Security Evaluation

- Introduce the major evaluation criteria.
- TCSEC (Orange book)
- ITSEC
- Common Criteria

Purpose of Evaluation

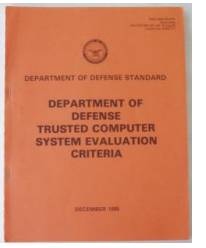
- **Evaluation:** assessing whether a product has the security properties claimed for it.
- **Certification:** assessing whether a product is suitable for a given application.
- **Accreditation:** deciding that a product will be used in a given application.

Who Should Evaluate?

- **Alternative 1:** One government body (Orange Book)
  - Fair, since the same body does all evaluations
  - Not all products are accepted for evaluation
  - Slow, for the same reason
- **Alternative 2:** Private evaluators
  - More difficult to make it fair: Will evaluations be consistent?
    - **Repeatability**: re-evaluation by the same team
    - **Reproducability**: re-evaluation by a different team
    - Formulation of criteria is important so there is no room for interpretation
  - More evaluators → faster evaluation
- We have to make sure that no commercial interests affect the result
  - Someone might pay for an evaluation of their own product (ITSEC, Common Criteria)
  - Also possible to have the service for free (Orange book)

TCSEC (Orange book)

- First work towards security evaluation guidelines, US 1967.
- US Department of Defense
- Orange book 1983 and 1985
- Evaluating security products (operating systems).
- Evaluation examines the TCB.

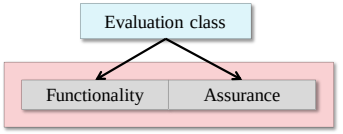


Ideas

Orange Book motivation

- Help users/organizations
  - To know how much they can trust a system
  - To specify security requirements when acquiring computer security system
- Help manufacturers
  - to construct secure systems

- Uses **evaluation classes** that *combines*
  - Security features (functionality)
  - Assurance requirements



Identifying an Evaluation Class

1. **Security policy** – MAC and/or DAC
2. **Marking of objects** – security labels
3. **Identification and authentication**
4. **Accountability** – security logs
5. **Assurance** – design methods and security architecture
6. **Documentation** – user guides and design documentation
7. **Continuous protection** – possibilities to tamper with security system

- The vendor selects an evaluation class to pursue based on above features

Security Divisions and Classes

- 4 security divisions, 7 security classes
- D – Minimal protection
- C – Discretionary protection
- B – Mandatory protection
- A – Verified protection

- A higher class automatically require all requirements of lower classes

Classes

- D – Minimal protection
  - Submitted but does not meet requirements of any class
- C1 – Discretionary security protection
  - Discretionary access control for users and/or groups, co-operating users process data at the same level, identification & authentication, user's guide, test documentation and design documentation have to be provided. Suitable for "friendly" environment
- C2 – Controlled access protection
  - Discretionary access control for individual users, no object reuse, audit needed
  - Common for commercial applications

Classes

- B1 – Labelled security protection
  - Mandatory access control (for some objects), labels constructed from levels and categories, documentation and source code analyzed
- B2 – Structured protection
  - Mandatory access control (for all objects), trusted path for login, formal model of security policy
- B3 – Security domains
  - Security administrator, automatic warnings from audit
- A1 – Verified design
  - Formal models and formal analysis. Stringent configuration management and distribution control.

Limitations of Orange Book

- Only recognized in the US
- Evaluations in other countries not valid in the US
- Focused on operating systems
  - Versions for networks and databases were developed but not much used
- Mandatory access control rarely used in commercial operating systems
- Integrity and availability not addressed
- Criteria creep – criteria had to be interpreted to fit the products
  - Criteria became more and more specific
  - C2 year X became more difficult to get than C2 year X-1
- Very slow
  - It was for free

ITSEC

- Information Technology Security Evaluation Criteria
- Cooperation between European countries
- 1990, Recommendation in EU 1995
- Orange book too rigid
- ITSEC removes link between functionality and assurance
- Applies to both products and systems

ITSEC

- **Target of evaluation** (TOE)
- **Security target** specifies all aspects relevant for evaluation and describes **security functions**
- **Security functions** specified individually or by predefined **functionality class**
- **Evaluation levels** determine level of confidence and correctness
  - Each level specify items to be delivered to evaluator, E0 – E6
  - Close cooperation between sponsor/developer and evaluator.

