CS 392/681 - Computer Security

Nasir Memon - Polytechnic University
Module 10 - Evaluating Systems
Logistics

- Final – December 15th
- Make up class for Review. Monday – 11th? Or Friday 9th?
- Extra HW assigned. Lowest one will be dropped.
- Read Chap 21.
Trusted Systems

- Perfect security is an ultimate but unachievable goal.
- A trusted system is one that has been shown to meet specific security requirements under specific conditions.
- Formal security evaluation techniques facilitate the development of trusted systems.
- Different evaluation techniques and methodologies.
Evaluation methodologies

- Consist of:
  - Requirements defining security functionality of system.
  - Assurance requirements that delineate the steps for establishing system meets its functional requirements.
  - Methodology for determining product meets functional requirements based on analysis assurance evidence.
  - A measure of evaluation of the result (levels of trust).

- A formal evaluation methodology is a technique used to provide measurements of trust based on specific requirements and evidence of assurance.
Trusted System Design Elements

- Principles of the design of secure protection systems
  - Least privilege.
  - Economy of mechanism.
  - Open design.
  - Complete mediation.
  - Permission-based.
  - Separation of privilege.
  - Least common mechanism.
  - Easy to use.
Security Features of Ordinary OS

- User authentication.
- Protection of memory.
- File and I/O devise access control.
- Allocation and access control in general objects.
- Enforcement of sharing.
- Guarantee of fair service.
- Interprocess communication and synchronization.
- Protection of OS data.
Security Features in Trusted OS

- User identification and authentication.
- Mandatory access control
- Discretionary access control
- Object reuse protection
- Complete mediation
- Audit
- Audit log reduction
- Trusted Path
- Intrusion Detection
Security Kernels

A security kernel is a small nucleus or core responsible for enforcing all security mechanisms of OS.

Advantages
- Provides separation
- Unity
- Modifiability
- Compactness
- Verifiability
- Coverage

Disadvantage
- Performance hit
Reference Monitor

- Reference monitor is portion of security kernel the controls access to objects.
- Collection of access controls for devices, files, memory, IPC, etc.
- It should be
  - Tamperproof
  - Always invoked
  - Small so that it can be analyzed for correctness and completeness
- Interacts with other parts of the security kernel like audit process, authentication process etc.
Trusted Computing Base (TCB)

- TCB - The totality of protection mechanisms within an OS including software, hardware and firmware.

- It could include
  - Hardware
  - Some notion of processes
  - Primitive files
  - Protected memory
  - Some IPC
Assurance in Trusted OS

- What does it mean to have confidence in security features of an OS?

- Typical OS Flaws
  - I/O processing
  - Ambiguity in access policy
  - Incomplete mediation
  - Generality
Assurance Methods - Testing

- Testing – Functional, Unit, Integration, System etc.
  - Can demonstrate existence but not absence
  - Hard to get adequate test coverage
  - Black box testing does not observe internal effects
  - White box testing needs code modification!

- Testing – Tiger team
  - Failure to penetrate does not mean there are no holes.
Assurance Methods - Formal Verification

- The OS is reduced to a theorem which is then proven.
- Not very practical in large systems as it needs:
  - Time
  - Complexity
- Theorem provers can assist but still too much human activity needed.
- Not used much
Assurance Methods - Validation

- Validation – Includes verification by one or more of the following
  - Requirement checking
  - Design and code reviews
  - Module and system testing
Assurance Methods - Evaluation

- For non-experts evaluation by independent experts is best.
  - US Orange book evaluation
  - European ITSEC evaluation
  - German Green Book
  - British Criteria
  - ITSEC criteria
  - US Combined Federal Criteria
  - Common Criteria
Formal Evaluation: Why?

