2025 CISSP Mentor Program

CHAPTER 9

Brad Nigh
FRSecure

CISSP® MENTOR PROGRAM – SESSION SIX

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 SIX

HELLO, NICE TO MEET YOU

- 25 years IT/Security experience
- Co-host of the UnSecurity Podcast (230 episodes and counting)
- Instructor for FRSecure's free CISSP Mentor Program (8 years)
- Try to make InfoSec fun
- All the dad jokes
- Happy to be here

CISSP® MENTOR PROGRAM – SESSION SIX

DOMAIN 3: SECURITY ARCHITECTURE & ENGINEERING

CISSP Exam Overview

https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline

3.1 Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Segregation of Duties (SoD)
- Keep it simple and small
- Zero trust or trust but verify
- Privacy by design
- Shared responsibility
- Secure access service edge

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices (e.g., application programming interface (API))
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems

3.6 Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public key infrastructure (PKI) (e.g., quantum key distribution)
- Key management practices (e.g., rotation)
- Digital signatures and digital certificates (e.g., non-repudiation, integrity)

CISSP® MENTOR PROGRAM – SESSION SIX

DOMAIN 3: SECURITY ARCHITECTURE & ENGINEERING

CISSP Exam Overview

https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline

3.7 Understand methods of cryptanalytic attacks

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

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and heating, ventilation, and air conditioning (HVAC)
- Environmental issues (e.g., natural disasters, man-made)
- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

3.10 Manage the information system lifecycle

- Stakeholders needs and requirements
- Requirements analysis
- Architectural design
- Development /implementation
- Integration
- Verification and validation
- Transition/deployment
- Operations and maintenance/sustainment
- Retirement/disposal

CISSP® MENTOR PROGRAM – SESSION SIX

QUESTIONS.

The most common questions:

Check your email for links

- Discord channels https://discord.gg/FWfjPnAZ
  - Use it for more in-depth questions / discussions
  - Before you ask a question, check
    - If it's been asked
    - The isc2.com website
- Live session links & recording
- Instructor slide deck https://learn.frsecure.com/
- Other Resources

CISSP® MENTOR PROGRAM – SESSION SIX

INTRODUCTION

Before we get too deep into this.

How about a dumb dad joke?

I asked the IT guy, "How do you make a Motherboard?" He said, "I tell her about my job."

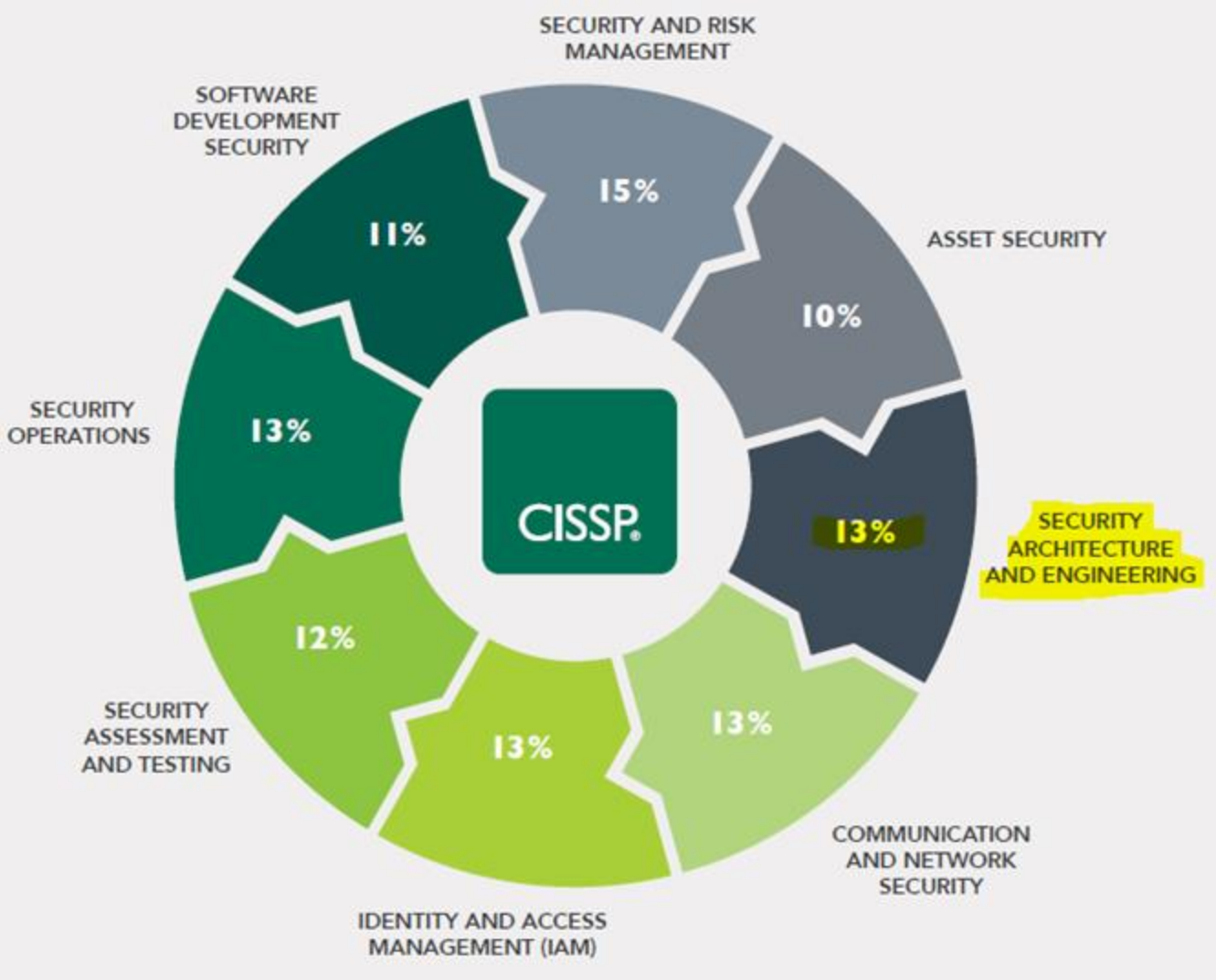
CISSP® MENTOR PROGRAM – SESSION SIX

DOMAIN 3: SECURITY ARCHITECTURE & ENGINEERING

CISSP Exam Overview

Caution!
Concepts overlap between domains.

https://www.isc2.org/-/media/ISC2/Certifications/Ultimate-Guides/UltimateGuideCISSP-Web.ashx



Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Security Architecture

Introduction

- Organization's security strategy must align with its mission, goals, objectives, and compliance environment.

- Success in security architecture is much more likely when one is aligned with the business and taking a risk management approach to security architecture.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

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

Shared Responsibility

The principle that organizations do not operate in isolation.

- Ultimately organizations are responsible to make good security decisions
- Understand the responsibility of the organization when working with third-parties, especially cloud.
  - (Cloud-shared responsibilities are covered later)
- If you discover or become aware of new vulnerabilities, you should disclose them to the vendor or threat intelligence service.
  - Automated indicator sharing (AIS) is an initiative by the Department of Homeland Security (DHS) to facilitate the open and free exchange of indicators of compromise (IoCs)
    - For more information on the AIS program, please visit us-cert.gov/ais.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

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

Data Localization and Data Sovereignty

- Data Localization
  - The storing and processing data within a specific country or region's physical borders or geographical boundaries.
- Data sovereignty
  - A broader set of principles related to data governance, jurisdiction, and legal compliance within a specific geopolitical boundary.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

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

Data Localization and Data Sovereignty

- Data Localization is a subset of Data sovereignty.
- Data Localization focused on where data is stored and processed.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

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

Hardware - any tangible part of a computer that you can reach out and touch.
Processor - The computer's nerve center. Governs all major operations and either directly performs or coordinates the complex calculations that allows a computer to perform its intended tasks.

Execution Types

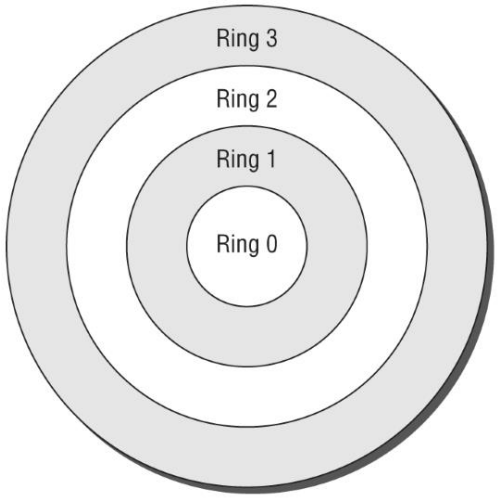
Multitasking - Handling two or more tasks simultaneously.
Multicore - The CPU is a chip containing two, four, eight, dozens, or more independent execution cores.
Multiprocessing – Using more than one processor to complete the execution of a multithreaded application.
Multiprogramming - A way to batch or serialize multiple processes so that when one process stops to wait on a peripheral, its state is saved, and the next process in line begins to process.
Multithreading – When multiple concurrent tasks are performed within a single process.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROTECTION RINGS - Organize code and components in an OS



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

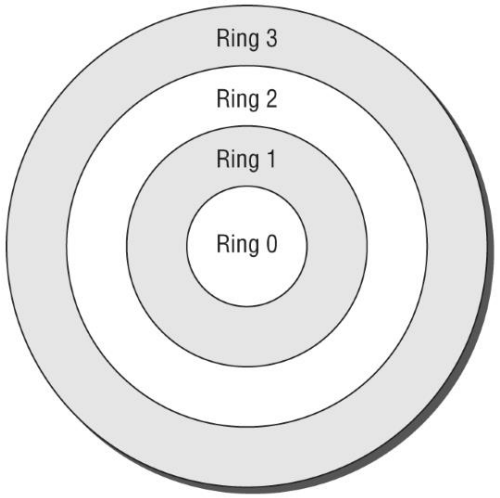
Ring 0: Kernel Mode (Most Privileged)
Ring 1: Supervisory Mode (Moderate Privileges)
Ring 2: System Mode (Less Privileged)
Ring 3: User Mode (Least Privileged)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROTECTION RINGS - Organize code and components in an OS



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

Ring 0: Kernel Mode (Most Privileged)

- The core of the operating system
- Full access to all hardware and resources
- Responsible for low-level tasks such as managing memory, executing processes, and communicating directly with hardware.

