An Experiment with CC Version 3.0 Migration

Thuy D. Nguyen, Cynthia E. Irvine
Department of Computer Science, Naval Postgraduate School
Richard M. Harkins
Department of Physics, Naval Postgraduate School

7th International Common Criteria Conference

Lanzarote, Spain
September 19-21, 2006
## An Experiment with CC Version 3.0 Migration

**Naval Postgraduate School, Center for Information Systems Security Studies and Research (NPS CISR), Department of Computer Science, Monterey, CA, 93943**

### Abstract

7th International Common Criteria Conference (ICCC 06), Lanzarote, Spain, 19-21 Sep 2006
Discussion Topics

- Motivations
- Project background
  - Draft Multilevel Print Server (MPS) PP
- CC Version 2.2 → CC Version 3.0
  - Objectives and Approach
  - Before and After
- Observations and Conclusion
Motivations

Why we did it …

• Stay current on latest CC developments
• Prepare for a new course on security requirements engineering
• Determine effectiveness of learning-by-doing as applied to the CC
• Meet sponsored program requirements
Project Background
• Sponsor needs shared printing capability in multilevel environment

• Use CC framework to establish security requirements for dedicated MPS
  – Draft PP based on CC Version 2.2 – Masters thesis
    • TOE description
    • Threats (16), assumptions (8), OSPs (6)
    • Security objectives – TOE (24), IT environment (9)
    • SFRs – TOE (9 Classes), IT environment (1 Class)
    • SARs – EAL4 with augmentation
  – Draft PP lacks
    • Traceability analysis & rationale description
TOE Description

Security Environment

- **Dedicated Printer**
- **Networked Printer**
- **Multilevel print server**

**Single-level clients**

- **MLS Print Server**
  - Handle print jobs of different sensitivity levels
  - Utilize Separation Kernel technology

- **Single-level clients**
  - Sensitivity levels determined by attached interface

- **Printers**
  - Located on system high network, physically protected
- Trusted base
- Trusted partitions
  - Runtime (TSF) Initialization
- Single-level partitions

Hardware, Separation Kernel
MLS Services, System High Services
Print spoolers, one per input port
CC Version 2.2 → CC Version 3.0
Objectives
• Complete translation of SFRs
• Partial translation of SARs
• Provide hands-on experience for team member unfamiliar with CC

Approach
• “Rote port” -- Focus only on requirements
• Supervised practice
• Weekly assessment

Progress
• First pass only – translated requirements still sketchy
• Stopped early due to CC V3.1 news
Translation of FAU Summary

<table>
<thead>
<tr>
<th>V2.2</th>
<th>V3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU_ARP</td>
<td>FAU_ARP</td>
</tr>
<tr>
<td>FAU_GEN</td>
<td>FAU_GEN</td>
</tr>
<tr>
<td>FAU_SAA</td>
<td>FAU_SAA</td>
</tr>
<tr>
<td>FAU_SAR</td>
<td>FDP_ACC, FAU_SAR_EXP</td>
</tr>
<tr>
<td>FAU_SEL</td>
<td>FDP_ACC, FAU_SEL_EXP</td>
</tr>
<tr>
<td>FAU_STG</td>
<td>FDP_ACC, FAU_STG_EXP</td>
</tr>
</tbody>
</table>

- **FAU_ARP, FAU_GEN, FAU_SAA**
  - Translation was straightforward

- **FAU_SAR, FAU_SEL, FAU_STG**
  - Required more work
  - Used FDP_ACC to control ability to review data, select auditable events, protect audit trail
  - Defined extended components for specific security functions
FAU_SAR.1.1: The TSF shall provide the security administrator with the capability to read all audit information from the audit records.

FAU_SAR.1.2: Refinement: The TSF shall provide the audit records in a manner suitable for the security administrator to interpret the information using a tool to access the audit trail.

FDP_ACC.1.1: Access control for audit review
The TSF shall allow an operation of a subject on an object if and only if all of the following hold:
   a) The role attribute of the subject is security.
   b) The type of the object is audit record in the audit trail.
   c) The subject has read access to the object.

FAU_SAR_EXP.1.1: Security audit review support
The TSF shall provide the audit records in a form suitable for the subject with the role attribute of security administrator to interpret the information.
### Challenges with FDP_IFC and FDP_IFF translation

- Separation Kernel enforces both information flow and MAC policies
  - Kernel configuration data defines policies

- MLS Services enforces MAC supporting policy for print job labeling
  - Map sensitivity level of jobs based on level of spooler partition
  - Label jobs with human readable markings

<table>
<thead>
<tr>
<th>V2.2</th>
<th>V3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDP_ETC</td>
<td>FCO_ETC</td>
</tr>
<tr>
<td>FDP_ITC</td>
<td>FCO_ITC</td>
</tr>
<tr>
<td>FDP_IFC</td>
<td>FDP_ACC</td>
</tr>
<tr>
<td>FDP_IFF</td>
<td>FDP_ISA</td>
</tr>
<tr>
<td>FDP_RIP</td>
<td>FPT_RIP</td>
</tr>
</tbody>
</table>
### Translation of FIA Summary

