Security Capabilities of Information Systems

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Discuss how to increase security and reduce risk for your organization through the implementation of security capabilities on information systems

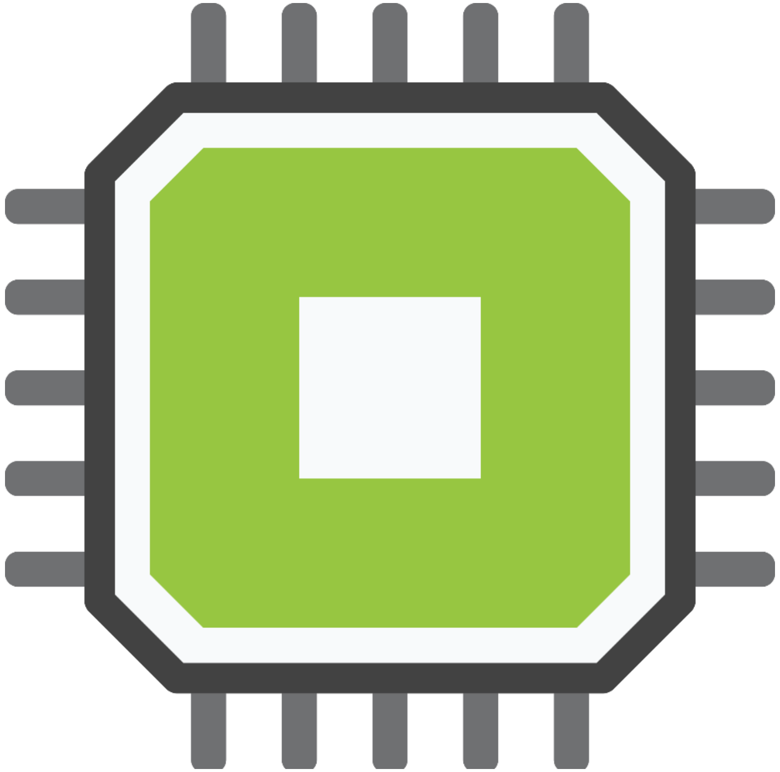
This is the 4th objective of the Security Engineering domain of the CISSP® Exam

Access Control Mechanisms

Fundamental control for any technology component

Determines who is vs. is not authorized to access an object (e.g., file, folder, setting)

Decisions are typically logged for analysis afterwards, as needed



Secure Memory Management

Memory is critical to any computing operation, whether through loading data for use (e.g., Random Access Memory (RAM)) or long term storage of data

Protection of data within memory is critical to ensuring data integrity, but also prevention of exploitation of memory vulnerabilities (e.g., buffer overflows)

Memory protection techniques, such as address space layout randomization (ASLR), can be employed to help mitigate these risks

