item (UDI) -** This includes all data other than CDIs, typically system inputs.
- **Integrity verification procedures (IVPs) -** These procedures check and ensure that all CDIs are valid.
- **Transformation procedures (TPs) -** These procedures enforce a system's integrity policy and maintain the integrity of CDIs.

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Brewer-Nash Model

- Simple Integrity Property - **No read down**, this rule prevents compromising the integrity of more secure information from a less secure source. In other words, higher integrity processes could produce untrustworthy results if they read and use data from lower integrity sources.
- Star Integrity Property (* integrity property) - **No write up**, this rule prevents the corruption of more secure information by a less privileged subject.

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Brewer-Nash Model

- Individual pieces of information related to a single company or client are called objects, in keeping with BLP's usage.
- All objects related to the same company (or client) are part of what is called a company data set.
- All company data sets in the same industry (i.e., that are competitors) are part of what is called a conflict of interest class.

Ethical wall / Cone of Silence

CISSP® MENTOR PROGRAM – SESSION FIVE

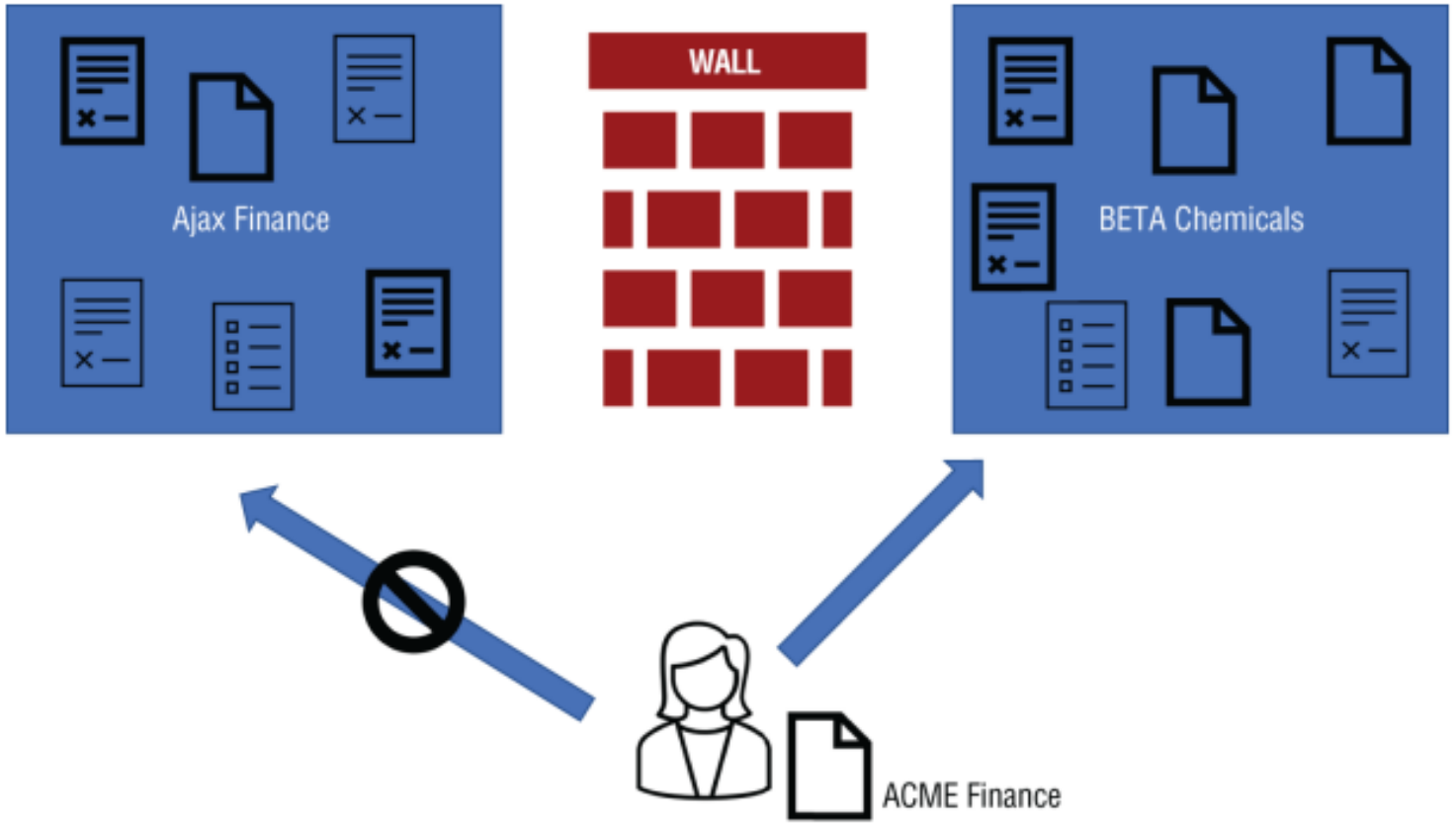
Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Brew

- Indiv
  in ke
- All o
  data
- All c
  calle



objects,

company

of what is

CISSP® MENTOR PROGRAM – SESSION FIVE

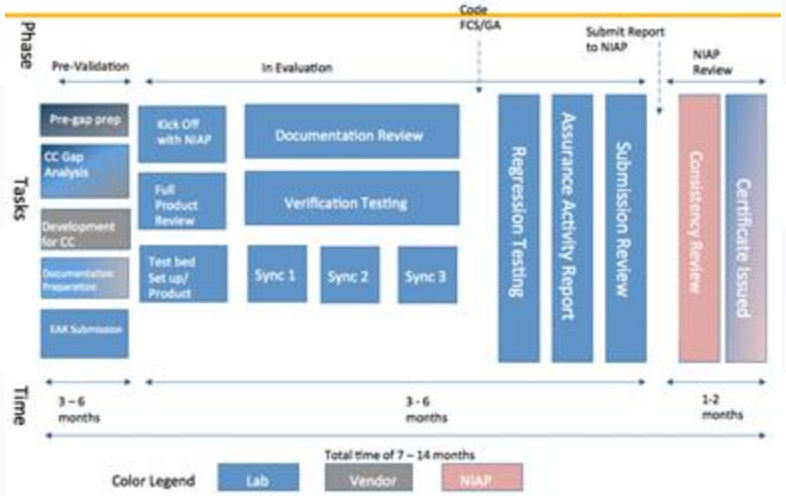
Security Models

Understand the Fundamental Concepts of Security Models

Primer on Common Model Components

Common Criteria

- Defines various levels of testing and confirmation of a systems' security capabilities
- adds buyer confidence in security of evaluated products
- to eliminate duplicate evaluations (across country, agency or valuation organization. Specific systems and Configurations noted to avoid duplicate work)
- to keep security evaluations more cost-effective and efficient
- To keep product to high adherence and consistent standards

