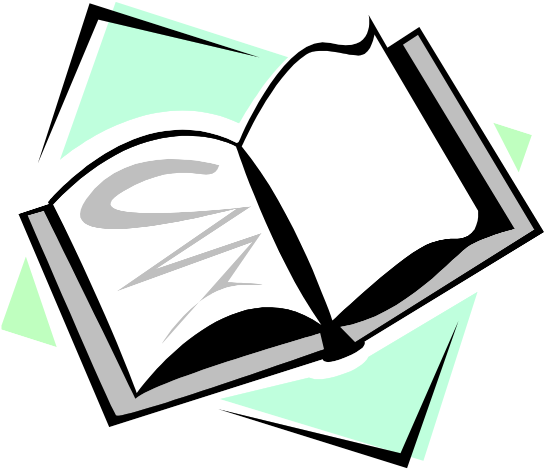
Information Security
CS 526

Topic 20: TCSEC and Common Criteria

Related Readings for This Lecture

- Wikipedia
  - Trusted computing base
  - TCSEC
  - Common Criteria,
  - Evaluation Assurance Level



Terminology: Trusted Computing Base (TCB)

- The set of all hardware, software and procedural components that enforce the security policy.
  - In order to break security, an attacker must subvert one or more of them.
  - The smaller the TCB, the more secure a system is.
- What consists of the conceptual Trusted Computing Based in a Unix/Linux system?
  - hardware, kernel, system binaries, system configuration files, setuid root programs, etc.

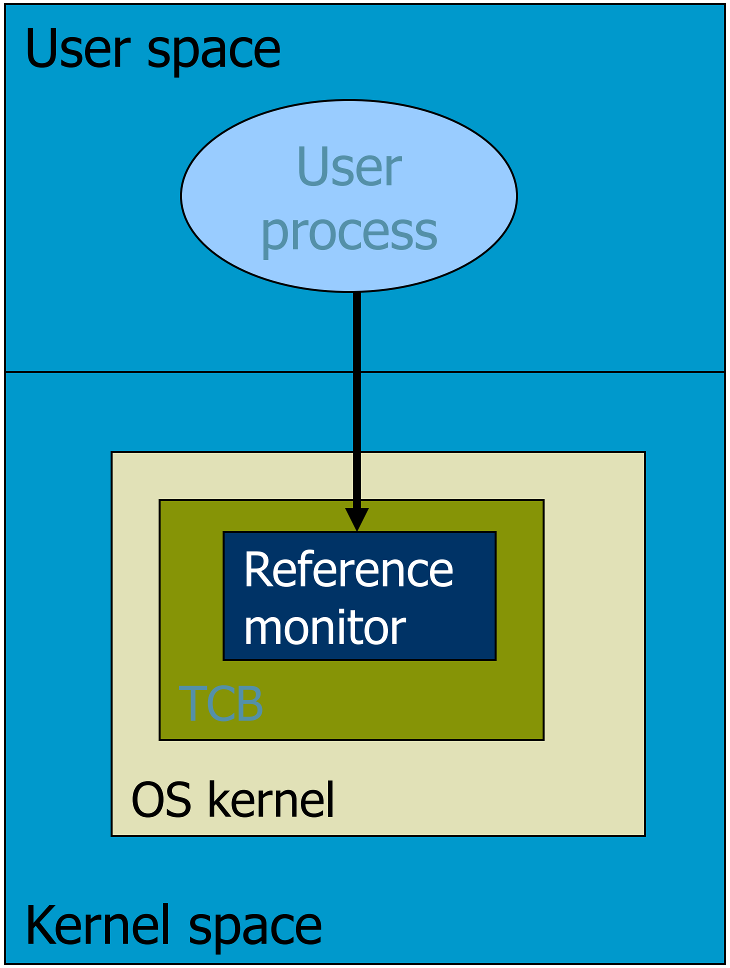
One approach to improve security is to reduce the size of TCB, i.e., reduce what one relies on for security.