Ring 1: Supervisory Mode (Moderate Privileges)

Ring 2: System Mode (Less Privileged)

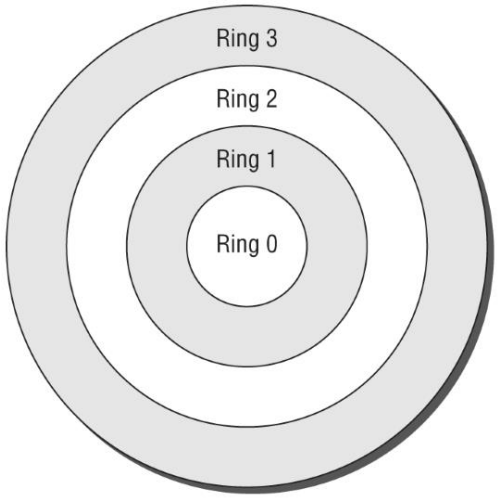
Ring 3: User Mode (Least Privileged)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROTECTION RINGS - Organize code and components in an OS



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

Ring 0: Kernel Mode (Most Privileged)

Ring 1: Supervisory Mode (Moderate Privileges)

- Used for managing the operating system's subsystems.
- Limited access compared to Ring 0 but still handles some critical system functions.
- Manages I/O operations and supervises other system functions.

Ring 2: System Mode (Less Privileged)

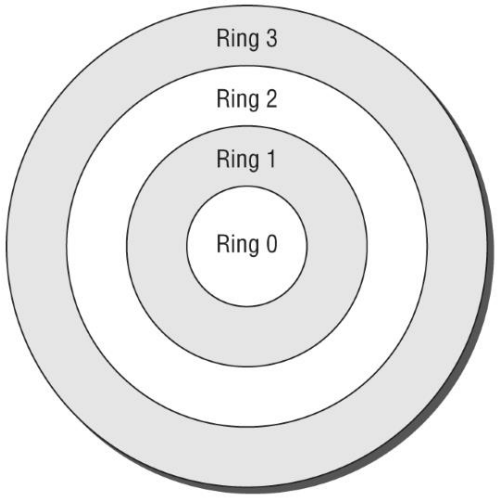
Ring 3: User Mode (Least Privileged)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROTECTION RINGS - Organize code and components in an OS



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

Ring 0: Kernel Mode (Most Privileged)
Ring 1: Supervisory Mode (Moderate Privileges)
Ring 2: System Mode (Less Privileged)

- Often used for higher-level system services.
- Can interact with kernel-level functionality but cannot directly access hardware.
- Acts as an intermediary between user applications and the kernel.

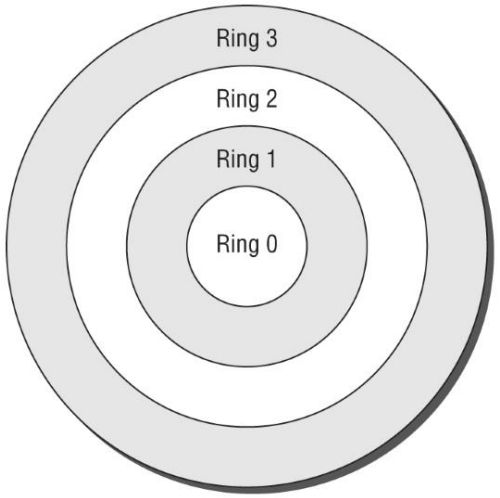
Ring 3: User Mode (Least Privileged)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROTECTION RINGS - Organize code and components in an OS



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

Ring 0: Kernel Mode (Most Privileged)
Ring 1: Supervisory Mode (Moderate Privileges)
Ring 2: System Mode (Less Privileged)
Ring 3: User Mode (Least Privileged)

- This is where regular user applications run.
- Restricted from directly accessing hardware or critical system resources.
- Ensures that user applications cannot compromise the system's stability or security.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

Can be in one of two modes at any given moment:

Supervisor state

- Kernal mode

Problem state

- User mode, where privileges are low and all access requests must be checked against credentials for authorization

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

- **Ready State**
- **Running State**
- **Waiting (Blocked) State**
- **Supervisory State**
- **Terminated (Exit) State**

Imagine a process lifecycle as a cycle:
New → Ready → Running → Waiting → Ready → Running → Terminated

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

Ready State

- Description: The process is ready to execute but is waiting for the CPU to be assigned to it.
- Key Actions: The process remains in the queue of ready processes.
- Transition: When the CPU becomes available, the process moves to the Running state.

Running State

Waiting (Blocked) State

Supervisory State

Terminated (Exit) State

Imagine a process lifecycle as a cycle:

New → Ready → Running → Waiting → Ready → Running → Terminated

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

Ready State
Running State

- Description: The process is actively executing instructions on the CPU.
- Key Actions: It performs tasks, computes results, or interacts with resources like memory and I/O devices.
- Transition: The process can be interrupted (moving to Waiting), can complete execution (moving to Terminated), or can voluntarily yield the CPU (returning to Ready).

Waiting (Blocked) State
Supervisory State
Terminated (Exit) State

Imagine a process lifecycle as a cycle:
New → Ready → Running → Waiting → Ready → Running → Terminated

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

Ready State
Running State
Waiting (Blocked) State

- Description: The process is waiting for an external event (e.g., I/O operation completion) to proceed.
- Key Actions: It releases the CPU but retains other allocated resources.
- Transition: Once the event occurs, the process moves back to the Ready state.

Supervisory State
Terminated (Exit) State

Imagine a process lifecycle as a cycle:
New → Ready → Running → Waiting → Ready → Running → Terminated

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

Ready State
Running State
Waiting (Blocked) State
Supervisory State

- Description: The mode where the OS or certain processes execute with elevated privileges.
- Key Actions: Typically done to manage critical system resources or services
- Transition: Once the event occurs, the process moves back to the Ready state.

Terminated (Exit) State

Imagine a process lifecycle as a cycle:
New → Ready → Running → Waiting → Ready → Running → Terminated

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Protection Mechanisms

PROCESS STATES - Forms of execution in which a process may run.

New (Created) State
Ready State
Running State
Waiting (Blocked) State
Terminated (Exit) State

- Description: The process has finished execution or has been terminated by the system.
- Key Actions: The operating system cleans up resources allocated to the process.
- Transition: The process is removed from the system.

Imagine a process lifecycle as a cycle:
New → Ready → Running → Waiting → Ready → Running → Terminated

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Memory

Read-Only Memory (ROM)

- Programmable Read-Only Memory (PROM)
- Erasable Programmable Read-Only Memory (EPROM)
- Electronically Erasable Programmable Read-Only Memory (EEPROM)
- Flash Memory

Random access memory (RAM)

- Real Memory
- Cache RAM

Registers

Memory Addressing

- Register
- Immediate Addressing
- Direct Addressing
- Indirect Addressing
- Base + Offset Addressing

Secondary Memory

Data Storage Devices

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Memory

- **Read-Only Memory (ROM)**
  - A type of computer memory that is used to store information that doesn't change, even when the power is turned off.
  - Think of it like a book—you can read what's written, but you can't erase or rewrite the content.
    - **Programmable Read-Only Memory (PROM)**
    - **Erasable Programmable Read-Only Memory (EPROM)**
    - **Electronically Erasable Programmable Read-Only Memory (EEPROM)**
    - **Flash Memory**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Memory

- **Read-Only Memory (ROM)**
  - A type of computer memory that is used to store information that doesn't change, even when the power is turned off.
  - Think of it like a book—you can read what's written, but you can't erase or rewrite the content.
  - **Programmable Read-Only Memory (PROM)**
    - PROM is permanent and unchangeable after programming.
  - **Erasable Programmable Read-Only Memory (EPROM)**
    - EPROM offers erasability but requires specialized UV light for reprogramming.
  - **Electronically Erasable Programmable Read-Only Memory (EEPROM)**
    - EEPROM is the most versatile, allowing electrical erasing and reprogramming.
  - **Flash Memory**
    - A type of non-volatile memory that retains data even without power.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Memory

Memory Type	Description	Reprogrammability	Usage
PROM	Write-once memory, permanently programmed.	Cannot be erased or rewritten.	Firmware, permanent configurations.
EPROM	Erasable using UV light; reprogrammable.	Erasable with UV light exposure.	Applications needing updates, but infrequently.
EEPROM	Electrically erasable; reprogrammable.	Erasable and rewritable in-circuit.	Configurations, frequent updates.
Flash Memory	Stores blocks of data; electrically erasable.	Erasable in blocks rather than byte-by-byte.	Data storage in devices like SSDs, USB drives, and smartphones.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- Secondary memory
  - Virtual memory
- Data Storage Devices
  - Primary vs. Secondary
  - Volatile vs. Nonvolatile
  - Random vs. Sequential

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Secondary memory**
  - A term commonly used to refer to magnetic, optical, or flash-based media or other storage devices that contain data not immediately available to the CPU.
  - Non-volatile storage used to permanently store data and programs. It retains information even when the computer is turned off.
  - **Virtual memory**
    - A special type of secondary memory that is used to expand the addressable space of real memory.
    - It allows the system to handle more tasks and larger applications than the physical RAM can accommodate. When RAM runs out, data that is not actively being used is temporarily stored in the virtual memory.
- **Data Storage Devices**
  - **Primary vs. Secondary**
  - **Volatile vs. Nonvolatile**
  - **Random vs. Sequential**

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- Secondary memory
  - Virtual memory
- Data Storage Devices
    - Any hardware used to store digital data
  - Primary vs. Secondary
  - Volatile vs. Nonvolatile
  - Random vs. Sequential

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- Secondary memory
  - Virtual memory
- Data Storage Devices
  - Primary vs. Secondary
    - Primary Storage:
      - RAM (Random Access Memory) for temporary, fast access to data.
  - Secondary Storage:
      - Hard Disk Drives (HDDs).
      - Solid-State Drives (SSDs).
      - Optical Media (CDs, DVDs, Blu-ray discs).
  - Volatile vs. Nonvolatile
  - Random vs. Sequential

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- Secondary memory
  - Virtual memory
- Data Storage Devices
  - Primary vs. Secondary
    - Primary Storage:
    - Secondary Storage:
  - Volatile vs. Nonvolatile
    - Volatile storage loses all stored data when power is turned off.
      - RAM (Random Access Memory)
    - Non-volatile storage retains data even when power is turned off.
      - Hard drives (HDDs), solid-state drives (SSDs), flash memory, optical discs, and ROM.
  - Random vs. Sequential

