Workshop: Developing a Protection Profile

The Common Criteria is an internationally-accepted standard used as a basis for the evaluation of security functions and properties within Information Technology products and systems. Protection Profiles specify an agreed set of security requirements for a class of IT products and are often used in purchasing decisions by IT product purchasers such as large corporations and government bodies.

There has been a lot of activity in developing Protection Profiles that are relevant and meaningful to a particular industry or IT product class. Recent success includes collaborative work on defining PPs for Operating Systems, Multi Function Printers, and Smartcards. Others are already underway or in the planning stages.

Writing a good Protection Profile that captures the security problem of the sponsor and can be used by developers and evaluators with specific TOEs requires a significant investment of effort.

A Protection Profile contains many sections, but as a security specification, the most important is the “security functional requirements.” It is mandatory to write these requirements in a special language to ensure that the Protection Profile is:

unambiguous: the language contains well defined terms, so that a developer as well as the user community can understand the requirements and interpret them correctly.

testable: the language is defined to contain only testable terms. Thus, it will be possible to assess in a later stage whether the product actually fulfils the PP.

general, but detailed enough: the language enforces a certain level of abstraction. This closely follows what should be the consumer requirements: the consumer wants something to be done but does not want to worry how this is accomplished. On the other hand, the requirements need to be defined with sufficient detail to assure the user that all products compliant to the PP satisfy his basic security requirements.

more complete: the language contains several constructions ("if this functionality is required then this other functionality is also required") to help ensure that implicit requirements are included.

Audience

This workshop is aimed at experts in information security with good knowledge of Common Criteria, who are engaged in developing Protection Profiles as part of their professional activities.

Topics in the Workshop:

a) Specifying the security problem definition:

- Identifying the informal security requirements
- How to identify and specify threats
- How to identify and specify assumptions

b) Defining security objectives to address the security problem:

- Structuring the threats, policies, and assumptions
- Identifying the non-IT operational environment objectives
- Identifying the IT operational environment objectives
- Identifying the TOE objectives
- Producing the objectives rationale

c) Specifying extended component definitions

d) Specifying security requirements that satisfy the security objectives for the proposed TOE:

- The security paradigms in Common Criteria
- Deriving a consistent model of the security functionality, structured into:
  - Controlling access to and use of resources and objects
  - TOE self protection
  - Securing communication
  - Security audit
  - Cryptography
  - Security management
  - Architectural requirements

e) How to specify security functional requirements in a PP:

- Principal SFRs
- Supporting SFRs
- Conditional SFRs
- Full and partial assignments for operations defined in part 2 of the Common Criteria
- Defining SFRs to define the product type without requiring a specific implementation

f) How to identify and specify assurance requirements in a PP

g) How to address the composition problem