PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Cert Guide

Advance your IT career with hands-on learning

CISSP

Fifth Edition

ROBIN ABERNATHY
Dr. DARREN R. HAYES

CISSP Cert Guide, Fifth Edition

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the **print book ISBN**: 9780135343999.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

the CPU. The CPU simply authorizes the access and then lets the device communicate with memory directly. A DACK signal is used to release the memory location back to the CPU. DMA is much faster than the other two methods. The operating system manages DMA assignments.

Firmware

Firmware is software that is stored on an EPROM or EEPROM chip within a device. While updates to firmware may become necessary, they are infrequent. Firmware can exist as the basic input/output system (BIOS) on a computer or device firmware.

BIOS/UEFI

A computer's BIOS contains the basic instruction that a computer needs to boot and load the operating system from a drive. The process of updating the BIOS with the latest software is referred to as flashing the BIOS. Security professionals should ensure that any BIOS updates are obtained from the BIOS vendor and have not been tampered with in any way.

The traditional BIOS has been replaced with the Unified Extensible Firmware Interface (UEFI). UEFI maintains support for legacy BIOS devices but is considered a more advanced interface than traditional BIOS. BIOS uses the master boot record (MBR) to save information about the hard drive data, while UEFI uses the GUID partition table (GPT). BIOS partitions were a maximum of 4 partitions, each being only 2 terabytes (TB). UEFI allows up to 128 partitions, with the total disk limit being 9.4 zettabytes (ZB) or 9.4 billion terabytes. UEFI is also faster and more secure than traditional BIOS. UEFI Secure Boot requires boot loaders to have a verifiable digital signature.

UEFI is an open standard interface layer between the firmware and the operating system that requires firmware updates to be digitally signed. Security professionals should understand the following points regarding UEFI:

- It was designed as a replacement for traditional PC BIOS.
- Additional functionality includes support for Secure Boot, network authentication, and universal graphics drivers.
- It protects against BIOS malware attacks including rootkits.

Secure Boot requires that all boot loader components (e.g., OS kernel, drivers) attest to their identity (digital signature) and the attestation is compared to the trusted list.

- When a computer is manufactured, a list of keys that identify trusted hardware, firmware, and operating system loader code (and in some instances, known malware) is embedded in the UEFI.
- It ensures the integrity and security of the firmware.
- It prevents malicious files from being loaded.
- Can be disabled for backward compatibility.

Device Firmware

Hardware devices, such as routers and printers, require some processing power to complete their tasks. This firmware is contained in the firmware chips located within the devices. Like with computers, this firmware is often installed on its own EEPROM to allow it to be updated. Again, security professionals should ensure that updates are obtained only from the device vendor and that the updates have not been changed in any manner, including modified by a third party.

Operating Systems

The operating system is the software that enables a human to interact with the hardware that comprises the computer. Without the operating system, the computer would be useless. Operating systems perform a number of noteworthy and interesting functions as part of the interfacing between the human and the hardware. In this section, we look at some of these activities.

A ***thread*** is an individual unit of an application for a specific process. A ***process*** is a set of threads that are part of the same larger application. An application's instructions are not considered processes until they have been loaded into memory where all instructions must first be copied to be processed by the CPU. A process can be in a running state, ready state, or blocked state. When a process is blocked, it is simply waiting for data to be transmitted to it, usually through user data entry. A group of processes that share access to the same resources is called a protection domain.

CPUs can be categorized according to the way in which they handle processes. A ***superscalar*** computer architecture is characterized by a processor that enables concurrent execution of multiple instructions in the same pipeline stage. A processor in which a single instruction specifies more than one concurrent operation is called a Very Long Instruction Word (VLIW) processor. A ***pipelined processor*** overlaps the steps of different instructions, whereas a scalar processor executes one instruction at a time, consequently increasing pipelining.

From a security perspective, processes are placed in a ring structure according to the concept of least privilege, meaning they are only allowed to access resources and components required to perform the task. A common visualization of this structure is shown in Figure 3-6.

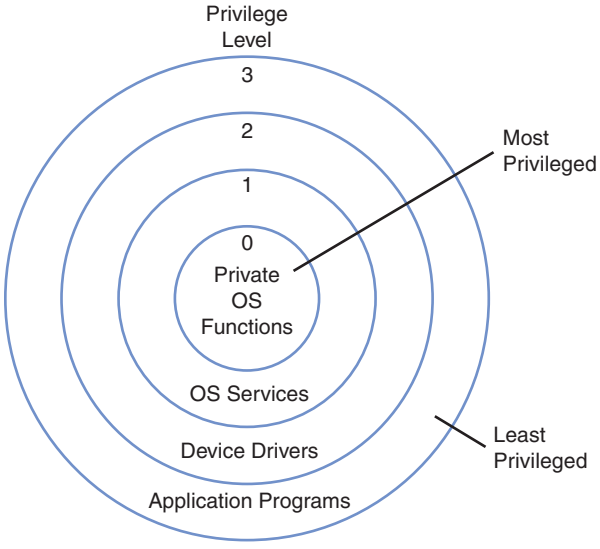

Figure 3-6 Ring Structure

When a computer system processes I/O instructions, it is operating in supervisor mode. The termination of selected, noncritical processing when a hardware or software failure occurs and is detected is referred to as a ***fail soft state***. It is in a ***fail safe state*** if the system automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

Memory Management

Because all information goes to memory before it can be processed, secure management of memory is critical. Memory space insulated from other running processes in a multiprocessing system is part of a protection domain.