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Secondary memory**
  - **Virtual memory**
- **Data Storage Devices**
  - **Primary vs. Secondary**
    - **Primary Storage:**
    - **Secondary Storage:**
  - **Volatile vs. Nonvolatile**
  - **Random vs. Sequential**
    - Random - data location is assigned an address, allowing immediate retrieval regardless of where it is stored.
      - Examples:
        - RAM: Enables rapid access to any memory location during active processing.
        - Hard Drives: Although slower, they support random access to files or sectors.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Secondary memory**
  - **Virtual memory**
- **Data Storage Devices**
  - **Primary vs. Secondary**
    - **Primary Storage:**
    - **Secondary Storage:**
  - **Volatile vs. Nonvolatile**
  - **Random vs. Sequential**
    - Sequential - To retrieve a particular piece of data, you must go through all preceding data sequentially.
      - Examples:
        - Magnetic Tape: Commonly used for backups; retrieving specific data requires reading through earlier sections.
        - Streaming Media: Sequential access ensures smooth playback.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Memory Security Issues**
  - Memory may retain sensitive data
- **Storage Media Security**
  - Data may remain on secondary storage devices even after it has been erased.
    - Known as Data Remanence
- **Emanation Security**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Memory Security Issues**
- **Storage Media Security**
- **Emanation Security**
  - Preventing unauthorized interception of electromagnetic signals that can unintentionally emanate from electronic devices.
    - Emanations are electromagnetic signals that devices emit during normal operation.
    - These signals can come from monitors, keyboards, printers, cables, or network equipment.
    - Malicious actors can intercept these signals using specialized equipment to reconstruct sensitive data.
  - **TEMPEST Attacks**: TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions) refers to the study and protection against compromising emanations (as part of U.S. standards for secure equipment).
    - Less common, Emission Security (EMSEC) is the current term.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Memory Security Issues**
- **Storage Media Security**
- **Emanation Security**
  - Emanation Security Controls:
    - Shielding: Use electromagnetic shielding (e.g., Faraday cages or shielded cables) to block emanations from being intercepted.
    - Distance: Maintain physical separation between sensitive devices and public or unsecured areas to reduce risk.
    - Encryption: Encrypt data transmitted over wireless networks to prevent interception of useful information.
    - Device Hardening: Use secure equipment certified to limit electromagnetic emissions (e.g., TEMPEST-compliant devices).
    - Noise Generation: Add noise or jamming signals to make intercepted emanations unreadable.
    - Policy and Procedures: Implement strict guidelines for placement, use, and disposal of sensitive equipment.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Emanation Security

- Input and Output Devices
  - Monitors
    - Eavesdropping on the video cable or the monitor
    - Shoulder surfing
  - Printers
  - Keyboards/ Mice
  - POTS Telephone Modems

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Emanation Security

- **Input and Output Devices**
  - **Monitors**
  - **Printers**
    - Walk out with sensitive information in printed form
    - If printers are shared, users may forget to retrieve their sensitive printouts
    - Multifunction printers (MFPs), if network connected could be compromised. They also often have hard drives that could contain sensitive information.
  - **Keyboards/ Mice**
  - **POTS Telephone Modems**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Emanation Security

- Input and Output Devices
  - Monitors
  - Printers
  - Keyboards/ Mice
    - Keystroke loggers
    - Bluetooth signals can be intercepted
  - POTS Telephone Modems
    - Legacy computer component.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Firmware

Firmware (also known as microcode) is a term used to describe software that is stored in a ROM or an EEPROM chip.

- **Basic input/ output system (BIOS)**
  - Firmware embedded on a computer's motherboard, responsible for initializing hardware components and booting the operating system.
- **Unified Extensible Firmware Interface (UEFI)**
  - **Boot attestation or secure boot**
  - **Measured boot**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Firmware

Firmware (also known as microcode) is a term used to describe software that is stored in a ROM or an EEPROM chip.

- **Basic input/ output system (BIOS)**
- **Unified Extensible Firmware Interface (UEFI)**
  - A modern replacement for the older BIOS (Basic Input/Output System), offering enhanced functionality, scalability, and security features
  - **Boot attestation or secure boot**
    - Prevents unauthorized code (e.g., malware) from loading during the boot process by verifying digital signatures of the bootloader and OS components.
  - **Measured boot**
    - Designed to enhance system integrity by creating a chain of trust during the boot process.
    - Unlike Secure Boot, which prevents unauthorized code from executing, Measured Boot focuses on recording the state of each boot process component for later verification.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Firmware

Feature	UEFI	BIOS
Boot Time	Faster due to optimized boot process.	Slower due to legacy design.
Security	Secure Boot and cryptographic validation.	Limited security capabilities.
Interface	Graphical, modern interface.	Text-based interface.
Partition Support	GPT support for larger drives.	MBR with limited partition sizes.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Client-Based Systems

Client-based vulnerabilities place the user, their data, and their system at risk of compromise and destruction. A client-side attack is any attack that is able to harm a client.

- **Mobile Code**
  - **Applets**
    - Code objects sent from a server to a client to perform some action.
    - Java and ActiveX are historical examples.
    - Not used very often anymore.
  - **JavaScript**
    - A lightweight, interpreted scripting language used primarily to create interactive and dynamic content on web pages.
    - More details of threats will be covered in Chapter 21, “Malicious Code and Application Attacks.”

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Server-Based Systems

- **Data flow control**
  - **Data flow** is the movement of data between processes, between devices, across a network, or over communication channels.
  - **Data flow control** refers to the processes, mechanisms, and technologies used to govern the movement of data, ensuring it flows only to authorized recipients, systems, or applications and does so securely.
- **Load balancer**
  - Spreads or distributes network traffic load across several network links or devices.
    - More in Chapter 12

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Large-Scale Parallel Data Systems

These systems consist of distributed or clustered computing resources working in parallel to process large datasets simultaneously.

- **Symmetric multiprocessing (SMP)**
  - A single computer contains multiple processors that are treated equally and controlled by a single OS
  - The collection of processors works collectively on a single or primary task, code, or project.
  - SMP for high-performance parallel computing.
- **Asymmetric multiprocessing (AMP)**
- **Massive parallel processing (MPP)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Large-Scale Parallel Data Systems

These systems consist of distributed or clustered computing resources working in parallel to process large datasets simultaneously.

- **Symmetric multiprocessing (SMP)**
  - A single computer contains multiple processors that are treated equally and controlled by a single OS
  - The collection of processors works collectively on a single or primary task, code, or project.
  - SMP for high-performance parallel computing.
- **Asymmetric multiprocessing (AMP)**
- **Massive parallel processing (MPP)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Large-Scale Parallel Data Systems

These systems consist of distributed or clustered computing resources working in parallel to process large datasets simultaneously.

- **Symmetric multiprocessing (SMP)**
- **Asymmetric multiprocessing (AMP)**
  - Processors are often operating independently of one another.
  - Usually, each processor has its own OS and/ or task instruction set, as well as a dedicated data bus and memory resources.
  - AMP for specialized systems with defined roles.
- **Massive parallel processing (MPP)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Large-Scale Parallel Data Systems

These systems consist of distributed or clustered computing resources working in parallel to process large datasets simultaneously.

- **Symmetric multiprocessing (SMP)**
- **Asymmetric multiprocessing (AMP)**
- **Massive parallel processing (MPP)**
  - Often involves multiple nodes working together in a coordinated system.
  - Data is distributed across nodes, enabling simultaneous access and processing

CISSP® MENTOR

Chapter 9: Se… …d Countermeas…

Large-Scale Parallel Dat…

Feature	Symmetric Multiprocessing (SMP)	Asymmetric Multiprocessing (AMP)	Massive Parallel Processing (MPP)
Definition	All processors share equal roles, memory, and resources.	One processor (master) controls others (subordinates).	A distributed system where many processors handle tasks simultaneously.
Processor Roles	All processors are equal and perform general tasks.	Master assigns tasks, and subordinate processors handle specific ones.	Processors work independently on smaller portions of a larger task.
Architecture	Shared memory architecture, managed by a single OS.	Hierarchical, with a central master processor.	Distributed across multiple nodes, each with its own memory.
Scalability	Moderately scalable, limited by shared memory contention.	Less scalable due to master-processor dependence.	Highly scalable by adding nodes or processors.
Performance	High performance for tasks requiring equal load distribution.	Best for predefined or specialized tasks.	Excellent for large-scale data or computation-intensive tasks.
Fault Tolerance	Better fault tolerance due to shared resources.	Dependent on the master processor, creating a potential single point of failure.	High fault tolerance with redundancy and distributed architecture.
Typical Use Cases	General-purpose systems like servers or databases.	Embedded systems, real-time operations (e.g., robotics).	Big data, high-performance computing, machine learning.
Security Considerations	Protect shared memory and prevent resource contention.	Secure the master node and subordinate communication.	Encrypt distributed data, ensure node security, and manage access control.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Grid Computing

- **Grid Computing**
  - A form of parallel distributed processing that loosely groups a significant number of processing nodes to work toward a specific processing goal.
  - Leverages the unused processing power, storage, and memory of systems in the grid.
    - SETI is an example of Grid Computing.
  - Sensitive data might be shared across different systems, increasing exposure risks.
- **Peer to Peer**
  - A decentralized approach to sharing and exchanging data or resources between devices (peers) in a network.
  - No centralized servers

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

- **Supervisory Control and Data Acquisition (SCADA)**
- **Distributed Control Systems (DCS)**
- **Programmable Logic Controllers (PLCs)**
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

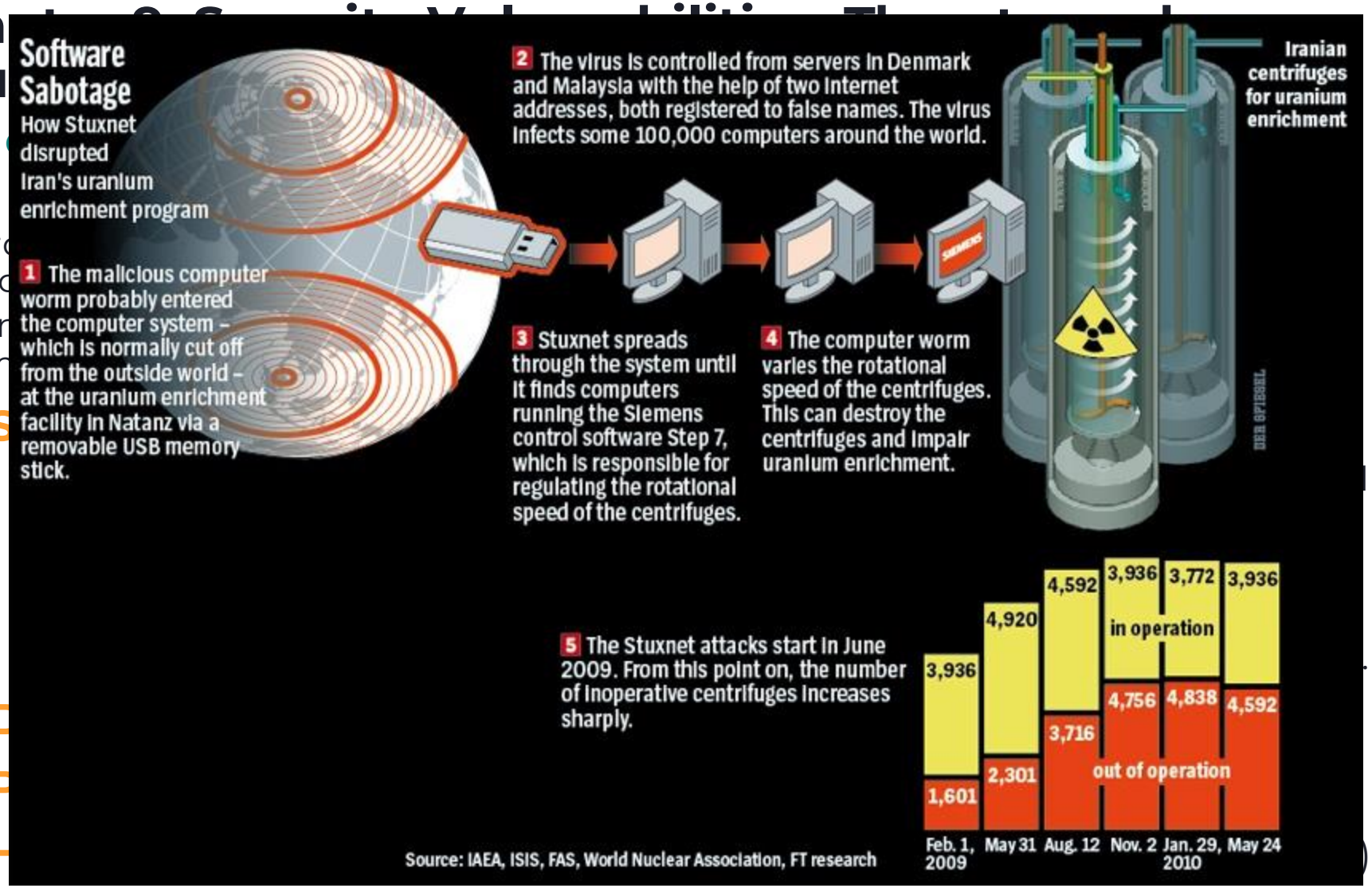
- **Supervisory Control and Data Acquisition (SCADA)**
  - Centralized control frameworks used to monitor and manage geographically dispersed assets, such as pipelines, power grids, and water treatment facilities.
  - Collects data from remote sensors and equipment.
  - Allows operators to monitor and control processes in real-time.
  - Require secure communication protocols (e.g., encryption) and network segmentation.
- **Distributed Control Systems (DCS)**
- **Programmable Logic Controllers (PLCs)**
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)

