

CS574

Computer Security

San Diego State University

Spring 2008

Lecture #16

Today's Structure

- Administrivia
- Recent News
- Questions
- Lecture

Administrivia

- Assignment #1
 - Partial Credit “make up” - resubmit friday.
- Assignment #2
 - One Approval So Far
- Midterm #2

Recent News

- Easter Eggs
- PKI (TRUSTe)
- Sun & NSA
- IRS security review
- Keystroke Timings
- Mission Patches

Questions?

Lecture

Evaluation

- End-users are the ones who need assurance.
- End-users are generally not qualified to make such assessments:
 - no time
 - no money
 - no training / skill
- Vendors, naturally, will say “Just Trust Us”.

Evaluation

- Need independent, trustable, objective third party to perform an evaluation.
- Need a rating scheme so an end-user can compare systems in a meaningful way.
- Need a standard approach to evaluation.

Evaluation

- Trusted Computer Security Evaluation Criteria (TCSEC) – “Orange Book”
- German Green Book
- British Criteria
- ITSEC
- Common Criteria
- FIPS

TCSEC

- The DoD as a customer was interested in a standard evaluation system.
- National Computer Security Center [NCSC] – part of NSA – guided and sanctioned the standard.
- TCSEC was published in 1985.

TCSEC Purpose

- Provide a standard as to what security features vendors should plan for new products or build into current products.
- Provide the DoD with an evaluation metric.
- Provide the basis for specifying security requirements for purchases.

TCSEC Requirements

- Security Policy
- Marking (labels)
- Identification (authentication)
- Accountability (auditing)
- Assurance
- Continuous Protection

TCSEC

- Defined four divisions: D, C, B, and A
- Each division has a checklist:
 - features
 - development processes
 - requirements
- Points fall into fairly distinct categories:
 - capabilities
 - assurances
 - documentation

TCSEC

- Divisions are ordered so that each is better than the lower one(s).
- Should be able to match environment to some set of requirements that could be used to identify the appropriate division.
- Division further subdivided, so classes are:
D C1 C2 B1 B3 B3 A1

TCSEC

Division D

- “Minimal Protection”
- No subdivisions.
- Used for those systems that have been evaluated but failed to achieve a higher rank.
- Not the same as “unrated”.
- A very expensive way to get a zero score.

TCSEC

Division C

- “Discretionary Protection”
- Two Subdivisions:
 - C1 – “Discretionary Security Protection”
 - C2 – “Controlled Access Protection”
- Documentation
 - User’s Guide to Security Features
 - Trusted Facility Manual
 - Test Documentation
 - Design Documentation

TCSEC

Class C1

- “Discretionary Security Protection”
- DAC
- Identification & Authentication
- TCB keeps a domain free from external influence and tampering for itself.
- Can periodically validate correct operation & lack of tampering of the TCB.

TCSEC

Class C2

- “Controlled Access Protection”
- Finer granularity for access controls.
- Protect against object reuse.
- Auditing capabilities.
- Many operating systems managed to get this.

TCSEC

Division B

- “Mandatory Access Control”
- Three subdivisions:
 - BI – “Labeled Security Protection”
 - B2 – “Structured Protection”
 - B3 – “Security Domains”
- Sensitivity labels for *at least* the important data structures / objects.
- At least 16 levels and 64 compartments.

TCSEC

Class B1

- “Labeled Security Protection”
- Nondiscretionary (i.e., mandatory) access control.
- Each controlled subject and object have a security level. (Not every object needs to be controlled.)
- Controlled objects must be individually labeled.

TCSEC

Class B1

- Must use Bell-LaPadula model + DAC.
- Requires some sort of reference monitor.
- Every access to a controlled object must be audited.

TCSEC

Class B2

- “Structured Protection”
- The TCB must notify the user of changes in security level, and allow the user to query for their current security level.
- Devices get (MAC) labels.
- Adds in some design constraints.

TCSEC

Class B2

- TCB based on a formal security policy model.
- More testing, review, and validation needed.
- OS design constraints:
 - incorporate security
 - structured / modular kernel
 - least privilege in OS

TCSEC

Class B2

- Developed using configuration management.
- Requires covert channel analysis.
- Requires trusted path for identification and authentication.
- Security kernel helpful (but not quite mandatory).

TCSEC

Class B3

- “Security Domains”
- Trusted Recovery (a system failure/crash won't result in a compromise).
- Security administrator role required.
- TCB must exclude code not *essential* to security policy enforcement (for verification).
- Audit systems signals security-related events.

TCSEC

Class B3

- Additional design constraints
 - layering
 - abstraction
 - information hiding
- High-level design coupled with a “convincing” argument that the system implements that design.

TCSEC

Division A

- “Verified Protection”
- One subdivision:
AI - “Verified Design”
- Introduces formal security verification methods.
- Requires *extensive* documentation.

TCSEC

Class A1

- “Verified Design”
- No new features beyond B3.
- More stringent configuration management.
- Trusted distribution added to the life cycle.
- Formal top-level model of protection system and mathematical proof of consistency.

TCSEC

Class A1

- Formal top-level specification of the protection system.
- Demonstration that the specification corresponds to the formal model.
- Demonstration that implementation is consistent with the specification.
- Formal analysis to identify and analyze covert channels.