<table>
<thead>
<tr>
<th>V2.2</th>
<th>V3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIA_AFL</td>
<td>→ FIA_AFL, FIA_URE</td>
</tr>
<tr>
<td>FIA_ATD</td>
<td>→ FDP_ISA</td>
</tr>
<tr>
<td>FIA_SOS</td>
<td>→ FIA_QAD</td>
</tr>
<tr>
<td>FIA_UID</td>
<td>→ FIA_UID</td>
</tr>
<tr>
<td>FIA_UAU</td>
<td>→ FIA_UAU</td>
</tr>
<tr>
<td>FIA_USB</td>
<td>→ FIA_USB</td>
</tr>
</tbody>
</table>

- Mostly straight forward translation
- A lesson on indirect dependencies
  - E.g., FIA_AFL indirectly depends on FIA_URE because of FIA_UAU
- Dependency tables in Annex A were utilized
  - Per-class tables in V3.0 are easier to use
### Translation of FMT Summary

<table>
<thead>
<tr>
<th>V2.2</th>
<th>V3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMT_MOF</td>
<td>FDP_ACC</td>
</tr>
<tr>
<td>FMT_MSA</td>
<td>FDP_MSA</td>
</tr>
<tr>
<td>FMT_MTD</td>
<td>FDP_ACC, FDP_MSA, FPT_RSA</td>
</tr>
<tr>
<td>FMT_SAE</td>
<td>FDP_ACC, FDP_MSA</td>
</tr>
<tr>
<td>FMT_SMF</td>
<td>FDP_ACC, FDP_MSA</td>
</tr>
<tr>
<td>FMT_SMR</td>
<td>FDP_ACC, FDP_MSA, FIA_USB</td>
</tr>
</tbody>
</table>

- No FMT in V3.0 -- Most dreaded part of the exercise
- General mapping rules
  - Use FDP_ACC for restricting ability to perform certain function
  - Use FDP_MSA for managing functions related to security attributes
- FMT_MTD, FMT_SMR require other families
**FMT_MTD.2.1:** The TSF shall restrict the specification of the limits for print jobs sent to the printer to the security administrator.

**FDP_ACC.1.3:** Management of print job limits

The TSF shall allow an operation of a subject on an object if and only if all of the following hold:

a) The role attribute of the subject is security administrator.

b) The type of the object is print job.

c) The operation is to specify the limits for print jobs sent to the printer.

**FDP_MSA.1.3:** Management of print job limits

The TSF shall determine if a subject is allowed to change the limits of print jobs sent to the printer or not, as follows:

a) The role attribute of the subject is security administrator.

b) The values of the new print job limits are valid.
FMT_MTD.2.2: The TSF shall take the following actions, if the TSF data are at or exceed, the indicated limits: <list of actions>

FPT_RSA.1: Resource allocation (print job limits)
  FTP_RSA.1.1: The TSF shall enforce maximum quotas for print jobs that a subject can use over a specified period of time.
  FTP_RSA.1.2: The TSF shall take the following actions when a maximum quota for print jobs is surpassed: <list of actions>
Assurance Requirements
• Base requirements for EAL 4
• Extended requirements include
  – Flaw remediation procedures
  – Assurance maintenance plan
  – Administrative guidance regarding proper setting of configuration data
    • MAC enforcement: SK configuration data
    • MAC supporting: MPS configuration data
  – Administrative guidance regarding proper handling of printed material
SARs for V3.0

- No specific translation
  - Project stopped before getting to SARs
- V3.0 ADV requirements were reviewed for a different project (SKPP)
  - Provided comments to US scheme
- TOE relies on evaluated separation kernel
  - Composition challenge: Allocation of mandatory and supporting policies among TOE components
- US Precedent PD-0117 facilitated several decisions in original PP
- Class ACO is not as expected
  - Only address composition of evaluated TOEs
Observations and Conclusion
Observations

• Validated general assessments of CC V3.0
  – New functional paradigm not ready for general use
  – Difficult to express TOE security behavior
  – Correct usage of FDP_ACC was difficult to determine
• Ordering of classes/families was hard to navigate if not already familiar with CC
• “V3.0 transition” document was helpful
  – Example of translated PP/ST would be better
Other Observations

- Team lost momentum/interest after CC V3.1 news
  - Part 2 is back to V2.3 with minor changes
- Project took longer than expected
  - Conducted as a teaching exercise
  - Steep learning curve for novice team member
  - Worked as time allowed → high overhead revving up
- 20/20 hindsight: high-level translation might be better than rote
- Cyclical learning-by-doing methodology was effective

Task definition

Reflection on experience

Team exploration
• 3 out of 4 objectives met
  ✓ Stay current on latest CC developments
  ✓ Prepare for a new course on security requirements engineering
  ✓ Determine effectiveness of learning-by-doing as applied to the CC

• Future work to meet sponsored program requirements
  – Full CC V3.1 migration under consideration
Thuy D. Nguyen

Center for Information Systems Security Studies and Research
http://cisr.nps.edu
Department of Computer Science
Naval Postgraduate School
Monterey, California, USA

tdnguyen@nps.edu