Cha… Cou…

Industrial …

Hard… proc… man… com…

- S…
- D…
- P…
- H…



CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

- **Supervisory Control and Data Acquisition (SCADA)**
- **Distributed Control Systems (DCS)**
  - Localized control systems used primarily in manufacturing plants and industries. They distribute control across multiple stations.
  - Handle complex operations, such as chemical production or assembly lines.
  - Operate within a specific facility, unlike SCADA systems.
  - Threats arise from internal network vulnerabilities and insider attacks.
- **Programmable Logic Controllers (PLCs)**
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

- **Supervisory Control and Data Acquisition (SCADA)**
- **Distributed Control Systems (DCS)**
  - Localized control systems used primarily in manufacturing plants and industries. They distribute control across multiple stations.
  - Handle complex operations, such as chemical production or assembly lines.
  - Operate within a specific facility, unlike SCADA systems.
  - Threats arise from internal network vulnerabilities and insider attacks.
- **Programmable Logic Controllers (PLCs)**
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

- **Supervisory Control and Data Acquisition (SCADA)**
- **Distributed Control Systems (DCS)**
- **Programmable Logic Controllers (PLCs)**
  - Embedded systems designed to control specific machinery or processes, such as conveyor belts or robotic arms.
  - Execute pre-programmed instructions for specific tasks.
  - Can be reprogrammed for flexibility in operations.
  - Vulnerable to physical tampering and malware attacks.
  - Require secure programming practices and regular firmware updates.
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Control Systems

Hardware and software systems used to monitor, control, and automate industrial processes. These systems are integral to critical infrastructure sectors such as manufacturing, energy, water, transportation, and more. **Modbus** is a widely used communication protocol in industrial automation and control systems.

- **Supervisory Control and Data Acquisition (SCADA)**
- **Distributed Control Systems (DCS)**
- **Programmable Logic Controllers (PLCs)**
- **Human-Machine Interfaces (HMIs)** (not in the exam but important)
  - Interfaces that allow operators to interact with ICS components and monitor system status.
  - Provide visual displays of system data and controls.
  - Serve as the communication point between humans and machines.
  - Could be exploited through weak credentials or insecure network connections.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Distributed Systems

- A collection of individual systems that work together to support a resource or provide a service.
  - DCE solutions are implemented as client-server architectures
  - As a three-tier architecture (such as basic web applications),
  - As multitiered architectures (such as advanced web applications)
  - And as peer-to-peer architectures (such as BitTorrent and most cryptocurrency blockchain ledgers
- Typically includes an interface definition language (IDL).
  - Remote procedure calls (RPCs),
  - Common Object Request Broker Architecture (CORBA),
  - Distributed Component Object Model (DCOM).

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

High-Performance Computing (HPC) Systems

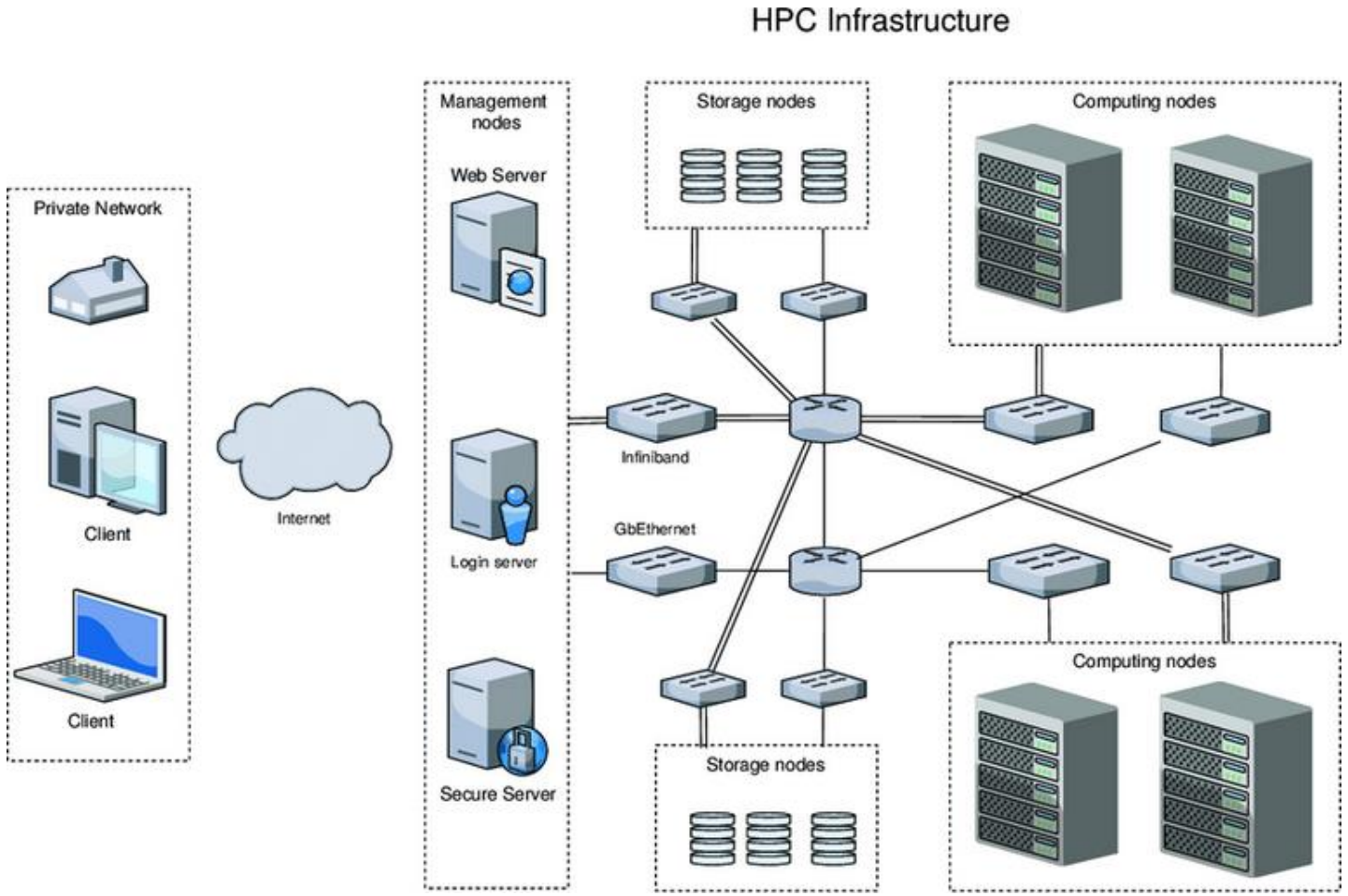
Advanced computing environments designed to perform complex calculations and process massive amounts of data at extremely high speeds.

- Handle computation-intensive workloads (e.g., simulations, modeling).
- Process vast datasets in fields like big data, artificial intelligence, and weather forecasting.
- HPC systems process sensitive data, such as intellectual property or classified information, making encryption a necessity.
- Vulnerabilities in one node could compromise the entire HPC environment.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

High-Performance Computing (HPC) Systems



Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Real-Time Operating Systems

Specialized operating systems designed to process data and execute tasks within strict timing constraints, often critical for applications where delays can have severe consequences.

- Designed to ensure predictable and timely execution of tasks. It prioritizes time-sensitive operations over others, ensuring tasks are completed within a defined deadline.
- Provide consistent performance for real-time applications, such as embedded systems, industrial control systems (ICS), and medical devices.

- **Event driven**
  - Will switch between operations or tasks based on preassigned priorities.
- **Time-sharing**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Internet of Things