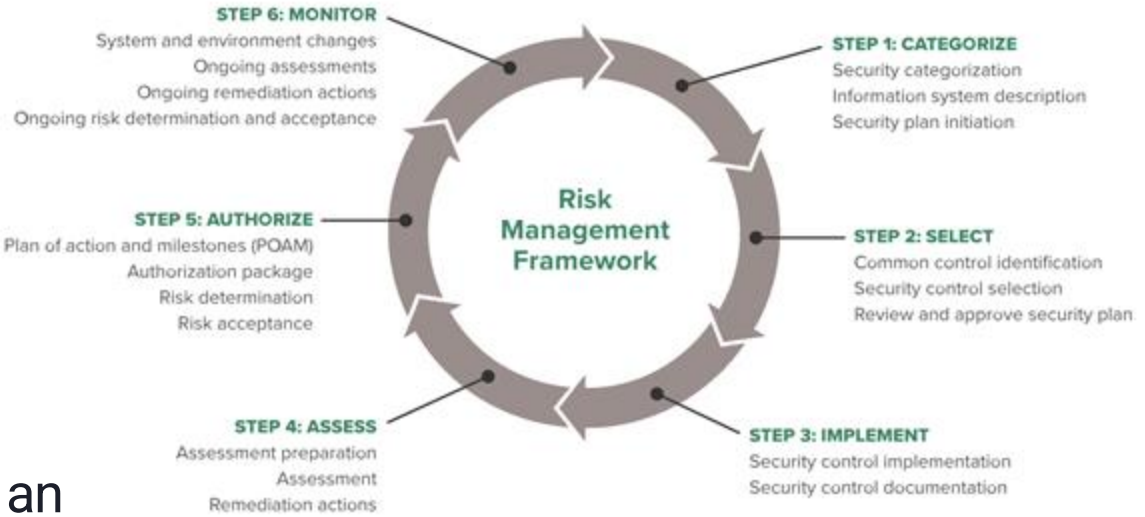


CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Authorization to Operate (ATO)

- Replaces the previous term from accreditation
- is an official authorization to use a specific collection of secured IT/IS systems to perform business tasks and accept the identified risk.
- Authorization Official is authorized to evaluate an IT/IS system, its operation, its risk and potentially issue an ATO
    - Finite time frame - 3 years
    - Needs to be obtained in the event the system has as significant security breach or change in security.



Security Models

Understanding Security Capabilities of Information Systems

Foundational Capabilities of Information Systems

- Memory protection
- Trusted Platform Modules (TPMs)
- Cryptographic modules
- Hardware Security Modules (HSMs)

Security Models

Understanding Security Capabilities of Information Systems

Memory Protection

- Foundational security controls on all systems that allows multiple programs to run simultaneously is memory protection.
- Prevents one program from referencing memory not specifically assigned to it.
- If a program attempts to reference a memory address it is not permitted to access, the system blocks the access, suspends the program, and transfers control to the operating system.

Question: What common attack type is prevented with memory protection?

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understanding Security Capabilities of Information Systems

Memory Protection

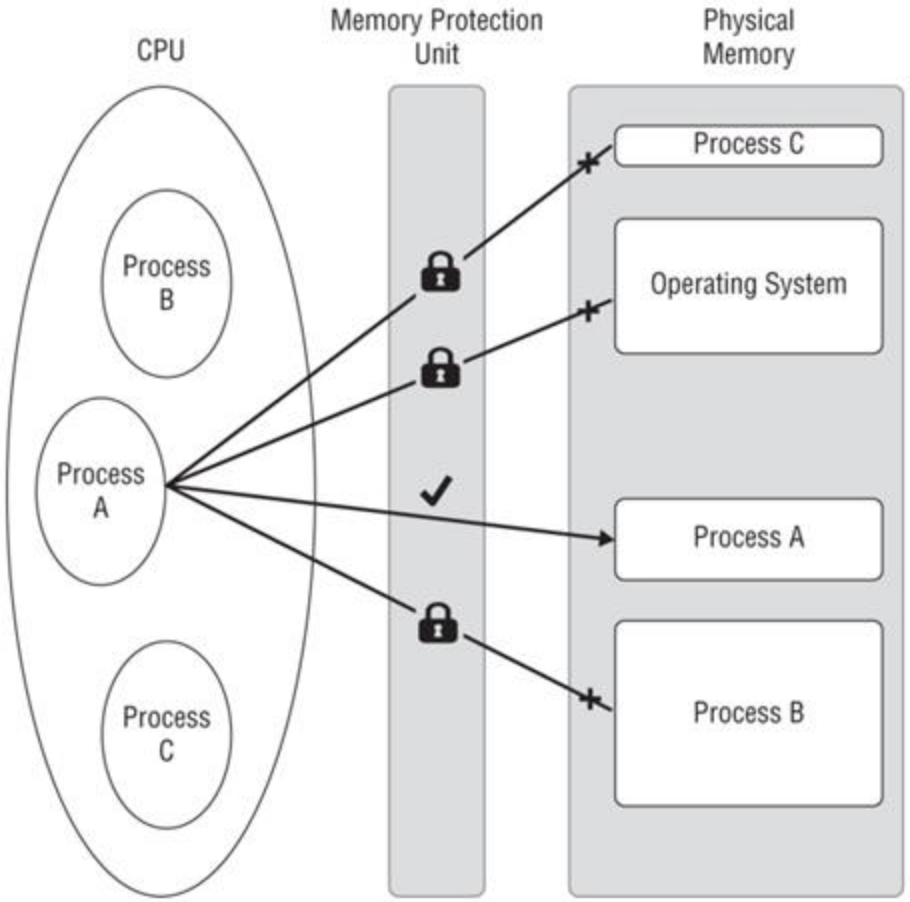


FIGURE 3.7 Operating system memory protection

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understanding Security Capabilities of Information Systems

Memory Protection – Dual-mode operation

- **Hardware feature** that is required to support memory protection is dual-mode operation.
- Processor can operate in one of (at least) two modes:
  - Privileged (or kernel) mode and
  - Unprivileged (or user) mode
- The *operating system runs in privileged mode*, which grants it permission to set up and control the memory protection subsystem. Privileged mode also permits the operating system to execute special privileged instructions that control the processor environment.
- The *program runs in unprivileged mode*, which limits it to accessing only the specific memory area dictated by the operating system.

