Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 9 of the official CISSP study guide. Here are the top things you need to know from this chapter on security vulnerabilities, threats and countermeasures.

Understand shared responsibility. The security design principle indicates that organizations do not operate in isolation. It's because we participate in shared responsibility that we must research, implement and manage engineering processes using secure design principles.

Understand the concept of protection rings. From a security standpoint, protection rings organize code and components in an OS into concentric rings. The deeper inside the circle you go, the higher the privilege level associated with the code that occupies a specific ring. Describe the different types of memory used by a computer. ROM is non-volatile and can't be written to by the end user. Data can be written onto PROM chips only once. EPROM or UV EPROM chips maybe erased with ultraviolet light. EEPROM chips maybe erased with electrical current. RAM chips are volatile and lose their contents when the computer is powered off.

Know the security issues surrounding memory components. Some security issues surround memory components. The fact that data may remain on the chip after power is removed and the control of access to memory in a multi-user system.

Know the concepts of memory addressing. Means of memory addressing include register addressing, immediate addressing, direct addressing, indirect addressing and base plus offset addressing. Describe the different characteristics of storage devices used by computers. Primary storage is the same as memory. Secondary storage consists of magnetic flash and optical media that must first be read into primary memory before the CPU can use the data. Random access storage devices can be read at any point, whereas sequential access devices require scanning through all the data physically stored before the desired location.

Know the security issues surrounding secondary storage devices. Three main security issues surround secondary storage devices. Removable media can be used to steal data, access controls and encryption must be applied to protect data and data can remain on media even after file deletion or media formatting.

Know about emanation security. Many electrical devices emanate electrical signals or radiation that can be intercepted by unauthorized individuals. These signals may contain confidential, sensitive or private data. TEMPEST or MSEC countermeasures to Van Eck phreaking include Faraday cages, white noise, control zones and shielding.

Understand security risks that input and output devices can pose. Input output devices can be subject to eavesdropping and tapping, are subject to shoulder surfing, are used to smuggle data out of an organization or can be used to create unauthorized insecure points of entry into an organization's systems and networks. Be prepared to recognize and mitigate these vulnerabilities, be aware of JavaScript concerns. JavaScript is the most widely used scripting language in the world and is embedded into many HTML documents. Whenever you allow code from an unknown and untrusted source to execute on your system, you're putting your system at risk of compromise.

Know about large scale parallel data systems. Systems designed to perform numerous calculations simultaneously include SMP, AMP and MPP. Grid computing is a form of parallel distributed processing that loosely groups a significant number of processing nodes to work toward a specific processing goal. Peer-to-peer P2P technologies are networking and distributed application solutions that share tasks and workloads among peers. Be able to define OT and ICS. An industrial control system ICS or an operational technology OT is a form of computer management device that controls industrial processes and machines. ICS examples include distributed control systems, programmable logic controllers and supervisory control and data acquisition or SCADA systems.

Be aware of distributed systems. A distributed system or distributed computing environment is a collection of individual systems that work together to support a resource or provide a service. The primary security concern is the interconnectedness of the components.

Understand data sovereignty. Data sovereignty is the concept that once information has been converted into binary form and stored as digital files, it is subject to the laws of the country within which the storage device resides. Be able to define IoT. The internet of things, IoT is a class of devices that are internet connected to provide automation, remote control or AI processing to appliances or devices. The security issues related to IoT often relate to access and encryption.

Understand microservices. A microservice is simply one element, feature capability, business logic or function of a web application that can be called upon or used by other web applications. It is the conversion or transformation of a capability of one web application into a microservice that can be called upon by numerous other web applications. It allows large complex solutions to be broken into smaller self-contained functions.

Be able to define IAC. Infrastructure as code or IAC is a change in how hardware management is perceived and handled. Instead of seeing hardware configuration as a manual, direct hands-on one-on-one administration hassle, it's viewed as just another collection of elements to be managed in the same way that software and code are managed under DevSecOps development, security and operations.

Understand hypervisors. The hypervisor, also known as the virtual machine monitor or manager VMM is the component of virtualization that creates, manages and operates virtual machines.

Understand virtual software. A virtual application or virtual software is a software product deployed in a way that is fooled into believing it is interacting with a full host operating system. A virtual or virtualized application has been packaged or encapsulated so that it can execute, but operate without full access to the host operating system. A virtual application is isolated from the host operating system so that it cannot make any direct or permanent changes to the host.

Know about virtual networking. A virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity. The resulting solution allows for software control over all network functions, management, traffic shaping, address assignment and so on.

Know about SDx. Software- defined everything SDx refers to a trend of replacing hardware with software using virtualization. SDx includes virtualization, virtualized software, virtual networking, containerization, serverless architecture, infrastructure as code, SDN, vSAN, software-defined storage, VDI, VMI, SDV and software defined data center.