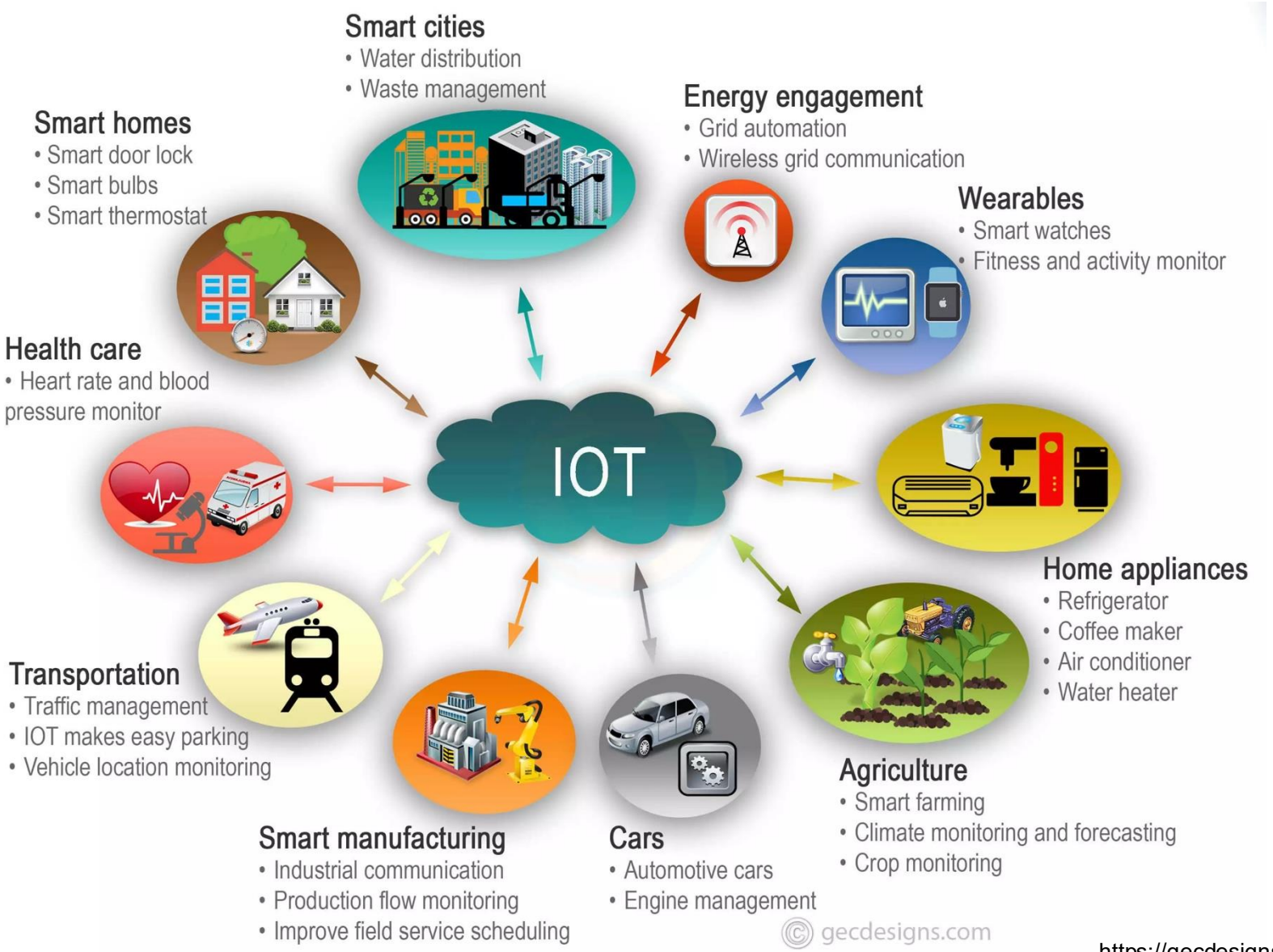
Specialized operating systems designed to process data and execute tasks within strict timing constraints, often critical for applications where delays can have severe consequences.

- Designed to ensure predictable and timely execution of tasks. It prioritizes time-sensitive operations over others, ensuring tasks are completed within a defined deadline.
- Provide consistent performance for real-time applications, such as embedded systems, industrial control systems (ICS), and medical devices.

- **Event driven**
- **Time-sharing**
  - Will switch between operations or tasks based on clock interrupts or specific time intervals.
- Resource constraints in RTOS environments may limit the implementation of robust security measures.
- Many RTOS applications use legacy systems that cannot be patched without interrupting operations.

Chapt
Count

Internet of T



https://gecdesigns.com/img/blog/iot/iot-02.jpg

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Internet of Things (IIoT)

A derivative of IoT that focuses more on industrial, engineering, manufacturing, or infrastructure level oversight, automation, management, and sensing.

- **Edge computing**
- **Fog computing**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Internet of Things (IIoT)

A derivative of IoT that focuses more on industrial, engineering, manufacturing, or infrastructure level oversight, automation, management, and sensing.

- **Edge computing**
  - Processing data at or near the source of data generation — such as sensors, IoT devices, or local edge servers.
  - A smart camera analyzing footage on the device without sending data to the cloud.
  - Security Considerations:
    - Devices at the edge have limited resources for security protections.
    - Requires encryption for local data processing and secure device authentication.
    - Vulnerable to physical tampering and cyberattacks on edge nodes.
- **Fog computing**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Industrial Internet of Things (IIoT)

A derivative of IoT that focuses more on industrial, engineering, manufacturing, or infrastructure level oversight, automation, management, and sensing.

- **Edge computing**
- **Fog computing**
  - Extends cloud capabilities closer to the edge, using intermediate nodes (fog nodes) to process data before sending to the cloud.
  - Data processing occurs on local area network (LAN) nodes, like routers or gateways — not directly on the edge device.
  - Security Considerations:
    - Fog nodes must have access control mechanisms to prevent unauthorized access.
    - Requires strong encryption for securing data during transit between edge devices and fog nodes.
    - Security challenges increase with a larger attack surface due to multiple intermediary nodes.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Feature	Edge Computing	Fog Computing
Processing Location	Directly at the edge (on the device itself).	At intermediary fog nodes before reaching the cloud.
Latency	Extremely low (processed at the source).	Moderate (processed close but not at the source).
Security Challenges	Device security and physical tampering risks.	Node authentication and data protection during transit.
Use Cases	Autonomous vehicles, real-time monitoring.	Smart cities, industrial IoT, data aggregation.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- Embedded system
- Microcontrollers
- Static Systems

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- **Embedded system**
  - Specialized computing systems integrated into larger devices or machines to perform dedicated functions. They are designed for efficiency, reliability, and specific task execution, making them widely used in industrial, medical, automotive, and consumer electronics.
- **Microcontrollers**
- **Static Systems**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- **Embedded system**
- **Microcontrollers**
  - A microcontroller is a small computer consisting of a CPU, various input/ output capabilities, RAM, and often nonvolatile storage in the form of flash or ROM/ PROM/ EEPROM.
- **Static Systems**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- **Embedded system**
- **Microcontrollers**
- **Static Systems**
  - Changes to hardware, software, or configurations are infrequent, often due to security, operational, or regulatory requirements.
  - Industrial Control Systems (ICS), Military and Defense Systems, Healthcare Systems, check-in kiosk at the airport, an ATM/

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- **Embedded system**
- **Microcontrollers**
- **Static Systems**
  - Changes to hardware, software, or configurations are infrequent, often due to security, operational, or regulatory requirements.
  - Industrial Control Systems (ICS), Military and Defense Systems, Healthcare Systems, check-in kiosk at the airport, an ATM/

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Embedded Devices and Cyber-Physical Systems

- **Cyber-Physical Systems**
  - Integrated systems that combine computing elements with physical processes to enable autonomous control, monitoring, and real-time decision-making
  - Physical components (e.g., sensors, actuators) interact with computing elements (software, networks) to optimize performance and automate processes.

CISSP® ME

Chapter S
Counterr

Embedded Device

Feature	Embedded Devices	Cyber-Physical Systems (CPS)
Definition	Standalone computing devices performing specific tasks within larger systems.	Integrated systems where computing elements interact with physical processes.
Scope	Typically limited to a single function within a device or system.	Larger-scale networks incorporating embedded devices, sensors, and actuators.
Components	Microcontrollers, firmware, sensors, actuators.	Embedded systems, software, communication networks, and real-time analytics.
Connectivity	Often operates independently or with minimal networking.	Strongly connected with IoT, cloud, and industrial control systems.
Real-Time Capabilities	Can operate in real-time but with limited adaptive control.	Real-time monitoring and autonomous decision-making.
Security Concerns	Firmware vulnerabilities, hardware tampering, weak authentication.	Complex attack surfaces, network vulnerabilities, data integrity risks.
Attack Vectors	Physical tampering, malware injection, unauthorized firmware modifications.	Network-based cyberattacks, denial-of-service (DoS), AI-driven exploits.
Mitigation Strategies	Secure boot, encryption, access control, regular patching.	Secure network segmentation, anomaly detection, strict authentication mechanisms.
Use Cases	Medical implants, automotive ECU, industrial sensors, IoT devices.	Smart grids, autonomous vehicles, industrial control systems, smart cities.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Security Concerns of Embedded and Static Systems

- Usually more limited or constrained based on their design or hardware capabilities compared to typical endpoint, server, and networking hardware.
- May run on replaceable or rechargeable batteries or USB plug or special power adapter/ converter.
- Limited networking capabilities
- Many embedded systems lack built-in security due to resource constraints
- Unpatched or outdated firmware can be exploited.
- Hardcoded or default credentials are a common vulnerability.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Microservices

- **Microservices**
  - An architectural approach to software development where applications are built as a collection of small, independent services, each responsible for a specific function.
  - Allow large, complex solutions to be broken into smaller, self-contained functions.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Microservices

- **Security Challenges in Microservices:**
  - API Security Risks
    - APIs serve as the main communication channel and can be targeted for attacks.
  - Data Security
    - Each microservice may handle sensitive data, requiring secure storage and transmission.
  - Identity and Access Management (IAM)
    - Managing user permissions across multiple services can be complex.
  - Service-to-Service Authentication
    - Microservices need to authenticate each other securely.
  - Container Vulnerabilities
    - Containers may introduce security risks if improperly configured.
  - Monitoring and logging
    - Tracking access patterns, detecting anomalies, and logging security-relevant events.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Infrastructure as Code**
  - A methodology that allows organizations to provision, configure, and manage infrastructure (servers, networks, storage) using code instead of physical hardware setup.
  - Version-Controlled Configurations
    - Uses code repositories to track changes and enforce repeatability.
  - Declarative vs. Imperative Models:
    - Declarative: Defines desired end-state (e.g., Terraform, AWS CloudFormation).
    - Imperative: Specifies step-by-step actions to reach a state (e.g., Ansible, Chef).
  - Automation & Efficiency:
    - Reduces human errors and speeds up infrastructure provisioning.
  - Integration with DevOps:
    - Works with CI/CD pipelines to automate deployments securely.
- **Immutable Architecture**
- **Software-Defined Networking (SDN)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Infrastructure as Code**
- **Immutable Architecture**
  - A security and reliability-focused approach in IT infrastructure design where components—such as servers, containers, or virtual machines—are never modified after deployment.
  - Instead of updating or patching a live system, a new instance is built, tested, and deployed to replace the old one.
  - Infrastructure is provisioned using Infrastructure as Code (IaC) (e.g., Terraform, CloudFormation).
  - Uses containers (Docker, Kubernetes) to deploy isolated applications with fixed configurations.
- **Software-Defined Networking (SDN)**

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- **Infrastructure as Code**
- **Immutable Architecture**
- **Software-Defined Networking (SDN)**
  - A derivative of IaC and DCE.
  - More details in Chapter 11

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtualization technology**
  - Used to host one or more OSs within the memory of a single host computer or to run applications that are not compatible with the host OS.
- **Hypervisor or virtual machine monitor/ manager (VMM)**
  - **Type 1 Hypervisor (Bare-Metal)**
  - **Type 2 Hypervisor (Hosted)**
- **Elasticity**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtualization technology**
- **Hypervisor or virtual machine monitor/ manager (VMM)**
  - A software or hardware-based solution that enables the creation and management of virtual machines (VMs) by abstracting physical hardware resources.
  - **Type 1 Hypervisor (Bare-Metal)**
  - **Type 2 Hypervisor (Hosted)**
- **Elasticity**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- Virtualization technology
- Hypervisor or virtual machine monitor/ manager (VMM)
  - Type 1 Hypervisor (Bare-Metal)
    - Runs directly on the physical hardware without needing an underlying operating system.
    - Examples: VMware ESXi, Microsoft Hyper-V, Xen.
  - Type 2 Hypervisor (Hosted)
    - Runs as an application on an existing operating system.
    - Examples: VMware Workstation, Oracle VirtualBox.
- Elasticity

