NAVAL POSTGRADUATE SCHOOL

A Note on High Robustness Requirements for Separation Kernels

Timothy E. Levin, Cynthia E. Irvine, Thuy D. Nguyen

Department of Computer Science, Naval Postgraduate School

6th International Common Criteria Conference (ICCC'05)

ANA Hotel, Tokyo, Japan

September 28 - 29, 2005

CISR The Center for Information Systems Security Studies and Research

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **SEP 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE **A Note on High Robustness Requirements for Separation Kernels**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Information Systems Security Studies and Research (NPS CISR),Department of Computer Science,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
6th International Common Criteria Conference (ICCC 05), September 28-29, 2005, Tokyo, Japan

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Presentation Overview

- Problem Definition
- Separation Kernel and PP Description
- High Robustness PP Issues
  - Least Privilege
  - Dynamic Reconfiguration
- CC v3.0 Transition Issues
- Summary

Problem Definition

- Need for U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP)
  - Various products forthcoming
  - High Robustness - uncharted Common Criteria territory
- Preliminary Analysis: Protection Profile (PP) requires
  - CC-oriented description of TOE abstractions
  - Extensions to several Common Criteria requirements
  - Extrapolation from existing guidance and examples
    - E.g., US scheme medium robustness CIM
    - Medium Robustness MLS OS PP draft

General Separation Kernel Characteristics

- Separation Kernel (Rushby, 1981, etc.)
- Manages computing and communication resources
  - Self-protecting
- Creates abstractions of resources for export at SK interface
- SK *Partitions* resources into policy *equivalence classes**
- Controlled separation of equivalence classes
  - No interaction between classes unless explicitly allowed

* *These equivalence classes are sometimes also called "partitions"*

General SK Characteristics

- Taxonomy of SK runtime resources
  - Internal
    - Used for implementation of kernel
  - Exported
    - Subjects
      - Programs, asynchronous devices, etc.
    - All other
      - Memory, files, devices, buffers, volumes etc.
      - “objects”

Specific SK Characteristics

- Limited functionality expected
  - E.g., embedded systems
- No runtime user interface
  - No user identification and authentication
- Static runtime configuration of security policy and resource allocation
  - Specified in “TSF configuration data”
  - Exceptions allowed for exigencies
- Support privileged subjects
  - Limit access to privileged interfaces
- Support trusted delivery, trusted recovery
- Export or store audit records
  - At least one is required

Evaluation Target

- EAL6
- + Formal Security Policy Model

- TOE Components
  - TSF
    - Software
    - Hardware base
  - Initialization mechanism
  - Configuration mechanism
  - Delivery and recovery mechanisms

SKPP High Robustness Issues

- Principle of least privilege (PoLP)
  - All-or-nothing security cannot be high robustness
- Dynamic configuration
  - On-the-fly security policy changes may be intractable to analyze with respect to the separation of equivalence classes (e.g., Harrison et al, 1976)
- Hardware as part of the TSF
  - A classic third-party assurance composition problem

Principle of Least Privilege (PoLP)

- PoLP (reviewed in Saltzer, Schroeder, 1975)
  - Mechanisms should have no more privilege than what is necessary to perform the actions for which they were designed
- PoLP Applied to SKPP
  - TSF must have capability to restrict subjects'…
    - access to privileged operations
    - access to resources within a partition
  - TSF must be structured to restrict privileges of internal modules/functions

Least Privilege in FDP_ACC

- Use Case:
  - TSF supports multiple heterogeneous subjects in a partition
  - TSF must discern between those subjects for the purpose of information flow control
- **FDP_ACC:**
  - *TSF may allow an operation of a subject on an exported resource only if:*
    - *Partition-to-Partition flow rule explicitly authorizes operation*
    - *Subject-to-Resource flow rule explicitly authorizes operation*

Least Privilege in ADV_ARC/ADV_INT

- PoLP advantages for design and internal structure
  - Affords simplicity to implementation
  - Coupled with layering and minimization, increases confidence in analysis of TSF correctness

