Common Criteria (CC) Complete Overview

Yanet Manzano
Florida State University
manzano@cs.fsu.edu

Outline

- CC History
- CC Informally Defined
- CC Goals
- Interested Parties
  - Interested Parties: Details
- CC Part 1
- CC Part 2
  - Functional Requirements
  - Classes of Functional Requirements
- CC Part 3
  - Assurance Requirements
  - Classes of Functional Requirements
  - Protections Profiles
  - Security Targets
  - Levels of Evaluation
- Evaluation Process
CC History

- Developed through a collaboration among national security and standards organizations within:
  - Canada,
  - France,
  - Germany,
  - The Netherlands,
  - The United Kingdom
  - The United States

- As a common standards to replace their existing security evaluation criteria.

CC Informally Defined

- A standard method of expressing requirements
- A catalog of possible security requirements
- A matching set of assurance test procedures
- A standard testing methodology
NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS)

- Established by NIST and NSA under NIAP

- Provides:
  - cost-effective evaluation of IT products performed to consistent standards
  - a wider choice of evaluated products for consumer
  - greater understanding of consumer requirements
  - greater access to markets for developers

Interested Parties

[Diagram showing the relationships between developers, product vendors, accreditors, approvers, consumers, certifiers, evaluators, and Common Criteria]
Interested Parties: Details

<table>
<thead>
<tr>
<th>CONSUMERS</th>
<th>DEVELOPERS</th>
<th>EVALUATORS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part 1: Introduction and General Model</strong></td>
<td>Background info and reference purposes</td>
<td>Background info and Reference for developments of requirements and formulating security specification for TOE</td>
</tr>
<tr>
<td><strong>Part 2: Security Functional Requirements</strong></td>
<td>Guidance and reference when formulating statements of requirements for security functions</td>
<td>Reference when interpreting statements of functional requirements and formulating functional specifications for TOE</td>
</tr>
<tr>
<td><strong>Part 3: Security Assurance Requirements</strong></td>
<td>Guidance when determining required levels of assurance</td>
<td>For reference when interpreting statements of assurance requirements</td>
</tr>
</tbody>
</table>

TOE = Target of Evaluation

CC Part 1

**Part 1: Introduction and General Model**

- Defines general concepts and principles of IT security evaluation
- Presents a general model of evaluation and constructs for:
  - expressing IT security objectives
  - selecting and defining IT security requirements
  - writing high-level specifications for products and systems
Part 2: Security Functional Requirements

- Establishes a set of functional components as a standard way of expressing the functional requirements for TOEs
- Catalogues the set of functional components, families, and classes.

**Functional Requirements:**

- Define security Behavior of the IT product or system
- Implemented requirements become security functions

### Classes of Functional Requirements

<table>
<thead>
<tr>
<th>Class</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU</td>
<td>Audit</td>
</tr>
<tr>
<td>FCO</td>
<td>Communications</td>
</tr>
<tr>
<td>FCS</td>
<td>Cryptographic Support</td>
</tr>
<tr>
<td>FDP</td>
<td>User Data Protection</td>
</tr>
<tr>
<td>FIA</td>
<td>Identification &amp; Authentication</td>
</tr>
<tr>
<td>FMT</td>
<td>Security Management</td>
</tr>
<tr>
<td>FPR</td>
<td>Privacy</td>
</tr>
<tr>
<td>FPT</td>
<td>Protection of TOE Security Functions</td>
</tr>
<tr>
<td>FRU</td>
<td>Resource Utilization</td>
</tr>
<tr>
<td>FTA</td>
<td>TOE Access</td>
</tr>
<tr>
<td>FTP</td>
<td>Trusted Path / Channels</td>
</tr>
</tbody>
</table>
CC Part 3

- **Part 3: Security Assurance Requirements**
  - Defines set of assurance components, families and classes as a standard way of expressing the assurance requirements for TOEs
  - Defines evaluation criteria for PP* and ST`
  - Presents evaluation assurance levels (EAL)
    - CC scale for rating assurance for TOEs

- **Assurance Requirements:**
  - For establishing confidence in security functions
    - Correctness of implementation
    - Effectiveness in satisfying objectives

### Classes of Assurance Requirements

<table>
<thead>
<tr>
<th>Class</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>ADO</td>
<td>Delivery &amp; Operation</td>
</tr>
<tr>
<td>ADV</td>
<td>Development</td>
</tr>
<tr>
<td>AGD</td>
<td>Guidance Documents</td>
</tr>
<tr>
<td>ALC</td>
<td>Life Cycle Support</td>
</tr>
<tr>
<td>ATE</td>
<td>Tests</td>
</tr>
<tr>
<td>AVE</td>
<td>Vulnerability Assessment</td>
</tr>
<tr>
<td>APE</td>
<td>Protection Profile Evaluation</td>
</tr>
<tr>
<td>ASE</td>
<td>Security Target Evaluation</td>
</tr>
<tr>
<td>AMA</td>
<td>Maintenance of Assurance</td>
</tr>
</tbody>
</table>
Protection Profiles (PP)

- An implementation independent statement of security requirements that is shown to address threats that exist in a specified environment
- States general security problem to be solved
- Can be adopted, tailored, or develop for a product of the type it defines
- Developers build specific products to satisfy PPs to:
  - Satisfied customer demand
  - For competitive advantage
  - To define market expectations
- Examples: OS, Database Management Systems, and Firewalls

Protection Profiles: Benefits

- Standard framework for capturing specific policies, regulations, and objectives
- Standard structure for articulating security functional and assurance requirements of solutions (products)

PP Content

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threads
  - Organization Security Policies
- Security Objectives
- Security Requirements
  - Functional Requirements
  - Assurance Requirements
- Rationale
Security Target (ST)

- Tailored for each specific TOE
- Are the basis against which an evaluation is performed

**ST Content**

- Introduction
- TOE Description
- Security Environment
  - Assumptions
  - Threads
  - Organization Security Policies
- Security Objectives
- Security Requirements
  - Functional Requirements
  - Assurance Requirements
- TOE Summary Specification
- PP Claims
- Rationale

Levels of Evaluation

<table>
<thead>
<tr>
<th>EAL</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL1</td>
<td>Functionally Tested</td>
</tr>
<tr>
<td>EAL2</td>
<td>Structurally Tested</td>
</tr>
<tr>
<td>EAL3</td>
<td>Methodically Tested &amp; Checked</td>
</tr>
<tr>
<td>EAL4</td>
<td>Methodically Designed, Tested &amp; Reviewed</td>
</tr>
<tr>
<td>EAL5</td>
<td>Semiformally Designed &amp; Tested</td>
</tr>
<tr>
<td>EAL6</td>
<td>Semiformally Verified Design &amp; Tested</td>
</tr>
<tr>
<td>EAL7</td>
<td>Formally Verified Design &amp; Tested</td>
</tr>
</tbody>
</table>
Evaluation Process

Evaluate PP
→ PP Evaluation Results
→ Catalogue PP
→ Evaluated PP

Evaluate ST
→ ST Evaluation Results

Evaluate TOE
→ TOE Evaluation Results
→ Catalogue Certificates
→ Evaluated TOE