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understanding Security Capabilities of Information Systems

Memory Protection – ASLR

- *Address space layout randomization* (*ASLR*), seeks to mitigate the risks of **predictable memory address location**. (The location in memory for a known instruction becomes a risk when there is a threat of exploiting that location for an attack.)
- For example, a buffer overflow attack requires knowing two things: the exact amount by which to overflow the memory to facilitate executing malicious code, and where exactly to send the overflow. ASLR defeats the second item by randomizing the location.

Security Models

Understanding Security Capabilities of Information Systems

Memory Protection (*Potential Weaknesses*)

- Proper memory protection **relies upon both** the correct **operation of the hardware** and the correct **design of the operating system** to prevent programs from accessing memory they have not been given permission to access.
- A defect in either can compromise the security provided by memory protection. Note that this protection prevents the direct disclosure of memory contents that are blocked from an unauthorized program, but does not necessarily prevent side-channel exploits from revealing information about memory that is protected from access.
- Attacks that leverage ineffective isolation and memory protection can have catastrophic effects. Spectre and Meltdown exploits in 2018 revealed, flaws in the design of Intel and some other CPU chips permitted clever programming techniques to deduce the contents of memory locations that those programs were not permitted to access directly.

Security Models

Understanding Security Capabilities of Information Systems

Secure Cryptoprocessor (*Features*)

- **Tamper detection** with automatic destruction of storage in the event of tampering.
- **Chip design features** such as shield layers to prevent eavesdropping on internal signals using ion probes or other microscopic devices.
- **Hardware-based cryptographic accelerator** (i.e., specialized instructions or logic to increase the performance of standard cryptographic algorithms such as AES, SHA, RSA, ECC, DSA, and ECDSA.
- **Trusted boot process** that validates the initial boot firmware and operating system load.

Security Models

Understanding Security Capabilities of Information Systems

Secure Cryptoprocessor (*Types*)

- Proprietary, such as Apple's “Secure Enclave” found in iPhones
- Open standard, such as the TPM as specified by the ISO/IEC 11889 standard and used in some laptops and servers
- Standalone (e.g., separate standalone device with external communications ports)
- Smartcards

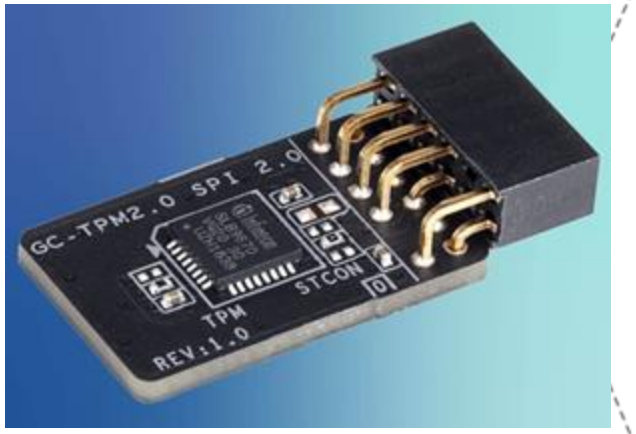
CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understanding Security Capabilities of Information Systems

Trusted Platform Module (TPM)

Provides secure storage and cryptographic services as specified by ISO/IEC 11889



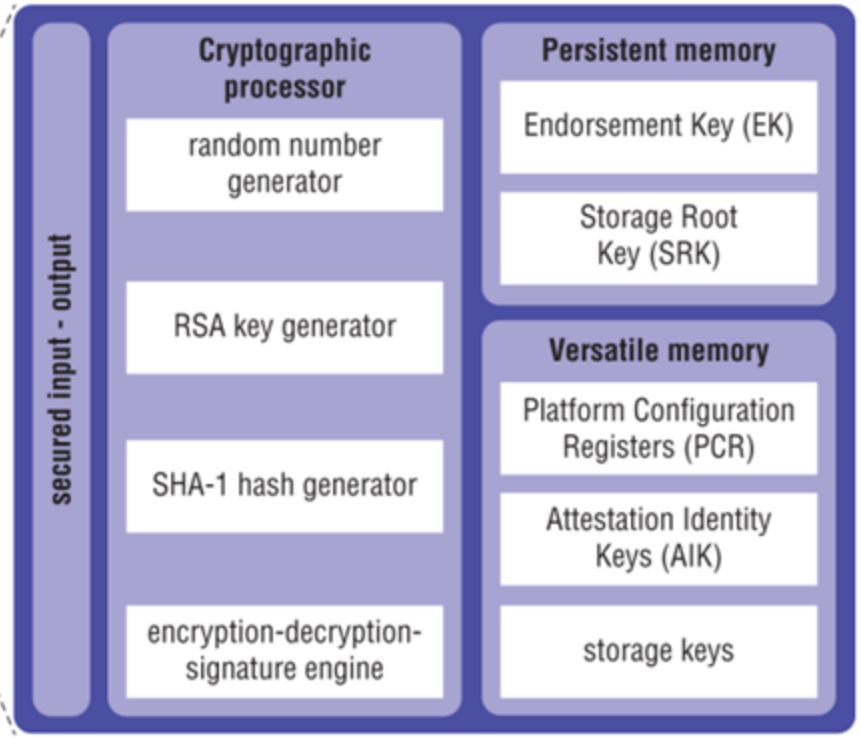


FIGURE 3.8 Trusted Platform Module processes

Security Models

Understanding Security Capabilities of Information Systems

Trusted Platform Module (TPM)

- **Attestation**: Creates a cryptographic hash of the system's known good hardware and software state, allowing third-party verification of the system's integrity
- **Binding**: Encrypts data using a cryptographic key that is uniquely associated with (or bound to) the system
- **Sealing**: Ensures that ciphertext can be decrypted only if the system is attested to be in a known good state

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Understanding Security Capabilities of Information Systems

Trusted Platform Module

- Generate ***private/public key pairs*** such that the **private key never leaves the TPM** in plaintext - Increasing the security related to the private key.
- **Digitally sign** data using a private key that is stored on the TPM and that never leaves the confines of the TPM. Significantly decreasing the possibility that the key can become known by an attacker and used to forge identities and launch man-in-the-middle (MITM) attacks.
- Encrypt data such that it can **only be decrypted using the same TPM**.
- Verify the state of the machine the TPM is installed on to detect certain forms of tampering (i.e., with the BIOS) and ensure platform integrity.