- **ADV_ARC*: requires justification that TSF design achieves PoLP***
- **ADV_INT*: requires PoLP to be applied to all TSF modules/functions***

Exceptions to PoLP

- FDP_ACC allows certain PoLP "exceptions"
  - Configurations where subject-resource interaction is "policy-equivalent" to that of their partition
    - Interaction between single-subject and single-resource partitions
      - ***Only one subject in subject's partition***
      - ***Only one exported resource in resource's partition***
    - Homogeneous functionality of subjects in a partition
      - ***All subjects in subject's partition require same operation on all exported resources in resource's partition***

SK Configuration

- Static Configuration SK
  - Initial configuration data determines runtime behavior
    - All resource allocations
      - Time - e.g., CPU time slices
      - Space - e.g., per-partition memory regions
    - All allowed information flows
  - Ideal for embedded systems and security research
    - Simple design and implementation
    - Evaluatable size
  - Provides fundamental security service: separation
  - Building block for more complex systems
  - ***Assurance issue with configuration-data based policy mechanism:***
    - ***Ensure resulting security policy reflects the organization's intent***

Dynamically Configurable SK

- Problem scenario
  - Failure of a peripheral device in a mission critical application, or
  - Overriding environmental security conditions
- Desirable for TOE to be able to change its configuration
- SKPP allows TOE to change resource allocations and policy rules during runtime
  - Several problems

Dynamic Configuration Problems

- Continuity of security across a policy transition
  - Undefined security during transition?
  - Undefined combinations of policies after transition?
- Arbitrary changes are hard to understand w.r.t. policy
  - Formal models often have static attributes because of this
- Approach:
  - Limit how policy may change
  - Four hierarchical modes of change defined

SKPP Dynamic Configuration Options

1. Off-line transitions and pre-loaded configurations
   - Allows complete removal of previous security state
   - Allows pre-analysis of subsequent security policies
   - Triggered by privileged subject or offline actions
   - ***Assurance issue: TSF must ensure***
     - ***Only authorized subject may request configuration change***
     - ***TOE fully and properly executes the change request***
2. On-line transitions and pre-loaded, configurations
   - Allows dynamic change of configuration
   - ***Additional assurance issue: TSF must continuously maintain secure state***
     - ***Before, during and after the configuration change***

SKPP Dynamic Configuration Options (continued)

3. On-line transitions and limited configuration changes
   - Changes limited by static rules enforced by TSF
   - ***Additional assurance issue:***
     - ***Ensure ad hoc policy change requests are consistent with organization's policy intents***
4. On-line transitions and arbitrary configuration changes
   - ***Additional assurance issue:***
     - ***TOE vendor must provide convincing definition of "secure transition" in SFP model***

- Options 3 and 4 are beyond the scope of the SKPP
  - Will require an ST- rather than PP-based evaluation

SKPP DC Requirements

Details of SKPP functional and assurance requirements for dynamic configuration are ST-specific

SKPP Transition to CC V3.0

- SKPP
  - Developed to be conformant to CC V2.2
- CC V3.0 significantly different
- FDP_ACC simpler than FDP_IFF/IFC
- Challenges include
  - Hardware assurance undefined
  - Non-user Security Attributes
  - Covert Channel Analysis by developer

Security Attributes Binding

- SKPP requires binding of security attributes to exported resource when resource is created
- Two-step process: registration and initialization
  - **FIA_URE:** ***TSF must store attributes of exported resources in identified internal resources***
    - e.g., kernel structures
  - **FIA_ISA:** ***TSF must bind (those) attributes to corresponding exported resources when resource is created***

Summary

- High Robustness Requires
  - PoLP
  - Control of Dynamic Re-Configuration
- Common Criteria Version 3.0 transition
  - Most SK requirements fit into existing families
  - A few new explicit requirements required to cover scope of TOE

Acknowledgements

The authors would like to express their appreciation to the entire SKPP development team, without whom this work could not have been completed.

Questions?

Thuy D. Nguyen
tdnguyen@nps.edu