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtualization technology**
- **Hypervisor or virtual machine monitor/ manager (VMM)**
  - **Type 1 Hypervisor (Bare-Metal)**
  - **Type 2 Hypervisor (Hosted)**
- **Elasticity**
  - Expand or contract resource utilization based on need.
  - Can also refer to the ability of a VM/ guest OS to take advantage of any unused hardware resources on the fly as needed but then release those resources when they are not needed.
  - Scalability is considered a long-term characteristic, while elasticity is more short-term.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Benefits**
  - Improved Security & Isolation
    - Segmentation: Virtual machines (VMs) are isolated from each other, reducing the risk of cross-contamination in case of an attack.
    - Can provide a reasonably secure means to continue to operate end of life (EOL) and end of service life (EOSL)/ end of support (EOS) OSs to support legacy business applications.
  - Resource Optimization
    - Multiple VMs can run on a single physical machine, reducing hardware costs.
  - Enhanced Disaster Recovery & Business Continuity
    - VMs can be easily backed up, restored, or migrated in case of a failure.
  - Secure Testing & Development
    - Developers can quickly set up virtualized environments without impacting production systems.
  - Centralized Management & Compliance
    - Administrators can enforce standardized security policies across VMs.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
  - Allows multiple virtualized instances to operate on the same physical infrastructure, creating isolated environments for applications and systems.
  - Software-based solutions that simulate physical computing environments to run applications, operating systems, or services independently from the underlying hardware.
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
  - **Containers**
  - **Application Virtualization**
  - **Network Virtualization**
  - **Storage Virtualization**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
    - Full-fledged OS environments running on a hypervisor.
    - Emulates a complete computer system, allowing multiple OS instances to run on the same physical hardware.
  - **Containers**
  - **Application Virtualization**
  - **Network Virtualization**
  - **Storage Virtualization**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
  - **Containers**
    - Virtualize only the operating system layer, sharing the host OS kernel while maintaining separate runtime environments.
    - Since containers share the same OS kernel, their isolation is weaker than VMs, making security policies around container management crucial.
  - **Application Virtualization**
  - **Network Virtualization**
  - **Storage Virtualization**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
  - **Containers**
  - **Application Virtualization**
    - Isolates applications from the underlying OS.
    - Allows users to run applications that may not be natively installed on their system. Examples include Microsoft App-V or Citrix XenApp, which stream applications rather than requiring full installations.
  - **Network Virtualization**
  - **Storage Virtualization**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
  - **Containers**
  - **Application Virtualization**
  - **Network Virtualization**
    - Abstracts networking resources, creating software-defined networks (SDN) where virtual network devices and paths can be managed independently from physical infrastructure.
    - Enhances flexibility, scalability, and security by segmenting and controlling data flow without physical changes to hardware.
  - **Storage Virtualization**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualized Systems

- **Virtual Software**
- **Types of Virtual Software**
  - **Virtual Machines (VMs)**
  - **Containers**
  - **Application Virtualization**
  - **Network Virtualization**
  - **Storage Virtualization**
    - Combines multiple physical storage resources into a single virtualized storage pool.
    - Instead of managing each physical storage device separately, administrators can dynamically allocate storage without worrying about its physical location.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Software-Defined Everything

- **Software-defined everything (SDx)**
  - **A trend of replacing hardware with software using virtualization.**
    - Only a subset will be discussed today, others will be covered in Chapters 11 and 16
  - **Virtual desktop infrastructure (VDI)**
  - **Thin client**
  - **Software-defined visibility (SDV)**
  - **Software-defined data center (SDDC) or virtual data center (VDC)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Software-Defined Everything

- **Software-defined everything (SDx)**
  - **A trend of replacing hardware with software using virtualization.**
    - Only a subset will be discussed today, others will be covered in Chapters 11 and 16
  - **Virtual desktop infrastructure (VDI)**
    - A centralized desktop environment hosted on a server rather than running locally on users' computers.
    - Enhances security by centralizing data management and restricting local storage.
    - VDI improves scalability and control while mitigating endpoint security risks.
  - **Thin client**
  - **Software-defined visibility (SDV)**
  - **Software-defined data center (SDDC) or virtual data center (VDC)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Software-Defined Everything

- **Software-defined everything (SDx)**
  - **A trend of replacing hardware with software using virtualization.**
    - Only a subset will be discussed today, others will be covered in Chapters 11 and 16
  - **Virtual desktop infrastructure (VDI)**
  - **Thin client**
    - A lightweight computer or terminal that relies on a centralized server for computing power, applications, and storage.
    - Have minimal hardware and limited local processing capabilities, reducing security risks associated with local data breaches or malware infections.
  - **Software-defined visibility (SDV)**
  - **Software-defined data center (SDDC) or virtual data center (VDC)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Software-Defined Everything

- **Software-defined everything (SDx)**
  - **A trend of replacing hardware with software using virtualization.**
    - Only a subset will be discussed today, others will be covered in Chapters 11 and 16
  - **Virtual desktop infrastructure (VDI)**
  - **Thin client**
  - **Software-defined visibility (SDV)**
    - Enables dynamic, software-driven monitoring and security control over network traffic and systems.
    - Provides granular, real-time visibility into network activities and security threats without relying solely on physical appliances.
  - **Software-defined data center (SDDC) or virtual data center (VDC)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Software-Defined Everything

- **Software-defined everything (SDx)**
  - **A trend of replacing hardware with software using virtualization.**
    - Only a subset will be discussed today, others will be covered in Chapters 11 and 16
  - **Virtual desktop infrastructure (VDI)**
  - **Thin client**
  - **Software-defined visibility (SDV)**
  - **Software-defined data center (SDDC) or virtual data center (VDC)**
    - Virtualizes all data center components, including compute, storage, and networking, through software-based management.
    - Enhances automation, scalability, and security by allowing dynamic allocation of resources, reducing hardware dependencies, and implementing security policies centrally.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualization Security Management

- **Software-defined everything (SDx)**
  - **Key Differences:**
    - Centralization & Management – VDI centralizes desktop environments, while thin clients depend on central computing power. SDDC/VDC abstracts infrastructure, and SDV focuses on visibility and monitoring.
    - Security Implications – VDI and thin clients reduce endpoint security risks. SDV improves threat detection, while SDDC/VDC streamlines security management across virtualized environments.
    - Hardware Dependency – Thin clients rely on a server, while VDI virtualizes desktops. SDDC/VDC eliminates dependency on traditional hardware management, and SDV operates virtually without physical monitoring devices.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualization Security Management

- VM sprawl
- VM escaping
- Shadow IT

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualization Security Management

- **VM sprawl**
  - The uncontrolled proliferation of virtual machines (VMs) in an organization. When VMs are created rapidly without proper governance, security risks arise, including:
    - Unpatched systems that become vulnerable to exploits.
    - Increased attack surface due to unmanaged resources.
    - Resource depletion impacting system performance.
    - Difficulty in monitoring virtual assets, leading to compliance gaps.
- **VM escaping**
- **Shadow IT**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualization Security Management

- **VM sprawl**
- **VM escaping**
  - VM escaping is a serious security vulnerability where a malicious actor exploits flaws in the hypervisor to break out of a virtual machine and access the host system or other VMs. If successful, an attacker can gain unauthorized control over multiple environments.
- **Shadow IT**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Virtualization Security Management

- **VM sprawl**
- **VM escaping**
- **Shadow IT**
  - Shadow IT refers to unauthorized technology (devices, applications, or cloud services) used by employees without IT department approval. While it can enhance productivity, it introduces security and compliance risks, including:
    - Data breaches due to unprotected systems.
    - Non-compliance with regulatory policies (GDPR, HIPAA, etc.).
    - Lack of visibility over corporate data movement.
    - Potential malware infections from unvetted applications.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Containerization

- **Containerization**
  - A virtualization method where applications and their dependencies are packaged into containers that run isolated from other applications but share the host operating system kernel.
  - Based on the concept of eliminating the duplication of OS elements in a virtual machine.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Containerization

- **Application cells**
  - A concept where applications run in secure, isolated execution environments within an operating system—somewhat similar to sandboxing.
- **Application containers**
  - Lightweight, isolated environments that package an application and its dependencies, ensuring it runs consistently across different computing environments. Technologies like Docker, Kubernetes, and LXC are popular in containerized application deployment.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Containerization

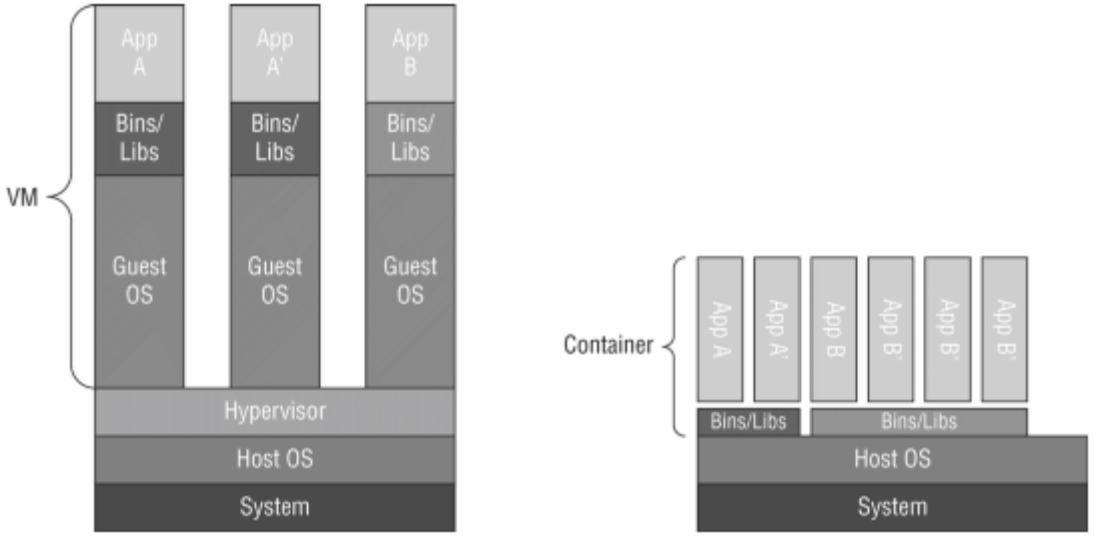


FIGURE 9.4 Application containers versus a hypervisor

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Devices**
  - Anything with a battery

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Devices**
  - Mobile devices store sensitive business and personal data.
  - Mobile devices are prone to loss or theft.
  - Organizations should enforce security policies for BYOD (Bring Your Own Device).