We'll cover cryptography in session five.

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Information System Life Cycle

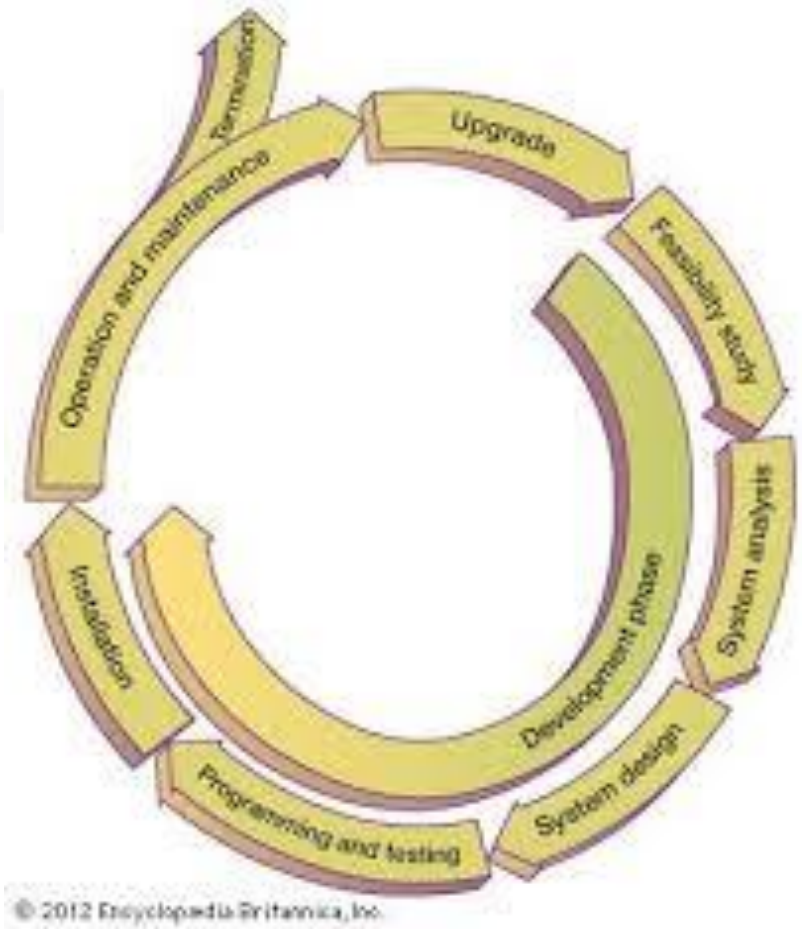
- The management of information system from assessment of needs through the decommissioning of the system.
- **Needs and Requirements** - understanding the needs, expectations and requirements of stakeholders and how they will interact with the information system.
- **Requirements analysis** - the examination of requirements for both functional and non-functional requirements considering constraints and in alignment with the overall goals of the organization

CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Information System Life Cycle

- **Architectural Design** - this is the blueprint of the information system defining the overall structure, components, models, data flow and system interfaces
- **Development and Implementation** - this is the where the actual coding and developing the software of the system, configuring the hardware, various the different components
- **Integration** - the process of combining the different modules or components of the system together so that they function seamlessly