Common Criteria (CC)

Motivation: A common standard is more commercially attractive

Derived from existing standards
- ITSEC (Europe, 1991)
- TCSEC (Orange book, US Department of Defense, 1985)
- CTCPEC (Canada)
- Federal Criteria (NIST & NSA)

- Common Criteria is also ISO 15408
- Both products and systems can be evaluated
- Started 1998

CC Key Concepts

- A **Protection Profile (PP)** is a document that identifies security requirements relevant to that user. Exist for operating systems, database management systems, firewalls, smart cards etc
- A **Security Target (ST)** is a document that identifies the security capabilities of a particular product. It forms the basis for evaluating that product. An ST may claim conformance to one or more PPs.
- The **Target Of Evaluation (TOE)** is simply the product described in the ST, about which the security claims are made.
- **Security Functional Requirements (SFRs)** are descriptions of individual security functions which may be provided by a product. CC presents a standard catalogue of such functions.
- An **Evaluation Assurance Level (EAL)** is a package of Assurance requirements which covers the complete development of a product, with a given level of strictness. There are 7 levels, EAL1 – EAL7

Evaluation Assurance Levels

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

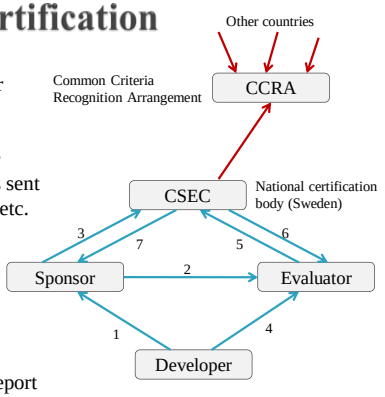
- Higher EAL means more expensive, EAL4 is most common
- EAL5 – EAL7 are only accepted within one country

Other Aspects

- Some public sector costumers require security evaluation
- Popular in smart cards sector
- Criticism:
  - Expensive and driven by government requirements
  - Cost can be 10% - 40% of development cost
  - Time delay
  - Re-evaluating new versions is expensive
  - Only applies to one version and one configuration

Evaluation and Certification

1. Evaluation Agreement. Developer not needed for EAL1.
2. Evaluation order – produce a certification application together
3. Certification order – application is sent
4. Send documentation, source code etc.
5. Evaluation report – Evaluator follows procedures given in Common Criteria in the evaluation process
6. Report is approved after an independent review of the report
7. Send certificate and a certificate report



Does Certified Mean Secure?

- Example
  - Apple Mac OS X 10.6 → EAL 3+
  - Windows Vista Enterprise → EAL 4+
  - Windows Server 2008 → EAL 4+
  - SUSE Linux Enterprise Server → EAL 4+
  - Red Hat Enterprise Linux version 5 → EAL 4+
- All these (and many more) are evaluated using the protection profile (PP) *Controlled Access Protection Profile (CAPP)*
- So what does this profile say?

Does certified mean secure?

From the introduction:

The Common Criteria (CC) Controlled Access Protection Profile, hereafter called CAPP, specifies a set of security functional and assurance requirements for Information Technology (IT) products**. CAPP conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. CAPP-conformant products also provide an audit capability which records the security-relevant events which occur within the system.**

The CAPP provides for a level of protection which is appropriate for an **assumed non-hostile and well managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security.** The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The CAPP does not fully address the threats posed by malicious system development or administrative personnel. CAPP-conformant products are suitable for use in both commercial and government environments.