System Security Evaluation Models

In an attempt to bring order to the unexpected security threats that happen, several evaluation models have been created to assess and rate the security of these products. An assurance level examination attempts to examine the security-related

components of a system and assign a level of confidence that the system can provide a particular level of security. In the following sections, we discuss organizations that have created such evaluation systems.

TCSEC

The ***Trusted Computer System Evaluation Criteria (TCSEC)*** was developed by the National Computer Security Center (NCSC) for the U.S. DoD to evaluate products. NCSC has issued a series of books focusing on both computer systems and the networks in which they operate. They address confidentiality, but not integrity. In 2005, TCSEC was replaced by the Common Criteria, discussed later in the chapter. However, security professionals still need to understand TCSEC because of its effect on security practices today and because some of its terminology is still in use.

With TCSEC, functionality and assurance are evaluated separately and form a basis for assessing the effectiveness of security controls built into automatic data-processing system products. For example, the concept of least privilege is derived from TCSEC. In the following sections, we discuss those books and the ratings they derive.

Rainbow Series

The original publication created by the TCSEC was the Orange Book, but as time went by, other books were also created that focused on additional aspects of the security of computer systems. Collectively, this set of more than 20 books is now referred to as the Rainbow Series, alluding to the fact that each book is a different color. For example, the Green Book focuses solely on password management. Next, we cover the most important books: the Red Book, Orange Book, and Green Book.

Red Book

The Trusted Network Interpretation (TNI) extends the evaluation classes of the TCSEC (DOD 5200.28-STD) to trusted network systems and components in the ***Red Book***. So where the Orange Book focuses on security for a single system, the Red Book addresses network security.

Orange Book

The ***Orange Book*** is a collection of criteria based on the Bell-LaPadula model that is used to grade or rate the security offered by a computer system product. Covert channel analysis, trusted facility management, and trusted recoveries are concepts discussed in this book.

The goals of this system can be divided into two categories, operational assurance requirements and life cycle assurance requirements, the details of which are defined next.

The operational assurance requirements specified in the Orange Book are as follows:

- System architecture
- System integrity
- Covert channel analysis
- Trusted facility management
- Trusted recovery

The life cycle assurance requirements specified in the Orange Book are as follows:

- Security testing
- Design specification and testing
- Configuration management
- Trusted distribution

TCSEC uses a classification system that assigns an alphabetic letter and a number to describe systems' security effectiveness. The assigned letter refers to a security assurance level or division as A, B, C, D, and the number refers to gradients within that security assurance level or class. Each division and class incorporates all the required elements of the ones below it.

In order of least secure to most secure, the four classes and their constituent divisions and requirements are as follows:

Key Topic

- **D—Minimal Protection**

Reserved for systems that have been evaluated but that fail to meet the requirements for a higher division.

- **C—Discretionary Protection**
  - *C1—Discretionary Security Protection*
    - Requires identification and authentication.
    - Requires separation of users and data.
    - Uses discretionary access control (DAC) capable of enforcing access limitations on an individual or group basis.
    - Requires system documentation and user manuals.

- *C2—Controlled Access Protection*
  - Uses a more finely grained DAC.
  - Provides individual accountability through login procedures.
  - Requires protected audit trails.
  - Invokes object reuse theory.
  - Requires resource isolation.

- **B—Mandatory Protection**
  - *B1—Labeled Security Protection*
    - Uses an informal statement of the security policy.
    - Requires data sensitivity or classification labels.
    - Uses MAC over selected subjects and objects.
    - Capable of label exportation.
    - Requires removal or mitigation of discovered flaws.
    - Uses design specifications and verification.
  - *B2—Structured Protection*
    - Requires a clearly defined and formally documented security policy.
    - Uses DAC and MAC enforcement extended to all subjects and objects.
    - Analyzes and prevents covert storage channels for occurrence and bandwidth.
    - Structures elements into protection-critical and non-protection-critical categories.
    - Enables more comprehensive testing and review through design and implementation.
    - Strengthens authentication mechanisms.
    - Provides trusted facility management with administrator and operator segregation.
    - Imposes strict configuration management controls.
  - *B3—Security Domains*
    - Satisfies ***reference monitor*** requirements.
    - Excludes code not essential to security policy enforcement.
    - Minimizes complexity through significant systems engineering.
    - Defines the security administrator role.
    - Requires an audit of security-relevant events.
    - Automatically detects and responds to imminent intrusion detection, including personnel notification.
    - Requires trusted system recovery procedures.