Assurance

- Assurance: “estimate of the likelihood that a system will not fail in some particular way”
- Based on factors such as
  - Software architecture
    - E.g., kernelized design,
  - Development process
  - Who developed it
  - Technical assessment

Kernelized Design

- Trusted Computing Base
  - Hardware and software for enforcing security rules
- Reference monitor
  - Part of TCB
  - All system calls go through reference monitor for security checking
  - Most OS not designed this way



Reference Monitor

- Three required properties for reference monitors in "trusted systems"
  - tamper-proof
  - non-bypassable (complete mediation)
  - small enough to be analyzable

Assurance Criteria

- Criteria are specified to enable evaluation
- Originally motivated by military applications, but now is much wider
- Examples
  - Orange Book (Trusted Computer System Evaluation Criteria)
  - Common Criteria

TCSEC: 1983–1999

- Trusted Computer System Evaluation Criteria
  - Also known as the Orange Book
  - Series that expanded on Orange Book in specific areas was called *Rainbow Series*
  - Developed by National Computer Security Center, US Dept. of Defense

- Heavily influenced by Bell-LaPadula model and reference monitor concept

- Emphasizes confidentiality

Evaluation Classes C and D

Division D: Minimal Protection

D Did not meet requirements of any other class

Division C: Discretionary Protection

C1 *Discretionary protection*; DAC, Identification and Authentication, TCB should be protected from external tampering, …

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

Division B: Mandatory Protection

B1 *Labeled security protection*; informal security policy model; MAC for named objects; label exported objects; more stringent security testing

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

B3 *Security domains*; satisfies three reference monitor requirements; system recovery procedures; constrains code development; more documentation requirements

Division A: Verification Protection

A1 *Verified design*;

functionally equivalent to B3, but require the use of formal methods for assurance; trusted distribution; code, formal top-level specification (FTLS) correspondence

Requirement for Verified Design in A1

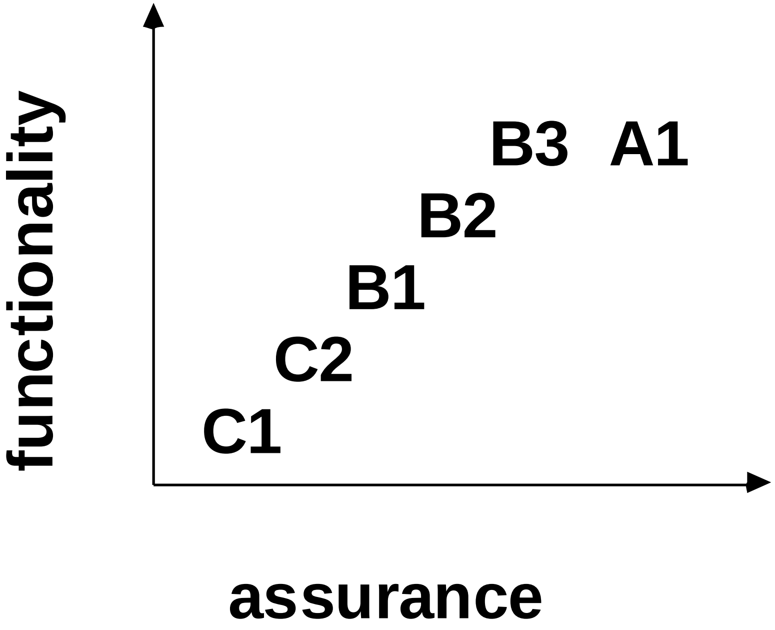
- A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent and is sufficient to support the security policy.
- An formal top-level specification (FTLS) must be produced .
- The FTLS of the TCB must be shown to be consistent with the model by formal techniques where possible (i.e., where verification tools exist) and informal ones otherwise.
- The TCB implementation (i.e., in hardware, firmware, and software) must be informally shown to be consistent with the FTLS.
- Formal analysis techniques must be used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels.

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 BLP
  - Most commercial firms do not need MAC
- Does not address data integrity or availability
  - Critical to commercial firms
- Combine functionality and assurance in a single linear scale

FUNCTIONALITY VS ASSURANCE

- functionality is multi-dimensional
- assurance has a linear progression



Common Criteria: 1998–Present

- An international standard (ISO/IEC 15408)
- 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, replaces TCSEC

Sample Products Evaluated

VMware® ESXi Server 3.5 and VirtualCenter 2.5	EAL4+	24-FEB-10
Microsoft Windows Mobile 6.5	EAL4+	09-FEB-10
Apple Mac OS X 10.6	EAL3+	08-JAN-10
Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers	EAL4+	23-DEC-09
Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition	EAL4+ ALC_FLR.3	31-AUG-09
Oracle Enterprise Linux Version 5 Update 1	EAL4+ ALC_FLR.3	15-OCT-08
Green Hills Software INTEGRITY-178B Separation Kernel, comprising: INTEGRITY-178B Real Time Operating System (RTOS),	EAL6+	01-SEP-08

Criteria

Common Criteria

- Does not provide one list of security features
- Describes a framework where security requirements can be specified, claimed, and evaluated
- Key concepts
  - **Target Of Evaluation (TOE)**: the product or system that is the subject of the evaluation.
  - **Protection Profile (PP)**: a document that identifies security requirements relevant to a user community for a particular purpose.
  - **Security Target (ST)**: a document that identifies the security properties one wants to evaluate against
  - **Evaluation Assurance Level (EAL)** - a numerical rating (1-7) reflecting the assurance requirements fulfilled during the evaluation.