- Organizations require assurance
  - Defense
  - Telephone / Utilities
  - “Mission Critical” systems
- Formal verification of entire systems not feasible
- Instead, organizations develop formal evaluation methodologies
  - Products passing evaluation are trusted
  - Required to do business with the organization
Orange Book

- DoD. Late 70’s.
- Four basic divisions A, B, C and D. With A highest degree of security and D lowest (no requirements!).
- Complete set of ratings
  - D, C1, C2, B1, B2, B3 and A1
- See text for detailed description for each level.
Orange Book

- TCSEC Functional Requirements
  - Discretionary access control requirements
  - Object reuse requirements
  - Mandatory access control requirements
  - Label requirements
  - Identification and authentication requirements
  - Trusted path requirements
  - Audit requirements
  - System architecture requirements – tamperproof, process isolation, principle of least privilege, well defined user interface etc.
Orange Book

- Assurance Requirements
  - Configuration management requirements
  - Trusted distribution requirement
  - Design specification and verification requirements
  - Testing requirements
  - Product documentation requirements
Orange Book

- **C1 – Discretionary security protection.**
  - Co-operating users processing data at same level of integrity.
  - DAC provides access control.
  - TCB has to have its own execution domain

- **C2 – Controlled access protection**
  - discretionary control with fine granularity.
  - Audit logs.
  - Objects accessed by TCB should not be accessible to subjects.
  - No object reuse
  - Many commercial systems
B1 – Labeled Security Protection
- Intended for products that handle classified data and enforce mandatory BLP policies.
- Labels for subjects and objects.
- Formal or informal model for security policy required.

B2 – Structured Protection
- Adds requirements to design of system
- MAC governs control to physical devices
- Trusted path for login and authentication
- A formal model for security policy and Descriptive Top Level Specification required.
- Covert channel analysis
- TCB and hardware provide separation mechanisms
- Security testing
B3 – Security Domains

- Highly resistant to penetration
- Tight security management policies and procedures
- Intrusion detection
- Trusted recovery
- Convincing argument needed for consistency between formal model and informal DTLS.
Orange Book

A1 – Verified Design
- A formal model for security policy
- A formal top level specification
- Consistency proofs between model and FTLS
- TCB informally shown to be consistent with FTLS
- A formal analysis of covert channels
- Stringent configuration management and distribution control
How is Evaluation Done?

- Government-sponsored independent evaluators
  - Application: Determine if government cares
- Preliminary Technical Review
  - Discussion of process, schedules
  - Development Process
  - Technical Content, Requirements
- Evaluation Phase
TCSEC:
Evaluation Phase

- Three phases
  - Design analysis
    - Review of design based on documentation
  - Test analysis
  - Final Review

- Trained independent evaluation
  - Results presented to Technical Review Board
  - Must approve before next phase starts

- Ratings Maintenance Program
  - Determines when updates trigger new evaluation
TCSEC: Problems

- Based heavily on confidentiality
- Tied security and functionality
- Base TCSEC geared to operating systems
  - TNI: Trusted Network Interpretation
  - TDI: Trusted Database management System Interpretation
Later Standards

- CTCPEC – Canada
- ITSEC – European Standard
  - Did not define criteria
  - Levels correspond to strength of evaluation
  - Includes code evaluation, development methodology requirements
  - Known vulnerability analysis
- CISR: Commercial outgrowth of TCSEC
- FC: Modernization of TCSEC
- FIPS 140: Cryptographic module validation
- Common Criteria: International Standard
- SSE-CMM: Evaluates developer, not product
ITSEC: Levels

- **E1**: Security target defined, tested
  - Must have informal architecture description
- **E2**: Informal description of design
  - Configuration control, distribution control
- **E3**: Correspondence between code and security target
- **E4**: Formal model of security policy
  - Structured approach to design
  - Design level vulnerability analysis
- **E5**: Correspondence between design and code
  - Source code vulnerability analysis
- **E6**: Formal methods for architecture
  - Formal mapping of design to security policy
  - Mapping of executable to source code
ITSEC Problems:

- No validation that security requirements made sense
  - Product meets goals
  - But does this meet user expectations?
- Inconsistency in evaluations
  - Not as formally defined as TCSEC
FIPS 140

For evaluating cryptographic modules:

- cryptographic algorithms,
- specification, ports and interfaces,
- roles, services and authentication,
- finite state model,
- physical security,
- operational environment,
- key management,
- electromagnetic interference,
- self testing, design assurance, etc.
- Replaced TCSEC, ITSEC
- CC Documents
  - Functional requirements
  - Assurance requirements
  - Evaluation Assurance Levels
- CC Evaluation Methodology
  - Detailed process model for each level
- National Scheme
Common Criteria: Origin

