ACS-2821-001
Information Security in Business

Security Architecture and Design

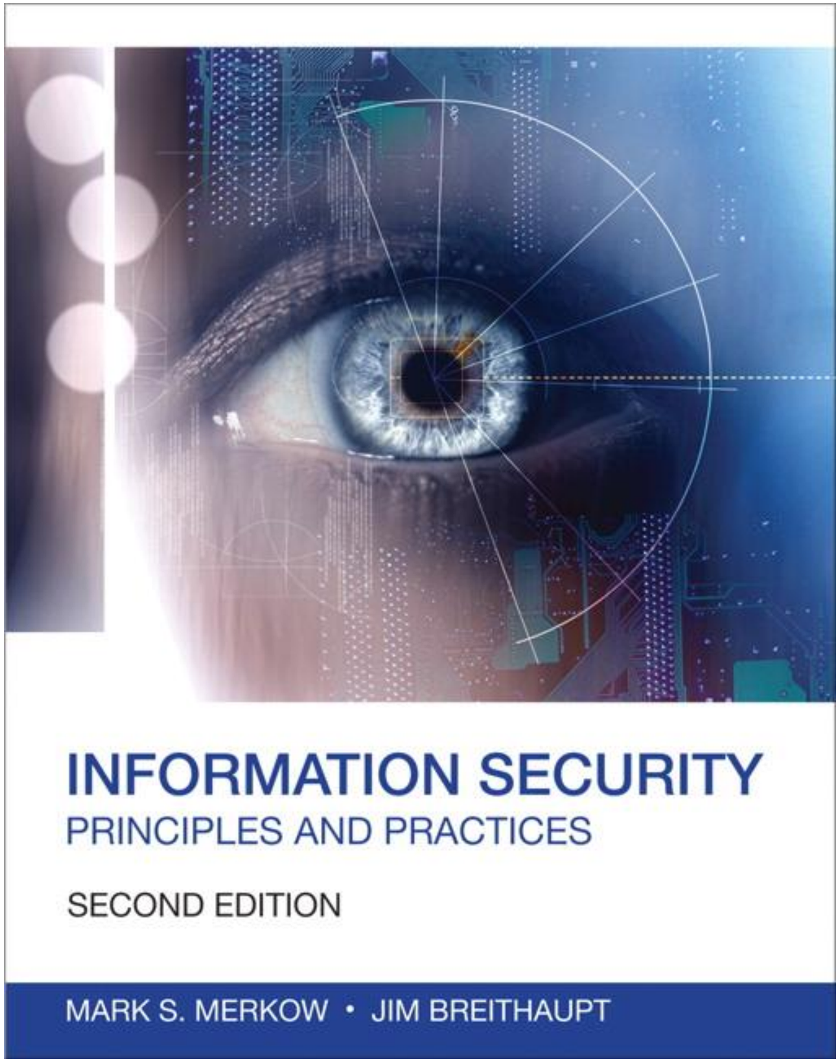
ACS-2821-001 – Slides Used In The Course

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUPT

Objectives

- Summarize the concept of a trusted computing base (TCB)
- Illustrate the concept of rings of trust
- Distinguish among the protection mechanisms used in a TCB
- Defend the purposes of security assurance testing
- Apply the Trusted Computer Security Evaluation Criteria (TCSEC) for software evaluations
- Apply the Trusted Network Interpretation of the TCSEC
- Categorize the role of the Federal Criteria for Information Technology Security
- Apply the Common Criteria for Information Security Evaluation
- Summarize the principles behind confidentiality and integrity models and their role in security architecture