TCSEC

Beyond AI

- Demonstrate self-protection.
- Automatic test-case generation.
- Verification down to the source-code level.
- Designed in a trusted environment using only cleared people.

TCSEC Cost

- In 1988, cost about \$1.5 million to get an A1 rating.
- It took ~15 people at NCSC and 1 to 30 people from the vendor to get a rating.
- Evaluation took 18-24 months.

Orange Book

What It Got Wrong

- Defines only one metric (coupling between features and assurance – e.g., no high assurance + low security divisions).
- Doesn't cover removable media or networks.
- Tied to specific models of hardware.
- Evaluation is expensive and slow.
- Doesn't map well to commercial use.

Orange Book

Other Problems

- Heavy on the structured-programming models.
- Considered too prescriptive.
- Enforced a development model.
- Government mandate not backed up by purchasing resulting system.

Orange Book

What It Got Right

- Was the first one-stop reference for *real* computer security.
- Established framework and terminology.
- Set agenda for future efforts.
- Is still useful, despite being 'retired' in 2000.

Post Orange Book

- TCSEC was extended and explained; result was the “rainbow series”.
- Other nations wanted their own criteria:
 - German Green Book
 - British Criteria
 - ITSEC (Europe)
- Finally, the “Common Criteria”

German Green Book

- Defined 8 basic security functions.
- Defined 10 evaluation classes.
- Defined 8 quality/effectiveness levels.
- Gives 80 possible evaluation results.
- Introduced commercial evaluation facilities.

German Green Book

Security Functions

- Identification & Authentication
- Administration of rights
- Verification of rights (mediation)
- Auditing
- Object Reuse

German Green Book

Security Functions

- Error Recovery
- Continuity of Service (availability & tolerances)
- Data Communication Security
 - peer entity authentication
 - control access to communication resources
 - data confidentiality & integrity
 - data origin authentication
 - non-repudiation

British Criteria

- Uses a “claim language” for generality.
- Vendors assert qualities, evaluators verify claims.
- Six levels of assurance correspond to TCSEC, but no direct correlation to TCSEC.
- Expected “popular functions” to be bundled together (eventually).

ITSEC

- “Information Technology Security Evaluation Criteria”
- Blended
 - German functionality levels
 - British flexibility
 - American assurance levels
- A vendor/sponsor defines a Target of Evaluation (or TOE) that an evaluator evaluates.

Common Criteria

- Version 1.0 published in 1996.
- Leverages TCSEC, Federal Criteria, ITSEC, etc.
- Defines security targets and protection profiles.
- Has separate functionality and assurance classes.
- Predefines “packages” of features and assurance.
- Designed to transition from TCSEC easily.
- Seven Evaluation Assurance Levels (EALs).

Common Criteria

- Classes have families of function/assurance needs.
- Families have components.
- Components are combined into packages.
- Packages are combined into assertions.

Common Criteria Classes

- Eleven classes of Security Functional Requirements.
- Ten classes of Assurance Requirements.
- Seven levels of Assurance.

Common Criteria EALs

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

CC / TCSEC Comparison

Common Criteria	TCSEC
–	D
EAL 1	–
EAL 2	C1
EAL 3	C2
EAL 4	B1
EAL 5	B2
EAL 6	B3
EAL 7	A1

CC / TCSEC Comparison

- Common Criteria is more flexible.
- Common Criteria is more complicated.
- Common Criteria is probably more useful.
- Common Criteria used for more than just OSes.

FIPS

- Why ignore the golden hammer of cryptography?
- Various FIPS standards address cryptographic security.
- Managed by NIST (National Institute for Standards and Technology), so US-specific.
- NIST sanctions laboratories to perform evaluations.
- Catch-all standard for “secure cryptographic modules” is FIPS-140

FIPS-140

- Four levels of validation: Level 1, 2, 3, 4
- Level 1 is lowest, level 4 is most stringent.
- Various rules depending on device type
single-chip/multi-chip
standalone/embedded
etc.

Evaluation

Desirable Features

- Extensibility
Can we extend the evaluation as the product is enhanced?
- Granularity
Is the evaluation at the right level of detail for the product?
- Speed
How fast can the evaluation be done?

Evaluation

Desirable Features

- Thoroughness
Does the evaluation cover all relevant aspects of the product?
- Objectivity
Do different evaluators / different evaluations result in the same assurance level?
- Portability
Does the (hardware) platform matter?

Evaluation

Desirable Features

- Consistency
Do similar products get similar assurance ratings?
- Compatibility
Does the product get similar results when evaluated under different criteria?
- Exportability
Will an evaluation under one scheme be accept as meeting at least some of the requirements of another scheme?

End Lecture

Lecture References

- Pfleeger, *Security in Computing*, 3rd & 4th edition
- Bishop, *Introduction to Computer Security*
- *Common Criteria - An Introduction*, Syntegra, Sponsored by CESG/NIST
- *Department of Defense Trusted Computer System Evaluation*, DoD 5200.28-STD
- *The Craft of System Security*, Sean Smith & John Marchesini

Reading

- Prepare for Midterm

Finis