ORANGE BOOK (TCSEC) 1985

UK CONFIDENCE LEVELS 1989

GERMAN CRITERIA 1991

FRENCH CRITERIA

CANADIAN CRITERIA 1993

FEDERAL CRITERIA DRAFT 1993

ITSEC

COMMON CRITERIA V1.0 1996 V2.0 1998
Common Criteria: Protection Profile

Domain-specific set of security requirements
- Narrative Overview
- Domain description
- Security Environment (threats, overall policies)
- Security Objectives: System, Environment
- IT Security Requirements
  - Functional drawn from CC set
  - Assurance level
- Rationale for objectives and requirements
Common Criteria: Security Target

Specific requirements used to evaluate system

- Narrative introduction
- Environment
- Security Objectives
  - How met
- Security Requirements
  - Environment and system
  - Drawn from CC set
- Mapping of Function to Requirements
- Claims of Conformance to Protection Profile
Common Criteria: Functional Requirements

- 362 page document
- 17 Classes
  - Audit, Communication, Cryptography, User data protection, ID/authentication, Management, Privacy, Protection of Security Functions, Resource Utilization, Access, Trusted paths
- Several families per class
- Lattice of components in family
Class Example: Communication

- Non-repudiation of origin
  1. Selective Proof. Capability to request verification of origin
  2. Enforced Proof. All communication includes verifiable origin
Class Example: Privacy

1. 
Pseudonymity

1. TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects]

2. TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects]

3. The TSF shall [selection: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric]

2. Reversible Pseudonymity

1. …

3. Alias Pseudonymity

1. …
Common Criteria: Assurance Requirements

- 216 page document
- 10 Classes
  - Protection Profile Evaluation, Security Target Evaluation
  - Configuration management, Delivery and operation, Development, Guidance, Life cycle, Tests, Vulnerability assessment
  - Maintenance
- Several families per class
- Lattice of components in family
Example: Protection Profile Evaluation

Security environment

- In order to determine whether the IT security requirements in the PP are sufficient, it is important that the security problem to be solved is clearly understood by all parties to the evaluation.

1. Protection Profile, Security environment, Evaluation requirements
   - Dependencies: No dependencies.
   - Developer action elements:
     - The PP developer shall provide a statement of TOE security environment as part of the PP.
   - Content and presentation of evidence elements:
     - The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.
     - The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.
   - Evaluator action elements:
     - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
     - The evaluator shall confirm that the statement of TOE security environment is coherent and internally consistent.

Class APE: Protection Profile evaluation

APE_DES: Protection Profile, TOE description

APE_ENV: Protection Profile, Security environment

APE_INT: Protection Profile, PP introduction

APE_OBJ: Protection Profile, Security objectives

APE_REQ: Protection Profile, IT security requirements

APE_SRE: Protection Profile, Explicitly stated IT security requirements
Example:
Delivery and Operation

Class ADO: Delivery and operation

ADO_DEL Delivery

ADO_IGS Installation, generation and start-up

Installation, generation and start-up
A. Installation, generation, and start-up procedures
   - Dependencies: AGD_ADM.1 Administrator guidance
B. Developer action elements:
   - The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
C. Content and presentation of evidence elements:
   - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.
D. Evaluator action elements:
   - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
   - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Generation Log
Common Criteria:
Evaluation Assurance Levels

1. Functionally tested
2. Structurally tested
3. Methodically tested and checked
4. Methodically designed, tested, and reviewed
5. Semiformally designed and tested
6. Semiformally verified design and tested
7. Formally verified design and tested
Common Criteria: Evaluation Process

- National Authority authorizes evaluators
  - U.S.: NIST accredits commercial organizations
  - Fee charged for evaluation
- Team of four to six evaluators
  - Develop work plan and clear with NIST
  - Evaluate Protection Profile first
  - If successful, can evaluate Security Target
Common Criteria: Status

- About 80 registered products
  - Only one at level 5 (Java Smart Card)
  - Several OS at 4
  - Likely many more not registered
- New versions appearing on regular basis