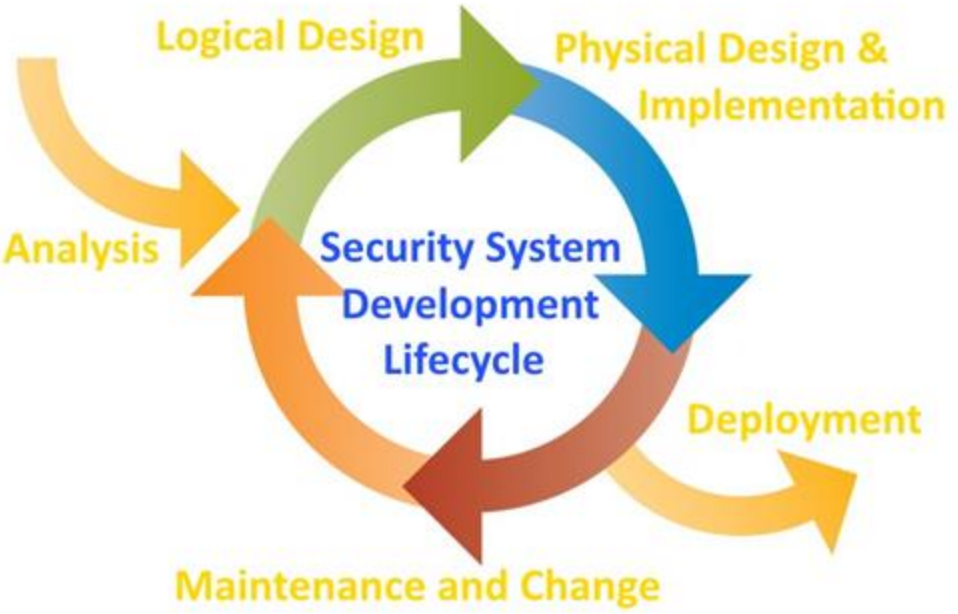


CISSP® MENTOR PROGRAM – SESSION FIVE

Security Models

Information System Life Cycle

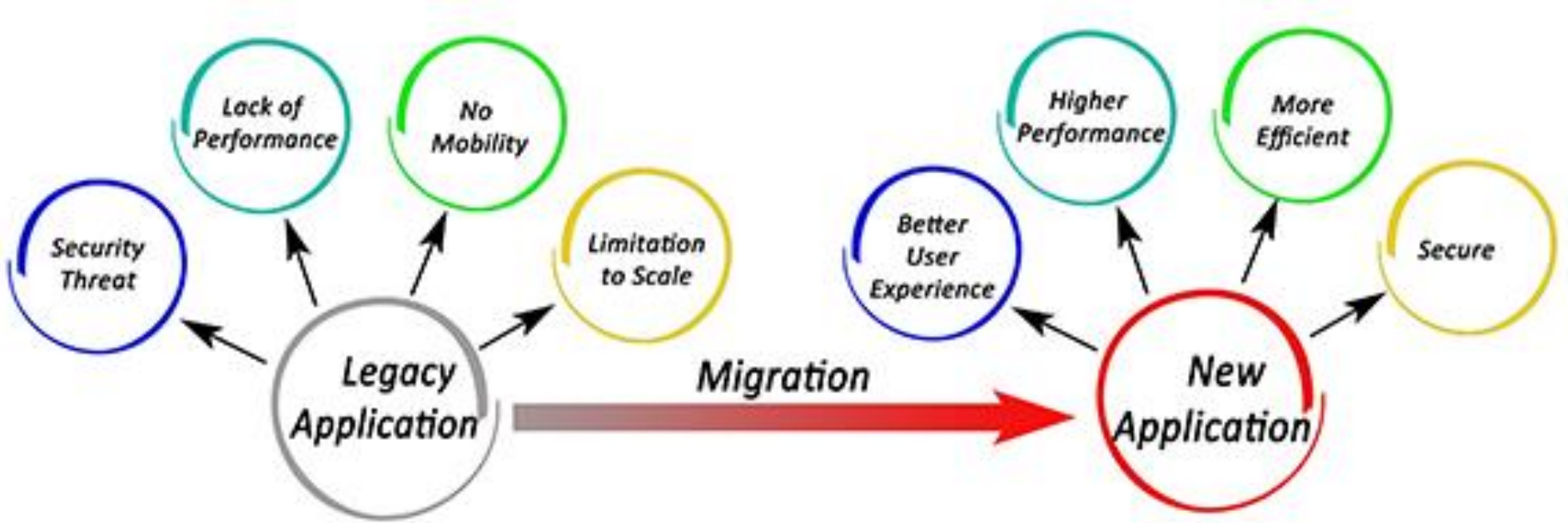
- **Verification and Validation** - is focused on ensuring that the developed system meets the specified requirements and each component is correctly implemented.
- **Transition/Deployment** - the system is deployed in the operation environment for actual use and available to end users
- **Operations and Maintenance** - ensuring the system functions as designed and functionals as expected for end users, includes management, support, and maintenance which can help extend its operational life.



Security Models

Information System Life Cycle

- **Retirement/Disposal** - at the end of the life cycle, and involves the planning, decommissioning and disposal of system and data.



Physical Security

Apply Security Principles to Site and Facility Design

Introduction

- Physical assets: people, buildings, systems, and data
- CISSP® exam considers **human safety** as the most critical concern of this domain - trumps all other concerns
- Physical security protects against threats such as unauthorized access and disasters, both man-made and natural

Physical Security

Apply Security Principles to Site and Facility Design

The general security principles outlined earlier for information security also have application to site and facility design.

Confidentiality and Integrity: The primary physical threat to confidentiality and integrity is unauthorized access (e.g., intruders and theft).

Availability: In addition to the threat to availability from unauthorized access, availability can also be compromised intentionally or accidentally by a range of events:

- Environmental events such as fire, floods, storms, or earthquakes
- Infrastructure events such as power outages, cooling (HVAC) failure, floods (from burst water pipes)

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Wiring Closets/Intermediate Distribution Facilities

Vulnerabilities related to networking distribution differ slightly between a data center and an office.

- Data center owned and managed for a single company (or cloud-hosting provider), the network distribution will be within the same perimeter as the servers themselves, so the physical and environmental security controls will apply to both.
- Colocation facility, different clients will have access to different areas of the facility (to access the equipment owned by or assigned to them for their exclusive use).
  - Wiring closets are managed by the hosting provider and must not be accessible to clients, as it would permit even authorized clients to access or affect service to other clients.
- Office, intermediate distribution facilities need to be protected from both malicious outsiders and insider threats, not to mention environmental risks.

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Location

- Avoid keeping combining wiring closets with other building services, as they often lack sufficient circulation and security
  - Small wiring closet full of network switches with poor (or no) ventilation can overheat, at a minimum shortening the life of your equipment, causing random resets, errors, and even total failure in the worst case.
  - Wiring closets can also be at risk from threats such as burst or leaking pipes that pass through or near the space or overflowing washrooms on the floors above

Consider compensating controls to secure access, add circuiation as well as plan for worse case scenarios like floods and power outages and the effect on equipment

Physical Security

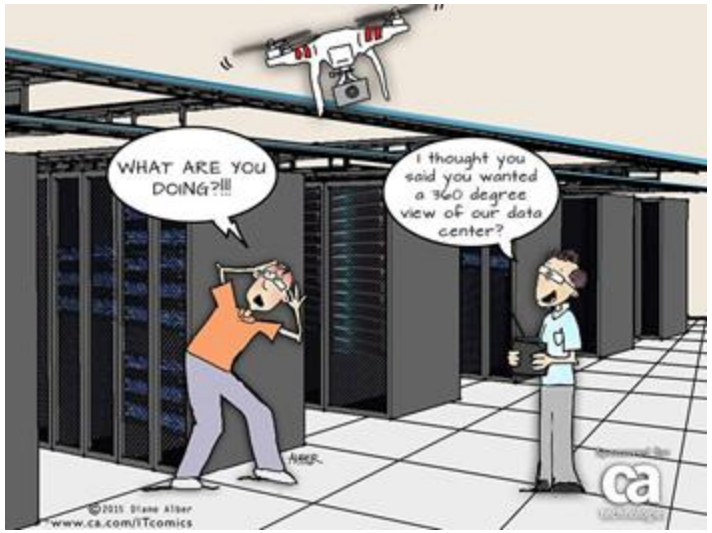
Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

Security controls need to be selected to address the following:

- **Physical access risks**
- **HVAC**
- **Environmental risks**
- **Fire risks**



Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

These controls should cover, at a minimum, the following:

- **Personnel** (e.g., background checks, training, or access procedures)
- **Maintenance**
- **Logging, monitoring, and alerting**
- **Control testing and auditing**

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

Review the guidance available from organizations such as the following:

- American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)
- ANSI / BICSI: ANSI/BICSI 002-2014, Data Center Design and Implementation Best Practices
- Electronic Industries Association and Telecommunications Industries Association (EIA/TIA): ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers
- European Union (EU): EN 50600 series of standards
- International Organization for Standardization (ISO): ISO/IEC 30134 series, “Information technology – Data centres – Key performance indicators”
- Uptime Institute: Tier Standards

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Recommended Controls:

- Controlled and stable temperature and humidity
- Air filtration and positive air pressure to minimize infiltration by airborne dust and microfine particulate matter or contaminants (such as corrosive fumes and engine exhaust from diesel generators or nearby vehicles)
- Appropriate floor covering to minimize static electricity
- Careful siting of the media storage facilities to avoid magnetic fields that might arise from electrical equipment (e.g., transformers or motors)

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Other considerations with respect to media storage include the following:

- If the environment of the media storage facility is different (in temperature or humidity) than the production environment in which the tape will be read, then time must be allowed for the tape to acclimate to the different environment before being processed.
- Some tape media needs to be “retensioned” (i.e., unspooled and respooled), depending on the tape manufacturer's recommendations (e.g., every three years).
- For longer archival storage, it is advisable to read the data from the stored media and rerecord on new media. Again, the tape manufacturer's recommendations ought to be followed with respect to the appropriate frequency (e.g., every six years).
- Appropriate procedures are necessary for the tracking of media that are placed in, and removed from, storage. This may include bar code scanning and separation-of-duties controls requiring two people to sign in and sign out media items.
- Fire detection and suppression systems may need to be installed.

Physical Security

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Other considerations with respect to media storage include the following:

- Proper housekeeping is required to reduce the possibility of fire and to reduce the fuel available should a fire break out. On a related note, media storage facilities ought to be used only to store media and should not be shared with other general storage.
- Depending on the risk analysis and costs associated with managing on- premises media storage, it may be appropriate to retain the services of an off-site media storage service that will handle the physical security and environmental concerns related to secure long-term storage of media. This can be used for all media, or a portion, in order to provide disaster recovery should the primary media storage facility be damaged by fire or other calamity.
- Appropriate media end-of-life procedures must be enforced to sanitize (e.g., by degaussing magnetic media) and securely destroy media before disposal so that sensitive information cannot be extracted from the media once it leaves the control of the organization.

Physical Security

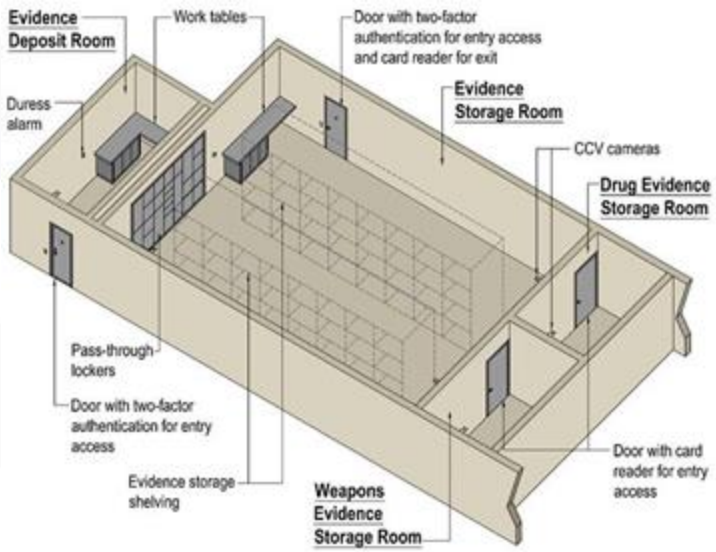
Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Evidence Storage

The evidence storage room include the following:

- **Strict policies surrounding who is permitted access** to the evidence storage room, the information that is to be entered into the log, and procedures governing the management of the access keys to the evidence storage room
- **Video monitoring**
- **Double locks on the evidence storage room doors**, or a locked storage cabinet inside the locked evidence storage room, with separation of duties surrounding the control of the keys, so that two people are required to access the evidence storage



Physical Security

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Work area security must be designed in response:

- **Risk assessment** (including threat modeling)
- **Security principles** and the appropriate controls to mitigate risk. The considerations to be addressed include:
  - **least privilege**
  - **need-to-know**
  - **separation of duties**
  - **dual control**
  - **defense in depth**
  - **compliance obligations**

Physical Security

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Least Privilege and Need-to-Know

- Access to restricted and secure areas must be granted only to the extent necessary for individuals to carry out their responsibilities, in accordance with formally approved policies and procedures.
- Access also must be periodically reviewed to ensure that the justification for access has not changed.
- Detailed auditable records attesting to the previous must be maintained.

Separation of Duties and/or Dual Control

- Depending on the risk assessment, it may be appropriate to require more than one authenticated staff member to be present in order to obtain access to the secure work area.
- Administrative control, verified through guard records or video surveillance, or it can be enforced through multiple locks or electronic access controls.

Physical Security

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Defense in Depth
Mantrap - A preventive physical control with two doors. Each door requires a separate form of authentication to open
Bollard—A post designed to stop a car, typically deployed in front of building entrances
Smart card—A physical access control device containing an integrated circuit
Tailgating—Following an authorized person into a building without providing credentials
Perimeter Defenses - Help prevent, detect, and correct unauthorized physical access. Should employ defense-in-depth Fences, doors, walls, locks, etc.

