Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 8 of the official CISSP study guide. Here are the top things that you need to know from this chapter on principles of security models, design and capabilities. Be able to describe open and closed systems. Open systems are designed using industry standards and are usually easy to integrate with other open systems. Closed systems are generally proprietary hardware and or software. Their specifications are not normally published and they're usually harder to integrate with other systems.

Know about secure defaults. Never assume the default settings of any product are secure. It is always up to the system administrator and or company security staff to alter our product settings to comply with the organization's security policies.

Understand the concept of fail securely. Failure management includes programmatic error handling or exception handling and input sanitization. Secure failure is integrated into the system.

Know about the principle of keep it simple. Keep it simple is the encouragement to avoid overcomplicating the environment, organization or product design. The more complex the system, the more difficult it is to secure.

Understand zero trust. Zero trust is a security concept where nothing inside the organization is automatically trusted. Each request for activity or access is assumed to be from an unknown and untrusted location until otherwise verified. The concept is never trust, always verify. The zero trust model is based around the assume breach principle and micro-segmentation.

Know about privacy by design. Privacy by design is a guideline to integrate privacy protections into products during the early design phase rather than attempting to tack them on at the end of development. The privacy by design framework is based on seven foundational principles.

Understand, trust and assurance. A trusted system is one in which all protection mechanisms work together to process sensitive data for many types of users while maintaining a stable and secure computing environment. In other words, trust is the presence of a security mechanism or capability. Assurance is the degree of confidence in the satisfaction of security needs. Assurance is how reliable the security mechanisms are at providing security.

Define a trusted computing base or TCB. A TCB is the combination of hardware, software and controls that form a trusted base that enforces the security policy.

Know details about each of the security models. The state machine model ensures that all instances of subjects accessing objects are secure. The information flow model is designed to prevent unauthorized, insecure or restricted information flow. The non-interference model prevents the actions of one subject from affecting the system state or actions of another subject. The take-grant model dictates how rights can be passed from one subject to another or from a subject to an object.

An access control matrix is a table of subjects and objects that indicates the actions are functions that each subject can perform on each object. Bell-LaPadula subjects have a clearance level that allows them to access only those objects with the corresponding classification levels, protecting confidentiality. Biba prevents subjects with lower security levels from writing to objects at higher security levels. Clark-Wilson is an integrity model that relies on the access control triplet of subject, program, object.

NOLA controls used for evaluating computer security systems. The common criteria is a subjective security function evaluation tool that uses protection profiles and security targets and assigns an evaluation assurance level. Authorization to operate is a formal approval to operate ITIS based on an

acceptable risk level, which is based on the implementation of an agreed upon set of security and privacy controls.

Understand the security capabilities of information systems. Common security capabilities include memory protection, virtualization, the trusted platform module, encryption, decryption, interfaces and fault tolerance.

Know about the information system lifecycle. Managing the information system lifecycle is a comprehensive process that involves various stages, each with specific activities and considerations. Managing the information system lifecycle involves a structured and organized approach to developing, deploying and maintaining an information system. Those are the study essentials that you'll need to know for Chapter 8, principles of security models, design and capabilities.

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter8

Last update: **2025/05/18 17:15**