

Evaluating Systems

Information Assurance

Fall 2010

Reading Material

- Chapter 21 Computer Security: Art and Science
- The orange book and the whole rainbow series
 - <http://nsi.org/Library/Compsec/orangebo.txt>
- The common criteria
 - Lists all evaluated protection profiles and products
 - <http://www.commoncriteriaportal.org>

Outline

- Motivation for system evaluation
- Specific evaluation systems
 - TCSEC/Orange Book
 - Interim systems
 - Common Criteria

Evaluation Goals

- Oriented to purchaser/user of system
- Assurance that system operates as advertised

Evaluation Options

- Rely on vendor/developer evidence
 - Self-evaluate vendor design docs, test results, etc
 - Base on reputation of vendor
- Rely on an expert
 - Read product evaluations from trusted source
 - Penetration testing

Formal Evaluation

- Provide a systematic framework for system evaluation
 - More consistent evaluation
 - Better basis for comparing similar product
- Trusted third party system for evaluation
- Originally driven by needs of government and military

TCSEC: 1983-1999

- Trusted Computer System Evaluation Criteria (TCSEC) also called the Orange Book
 - Specifies evaluation classes (C1, C2, B1, B2, B3, A1)
 - Specifies functionality and assurance requirements for each class
- Functional Model builds on
 - BLP (mandatory labeling)
 - Reference Monitors

Reference Monitor

- Reference Monitor – abstract machine that mediates all access to objects by subjects
- Reference Validation Mechanism (RVM) – Implementation of a Reference Monitor
 - Tamper-proof
 - Well defined
 - Never bypassed
 - Small enough for analysis and testing

Trusted Computing Base (TCB)

- Includes all protection mechanisms including HW, firmware, and software responsible for enforcing the security policy
- Strong boundary around the TCB is critical
 - Any code trusted by element of TCB must be part of TCB too.
 - If portion of TCB is corrupted, must consider that all of the TCB can be corrupted

TCSEC Functional Requirements

- DAC
- Object Reuse
 - Sufficient clearing of objects between uses in resource pool
 - E.g. zero pages in memory system
- MAC and Labels
- Identification and Authentication
- Audit
 - requirements increase at higher classes
- Trusted Path
 - Non-spoofable means to interact with TCB
 - Ctl-Alt-Del in Windows

TCSEC Assurance Requirements

- Configuration Management
 - For TCB
- Trusted Distribution
 - Integrity of mapping between master and installations
- System Architecture
 - Small and modular
- Design Specification – vary between classes
- Verification – Vary between classes
- Testing
- Product Documentation

TCSEC Classes

- D – Catch all
- C1 – Discretionary Protection
 - Identification and authentication and DAC
 - Minimal Assurance
- C2 – Control access protection
 - Adds object reuse and auditing
 - More testing requirements
 - Windows NT 3.5 evaluated C2

TCSEC Classes

- B1 – Labeled Security Protection
 - Adds MAC for some objects
 - Stronger testing requirements. Information model of security policy.
 - Trusted Unixes tended to be B1
- B2 – Structured protection
 - MAC for all objects. Additional logging. Trusted Path. Least privilege.
 - Covert channel analysis, configuration management, more documentation, formal model of security policy

TCSEC Classes

- B3 – Security Domains
 - Implements full RVM. Requirements on code modularity, layering, simplicity.
 - More stringent testing and documentation.
- A1 – verified protection
 - Same functional requirements as B3
 - Significant use of formal methods in assurance
 - Honeywell's SCOMP

TCSEC Evaluation process

- Originally controlled by government
 - No fee to vendor
 - May reject evaluation application if product not of interest to government
- Later introduced fee-based evaluation labs
- Evaluation phases
 - Design analysis – no source code access
 - Test analysis
 - Final review

TCSEC Evaluation Issues

- Evaluating a specific configuration
 - E.g., Window NT, no applications installed, no network
 - New patches, versions require re-certification
 - RAMP introduced to ease re-certifications
- Long time for evaluation
 - Sometimes product was obsolete before evaluation finished
- Criteria Creep
 - B1 means something more in 1999 than it did in 1989

Interim Efforts in the '90s

- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
- Information Technology Security Evaluation Criteria (ITSEC) – Western Europe
- Commercial International Security Requirements (CISR) – AmEx and EDS
- Federal Criteria – NSA and NIST

FIPS 140

- Framework for evaluating Cryptographic Modules
- Still in Use
- Addresses
 - Functionality
 - Assurance
 - Physical security

FIPS 140-2 Security Levels

- Security Level 1 – Uses a FIPS-approved crypto algorithm.
- Security Level 2 – Adds physical security requirements, e.g. Tamper-evident coatings
- Security Level 3 – Greater physical security. Protect data hardware falls into the wrong hands.
- Security Level 4 – Greatest physical security. Detects and responds to environmental and unauthorized attacks.