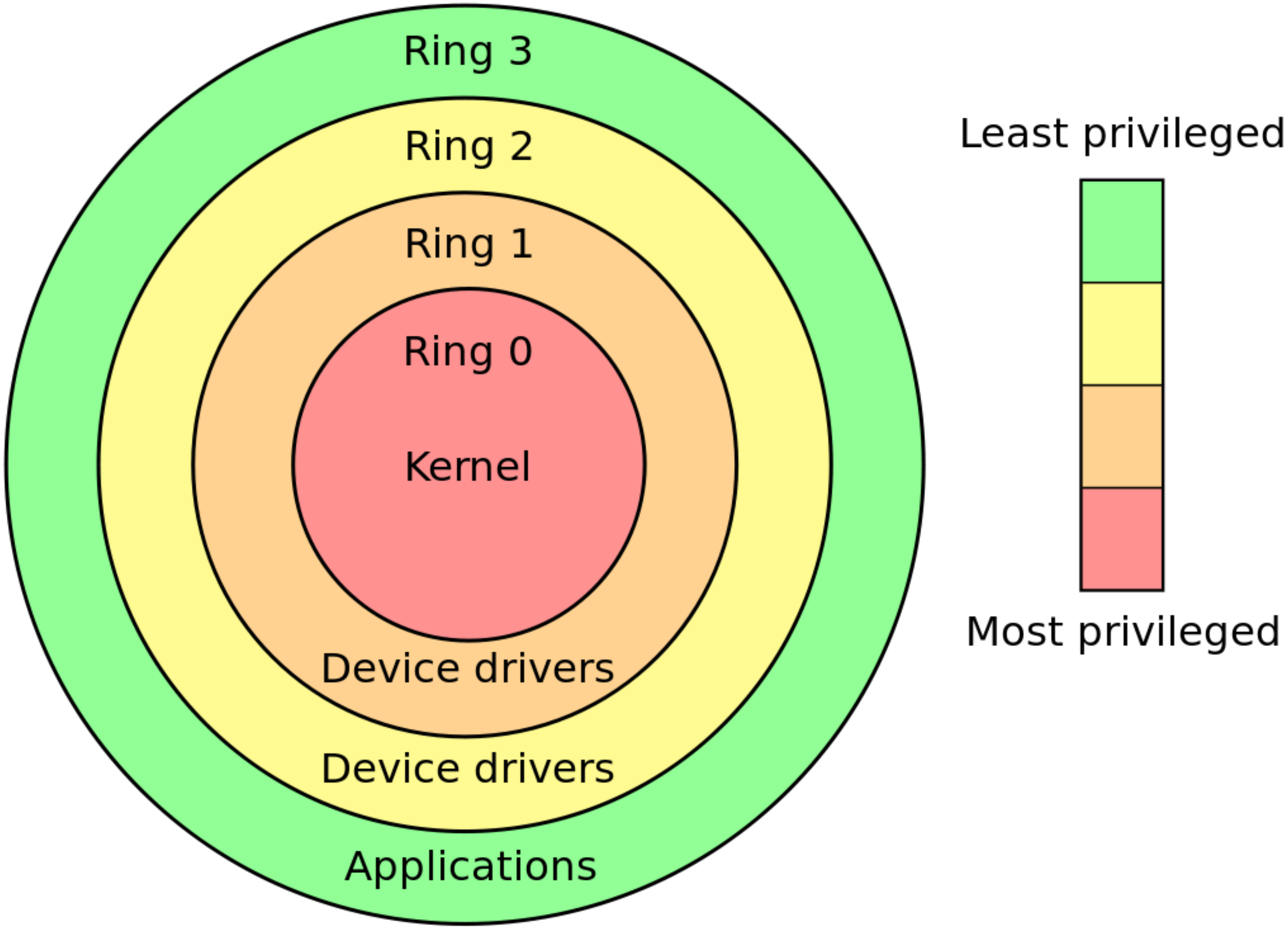
Defining the Trusted Computing Base

- Trusted Computing Base
  - Is the totality of protection mechanisms within a computer system including hardware, firmware, and software
  - Consists of one or more components that together enforce a unified security policy over a product or system
  - Describes the isolation of objects on which the protection is based, following the concept of the **reference monitor**
- Reference Monitor
  - A software model or abstract machine that mediates all access from any subject (user or other device) to any object (resource, data, and so forth) and cannot be bypassed
  - Security kernel is an implementation of a reference monitor for a specific hardware base such as Sun Solaris, Red Hat Linux, or Mac OS X

Rings of Trust

- Trust in a system moves from the outside to the inside in a unidirectional mode
- The concept of rings of trust can also be applied to a network environment and defense in depth concept
  - Each host trusts hosts in a more inner ring than its own or hosts in the same ring as its own
  - No host trusts any hosts in a more outer ring that its own
  - If a ring has been segmented into separate subnetworks, a host in one segment does not trust a host in another segment

Rings of Trust



Protection Mechanisms in a Trusted Computing Base

- Process isolation
  - Is a design objective in which each process has its own distinct address space for its application code and data
  - Prevents data or information leakage and prevents modification of the data while it is memory
- Principle of least privilege
  - Dictates that a process (program) has no more privilege than what it really needs to perform its functions
- Hardware segmentation
  - Relates to the segmentation of memory into protected segments
  - Prevents user processes from being able to access both another process's allocated memory and system memory

