Foundations of Computer Security

Lecture 77: The Common Criteria

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

The Common Criteria

The need for secure systems evaluation criteria led numerous countries to develop their own. This has largely been replaced by *The Common Criteria*, adopted by some 26 countries, including the U.S. It comprises:

- the CC documents,
- the CC Evaluation Methodology (CEM),
- country-specific evaluation methodologies called an *Evaluation Scheme* or *National Scheme*.

Evaluations (to a certain level) by one signing country are respected by all of the others.

Some Acronyms

Any discussion of the Common Criteria tends to be very acronym-heavy. Here are a few:

- TOE (Target of Evaluation) the system submitted for evaluation.
- ST (Security Target) set of security requirements to be used as the basis of evaluation.
- EAL (Evaluation Assurance Level) the level of certification sought.
- TSF (TOE Security Functions) the set of all hardware, software, and firmware needed for the enforcement of the policy.

Types of Evaluation

There are two types of evaluations under the CC.

1. *evaluations of protection profiles* (PP), a set of implementation-independent security requirements for a category of products or systems;
2. *evaluations of products or systems* against a security target (ST).

Protection Profile

A PP is a description of a family of products in terms of threats, environmental issues and assumptions, security objectives, and requirements of the Common Criteria. It includes:

1. Introduction, containing a system identification and overview;
2. Product or System Family Description;
3. Product or System Family Security Environment;
4. Security Objectives;
5. IT Security Requirements;
6. Rationale.

Some examples: antivirus on workstations, biometrics, firewalls, intrusion detection, operating systems, PKI, trusted database. Approximately 50 protection profiles currently exist with more under development.

Security Target

The Security Target is a document that contains the security requirements of a product to be evaluated (TOE), and specifies the measures offered by the product to meet those requirements. It may match a protection profile.

1. Introduction
2. TOE description
3. TOE security environment: assumptions, threats, organizational security policies
4. Security objectives
5. IT Security requirements
6. TOE summary specification
7. Protection Profile claims
8. Rationale: evident that the ST is a complete set of requirements and that the TOE provides measures to address the requirements.

Lessons

- The need for secure systems evaluation criteria led to incompatible national standards.
- These have largely been replaced by the Common Criteria, a set of standards recognized by 26 countries, including the U.S. and most E.U. nations.
- Two types of entities are evaluated under the Common Criteria:
  - a "protection profile" is a formal descriptions of security for a class of systems;
  - a "security target" is a specific system or family of systems.

Next lecture: Protection Profile Example