Development of Informal Security Policy Models

Erin Connor, Mark Gauvreau, and Samuel E. Moore
EWA-Canada, Limited

29 September 2005

Presenter: Erin Connor (econnor@ewa-canada.com)

Overview

- Introduction To EWA-Canada
- Introduction to Informal SPM
- Description of Informal SPM Elements
- Discussion of SPM Relevance to Development
- Summary

Introduction to EWA-Canada

- Who we are
  - EWA-Canada
- What we do
  - CC evaluators
  - Provide documentation assistance

Introduction to Informal SPM

- Objective
  - “provide additional assurance that the security functions in the functional specification enforce the policies in the TSP” [CC]
- How Achieved?
  - develop a security policy model based on the TSP
  - establish correspondence between the security policy model and
    - the policies in the TSP, as expressed in the ST; and
    - the functional specification.
- Definition of TOE Security Policy (TSP)
  - “ A set of rules that regulate how assets are managed, protected and distributed within a TOE.” [CC]

Introduction to Informal SPM

- Developer Actions
  - Provide a TSP model
  - Demonstrate correspondence between the functional specification and the TSP model
- Content and Presentation of Evidence
  - 4 elements, each of which will be examined in detail
    - CC Requirement
    - CC Requirement “in English”
    - What Evaluators are Looking For
    - What Developers Need to Know
    - Our Experience

ADV_SPM.1.1C

- CC Requirement
  - The TSP model shall be informal.
- CC Requirement “in English”
  - The security policy must be described in text format
  - Diagrams are permitted, provided they are explained
  - More formal presentations are permitted, but must be accompanied by a text description
- What Evaluators are Looking For
  - Clear, consistent description, in text format.
  - Text definitions that explain any diagrams or symbols

ADV_SPM.1.1C (cont'd)

- What Developers Need to Know
  - There is no predefined model, no standard document layout, and no predefined table of contents
  - If you use mathematical or logical models, you must add explanatory text to explain them
- Our Experience
  - Developers have trouble understanding what is required by the TSP model
  - Developers have trouble deciding how to structure the model

ADV_SPM.1.2C

- CC Requirement
  - The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
- CC Requirement "in English"
  - Describe the rules by which assets are managed, protected and distributed within the TOE
  - For an informal SPM, the phrase "that can be modeled" translates to "all".
  - Subjects
    - Entities that perform security functions
    - Within TOE scope of control
    - May be processes acting on behalf of externals
    - e.g., Administration module acts on behalf of administrator

ADV_SPM.1.2C (Cont'd)

- CC Requirements "in English" (cont'd)
  - Objects
    - Security-relevant entities on which subjects act
    - Includes assets that are to be protected by the TOE
    - Only those within the TOE scope of control, e.g., related to
      - Information Flow
      - Firewall Policy Rules
      - Access Control Data
      - I&A Data
    - For interfaces, consider Information Flow vs Input Queue/Output Queue
    - For each object, consider
      - What is protected?
      - How is protection achieved?

ADV_SPM.1.2C (Cont'd)

- CC Requirements “in English” (cont’d)
  - Operations
    - For each subject, there are allowed operations on objects
      - e.g., Firewall Decision:
        - pass
        - deny
        - log
  - Rules
    - For each operation, there are restrictions/conditions
      - e.g., Pass packet if it satisfies rules set by administrator

ADV_SPM.1.2C (Cont'd)

- What Evaluators are Looking For
  - Identification of subjects, objects, operations, rules
  - Initial conditions (startup states, etc.)
  - Error/Failure modes
  - Shutdown
  - Special functions, such as residual data protection, if applicable
- What Developers Need to Know
  - Although informal, the analysis and documentation must be complete, so allow enough time for the task

ADV_SPM.1.2C (Cont’d)

- What Developers Need to Know (cont’d)
  - How to Demonstrate Security?
    - Informal description is adequate for ADV_SPM.1
    - “Accepted” or “Best Practice” arguments
    - State transition approach (more formal)
      - Establish secure state
      - Ensure each transition is secure
      - Then all subsequent states are secure
  - Relate to Defined Security Models
    - Can refer to standard models, if relevant
    - Can often find pieces in literature
      - Windows Access Control Model
      - Rule-Set Based Access Control (Linux)
  - Our Experience
    - The analysis required by this section provides a valuable check on both the security target and the development documentation

ADV_SPM.1.3C

- CC Requirement
  - The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
- CC Requirement “in English”
  - Relate the model to the SFRs and policies of the Security Target
- What Evaluators are Looking For
  - A cross-reference that is easy to check
  - Rationale for the intersections in the cross-reference

ADV_SPM.1.3C (Cont'd)

- What Developers Need to Know
  - This provides a valuable check on the ST
- Our Experience
  - Options include two one-way tables or one bidirectional table
  - Number of elements will usually determine which is best