Protection Mechanisms in a Trusted Computing Base

- Layering
  - Is a process operation that is divided into layers by function
- Abstraction
  - Is a process that defines a specific set of permissible values for an object and the operations that are permissible on that object
- Data hiding (also known as information hiding)
  - Is a mechanism to assure that information available at one processing level is not available in another, regardless of whether it is higher or lower
- Information storage
  - Refers to the parts of a computer system that retain a physical state (information) for some interval of time, possibly even after electrical power to the computer is removed

Protection Mechanisms in a Trusted Computing Base

- Closed System versus Open System
  - Closed systems are of a proprietary nature
    - Use specific operating systems and hardware to perform the task and generally lack standard interfaces to allow connection to other systems
  - An open system is based on accepted standards and employs standard interfaces to allow connections between different systems
    - Promotes interoperability and allows the user to have full access to the total system capability
- Multitasking
  - Is a technique used by a system that is capable of running two or more tasks in a concurrent performance or interleaved execution

Protection Mechanisms in a Trusted Computing Base

- Multiprogramming system
  - Allows for the interleaved execution of two or more programs on a processor
- Multiprocessing
  - Provides for simultaneous execution of two or more programs by a processor (CPU)
- Finite-state machine
  - Stores the status or state of something at a given time that can operate based on inputs to change the stored status and/or cause an action or output to take place

System Security Assurance Concepts

- Functional requirements
  - Describe what a system should do
- Assurance requirements
  - Describe how functional requirements should be implemented and tested
- Security Testing
  - It verifies that the functions designed to meet a security requirement operate as expected
  - In addition, it validates that the implementation of the function is not flawed or haphazard

System Security Assurance Concepts

- Formal Security Testing Models
  - Trusted Computer System Evaluation Criteria (TCSEC)
    - United States in the early 1980s
  - Information Technology Security Evaluation Criteria (ITSEC)
    - Europe in 1991 by the European Commission
  - Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
    - Canada in early 1993
  - Federal Criteria for Information Technology Security (FC)
    - United States in early 1993
  - Common Criteria
    - Today’s standard

The Trusted Computer Security Evaluation Criteria (TCSEC)

- Division D: Minimal Protection
- Division C: Discretionary Protection
  - Class C1: Discretionary Security Protection
    - Identification and authentication
    - Separation of users and data
    - Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
    - Required System Documentation and user manuals
  - Class C2: Controlled Access Protection
    - More finely grained DAC
    - Individual accountability through login procedures
    - Audit trails
    - Object reuse
    - Resource isolation
    - An example of such as system is HP-UX

The Trusted Computer Security Evaluation Criteria (TCSEC)

- Division B: Mandatory Protection
  - Class B1: Labeled Security Protection
    - Informal statement of the security policy model
    - Data sensitivity labels
    - Mandatory Access Control (MAC) over selected subjects and objects
    - Label exportation capabilities
    - Some discovered flaws must be removed or otherwise mitigated Design specifications and verification

The Trusted Computer Security Evaluation Criteria (TCSEC)

- Division B: Mandatory Protection
  - Class B2: Structured Protection
    - Security policy model clearly defined and formally documented
    - DAC and MAC enforcement extended to all subjects and objects
    - Covert storage channels are analyzed for occurrence and bandwidth
    - Carefully structured into protection-critical and non-protection-critical elements
    - Design and implementation enable more comprehensive testing and review
    - Authentication mechanisms are strengthened
    - Trusted facility management is provided with administrator and operator segregation
    - Strict configuration management controls are imposed
    - Operator and Administrator roles are separated.
    - An example of such a system was Multics

The Trusted Computer Security Evaluation Criteria (TCSEC)

- Division B: Mandatory Protection
  - Class B3: Security Domains
    - Satisfies reference monitor requirements
    - Structured to exclude code not essential to security policy enforcement
    - Significant system engineering directed toward minimizing complexity
    - Security administrator role defined
    - Audit security-relevant events
    - Automated imminent intrusion detection, notification, and response
    - Trusted path to the TCB for the user authentication function
    - Trusted system recovery procedures
    - Covert timing channels are analyzed for occurrence and bandwidth
    - An example of such a system is the XTS-300, a precursor to the XTS-400

The Trusted Computer Security Evaluation Criteria (TCSEC)

- Division A: Verified Protection
  - Class A1: Verified Design
    - Functionally identical to B3
    - Formal design and verification techniques including a formal top-level specification
    - Formal management and distribution procedures
    - Examples of A1-class systems are Honeywell's SCOMP, Aesec's GEMSOS, and Boeing's SNS Server

Discretionary Access Control (DAC)

- Restrict access to objects based on the identity of subjects and/or groups to which they belong
- It is discretionary that subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject

Mandatory access control (MAC)

