Lecture 26

- Evaluating systems
  - TCSEC (Orange Book)
  - FIPS 140-2
  - Common Criteria
  - SSE-CMM

Assurance Requirements

- Configuration management requirements (B2 up)
  - Identify configuration items, consistent mappings among documentation and code, tools for generating TCB
- System architecture requirements
  - Modularity, minimize complexity, etc.
  - TCB full reference validation mechanism at B3
- Trusted distribution requirement (A1)
  - Address integrity of mapping between masters and on-site versions
  - Address acceptance procedures

Assurance Requirements

- Design specification, verification requirements
  - B1: informal security policy model shown to be consistent with its axioms
  - B2: formal security policy model proven to be consistent with its axioms, descriptive top-level specification (DTLS)
  - B3: DTLS shown to be consistent with security policy model
  - A1: formal top-level specification (FTLS) shown consistent with security policy model using approved formal methods; mapping between FTLS, source code

Assurance Requirements

- Testing requirements
  - Address conformance with claims, resistance to penetration, correction of flaws
  - Requires searching for covert channels for some classes
- Product documentation requirements
  - Security Features User's Guide describes uses, interactions of protection mechanisms
  - Trusted Facility Manual describes requirements for running system securely
- Other documentation: test, design docs

Evaluation Classes A and B

A1 *Verified protection*; significant use of formal methods; trusted distribution; code, FTLS correspondence

B3 *Security domains*; full reference validation mechanism; increases trusted path requirements, constrains code development; more DTLS requirements; documentation

B2 *Structured protection*; formal security policy model; MAC for all objects, labeling; trusted path; least privilege; covert channel analysis, configuration management

B1 *Labeled security protection*; informal security policy model; MAC for some objects; labeling; more stringent security testing

Evaluation Classes C and D

C2 *Controlled access protection*; object reuse, auditing, more stringent security testing

C1 *Discretionary protection*; minimal functional, assurance requirements; I&A controls; DAC

D Did not meet requirements of any other class

Evaluation Process

- Run by government, no fee to vendor
- 3 stages
  - Application: request for evaluation
    - May be denied if gov't didn't need product
  - Preliminary technical review
    - Discussion of evaluation process, schedules, development process, technical content, etc.
    - Determined schedule for evaluation
  - Evaluation phase

Evaluation Phase

- 3 parts; results of each presented to technical review board composed of senior evaluators *not* on evaluating team; must approve that part before moving on to next part
  - Design analysis: review design based on documentation provided; developed initial product assessment report
    - Source code not reviewed
  - Test analysis: vendor's, evaluators' tests
  - Final evaluation report
- Once approved, all items closed, rating given

RAMP

- Ratings Maintenance Program goal: maintain assurance for new version of evaluated product
- Vendor would update assurance evidence
- Technical review board reviewed vendor's report and, on approval, assigned evaluation rating to new version of product
- Note: major changes (structural, addition of some new functions) could be rejected here and a full new evaluation required

Impact

- New approach to evaluating security
  - Based on analyzing design, implementation, documentation, procedures
  - Introduced evaluation classes, assurance requirements, assurance-based evaluation
  - High technical standards for evaluation
  - Technical depth in evaluation procedures
- Some problems
  - Evaluation process difficult, lacking in resources
  - Mixed assurance, functionality together
  - Evaluations only recognized in US

Scope Limitations

- Written for operating systems
  - NCSC introduced "interpretations" for other things such as networks (*Trusted Network Interpretation*, the Red Book), databases (*Trusted Database Interpretation*, the Purple or Lavender Book)
- Focuses on needs of US government
  - Most commercial firms do not need MAC
- Does not address integrity or availability
  - Critical to commercial firms

Process Limitations

- Criteria creep (expansion of requirements defining classes)
  - Criteria interpreted for specific product types
  - Sometimes strengthened basic requirements over time
  - Good for community (learned more about security), but inconsistent over time
- Length of time of evaluation
  - Misunderstanding depth of evaluation
  - Management practices of evaluation
  - As was free, sometimes lacking in motivation

Contributions

- Heightened awareness in commercial sector to computer security needs
- Commercial firms could not use it for their products
  - Did not cover networks, applications
  - Led to wave of new approaches to evaluation
  - Some commercial firms began offering certifications
- Basis for several other schemes, such as Federal Criteria, Common Criteria

FIPS 140: 1994–Present

- Evaluation standard for cryptographic modules (implementing cryptographic logic or processes)
  - Established by US government agencies and Canadian Security Establishment
- Updated in 2001 to address changes in process and technology
  - Officially, FIPS 140-2
- Evaluates only crypto modules
  - If software, processor executing it also included, as is operating system

Requirements

- Four increasing levels of security
- FIPS 140-1 covers basic design, documentation, roles, cryptographic key management, testing, physical security (from electromagnetic interference), etc.
- FIPS 140-2 covers specification, ports and interfaces; finite state model; physical security; mitigation of other attacks; etc.