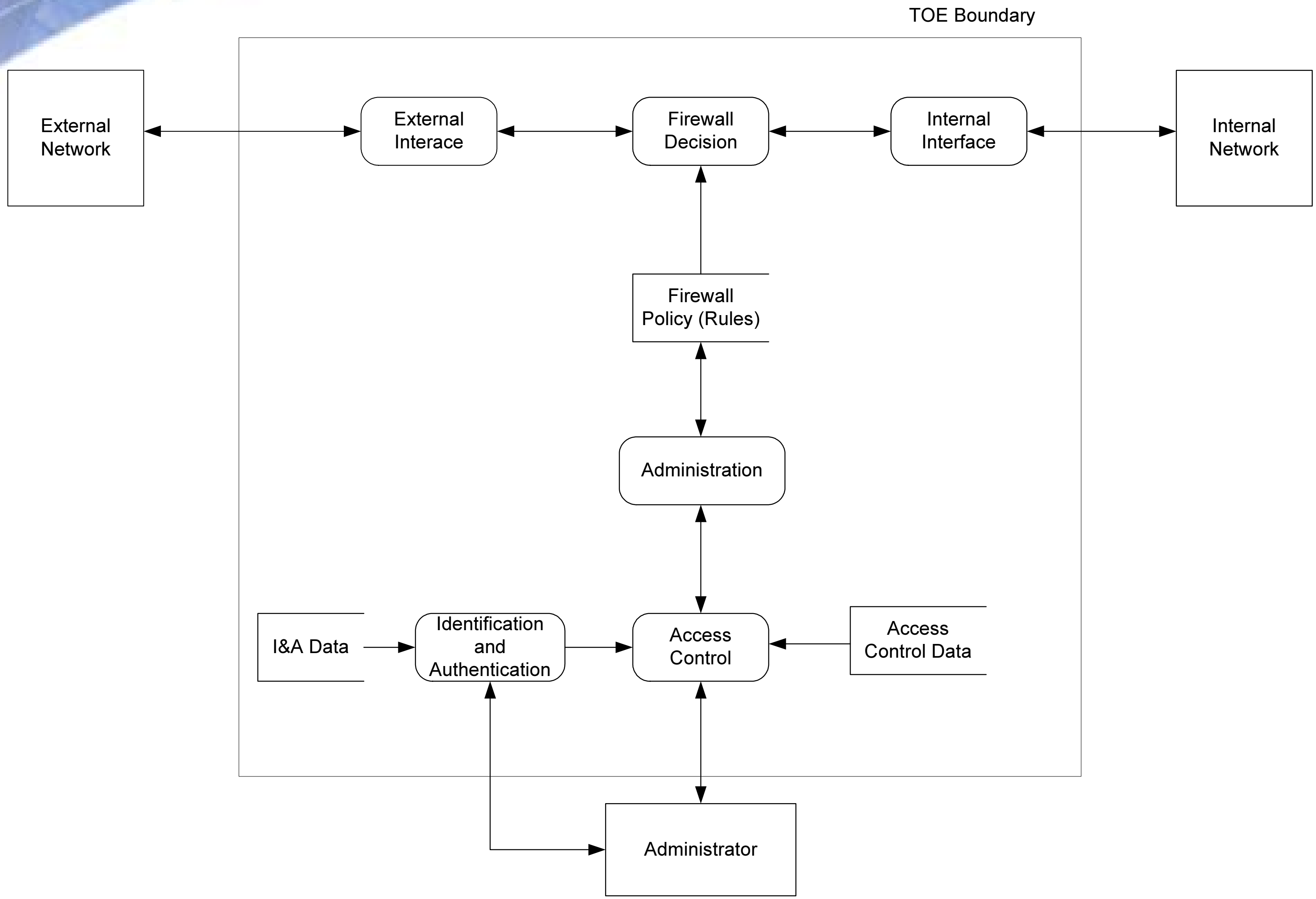
ADV_SPM.1.4C

- CC Requirement
  - The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model
- CC Requirement “in English”
  - The TSP model and the functional specification must be consistent
  - The developer must show that the TSP model reflects all of the security functionality that is described in the functional specification

ADV_SPM.1.4C (Cont'd)

- What Evaluators are Looking For
  - Consistency in nomenclature and description
  - Completeness
    - Bidirectional traceability between the TSP model and the FS
- What Developers Need to Know
  - Inconsistency leads to rework
- Our Experience
  - One-way or bidirectional tables as discussed above
  - Tables can be produced manually, but an automated method is recommended for ease of maintenance

Firewall Example



Relevance to Development

- Assurance gain, as expressed in the CC:
  - collecting the description of each security policy into a concise whole aids in understanding the details of the policies being enforced
  - a collected description makes it much easier to see any gaps or inconsistencies, and provides a clear characterisation of secure states.
- These are valid at the informal level because the policy is complete, although not expressed rigorously

Summary

- Reviewed SPM from the developer and evaluator viewpoints
- Presented an approach to producing a SPM
- Noted that SPM can be beneficial to development
- For further information:
  - econnor@ewa-canada.com

Questions

?