- Access is control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target
- Both subjects and objects each have a set of security attributes or labels
- When a subject attempts to access an object, the operating system kernel examines both the subject and object security attributes, authorization rule is use to determine whether the access can take place

The Information Technology Security Evaluation Criteria (ITSEC)

- ITSEC is a European-developed criterion
- Places increased emphasis on **integrity** and **availability**
- It also introduces the **security target (ST)**, a written document that contains
  - A system security policy
  - Required security enforcing functions
  - Required security mechanisms
  - Claimed ratings of minimum strength
  - Target evaluation levels, expressed as both functional and evaluation (F-xx and E-yy)

Comparing TCSEC and ITSEC

TCSEC Classes	ITSEC Functional and Assurance Classes
C1	F-C1, E1
C2	F-C2, E2
B1	F-B1, E3
B2	F-B2, E4
B3	F-B3, E5
A1	F-B3, E6

The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

- Published in 1993 by the Communications Security Establishment
- Combination of the TCSEC (also called Orange Book) and the European ITSEC approaches.
- It is somewhat more flexible than the TCSEC while maintaining fairly close compatibility with individual TCSEC requirements
- The CTCPEC and its approach to structure security functionality separate from assurance functionality influenced international standardization through the Common Criteria

The Federal Criteria for Information Technology Security

- Developed as a joint project by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)
- FC introduces the concept of a **protection profile (PP)** that empowers users or buyers of technology to specify their security requirements for hardware and software
- Supplanted by the Common Criteria and never moved beyond the draft stage

Common Criteria

- Common Criteria for Information Technology Security Evaluation or Common Criteria (CC) - ISO/IEC 15408
- A joint effort between United States, Canada, and Europe to harmonize security evaluation criteria
- CC provides a common language and structure to express IT security requirements
- CC enables the creation of catalogs of standards broken down into components and packages
- CC current in version 3.1 revision 5
- CC breaks apart the functional and assurance requirements into distinct elements that users can select for customized security device implementation
- Using the CC framework, users and developers of IT security products create protection profiles (PPs) as an implementation-independent collection of objectives and requirements for any given category of products or systems that must meet similar needs

Protection Profile Organization

- The Protection Profile is organized as follows:
  - Introduction Section
  - Target of evaluation (TOE) description
  - Security environment
    - Assumptions
    - Threats
    - Organizational security policies

Security Functional Requirements

- Classes of security functional requirements
- Audit
- Cryptographic support
- Communications
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of TOE security functions (TSF)
- Resource utilization
- TOE access

Evaluation Assurance Levels

- Define a scale for measuring the criteria for evaluating PPs and STs
- Provide an increasing scale that balances the levels of assurance claimed with the cost and feasibility of acquiring such assurance
- Seven assurance levels

The Common Evaluation Methodology (CEM)

- Companion document to the Common Core
- Focused on the actions that evaluators must take to determine that CC requirements for a TOE are present
- A tool that is used by evaluation schemes to ensure consistent application of the requirements across multiple evaluations and multiple schemes
- Contains three parts:
  - Introduction and General Model
  - CC Evaluation Methodology
  - Extensions to the Methodology

Confidentiality and Integrity Models

- Security models are mathematical representations of abstract machines that describe how a reference monitor is designed to operate
- Commonly used models:
  - Bell-LaPadula model
  - Biba integrity model
  - Clark and Wilson
  - Non-interference
  - State machine model
  - Access matrix model
  - Information flow model

Confidentiality and Integrity Models

- Bell-LaPadula model
  - Is a confidentiality model intended to preserve the principle of least privilege
  - Uses a clearance/classification scheme
  - Use a “Read down, write up” approach
- Biba integrity model
  - Is a integrity model to ensure data integrity
  - Uses a “read-up, write-down” approach. Subjects cannot read objects of lesser integrity and subjects cannot write to objects of higher integrity
- Clark and Wilson model
  - Requires mathematical proof that steps are performed in order exactly as they are listed, authenticates the individuals who perform the steps, and defines separation of duties

Confidentiality and Integrity Models

- Non-interference model
  - Covers ways to prevent subjects operating in one domain from affecting each other in violation of security policy
- State machine model
  - An abstract mathematical model consisting of state variables and transition functions
- Access matrix model
  - Is a state machine model for a discretionary access control environment
- Information flow model
  - Simplifies analysis of covert channels

Summary

- The trusted computing base is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and supporting the isolation of objects on which the protection is based
- Several evolving models of evaluation and assurance cover various aspects of confidentiality, integrity, and availability
- Common Criteria harmonizes the work of the various international efforts into a unified evaluation methodology that replaces the former methods

ACS-2821-001 – Questions?