Security Level 1

- Encryption algorithm must be FIPS-approved algorithm
- Software, firmware components may be executed on general-purpose system using unevaluated OS
- No physical security beyond use of production-grade equipment required

Security Level 2

- More physical security
  - Tamper-proof coatings or seals or pick-resistent locks
- Role-based authentication
  - Module must authenticate that operator is authorized to assume specific role and perform specific services
- Software, firmware components may be executed on multiuser system with OS evaluated at EAL2 or better under Common Criteria
  - Must use one of specified set of protection profiles

Security Level 3

- Enhanced physical security
  - Enough to prevent intruders from accessing critical security parameters within module
- Identity-based authentication
- Strong requirements for reading, altering critical security parameters
- Software, firmware components require OS to have EAL3 evaluation, trusted path, informal security policy model
  - Can use equivalent evaluated trusted OS instead

Security Level 4

- "Envelope of protection" around module that detects, responds to all unauthorized attempts at physical access
  - Includes protection against environmental conditions or fluctuations outside module's range of voltage, temperatures
- Software, firmware components require OS meet functional requirements for Security Level 3, and assurance requirements for EAL4
  - Equivalent trusted operating system may be used

Impact

- By 2002, 164 modules, 332 algorithms tested
  - About 50% of modules had security flaws
  - More than 95% of modules had documentation errors
  - About 25% of algorithms had security flaws
  - More than 65% had documentation errors
- Program greatly improved quality, security of cryptographic modules

Common Criteria: 1998–Present

- Began in 1998 with signing of Common Criteria Recognition Agreement with 5 signers
  - US, UK, Canada, France, Germany
- As of May 2002, 10 more signers
  - Australia, Finland, Greece, Israel, Italy, Netherlands, New Zealand, Norway, Spain, Sweden; India, Japan, Russia, South Korea developing appropriate schemes
- Standard 15408 of International Standards Organization
- *De facto* US security evaluation standard

Evaluation Methodology

- CC documents
  - Overview of methodology, functional requirements, assurance requirements
- CC Evaluation Methodology (CEM)
  - Detailed guidelines for evaluation at each EAL; currently only EAL1–EAL4 defined
- Evaluation Scheme or National Scheme
  - Country-specific infrastructures implementing CEM
  - In US, it's CC Evaluation and Validation Scheme; NIST accredits commercial labs to do evaluations

CC Terms

- *Target of Evaluation* (TOE): system or product being evaluated
- *TOE Security Policy* (TSP): set of rules regulating how assets managed, protected, distributed within TOE
- *TOE Security Functions* (TSF): set consisting of all hardware, software, firmware of TOE that must be relied on for correct enforcement of TSP
  - Generalization of TCB

Protection Profiles

- *CC Protection Profile* (PP): implementation-independent set of security requirements for category of products or systems meeting specific consumer needs
  - Includes functional requirements
    - Chosen from CC functional requirements by PP author
  - Includes assurance requirements
    - Chosen from CC assurance requirements; may be EAL plus others
  - PPs for firewalls, desktop systems, etc.
  - Evolved from ideas in earlier criteria

Form of PP

1. Introduction
   - PP Identification and PP Overview
2. Product or System Family Description
   - Includes description of type, general features of product or system
3. Product or System Family Security Environment
   - Assumptions about intended use, environment of use;
   - Threats to the assets; and
   - Organizational security policies for product or system

Form of PP (*con't*)

4. Security Objectives
   - Trace security objectives for product back to aspects of identified threats and/or policies
   - Trace security objectives for environment back to threats not completely countered by product or systemand/or policies or assumptions not completely met by product or system
5. IT Security Requirements
   - Security functional requirements drawn from CC
   - Security assurance requirements based on an EAL
     - May supply other requirements without reference to CC

Form of PP (*con't*)

6. Rationale
   - Security Objectives Rationale demonstrates stated objectives traceable to all assumptions, threats, policies
   - Security Requirements Rationale demonstrates requirements for product or system and for environment traceable to objectives and meet them
   - This section provides assurance evidence that PP is complete, consistent, technically sound