CC Functional Requirements

- Contains 11 classes of functional requirements
  - Each contains one or more families
  - Elaborate naming and numbering scheme
- Classes: Security Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of Security Functions, Resource Utilization, TOE Access, Trusted Path
- Families of Identification and Authentication
  - Authentication Failures, User Attribute Definition, Specification of Secrets, User Authentication, User Identification, and User/Subject Binding

CC Assurance Requirements

- Ten security assurance classes
- Classes:
  - Protection Profile Evaluation
  - Security Target Evaluation
  - Configuration Management
  - Delivery and Operation
  - Development
  - Guidance Documentation
  - Life Cycle
  - Tests
  - Vulnerabilities Assessment
  - Maintenance of Assurance

Protection Profiles (PP)

- "A CC protection profile (PP) is an implementation-independent set of security requirements for a category of products or systems that meet specific consumer needs"
  - Subject to review and certified
- Requirements
  - Functional
  - Assurance
  - EAL

Protection Profiles

- Example: Controlled Access PP (CAPP_V1.d)
  - Security functional requirements
    - Authentication, User Data Protection, Prevent Audit Loss
  - Security assurance requirements
    - Security testing, Admin guidance, Life-cycle support, …
  - Assumes non-hostile and well-managed users
  - Does not consider malicious system developers

Security Targets (ST)

- “A security target (ST) is a set of security requirements and specifications to be used for evaluation of an identified product or system”
- Can be based on a PP or directly taking components from CC
- Describes specific security functions and mechanisms

Evaluation Assurance Levels 1 – 4

EAL 1: Functionally Tested

- Review of functional and interface specifications
- Some independent testing

EAL 2: Structurally Tested

- Analysis of security functions, incl. high-level design
- Independent testing, review of developer testing

EAL 3: Methodically Tested and Checked

- More testing, Some dev. environment controls;

EAL 4: Methodically Designed, Tested, Reviewed

- Requires more design description, improved confidence that TOE will not be tampered

Evaluation Assurance Levels 5 – 7

EAL 5: Semiformally Designed and Tested

- Formal model, modular design
- Vulnerability search, covert channel analysis

EAL 6: Semiformally Verified Design and Tested

- Structured development process

EAL 7: Formally Verified Design and Tested

- Formal presentation of functional specification
- Product or system design must be simple
- Independent confirmation of developer tests

Example: Windows Vista, Server 2008, EAL 4+

- Level EAL 4 + Flaw Remediation
  - "EAL 4 … represents the highest level at which products not built specifically to meet the requirements of EAL 5-7 ought to be evaluated."

    (EAL 5-7 requires more stringent design and development procedures …)
  - Flaw Remediation: the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to customers.
- Catch:
  - Evaluation based on specific configurations specified by the vendor in which the vendor can make certain assumptions about the operating environment and the strength of threats, if any, faced by the product in that environment.

Implications of EALs

- A higher EAL means nothing more, or less, than that the evaluation completed a more stringent set of quality assurance requirements.
- It is often assumed that a system that achieves a higher EAL will provide its security features more reliably, but there is little or no published evidence to support that assumption.
- Anything below EAL4 doesn’t mean much
- Anything above EAL4 is very difficult for complex systems such as OS
- Evaluation is done for environments assumed by vendors

Criticism of CC:

- Evaluation is a costly process (often measured in hundreds of thousands of US dollars) -- and the vendor's return on that investment is not necessarily a more secure product
- Evaluation focuses primarily on assessing the evaluation documentation, not the product itself
- The effort and time to prepare evaluation-related documentation is so cumbersome that by the time the work is completed, the product in evaluation is generally obsolete
- Industry input, including that from organizations such as the Common Criteria Vendor's Forum, generally has little impact on the process as a whole

Coming Attractions …

- Privacy and Anonymity