Physical Security

Apply Security Principles to Site and Facility Design

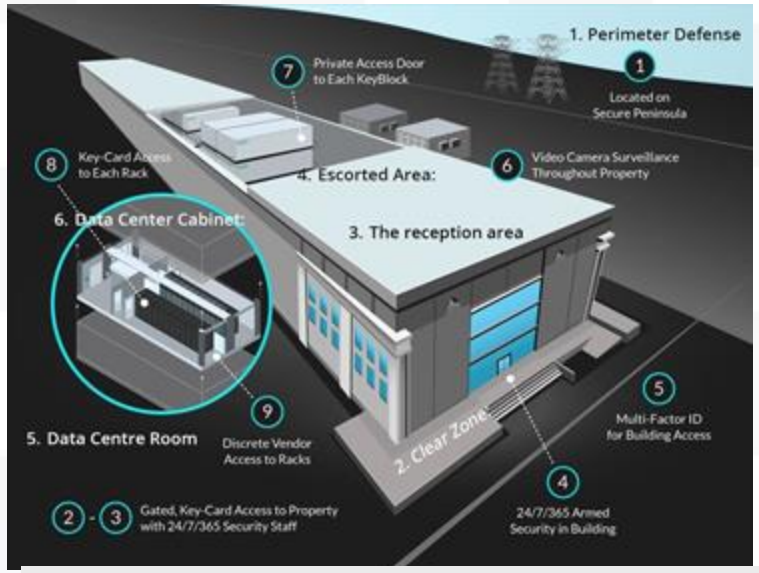
Restricted and Work Area Security

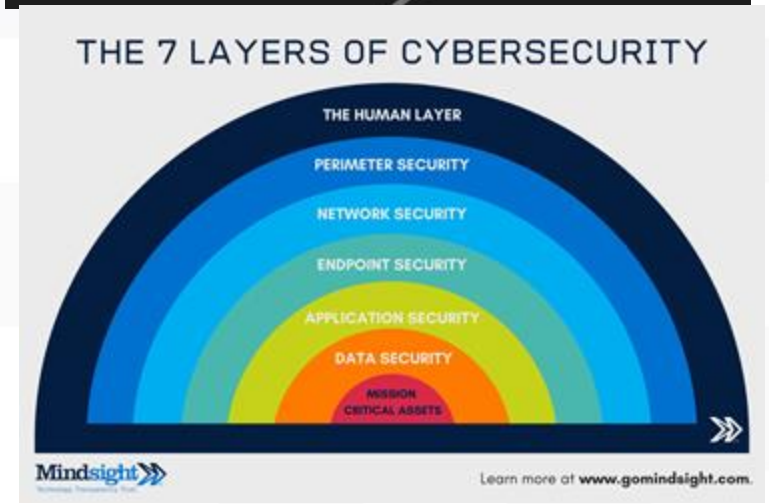
Defense in Depth
Mantrap - A preventive physical control with two doors. Each door requires a separate form of authentication to open
Bollard—A post designed to stop a car, typically deployed in front of building entrances
Smart card—A physical access control device containing an integrated circuit
Tailgating—Following an authorized person into a building without providing credentials
Perimeter Defenses - Help prevent, detect, and correct unauthorized physical access. Should employ defense-in-depth Fences, doors, walls, locks, etc.

Physical Security

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security





Defense in Depth

Different types of security controls ought to be considered for the higher security zones. In addition to preventive controls such as door locks, detective controls such as video monitoring and corrective controls such as motion detectors and alarms can be used as compensating controls should the primary preventive control (e.g., the door lock) fail or be compromised.

Multifactor authentication techniques are as valuable for physical access as for logical (e.g., login) access. Requiring a user to have an access card as well as enter a personal identification number (PIN) to unlock the door to higher security zones protects against loss of the access card and its use by an impostor. Requiring the card (and not the PIN alone) protects against shoulder-surfing by a threat actor observing staff enter their PINs.

Physical Security

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Compliance Obligations

Requirements for the following:

- Personnel identification Guards
- Electronic access control Electronic intrusion detection Video monitoring
- Interior access controls

One solution for having confidential discussions is the Sensitive Compartmented Information Facility (**SCIF**). SCIF is a common term among U.S. and British military and governmental agencies with a need for isolated space to preserve confidentiality.

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Controls

- Designed to provide a safe environment for personnel and equipment
- Power, HVAC, and fire safety are considered environmental controls

Electricity

- Reliable electricity is critical for any data center
- One of the top priorities when selecting, building, and designing a site

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Types of Electrical Faults

- All types of electrical faults can impact availability and integrity
- The following are common types of electrical faults:
  - **Blackout: prolonged loss of power**
  - **Brownout: prolonged low voltage**
  - **Fault: short loss of power**
  - **Surge: prolonged high voltage**
  - **Spike: temporary high voltage**
  - **Sag: temporary low voltage**

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Battery UPS systems can differ in a number of important aspects:

- **Load**: The capacity of the unit to deliver a specified level of continuous power
- **Capacity**: The time during which the unit can maintain the load
- **Filtering**: The ability of the unit to isolate the equipment from noise,surges, and other problems with the utility power Reliability: Some designs trade low cost for reliability

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

With both power (UPS and generator) and HVAC systems, due consideration has to be made for the following:

- **Regularly scheduled maintenance**
- **Regular testing under full load** (of UPS and generators, and backup HVAC equipment if not used in production)
- **System fault detection and alerting** (and regular tests of those subsystems)
- **Periodic checks and audits** to ensure all of the above are being properly and regularly performed

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Surge Protectors, UPSs, and Generators

Provide protection against electrical failures

Surge Protectors

- Protect equipment from damage due to electrical surges
- Contain a circuit or fuse which is tripped during a power spike or surge, shorting the power or regulating it down to acceptable levels

Uninterruptible Power Supplies

- Provide temporary backup power in the event of a power outage
- May also “clean” the power, protecting against surges, spikes, and other forms of electrical faults
- Backup power is provided via batteries or fuel cells
- Provide power for a limited period of time, and can be used as a bridge to generator power; generators typically take a short period of time to start up and begin providing power

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Generators

- Designed to provide power for longer periods of times than UPSs
- Will run as long as fuel is available
- Sufficient fuel should be stored onsite for the period the generator is expected to provide power
- Refueling strategies should consider a disaster's effect on fuel supply and delivery
- Generators should not be placed in areas which may flood or otherwise be impacted by weather events
- Should be tested and serviced regularly.
- http://www.cumminspower.com/www/literature/technicalpapers/PT-7006-Standby-Katrina-en.pdf

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

TIER LEVEL	AVAILABILITY %	REDUNDANCY
1	99.671	None. Multiple single points of failure.
2	99.741	Some. Nonredundant (e.g., N) UPS.
3	99.982	N+1 UPS. Able to take equipment out of service for maintenance without affecting operation.
4	99.995	2N UPS. No single point of failure, able to automatically compensate for any single failure.