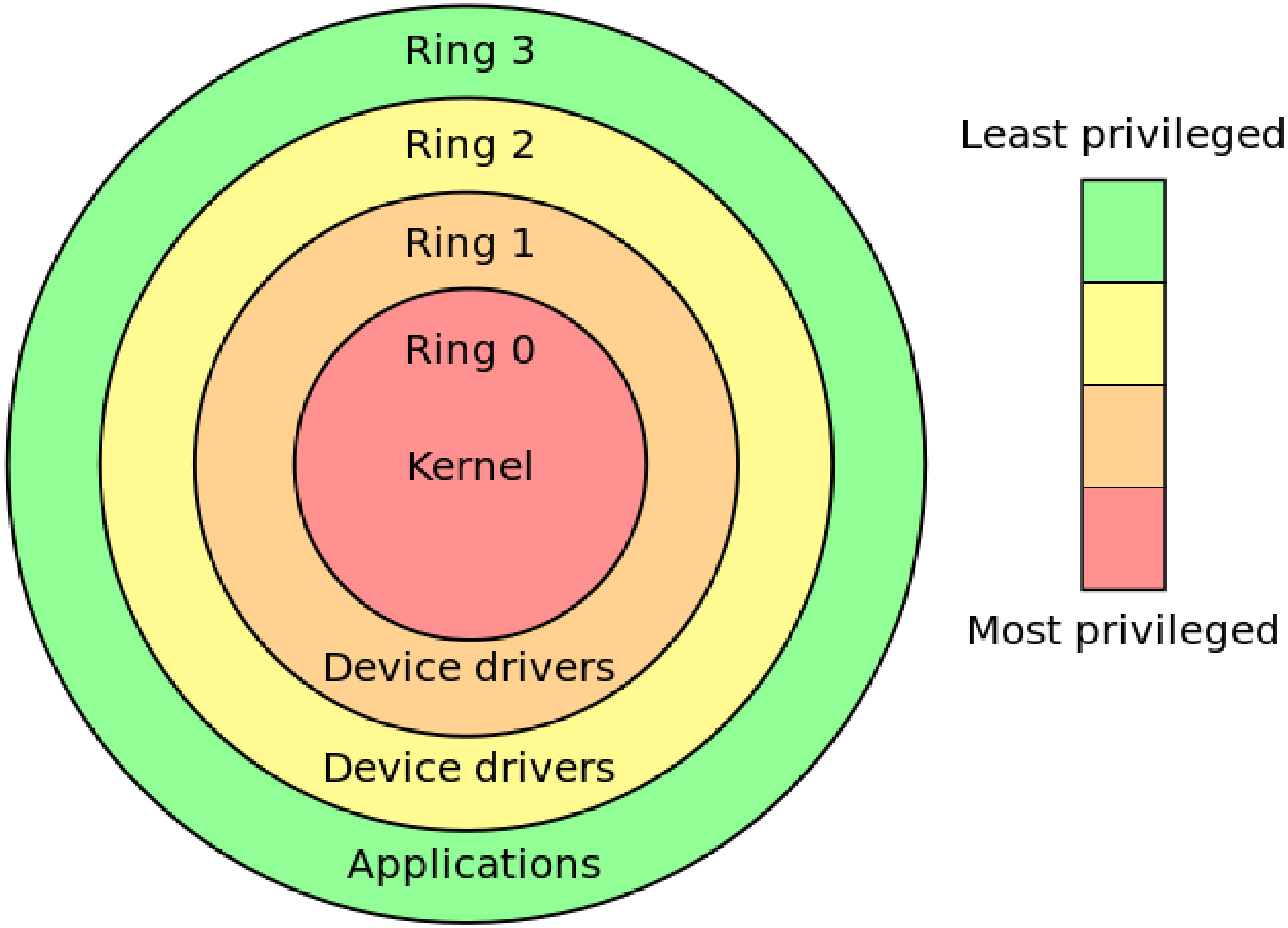
State and Layering

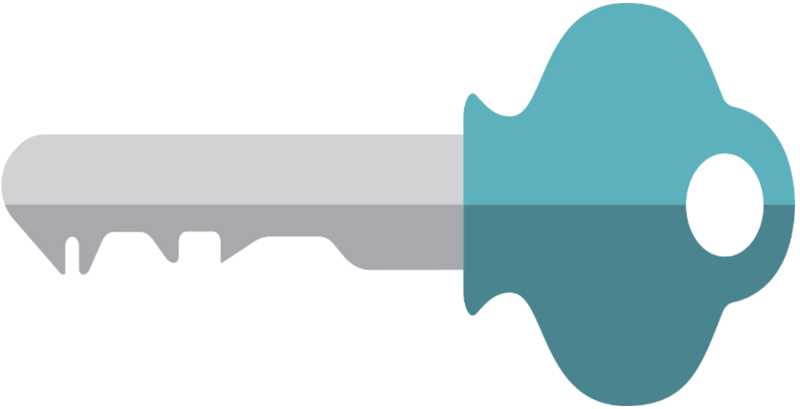
Allows for separation of process execution

Ring zero is for the system processes

All other rings are for less trusted processes

Enables control of process execution, isolation of processes, and hiding of data between rings





