Security Evaluation -
Common Criteria

Presented by

Erland Jonsson
Department of Computer Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

CERTIFICATION ACCORDING TO A SECURITY STANDARD

- **Evaluation** is assessing whether a product has the *security properties* claimed for it
- **Certification** is the formal assessment of the result of an *evaluation.*
- **Accreditation** is deciding that a (certified) product *may be used* in a given application
- Certification is made wrt to some established standard, such as the CC ("Common Criteria").
- The goal of the certification:
  - assess the trust of the system's correctness. (How secure is it?)
  - assess the quality of the evaluation. (How do we know?)

  Document it!!

EVALUATION STANDARDS

Earlier evaluation criteria:

- TCSEC (Trusted Computer Security Evaluation Criteria)
- ITSEC (Information Technology Security Evaluation Criteria)
- FC (Federal Criteria)
- Canadian, Japanese, etc

Evaluation criteria on the module level:

- In some cases we need to evaluate a specific security module. The FIPS 140-2 is an evaluation standard for cryptographic modules.
- It provides four increasing, qualitative security levels.

COMMON CRITERIA

- The Common Criteria[1] (CC) is aimed to be common to all countries. It defines a security evaluation methodology.
- It became the "official" evaluation standard in the USA in 1998. (TCSEC was discontinued in 2000.)

Central terms:

- Target of Evaluation (TOE):
  An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
- Evaluation Assurance Level (EAL):
  A package consisting of assurance components that represent a point in the predefined assurance scale

[1] Common Criteria for Information Technology Security Evaluation

COMMON CRITERIA

Central terms (cont'd):

- Protection Profile (PP):
  An implementation-independent set of security requirements for a category of TOEs
- Security Target (ST):
  A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
- Security Functional Requirements (SFR):
  The translation of the security objectives for the TOE.
- TOE Security Function (TSF):
  A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the SFR. (cp TCB)

COMMON CRITERIA

The Common Criteria comes in three (plus 1) parts:

1. **Introduction and general model** (79 pages)
   - general concepts, principles and evaluation model
2. **Security functional requirements** (127 pages)
   - describe the desired security behaviour expected of a Target of Evaluation (TOE) in order to meet the security objectives as stated in a Protection Profile (PP) or a Security Target (ST)
3. **Security assurance requirements** (242 pages)**:**
   - defines a scale for measuring assurance - Evaluation Assurance Levels (EALs)
   - defines criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs)

There is also a companion document to the Common Criteria:

4. **Common Methodology** for Information Technology Security Evaluation (**CEM**) (466 pages):

- descibes the minimum actions to be performed by an evaluator in order to conduct a CC evaluation.

CC URL: http://www.commoncriteriaportal.org/

There are three types of evaluation:

1. PP evaluation
- is carried out against evaluation criteria for PPs
- is to demonstrate that that the PP is suitable as a statement of requirements for an evaluatable TOE

2. ST evaluation
- is to demonstrate that the ST properly meets the requirements of the PP

3. TOE evaluation
- is to demonstrate that the TOE meets the requirements contained in the ST

The CC defines three types of requirements constructs:

• package, Protection Profile and Security Target

• a **component**
- describes a specific set of security requirements
- is the smallest selectable set of security requirements

• a **package**
- an intermediate combination of components is termed a package.
- gives a set of functional or assurance requirements that meet a subset of security objectives
- EALs are predefined assurance packages

There are seven predefined levels of assurance (EAL 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

An evaluation may also be carried out against a user-defined level of assurance