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

With both power (UPS and generator) and HVAC systems, due consideration has to be made for the following:

- Regularly scheduled maintenance
- Regular testing under full load (of UPS and generators, and backup HVAC equipment if not used in production)
- System fault detection and alerting (and regular tests of those subsystems)
- Periodic checks and audits to ensure all of the above are being properly and regularly performed

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Environmental issues that need to be considered include the likelihood of the following:

- Major storms (hurricanes, lightning, blizzards, ice storms, typhoons, tornadoes, blizzards, etc.)
- Earthquakes
- Floods and tsunamis Forest fires
- Internal building risks Vermin and wildlife
- Volcanoes

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Environmental issues that need to be considered include the likelihood of the following:

- Major storms (hurricanes, lightning, blizzards, ice storms, typhoons, tornadoes, blizzards, etc.)
- Earthquakes
- Floods and tsunamis Forest fires
- Internal building risks Vermin and wildlife
- Volcanoes

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Mitigations include the following:

- Monitoring announcements from public health authorities
- Having a sick-leave policy that does not incentivize employees to come to work ill
- Developing a plan to operate with: a reduced workforce; employees working from home; or work shifted to office locations less affected (in the case of larger companies with multiple offices)

Environmental Controls

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Cloud Computing and Availability

- **Organizations that want to take availability a step further use hybrid/multicloud deployments** so that they don't rely on a single CSP for their operations.

- The **availability increases that highly redundant data centers** can provide are impressive, with cloud providers claiming 99.99 percent or higher availability. That number is useful only if organizations also ensure that they will be able to access cloud providers that are highly available.
- **Redundant network routes and hardware that can stay online** through a local or regional disaster are a necessary part of cloud hosting availability designs that can take full advantage of these highly available remote infrastructures.

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Human safety is paramount, and any fire safety system must be designed first and foremost to protect the lives and health of those who work in the facility. Enabling occupants to safely exit the building and ensuring that fire suppression systems are unlikely to compromise health or safety are more important than protecting systems and buildings.

Balance the costs of the following:

- Downtime
- Restoration costs
- Fire suppression system costs (capital and ongoing maintenance)

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Most jurisdictions have standards and guidelines for the fire protection systems for IT equipment:

- **Canada and the United States: NFPA 75, "Standard for the Fire Protection of Information Technology Equipment," and NFPA 76, "Fire Protection of Telecommunications Facilities."**
- **UK: BS 6266:2011, "Fire protection for electronic equipment installations." Code of practice.**
- **Germany: The VdS series of guidelines for fire protection and suppression.**

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Heat, Flame, and Smoke Detectors

- Three methods for detecting fire
- Typically alert locally, and may also be centrally monitored by a fire alarm system
- An audible alarm and flashing lights should be used, so that both deaf and blind personnel will be aware of the alarm

Heat Detectors

- Alert when temperature exceeds an established safe baseline
- May trigger when a specific temperature is exceeded or when temperature changes at a specific rate (such as “10 °F in less than 5 minutes”)

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Smoke Detectors

- Work through two primary methods: ionization and photoelectric
- Ionization-based smoke detectors contain a small radioactive source which creates a small electric charge
- Photoelectric sensors work in a similar fashion, except that they contain an LED (Light Emitting Diode) and a photoelectric sensor that generates a small charge while receiving light
- Both types of alarm alert when smoke interrupts the radioactivity or light, lowering or blocking the electric charge
- Dust should always be avoided in data centers. Small airborne dust particles can trigger smoke detectors just as smoke does, leading to false alarms.

Flame Detectors

- Detect infrared or ultraviolet light emitted in fire
- One drawback to this type of detection is that the detector usually requires line-of-site to detect the flame; smoke detectors do not have this limitation

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Safety Training and Awareness

- Training provides a skill set such as learning to operate an emergency power system
- Awareness changes user behavior (“Don't let anyone follow you into the building after you swipe your access card”)

Evacuation Routes

- Evacuation routes should be prominently posted
- All personnel should be advised of the quickest evacuation route from their areas
- Guests should be advised of evacuation routes as well
- All sites should use a meeting point, where all personnel will meet in the event of emergency

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Evacuation Roles and Procedures

- The two primary evacuation roles are safety warden and meeting point leader
- The safety warden ensures that all personnel safely evacuate the building in the event of an emergency or drill
- The meeting point leader assures that all personnel are accounted for at the emergency meeting point
- Special care should be given to any personnel with handicaps, which could affect egress during an emergency
- Elevators should never be used during a fire
- All sites should have mitigating controls to allow safe egress for all personnel

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

ABCD Fires and Suppression

- Fire suppression systems are used to extinguish fires
- Different types of fires require different suppressive agents
- Class K fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish class K fires.

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Fires are categorized by the type of fuel:

- **Class A**: Ordinary solid combustibles (e.g., paper, wood, and plastic) Class B: Flammable liquids and gases (e.g., gasoline)
- **Class C**: Energized electrical equipment
- **Class D**: Combustible metals (e.g., lithium metal, but not lithium-ion batteries, which are considered Class B, although water will also work well with Li-ion battery fires)
- **Class F or K**: Cooking oils and greases

Type (Fire Type / Extinguisher Type)	Class A Organic Materials (e.g Paper & Coal)	Class B Flammable Liquids (e.g Petrol & Paint)	Class C Flammable Gases (e.g Butane & Methane)	Class D Flammable Metals (e.g Lithium & Magnesium)	Electrical Electrical Equipment (e.g Computers & Servers)	Class F Cooking Oils (e.g Olive Oil & Fat)	Businesses that may need this type of Extinguisher
Water	✓	✗	✗	✗	✗	✗	- Schools - Hospitals - Offices - Shops
Foam	✓	✓	✗	✗	✗	✗	- Apartments - Hospitals - Offices - Shops
Dry Powder	✓	✓	✓	✓	✓	✗	- Garages - Welding - Boiler Rooms - LPG Plants
CO2	✗	✓	✗	✗	✓	✗	- Server Rooms - Offices
Wet Chemical	✓	✗	✗	✗	✗	✓	- Kitchens - Canteens

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Make sure they know the following information:

- Where all the exits are (so they know the closest, and if blocked, the alternates)
- Where all the fire extinguishers are located as well as how and when to use them (different types of fire extinguishers are appropriate for different types of fires)
- How to disable (or delay the discharge of) the fire suppression system should a false fire detection be suspected
- How to manually trip the fire suppression system (in the case of gaseous suppression and some sprinkler systems) should early signs of fire be detected by staff before the fire detectors are triggered
- Where the fire alarm pull stations or call points are How to manually shut off power to the data center

Environmental Controls

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

HOLY MOLY! That was a long Domain with a lot of information!

We are ½ way for todays session!