Cryptographic Protections

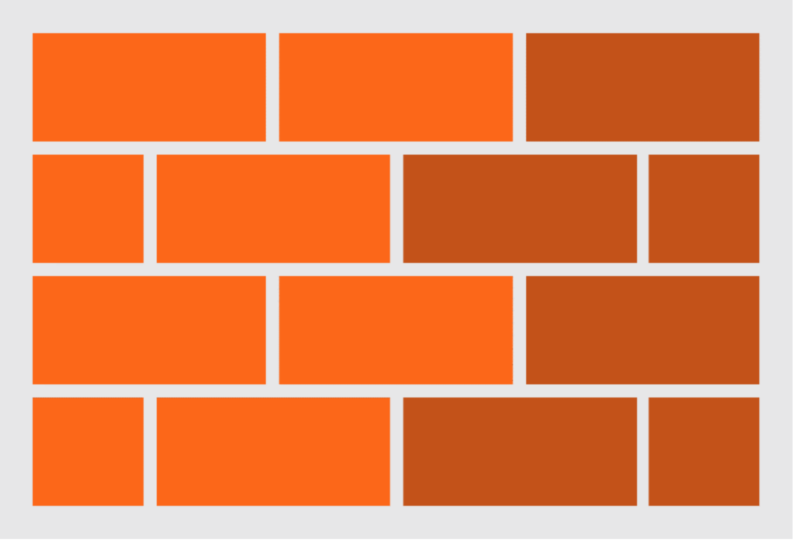
Increases confidentiality and integrity of data

Prevents disclosure of sensitive data to unauthorized users, processes, etc.

Can be employed in various ways (e.g., file-level, full disk, etc.)

Trusted Platform Modules (TPMs) are cryptoprocessors that secure the generation, usage, and storage of cryptographic keys

TPMs have been commonly included in new systems since 2006

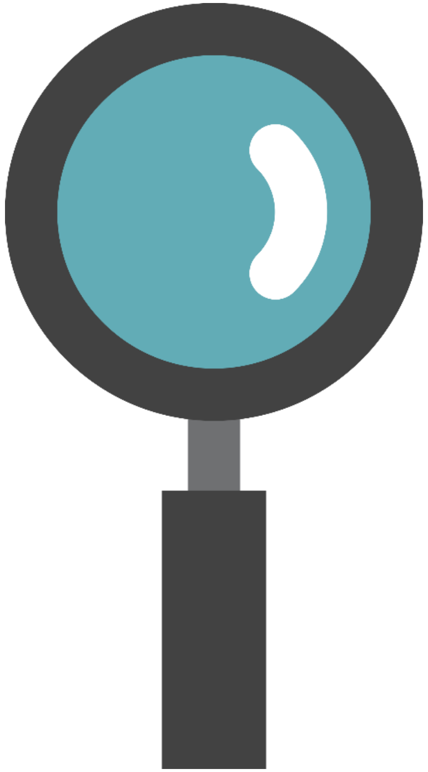


Host Firewalls and Intrusion Prevention

Built-in host-based firewalls are commonplace

Built-in intrusion prevention (or detection) capabilities are not

Various commercial and free options exist for expanding intrusion prevention / detection capabilities of systems



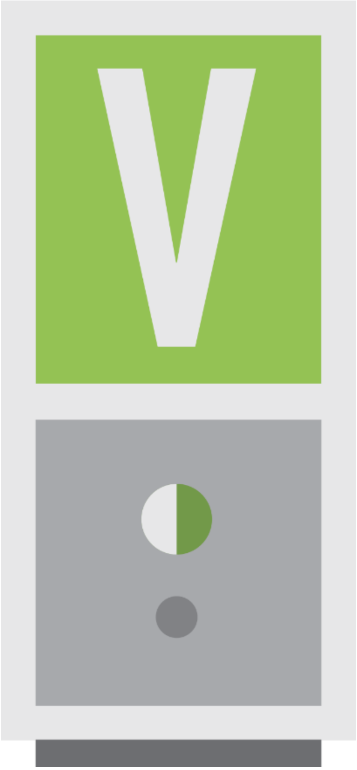
Auditing and Monitoring Controls

Logs are a critical element to any detection capability

Fine tune what is logged vs. not at your organization to meet your use cases

Logging everything isn’t the best economical solution, as it impacts the load on systems and can significantly increase storage costs, depending on retention time

Make sure to log enough though, as turning it on afterwards doesn’t help an investigation



Virtualization

Almost everything about an information system can be virtualized now (e.g., the system itself, applications, storage, etc.)

Virtualization provides a layer of abstraction to physical components that not only improve operations, but can also increase security for an organization

Leverage the benefits of virtualization, while adapting traditional security models to the new environment (e.g., network segmentation, host-based security, etc.)

Summary

Discussed how to increase security and reduce risk for your organization through the implementation of security capabilities on information systems

This is the 4th objective of the Security Engineering domain of the CISSP® Exam

What's Next?

Vulnerabilities in Security Architecture and Technology Components

What are they?

How do they relate to this module and the other modules?

Why are they important to this course and the CISSP® exam?