Security Target

- CC Security Target (ST): set of security requirements and specifications to be used as basis for evaluation of identified product or system
  - Can be derived from a PP, or directly from CC
    - If from PP, ST can reference PP directly
  - Addresses issues for *specific* product or system
    - PP addresses issues for a family of potential products or systems

How It Works

- Find appropriate PP and develop appropriate ST based upon it
  - If no PP, use CC to develop ST directly
- Evaluate ST in accordance with assurance class ASE
  - Validates that ST is complete, consistent, technically sound
- Evaluate product or system against ST

Form of ST

1. Introduction
   - ST Identification, ST Overview
   - CC Conformance Claim
     - Part 2 (or part 3) conformant if all functional requirements are from part 2 (or part 3) of CC
     - Part 2 (or part 3) extended if uses extended requirements defined by vendor as well
2. Product or System Description
   - Describes TOE as aid to understanding its security requirement

Form of ST (*con't*)

3. Product or System Family Security Environment
4. Security Objectives
5. IT Security Requirements
   - These are the same as for a PP

Form of ST (*con't*)

6. Product or System Summary Specification
   - Statement of security functions, description of how these meet functional requirements
   - Statement of assurance measures specifying how assurance requirements met
7. PP Claims
   - Claims of conformance to (one or more) PP requirements

Form of ST (*con't*)

8. Rationale
   - Security objectives rationale demonstrates stated objectives traceable to assumptions, threats, policies
   - Security requirements rationale demonstrates requirements for TOE and environment traceable to objectives and meets them
   - TOE summary specification rationale demonstrates how TOE security functions and assurance measures meet security requirements
   - Rationale for not meeting all dependencies
   - PP claims rationale explains differences between the ST objectives and requirements and those of any PP to which conformance is claimed

CC Requirements

- Both functional and assurance requirements
- EALs built from assurance requirements
- Requirements divided into *classes* based on common purpose
- Classes broken into smaller groups (*families*)
- Families composed of *components*, or sets of definitions of detailed requirements, dependent requirements and definition of hierarchy of requirements

Security Functional Requirements

- 11 classes
  - Including security management and auditing
- Organization of family
  - Management section
  - Audit section
  - Hierarchical issues
  - Nonhierarchical dependencies

The Security Functional Classes

- FAU, security audit
  FCO, communication
- FCS, cryptographic support
- FDP, user data protection
- FIA, identification and authentication
- FMT, security management
- FPR, privacy
- FPT, protection of security functions
- FRU, resource utilization
- FTA, TOE access
- FTP, trusted path

Example

- FAU (security audit) has 6 families
- FAU_SSA: security audit analysis has 4 components
  - FAU_SSA.1: potential violation analysis
    - Depends on FAU_GEN.1
  - FAU_SSA.2: profile-based anomaly detection
    - Subsumes FAU_SSA.1 (so is hierarchical to it)
    - Depends on FIA_UID.1

Assurance Classes

- APE: protection profile evaluation
- ASE: security target evaluation
- AMA: maintenance of assurance
- ACM: configuration management
- ADO: delivery and operation
- ADV: development

Assurance Classes

- AGD: guidance documentation
- ALC: life cycle
- ATE: tests
- AVA: vulnerabilities assessment

Evaluation Assurance Levels

- EAL1: functionally tested
- EAL2: structurally tested
- EAL3: methodically tested and checked
- EAL4: methodically designed, tested, and reviewed
- EAL5: semiformally designed and tested
- EAL6: semiformally verified design and tested
- EAL7: formally verified design and tested

Rough Comparison

TCSEC	CC	FIPS 140-2
D	No equivalent	
No equivalent	EAL1	
C1	EAL2	OS for L2
C2	EAL3	OS for L3
B1	EAL4	OS for L4
B2	EAL5	
B3	EAL6	
A1	EAL7	

Evaluation Process

- Controlled by CC Evaluation Methodology, NIST
  - Performed by NIST-accredited labs
- Vendor selects an accredited lab
  - Lab develops work plan, coordinates with validator, oversight board

Evaluation Process: PP

- Proceeds as in CEM, schedules
- When done, lab presents findings to validating agency, which decides whether to validate the PP evaluation and award the EAL rating

Evaluation Process: Other

- For product or system, vendor must first provide draft of ST
- Then lab co-ordinates with validating schedule
- When done, lab presents findings to validating agency, which decides whether to validate the product or system evaluation and award the EAL rating