Common Criteria
CC-101
CC Part 2 Basics

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

Outline

- Review
- Definition Review
- CC Part 2 Scope
- Description
- Security Functional Requirements
- Functional Requirements Paradigm
  - TSP = TOE Security Policy
  - SFP = Security Functional Policies
  - SF = Security Function
  - TSF = TOE Security Functions
  - SOF = Strength of Function
Review: CC Parts

- Part 1: Introduction and General Model
- Part 2: Security Functional Requirements
- Part 3: Security Assurance Requirements

CC-101

Previous Presentations:
- CC-101 > Introduction
- CC-101 > CC Part 1
Definition Review (1)

**Target of Evaluation (TOE):** An IT product or system and its associated administrator, and user guidance documentation that is the subject of an evaluation

**Component:** Describe a specific set of security requirements

**Family:** Group of components that share objectives, but may differ in emphasis or rigor

**Class:** Group of families that share a common focus

Definition Review (2)

**Protection Profile (PP):** An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs

**Security Target (ST):** A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

**Functional Requirements:**
- Define security Behavior of the IT product or system
- Implemented requirements become security
Security Functional Components are the basis for the TOE IT security functional requirement, expressed in a PP, or an ST

Describe the desire security behavior expected of a TOE, and are indented to meet the security objectives as stated in a PP or an ST

Establishes a set of functional components as a standard way of expressing the functional requirements for TOEs

Requirements describe security properties that users can detect by:

- Direct interaction with the TOE (e.g. inputs, output) or
- The TOE’s response to stimulus

Catalogues the set of functional components,
Security Functional Requirement (1)

- A set of well understood requirements that can be used to create trusted products or systems reflecting the need of the market
- Presented as the current state of the art in requirement specification and evaluation
- Contains those requirements that are known and agreed to be of value by authors at the time of release
  
  Needs to be maintained as customer needs change

Security Functional Requirements (2)

- Define security behavior of an IT product or system
- Implemented requirements become security functions

Aggregated in 11 functionality classes:

1. Audit
2. Cryptographic Support
3. Communication
4. User Data Protection
5. Identification and Authentication
7. Privacy
8. Protection of the TOE Security Functions
9. Resource Utilization
10. TOE Access
11. Trusted Path/Channel
Functional Requirements Paradigm

1. TOE Evaluation is concerned with ensuring that a defined TOE Security Policy (TSP) is enforced over the TOE Resources

   TOE Security Policy (TSP): Defines the rules by which the TOE governs access to its resources

2. The TOE Security Policy (TSP) is made up of multiple Security Function Policies (SFP)

   Security Function Policies (SFP): Has a scope of control that defines the subject, objects, and operations controlled under it
The Security Function Policies (SFP) is implemented by a Security Function (SF) whose mechanism enforce the policy and provide necessary capabilities.

Security Function (SF): A part(s) of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TOE Security Policy (TSP).

The portions of the TOE that must be relied on for the correct enforcement of the TOE Security Policy (TSP) are collectively referred to as the TOE Security Functions (TSF).

TOE Security Functions (TSF): consist of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement. It may consist of a reference validation mechanism and/or other Security Function (SF) for the operation of the TOE.
### Functional Requirements Paradigm Overview

- **TOE Security Policy (TSP)**
  - are made of multiple
- **Security Function Policies (SFP)**
  - are implemented by
- **Security Function (SF)**
  - can be part of the
- **TOE Security Functions (TSF)**

Includes all TOE parts relied upon for security enforcement.

---

### Strength of Function (SOF) (1)

- TOE may contain security functions that are realized by a probabilistic or permutational mechanism (e.g. a password or hash function)
- Assurance requirements may specify that a minimum strength level, consistent with the security objectives needs to be claimed.
- SOF can be defined on three levels:
  1) SOF-Basic
  2) SOF-Medium
  3) SOF-High
Strength of Function (SOF) (2)

SOF-Basic: provide adequate protection against casual breach of TOE security by attacker with low attack potential

SOF-Medium: provides adequate protection against straightforward or intentional breach of TOE security by attackers with moderate attack potential

SOF-High: provides adequate protection against deliberately planned or organized breach of TOE security by attackers with high attack potential

Future Presentations:
- CC-101 > CC Part 3