Common Criteria – 1998 to today

- Pulls together international evaluation efforts
 - Evaluations mean something between countries
- Three top level documents
 - Common Criteria Documents
 - Describe functional and assurance requirements. Defines Evaluation Assurance Levels (EALs)
 - CC Evaluation Methodology (CEM)
 - More details on the valuation. Complete through EAL5 (at least)
 - Evaluation Scheme
 - National specific rules for how CC evals are performed in that country
 - Directed by NIST in US

CC Terminology

- Target of Evaluation (TOE)
 - The product being evaluated
- TOE Security Policy (TSP)
 - Rules that regulate how assets are managed, protected, and distributed in a product
- TOE Security Functions (TSF)
 - Implementation of the TSP
 - Generalization of the TCB

Protection Profile (PP)

- Profile that describes the security requirements for a class of products
 - List of evaluated PP's
 - <http://www.commoncriteriaportal.org/pp.html>
- Replaces the fixed set of classes from TCSEC
- ISSO created some initial profiles to match TCSEC classes
 - Controlled Access Protection Profile (CAPP) corresponds to C2
 - Labeled Security Protection Profile (LSPP) corresponds to B1

Product evaluation

- Define a security target (ST)
 - May leverage an evaluated protection profile
- Evaluated with respect to the ST

CC Functional Requirements

- Defined in a taxonomy
 - Top level 11 classes
 - E.g., FAU – Security audit and FDP – User Data Protection
 - Each class divided into families
 - E.g., FDP_ACC – Access control policy
 - Each family divided into components
 - E.g., FDP_ACC.2 – Complete access control
 - Each component contains requirements and dependencies on other requirements

CC Assurance Requirements

- Similar class, family, component taxonomy
- Eight product oriented assurance classes
 - ACM – Configuration Management
 - ADO – Delivery and Operation
 - ADV – Development
 - AGD – Guidance Documentation
 - ALC – Life Cycle
 - ATE – Tests
 - AVA – Vulnerability Analysis
 - AMA – Maintenance of Assurance

Evaluation Assurance Levels

- 7 fixed EALs
 - EAL1 – Functionality Tested
 - EAL2 – Structurally Tested
 - EAL3 – Methodically tested and checked
 - Analogous to C2
 - EAL4 – Methodically Designed, Tested, and Reviewed
 - EAL5 – Semiformally Designed and Tested
 - EAL6 – Semiformally Verified Design and Tested
 - EAL7 – Formally Verified Design and Tested

CC Evaluation Process in US

- NIST provides accreditation of third party evaluation labs
 - Vendor pays lab
 - Lab works with oversight board
- Evaluate both PP's and Products
- List of evaluated products
 - <http://www.commoncriteriaportal.org/products.htm>

Certifying Process

- Gain assurance from knowledge of developers process
 - ISO 9000
 - SEI's Capability Maturity Model(CMM)
 - System Security Engineering Capability Maturity Model (SSE-CMM)
 - <http://www.sse-cmm.org>

System Security Engineering Capability Maturity Model

- SSE-CMM - <http://www.sse-cmm.org>
 - Based on SEI's SE-CMM
- Divide software development into process areas (which are further divided into processes)
 - E.g., Assess Threat, Coordinate Security, Assess impact
- Plus some process areas from base SE-CMM
 - E.g., Ensure Quality, Plan Technical Effort

Capability Maturity Levels

- An organization is evaluated at a maturity level for these process areas and processes
 1. Performed informally
 2. Planned and tracked
 3. Well-defined
 4. Quantitatively controlled
 5. Continuously improving

Key Points

- Evaluation for the benefit of the customer
- Product Evaluations
 - Functional Requirements
 - Assurance Requirements
- Process Evaluation