Know about VDI and VMI. Virtual desktop infrastructure VDI is a means to reduce the security risk and performance requirements of end user devices by hosting desktop or workstation operating system virtual machines on centralized servers that are remotely accessed by end users. Virtual mobile infrastructure VMI is where the operating system of a mobile device is virtualized on a central server. Be aware of SDV. Software Defined visibility, SDV is a framework to automate the processes of network monitoring and response. The goal is to enable the analysis of every packet and make deep intelligence-based decisions on forwarding, dropping or otherwise responding to threats.

Know some of the security issues of virtualization. Virtualization doesn't lessen the security management requirements of an operating system. Patch management is still essential. It's important to protect the stability of the host. Organizations should maintain backups of their virtual assets. Virtualized systems should be security tested. VM sprawl occurs when an organization deploys numerous virtual machines without an overarching IT management or security plan in place.

Understand containerization. Containerization or OS virtualization is based on the concept of eliminating the duplication of OS elements in a virtual machine. Each application is placed into a container that includes only the actual resources needed to support the enclosed application and the common or shared operating system elements are then part of the hypervisor.

Understand embedded systems. An embedded system is typically designed around a limited set of specific functions in relation to the larger product to which it is attached. A microcontroller is similar too, but less complex than a system on a chip SoC. A microcontroller maybe a component of an SoC. A microcontroller is a small computer consisting of a CPU with one or more cores, memory, various input output capabilities, RAM and non-volatile storage in the form of flash or ROM, PROM or EEPROM. Examples of microcontrollers include Raspberry Pi, Arduino, and FPGA.

Understand embedded systems and static environment security concerns. Static environments, embedded systems, cyber-physical systems, HPC systems, edge-computing devices, fog computing devices, mobile devices and other limited or single purpose computing environments need security management. These techniques may include network segmentation, security layers, application firewalls, manual updates, firmware version control and control redundancy and diversity.

Know about HPC systems. High performance computing or HPC systems are computing platforms designed to perform complex calculations or data manipulations at extremely high speeds. Supercomputers and MPP solutions are common examples of HPC systems. Be aware of RTOS. A real-time operating system RTOS is designed to process or handle data as it arrives on the system with minimal latency or delay. An RTOS is usually stored on read-only memory and is designed to operate in a hard real-time or soft real-time condition.

Understand edge computing. Edge computing is a philosophy of network design where data and compute resources are located as close as possible to each other to optimize bandwidth use while minimizing latency. In edge computing, the intelligence and processing are contained within each device. Thus, rather than having to send data off to a master processing entity, each device can process it's own data locally.

Know about fog computing. Fog computing is another example of advanced computation architectures, which is also often used as an element in an IoT deployment. Fog computing relies on sensors, IoT devices or even edge computing devices to collect data and then transfer it back to a central location for processing. Thus, intelligence and processing is centralized.

Understand mobile device security. Personal electronic device PED security features can often be managed using a mobile device management, MDM or unified endpoint management, UEM solution. These include device authentication, full device encryption, communication protection, remote wiping, screen locks, device lockout, GPS and location services management, content management, application control, push notification management, third-party application store control, storage segmentation, asset tracking, removable storage, deactivating unused features, routing, jailbreaking, side loading, custom firmware, carrier unlocking, firmware over the air updates, credential management and text messaging security.

Understand mobile device deployment policies. A number of deployment models are available for allowing and or providing mobile devices for employees to use while at work and to perform work tasks went away from the office. Examples include BYOD, CYOD, COPE and COMS slash COBO. You should also consider VDI and VMI options.

Understand process isolation. Process isolation requires that the operating system provides separate memory spaces for each processes, instructions and data. It also requires that the operating system enforce those boundaries, preventing one process from reading or writing data that belongs to another process. Be aware of hardware segmentation. Hardware segmentation is similar to process isolation and purpose. It prevents the access of information that belongs to a different processor security level. The main difference is that hardware segmentation enforces these requirements through the use of physical hardware controls rather than the logical process isolation controls imposed by an operating system.

Understand the need for system security policy. The role of a system security policy is to inform and guide the design, development, implementation, testing and maintenance of a particular system. Thus, this kind of security policy tightly targets a single implementation effort. Be able to explain what covert channels are. A covert channel is a method that is used to pass information over a path that is not normally used for communication. Using a covert channel provides a means to violate, bypass or circumvent a security policy undetected, basic types or timing and storage.

Know about vulnerabilities due to design and coding flaws. Certain attacks may result from poor design techniques, questionable implementation practices and procedures or poor or inadequate testing. Some attacks may result from deliberate design decisions when special points of entry built into code to circumvent access controls, login or other security checks often added to code while under development are not removed when that code is put into production. Poor coding practices and lack of security consideration are common sources or causes of vulnerabilities of system architectures that can be attributed to failures and design, implementation, pre-release code cleanup or out and out coding mistakes. Those are the study essentials that you need to know for chapter 9, security vulnerabilities, threats and countermeasures.