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Devices**
  - Deploy MDM and Endpoint Security Solutions
    - Control mobile access and apply security configurations.
  - Implement Strong Authentication Mechanisms
    - Use MFA and biometric authentication.
  - Enforce Full-Device Encryption
    - Protect stored and transmitted data from unauthorized access.
  - Educate Users on Mobile Security Best Practices
    - Train employees on safe mobile usage.

CISSP® MENTOR PROGRAM – SESSION SIX

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Communication Protection
- Remote Wiping
- Screen Locks
- Device Lockout
- GPS and Location Services

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Communication Protection**
  - Ensures secure transmission of data between mobile devices and networks.
    - End-to-End Encryption
      - Encrypting messages (e.g., Signal, WhatsApp, SSL/TLS) to prevent interception.
    - VPN (Virtual Private Network)
      - Securing internet traffic to protect against man-in-the-middle (MITM) attacks.
    - Secure Wi-Fi & Cellular Connections
      - Avoiding public Wi-Fi and using encrypted cellular networks.
- **Remote Wiping**
- **Screen Locks**
- **Device Lockout**
- **GPS and Location Services**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Communication Protection**
- **Remote Wiping**
  - Allows administrators to erase data from a lost or compromised mobile device remotely
    - MDM (Mobile Device Management) Integration
      - Organizations can configure devices for automatic wipe if compromised.
    - Factory Reset & Selective Wipe
      - Some solutions allow complete erasure or selective removal of corporate data.
    - Security Benefit
      - Prevents unauthorized access to sensitive information in case of theft or loss.
- **Screen Locks**
- **Device Lockout**
- **GPS and Location Services**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Communication Protection**
- **Remote Wiping**
- **Screen Locks**
  - Prevent unauthorized access to mobile devices
    - PIN Codes & Passwords
      - Traditional authentication methods.
    - Biometric Authentication
      - Fingerprint scanners, facial recognition, or iris scans for stronger security.
    - Pattern Locks
      - Graphical patterns used as an alternative authentication method.
- **Device Lockout**
- **GPS and Location Services**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Communication Protection**
- **Remote Wiping**
- **Screen Locks**
- **Device Lockout**
  - A security measure that restricts access after multiple failed login attempts
    - Brute Force Protection
      - After several incorrect password attempts, the device locks itself temporarily or permanently.
    - Two-Factor Authentication (2FA)
      - Reduces the risk of unauthorized login attempts.
- **GPS and Location Services**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Communication Protection**
- **Remote Wiping**
- **Screen Locks**
- **Device Lockout**
- **GPS and Location Services**
  - Allow mobile devices to track physical location
    - Security Risk
      - If compromised, attackers can track users' movements.
    - Privacy Controls
      - Users should restrict unnecessary location tracking permissions.
    - Use Cases
      - Location-based authentication or emergency recovery features.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Geotagging
- Geofencing
- Content Management
- Application Control
- Push Notifications
- Third-Party Application Stores

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
  - Embeds location metadata in images, videos, and posts
    - Security Risks
      - Can expose sensitive locations of users or employees
- **Geofencing**
- **Content Management**
- **Application Control**
- **Push Notifications**
- **Third-Party Application Stores**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
- **Geofencing**
  - Creates virtual geographic boundaries that trigger security actions when mobile devices enter or exit defined areas
    - Corporate Device Management
      - Restrict sensitive data access outside secure zones.
    - Authentication Enhancements
      - Location-based access control for VPN or corporate networks
- **Content Management**
- **Application Control**
- **Push Notifications**
- **Third-Party Application Stores**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
- **Geofencing**
- **Content Management**
  - The secure storage, organization, and distribution of digital content within an enterprise or application ecosystem.
    - Typically enforced with an MCM (mobile content management) system.
    - Protecting confidential data from unauthorized access.
    - Implementing access control policies for content distribution.
- **Application Control**
- **Push Notifications**
- **Third-Party Application Stores**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
- **Geofencing**
- **Content Management**
- **Application Control**
  - The process of regulating which applications can be installed, executed, or accessed on a device or network.
    - Enforced by Application control or application management solutions.
    - Allow-list and Deny-list Policies
      - Restrict unapproved applications.
- **Push Notifications**
- **Third-Party Application Stores**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
- **Geofencing**
- **Content Management**
- **Application Control**
- **Push Notifications**
  - Allow applications to send real-time alerts to users even when the app is not actively running.
    - Data Privacy Risks
      - Notifications may contain sensitive data.
    - Push Notification Spoofing
      - Prevent unauthorized actors from sending fake notifications.
- **Third-Party Application Stores**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Geotagging**
- **Geofencing**
- **Content Management**
- **Application Control**
- **Push Notifications**
- **Third-Party Application Stores**
  - App distribution platforms outside of official stores like Google Play or Apple's App Store. While they offer alternative apps, they increase security risks.
    - Apps may bypass security checks.
    - Unauthorized apps may collect sensitive information.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Storage Segmentation
- Asset Tracking
- Removable Storage
- Deactivating Unused Features
- Rooting or Jailbreaking

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Storage Segmentation**
  - Involves separating corporate and personal data on mobile or endpoint devices.
  - This ensures that sensitive business information remains isolated from personal applications.
- **Asset Tracking**
- **Removable Storage**
- **Deactivating Unused Features**
- **Rooting or Jailbreaking**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Storage Segmentation**
- **Asset Tracking**
  - Refers to monitoring and managing physical and digital assets, ensuring they remain secure, accounted for, and properly utilized.
    - Ensures inventory control and device lifecycle management.
    - Supports incident response if an asset is lost or compromised.
- **Removable Storage**
- **Deactivating Unused Features**
- **Rooting or Jailbreaking**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Storage Segmentation**
- **Asset Tracking**
- **Removable Storage**
  - Devices (e.g., USB drives, SD cards, external hard drives) that pose data security risks if not properly managed.
  - USB On-The-Go (OTG) is a specification that allows a mobile device with a USB port to act as a host and use other standard peripheral USB equipment.
- **Deactivating Unused Features**
- **Rooting or Jailbreaking**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Storage Segmentation**
- **Asset Tracking**
- **Removable Storage**
- **Deactivating Unused Features**
  - Disabling unused hardware and software features prevents exploitation by attackers.
  - Disable unused network protocols (Bluetooth, NFC, USB access) when not needed.
  - Restrict third-party app permissions to prevent unnecessary background activity.
- **Rooting or Jailbreaking**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Storage Segmentation**
- **Asset Tracking**
- **Removable Storage**
- **Deactivating Unused Features**
- **Rooting or Jailbreaking**
  - Rooting (Android) and jailbreaking (iOS) refer to removing built-in security restrictions to gain deeper system access.
  - Bypasses security controls, making devices vulnerable to attacks.
  - Reduces OS integrity, allowing unverified apps to modify system files.
  - “Bricking” refers to rendering a device completely nonfunctional or as useless as a brick.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Sideloading
- Custom Firmware
- Carrier Unlocking
- Firmware Over-the-Air (OTA) Updates
- Credential Management
- Text Messaging

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
  - The manual installation of apps onto a mobile device from sources outside official app stores (Google Play, Apple App Store).
  - Bypasses app store security checks, increasing exposure to malware.
  - Lack of vetting means apps may contain spyware or hidden vulnerabilities.
- **Custom Firmware**
- **Carrier Unlocking**
- **Firmware Over-the-Air (OTA) Updates**
- **Credential Management**
- **Text Messaging**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
- **Custom Firmware**
  - Replaces the manufacturer-provided operating system with a modified version, often for performance enhancements or feature unlocking.
  - Removes built-in security protections, making devices more vulnerable.
  - Bypasses official update mechanisms, increasing exposure to unpatched vulnerabilities.
  - Might violate compliance policies, particularly in regulated environments.
- **Carrier Unlocking**
- **Firmware Over-the-Air (OTA) Updates**
- **Credential Management**
- **Text Messaging**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
- **Custom Firmware**
- **Carrier Unlocking**
  - Allows a mobile device to be used with different network providers.
  - Maintain an inventory tracking system for unlocked enterprise devices.
  - Use IMEI tracking to prevent unauthorized use of unlocked devices.
- **Firmware Over-the-Air (OTA) Updates**
- **Credential Management**
- **Text Messaging**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
- **Custom Firmware**
- **Carrier Unlocking**
- **Firmware Over-the-Air (OTA) Updates**
  - OTA updates allow remote deployment of device firmware updates, ensuring security patches and performance improvements.
  - Fixes vulnerabilities before they can be exploited.
  - Enhances device functionality while maintaining security compliance.
- **Credential Management**
- **Text Messaging**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
- **Custom Firmware**
- **Carrier Unlocking**
- **Firmware Over-the-Air (OTA) Updates**
- **Credential Management**
  - Ensures secure handling of authentication credentials, such as passwords, tokens, and certificates.
  - Use password hashing and encryption for credential storage.
  - Implement single sign-on (SSO) and MFA for strong authentication.
- **Text Messaging**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Sideloading**
- **Custom Firmware**
- **Carrier Unlocking**
- **Firmware Over-the-Air (OTA) Updates**
- **Credential Management**
- **Text Messaging**
  - A widely used communication method, but it can pose data privacy and integrity risks.
  - Short Message Service (SMS), Multimedia Messaging Service (MMS), and Rich Communication Services (RCS)
  - SMS phishing (smishing) attempts to trick users into sharing sensitive information.
  - Unencrypted messages can be intercepted in transit.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies**
  - **Define how organizations handle mobile device usage while maintaining confidentiality, integrity, and availability (CIA Triad).**
  - **Bring Your Own Device (BYOD)**
  - **Choose Your Own Device (CYOD)**
  - **Corporate-Owned, Personally Enabled (COPE)**
  - **Corporate-Owned Mobile Strategy (COMS)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies**
  - **Bring Your Own Device (BYOD)**
    - Employees use their personal devices (smartphones, tablets, laptops) for work purposes.
    - High risk of data leakage
      - Mixing personal and corporate data.
    - Device security varies, leading to inconsistent protection.
    - Complicated compliance
      - Ensuring sensitive data is secure across different devices.
  - **Choose Your Own Device (CYOD)**
  - **Corporate-Owned, Personally Enabled (COPE)**
  - **Corporate-Owned Mobile Strategy (COMS)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies**
  - **Bring Your Own Device (BYOD)**
  - **Choose Your Own Device (CYOD)**
    - Employees select from pre-approved devices provided by the company, ensuring compatibility with security standards.
    - Reduces risk compared to BYOD, but users still own devices.
    - Enables better endpoint control with company-approved configurations.
  - **Corporate-Owned, Personally Enabled (COPE)**
  - **Corporate-Owned Mobile Strategy (COMS)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies**
  - **Bring Your Own Device (BYOD)**
  - **Choose Your Own Device (CYOD)**
  - **Corporate-Owned, Personally Enabled (COPE)**
    - The company owns the device, but employees can use it for personal activities alongside work tasks.
    - Stronger control compared to BYOD and CYOD.
    - Reduces risks of unauthorized applications and malware infections.
  - **Corporate-Owned Mobile Strategy (COMS)**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies**
  - **Bring Your Own Device (BYOD)**
  - **Choose Your Own Device (CYOD)**
  - **Corporate-Owned, Personally Enabled (COPE)**
  - **Corporate-Owned Mobile Strategy (COMS)**
    - The company fully owns and controls all mobile devices used by employees. Personal use is restricted or prohibited.
    - Highest security level with full enterprise oversight.
    - Ensures consistent security patches across all devices.
    - Limits data leakage risks by eliminating personal use.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

