PROCESS IMPROVEMENT FOR COMMON CRITERIA EVALUATION in Malaysian Context

Siti Fatimah Abidin (Presenter)
Norahana Salimin

Analyst, MySEF
Security Assurance, CyberSecurity Malaysia
Tuesday, 27th September 2011
Content

• Introduction
• Overview
• Analysis and discussions
• Conclusion
INTRODUCTION
Introduction

“Product evaluation and certification”

One of many ways to demonstrate that your ICT product or system is reliable and recognized

COMMON CRITERIA (CC)
“Although CC has become an international standard of IT security evaluation, it still contains many issues and limitations”

Changying Zhou & Stefano Ramacciotti
Introduction

CC Evaluation

Higher assurance longer duration, higher cost

Outdated evaluation result

Outdated vulnerability assessment result
Introduction

• Key aspect for process improvement to reduce evaluation duration:
  – Project management
  – Client collaboration
  – Product technology, development and testing methodologies
  – Evaluator expertise
OVERVIEW
ESP2 Project

• **Financial assistance** was provided by CyberSecurity Malaysia under the **Economic Stimulus Project 2 (ESP2)** for eligible Small Medium Enterprises (SMEs) developing ICT product **to obtain CC** certification through Malaysian Common Criteria Evaluation and Certification Scheme (MyCC)

• **16 products** has been accepted under ESP2 project for EAL 1 and EAL 2

• Targeted to be evaluated **by end of 2010**
ANALYSIS AND DISCUSSIONS
## Project Analysis

- **Project selection**
  - The shortest 2: Project AA & BB
  - The longest 2: Project YY & ZZ
  - EAL 1

<table>
<thead>
<tr>
<th>#</th>
<th>Project Code</th>
<th>EXE phase (months)</th>
<th>EAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AA</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>BB</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>CC</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>DD</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>EE</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>FF</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>GG</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>HH</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>JJ</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>KK</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>YY</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>LL</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>MM</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>NN</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>PP</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>ZZ</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>QQ</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>18</td>
<td>RR</td>
<td>24</td>
<td>4</td>
</tr>
</tbody>
</table>
Duration of Evaluation Project

18 months

YY: 6 5 7
ZZ: 2 7 3
BB: 5 3 2
AA: 3 1 3

12 months

10 months

7 months
Key Aspects for Process Improvement

- Project Management
- Client Collaboration
- Product Technology, Development and Evaluator Expertise
- Testing Methodologies
18 evaluation projects (concurrent)
5 projects per evaluator

Tight schedule
Delay
Process improvement

Reassign other evaluators to critical project
Client Collaboration

Total of days taken by developer/consultant to respond

- YY: 142 days
- ZZ: 156 days
- BB: 65 days
- AA: 65 days
Client Collaboration

Late respond by developer/consultant on issues raised by evaluator

commitment to other business activities

not understand clearly on the issue
Client Collaboration

Process improvement

- provide internal consultant
- direct discussion with developer and/or consultant
- take legal action as per stated in service agreement
Client Collaboration

Direct discussion with developer/consultant

- Yes: 10 projects
- No: 8 projects
Product Technology

Niche technology requires extensive research during evaluation

Smart card

Biometric

Cryptography
Process improvement

Engage subject matter expert to provide knowledge in terms of product technology
Evaluation concurrent with product development
Process improvement

Follow up developer progress every 2 weeks to ensure no delay to the project
Much effort on test plan development if product type has not yet encountered by lab
Testing Methodologies

Duration of AVA phase

- YY: 90 days
- ZZ: 45 days
- BB: 6 days
- AA: 4 days
Develop template of test plan for each type of product
Testing Methodologies

• Common Evaluation Methodology (CEM) is a guideline for evaluators in executing CC evaluation.
  – Consist of requirements of the product or product documentation for the product to be certified
  – Repetitive evaluation effort as several requirements are interrelated and interdependent.
Testing Methodologies

Common Evaluation Methodology (CEM)

Repetitive evaluation effort; as several CEM requirements are interrelated and interdependent.
Testing Methodologies

Process improvement

Summarized all interrelated and interdependent requirement in table format (ASE, AGD, ADV, ATE)
### Testing Methodologies

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>SFR-enforcing supporting non-interfering</th>
<th>Behavior</th>
<th>TSFI</th>
<th>SFR</th>
<th>Purpose</th>
<th>Method of use</th>
<th>Admin</th>
<th>Test case</th>
<th>params</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>FCS_COP</td>
<td>EXECutes opcodes fetched via the bus...</td>
<td>DATABASES</td>
<td>FCS_COP</td>
<td>Blah blah blah...</td>
<td>bus</td>
<td>No</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FMT_LIM</td>
<td></td>
<td></td>
<td>FMT_LIM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPT_PHP</td>
<td></td>
<td></td>
<td>FPT_PHP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESET</td>
<td>FCS_COP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reset line</td>
<td>No</td>
<td>42, 2501</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FMT_LIM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPT_PHP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Analysis of CC requirements in table format
Summary

• **Project Management:**
  – Rearranged or reassigned evaluators to critical project which is expected to delay.
  – Sharing the information or lesson learned from test that has been conducted or feedback from certification body with other evaluators to avoid duplicating unnecessary effort.

• **Client Collaboration:**
  – Provides internal consultant among evaluators who were not involved in the respective project to assist developer resolve evaluation issues.
  – Organize direct discussion with developer and/or consultant to speed up resolving issue in EOR.
Summary

• **Product Technology, Development and Evaluator Expertise:**
  - Engage subject matter expert for project on niche technology’s product to speed up knowledge transfer.
  - Regular follow up developer progress if evaluation is concurrent with product development.

• **Testing Methodologies:**
  - Develop test plan template for AVA execution.
  - Record evaluation results in table format which covers requirement in ASE, ADV, AGD and ATE.
CONCLUSION
Conclusion

• Common Criteria is a new initiative in Malaysia.
• Need improvement:
  – delivering evaluation service in a shorter period while not sacrificing the quality of evaluation results.
• Future research may be conducted to improve evaluation duration and cost in terms of testing methodologies using site certification and developing evaluation evidence template which contain all CC requirements.
Q&A
Corporate Office:
CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

T +603 8946 0999
F +603 8946 0888

www.cybersecurity.my