Policy	Ownership	Personal Use Allowed?	Security Level
BYOD	Employee	Yes	Medium (Higher risk of breaches)
CYOD	Employee	Yes (Limited)	Medium-High (Standardized security)
COPE	Company	Yes	High (Corporate control with flexibility)
COMS	Company	No	Very High (Strict security enforcement)

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Mobile Device Deployment Policies Details
  - Data Ownership
  - Support Ownership
  - Patch and Update Management
  - Security Product Management
  - Forensics
  - Privacy

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
    - Determines who controls, manages, and has rights over data stored on mobile devices.
    - Clear distinctions between personal and corporate data are necessary, especially in BYOD (Bring Your Own Device) scenarios.
  - **Support Ownership**
  - **Patch and Update Management**
  - **Security Product Management**
  - **Forensics**
  - **Privacy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
  - **Support Ownership**
    - Defines who is responsible for troubleshooting and managing device security issues.
      - In BYOD models, users may resist corporate control, leading to gaps in security enforcement.
      - In COPE and COMS models, organizations maintain full responsibility over device security.
  - **Patch and Update Management**
  - **Security Product Management**
  - **Forensics**
  - **Privacy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
  - **Support Ownership**
  - **Patch and Update Management**
    - Ensures devices remain updated to mitigate vulnerabilities.
  - **Security Product Management**
  - **Forensics**
  - **Privacy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
  - **Support Ownership**
  - **Patch and Update Management**
  - **Security Product Management**
    - Refers to implementing and maintaining security solutions for mobile devices.
    - Standardize security tools like anti-malware software, encrypted VPNs, and intrusion detection systems.
    - Integration with enterprise security frameworks (SIEM, EDR, MFA) strengthens defenses.
  - **Forensics**
  - **Privacy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
  - **Support Ownership**
  - **Patch and Update Management**
  - **Security Product Management**
  - **Forensics**
    - Should address forensics and investigations related to mobile devices.
    - Users need to be aware that in the event of a security violation or a criminal activity, their devices might be involved.
  - **Privacy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Data Ownership**
  - **Support Ownership**
  - **Patch and Update Management**
  - **Security Product Management**
  - **Forensics**
  - **Privacy**
    - Dictates how user data is collected, stored, and shared in mobile environments.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

In all legal matters, including mobile device forensics and privacy, consult your own attorney(s) for the best course of action and policy contents.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Mobile Device Deployment Policies Details
  - Architecture/ Infrastructure Considerations
  - Legal Concerns
  - Acceptable Use Policy
  - Onboard Camera/ Video

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Architecture/ Infrastructure Considerations**
    - Must align with secure network, application, and data management principles.
    - Mobile devices should be compatible with enterprise firewalls, VPNs, and endpoint security solutions.
    - Mobile devices accessing corporate cloud storage must comply with encryption standards.
  - **Legal Concerns**
  - **Acceptable Use Policy**
  - **Onboard Camera/ Video**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Architecture/ Infrastructure Considerations**
  - **Legal Concerns**
    - Covers data protection laws, employee privacy, and regulatory compliance.
    - Organizations must balance security monitoring with privacy rights.
    - In BYOD environments, businesses must define clear ownership policies for work-related data.
  - **Acceptable Use Policy**
  - **Onboard Camera/ Video**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Architecture/ Infrastructure Considerations**
  - **Legal Concerns**
  - **Acceptable Use Policy**
    - Defines rules for how employees should use corporate or personal mobile devices within the workplace.
  - **Onboard Camera/ Video**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Architecture/ Infrastructure Considerations**
  - **Legal Concerns**
  - **Acceptable Use Policy**
  - **Onboard Camera/ Video**
    - Device cameras could be used for covert data recording.
    - Unrestricted camera usage may lead to breaches of confidential information.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- Mobile Device Deployment Policies Details
  - Recording Microphone
  - Tethering and Hotspots
  - Contactless Payment Methods
  - SIM Cloning

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Recording Microphone**
    - Pose privacy and security risks if exploited.
    - Malware or rogue apps could secretly activate the microphone.
    - Sensitive conversations can be recorded without consent.
  - **Tethering and Hotspots**
  - **Contactless Payment Methods**
  - **SIM Cloning**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Recording Microphone**
  - **Tethering and Hotspots**
    - Allows a mobile device to share its internet connection with other devices, creating a potential attack surface.
    - Man-in-the-middle (MITM) attacks – Unauthorized users can intercept data.
    - Data leakage – Sensitive corporate data could be exposed over unsecured networks.
  - **Contactless Payment Methods**
  - **SIM Cloning**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Recording Microphone**
  - **Tethering and Hotspots**
  - **Contactless Payment Methods**
    - Perform contactless payments via NFC (Near Field Communication) or RFID-based technologies.
  - **SIM Cloning**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Mobile Devices

- **Mobile Device Deployment Policies Details**
  - **Recording Microphone**
  - **Tethering and Hotspots**
  - **Contactless Payment Methods**
  - **SIM Cloning**
    - Allows attackers to duplicate a SIM card, gaining access to a user's cellular identity, messages, and calls.
    - Cloned SIMs can be used for fraudulent activities.
    - If MFA codes are sent via SMS, an attacker could misuse them.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Essential Security Protection Mechanisms

- Process Isolation
- Hardware Segmentation
- Root of Trust
- System Security Policy

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Essential Security Protection Mechanisms

- **Process Isolation**
  - Ensures that each process operates independently, preventing unauthorized access or interference between applications running on a system.
  - Protects memory spaces from unauthorized access.
  - Reduces the risk of process manipulation attacks (e.g., buffer overflow exploits).
  - Ensures data confidentiality by limiting cross-process interactions.
- **Hardware Segmentation**
- **Root of Trust**
- **System Security Policy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Essential Security Protection Mechanisms

- **Process Isolation**
- **Hardware Segmentation**
  - Divides computing resources to ensure critical system components are isolated from non-essential applications.
  - Prevents direct hardware access by unauthorized applications.
  - Reduces the likelihood of hardware-level exploits, such as firmware-based attacks.
  - Supports secure multi-tenancy, ensuring virtualization remains protected.
- **Root of Trust**
- **System Security Policy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Essential Security Protection Mechanisms

- **Process Isolation**
- **Hardware Segmentation**
- **Root of Trust**
  - A foundational security mechanism ensuring system integrity through cryptographic validation and secure boot processes.
  - Trust anchor
    - A specific entity or component within a system that is inherently trusted.
  - Utilize TPM (Trusted Platform Module) to validate system firmware integrity.
- **System Security Policy**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Essential Security Protection Mechanisms

- **Process Isolation**
- **Hardware Segmentation**
- **Root of Trust**
- **System Security Policy**
  - Defines guidelines for managing access control, data protection, and cybersecurity practices across an organization.
  - Establishes clear governance for data security and system integrity.
  - Protects against unauthorized modifications or security breaches.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Common Security Architecture Flaws and Issues

- Covert Channels
- Attacks Based on Design or Coding Flaws
- Rootkits
- Incremental Attacks

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Common Security Architecture Flaws and Issues

- **Covert Channels**
  - An unauthorized method for transferring data outside normal security controls. Attackers use these to bypass access restrictions.
  - **Timing Covert Channels**
    - Exploiting the timing of processes to leak data.
  - **Storage Covert Channels**
    - Using system variables or files to secretly transfer information.
- **Attacks Based on Design or Coding Flaws**
- **Rootkits**
- **Incremental Attacks**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Common Security Architecture Flaws and Issues

- **Covert Channels**
- **Attacks Based on Design or Coding Flaws**
  - Poorly designed architecture or insecure coding practices that can lead to severe vulnerabilities.
    - Buffer Overflows – Attackers overflow memory to execute arbitrary code.
    - SQL Injection – Exploiting weak database queries to manipulate or steal data.
    - Logic Errors – Security flaws due to flawed system logic or authentication mistakes.
  - Apply secure coding best practices using frameworks like OWASP.
- **Rootkits**
- **Incremental Attacks**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Common Security Architecture Flaws and Issues

- **Covert Channels**
- **Attacks Based on Design or Coding Flaws**
- **Rootkits**
  - Stealthy forms of malware designed to gain persistent access to a system while hiding their presence from security tools.
  - Attackers gain deep system control, leading to data breaches or espionage.
  - Hard to detect and remove without specialized forensic tools.
- **Incremental Attacks**

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Common Security Architecture Flaws and Issues

- **Covert Channels**
- **Attacks Based on Design or Coding Flaws**
- **Rootkits**
- **Incremental Attacks**
  - Involve slow and gradual exploitation of system vulnerabilities, making detection difficult.
  - Types of Incremental Attacks:
    - Data diddling
    - Salami attack

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Understand shared responsibility.
- Understand the concept of protection rings.
- Describe the different types of memory used by a computer.
- Know the security issues surrounding memory components.
- Know the concepts of memory addressing.
- Describe the different characteristics of storage devices used by computers.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Know the security issues surrounding secondary storage devices.
- Know about emanation security.
- Understand security risks that input and output devices can pose.
- Be aware of JavaScript concerns.
- Know about large-scale parallel data systems.
- Be able to define OT/ ICS.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Be aware of distributed systems.
- Understand data sovereignty.
- Be able to define IoT.
- Understand microservices.
- Be able to define IaC.
- Understand hypervisors.
- Understand virtual software.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Know virtual networking.
- Know about SDx.
- Know about VDI and VMI.
- Be aware of SDV.
- Know some of the security issues of virtualization.
- Understand containerization.
- Understand embedded systems.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Be aware of microcontrollers.
- Understand embedded systems and static environment security concerns.
- Know about HPC systems.
- Be aware of RTOS.
- Understand edge computing.
- Know about fog computing.
- Understand mobile device security.
- Understand mobile device deployment policies.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Study Essentials

- Understand process isolation.
- Be aware of hardware segmentation.
- Understand the need for system security policy.
- Be able to explain what covert channels are.
- Know about vulnerabilities due to design and coding flaws.

CISSP® MENTOR PROGRAM – SESSION SIX

SESSION 6 - FIN

We made it! Next Session Info

Session 7 – Chapter 11 (pg. 491-574)

Lesson

Secure Network Architecture and Components

Instructor: Evan Francen

Lesson Release: 5/28 (after Session 6)

Live Mentor Session: 6/4