Multi-Level Certifications
Using Lower EALs as Project Milestones

Bertolt Krüger, SRC Security Research & Consulting GmbH
Christian Tobias, Utimaco Safeware
ICCC 2008, Jeju, South Korea
Highlights

► CC Market Requirements for Full Disk Encryption (FDE) Products

► Conflict of Goals for Vendors

► Proposed Approach: Multi-Level Certifications
  ◆ Introduction and Organisation
  ◆ Impact on project schedule and budget
  ◆ Challenges

► Wrap-up and Discussion
Utima-co Safeware
Celebrating 25 Years of Protecting Information Worldwide

- Founded in 1983
- Revenue FY 2007/08: €55.9 million
- 300+ employees worldwide
- Committed to provide evaluated and certified solutions (i.e. FIPS, Common Criteria, NATO Restricted...)
- About 3-5 certifications per year
- Certifications in Germany, Japan, and the US.
SRC Security Research and Consulting GmbH

► Background
  • Founded in August 2000 by German financial industry
  • Employees: 52
  • Headquarter: Bonn, Germany

► Consultancy on Secure Systems throughout the lifecycle
  • Independent
  • Customer- and project-oriented solutions
  • Through highly qualified consultants
  • With international focus

► Some fields of expertise
  • Common Criteria evaluation facility
  • Specialist for payment schemes, in particular smart card based
  • Information Security Management Systems
  • Ethical Hacking and Forensics
  • Auditor according to Payment Card Industry (PCI) Standards (PED, DSS, PA-DSS)

► More information available at: http://www.src-gmbh.de
General Conditions for Vendors

► Certain markets require a (Common Criteria) Certificate
  ◆ The Time-to-Certificate is one of the most critical parameters for vendors.

► Often heard critical comments regarding CC
  ◆ Takes too long
  ◆ Is too expensive

► Conflict of goals
Full Disk Encryption Market

► Certifications (CC and FIPS 140) are required in many calls for tender.

► Market situation:
  ◆ 6 Products with CC certificate
    • EAL 4: 3 products
    • EAL 3: 1 product
    • EAL 2: 1 product
    • EAL 1: 1 product
  ◆ 2 CC certifications in progress (EAL 4)
  ◆ 2 well-known vendors ignoring CC
Market Situation for Utimaco

- SafeGuard Easy is a full disk encryption solution with a strong certification history.
- Gradual displacement of SafeGuard Easy by the newly developed product suite SafeGuard Enterprise.
- CC Certification of SafeGuard Enterprise is a market need.
- Conflict of objectives:
  - EAL 4 is needed to be competitive.
  - A CC certificate is needed as soon as possible.
Approach to Resolve this Conflict

► Assumptions:
- EAL 4 is about 1.5 – 2 times as time-consuming as EAL 3
- The Low Level Design (LLD) is the main reason for this difference

► Solution: Do a multi-level certification!
- Step 1: EAL 3+
  - Can be obtained significantly faster
  - Sufficient to open part of the FDE market
  - Sufficient to start national approvals
- Step 2: EAL 4
  - Obtained via a re-certification
  - Sufficient to address all of the FDE market
## Comparison of Assurance Requirements

<table>
<thead>
<tr>
<th>Assurance Class</th>
<th>EAL 3</th>
<th>EAL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM_AUT</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>ACM_CAP</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>ACM_SCP</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ADO_DEL</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ADO_IGS</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ADV_FSP</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ADV_HLD</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>ADV_IMP</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>ADV_LLD</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>ADV_RCR</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ADV_SPM</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>AGD_ADM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AGD_USR</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_DVS</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_LCD</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>ALC_TAT</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>ATE_COV</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>ATE_DPT</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ATE_FUN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ATE_IND</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>AVA_MSU</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>AVA_SOF</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AVA_VLA</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

- All components depending on the LLD are marked in **orange**.
- All components that can be covered in EAL 3+ are marked in **blue**.
How Realistic is this Approach?

2 Core Questions:

- How much longer will the 2-step approach take (compared to a direct EAL 4 certification)?
- How much more will it cost?
# Estimated Lab Costs (before project start)

<table>
<thead>
<tr>
<th></th>
<th>Difference in project runtime</th>
<th>Difference in lab costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 1</td>
<td>30 %</td>
<td>≈ 37 %</td>
</tr>
<tr>
<td>Lab 2</td>
<td>0 %</td>
<td>&lt; 3%</td>
</tr>
<tr>
<td>Lab 3</td>
<td>40 %</td>
<td>≈ 18 %</td>
</tr>
</tbody>
</table>
## Ideal Timeline

<table>
<thead>
<tr>
<th>Start of Project</th>
<th>Product Release</th>
<th>Issuance of EAL 3+ Certificate</th>
<th>Issuance of EAL 4 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Work (EAL 3+)</td>
<td>Lab Work (EAL 3+)</td>
<td>Certifier Work (EAL 3+)</td>
<td>Vendor Work (EAL 4)</td>
</tr>
<tr>
<td></td>
<td>Lab Work (EAL 4)</td>
<td>Certifier Work (EAL 4)</td>
<td></td>
</tr>
</tbody>
</table>
Delays are Expensive

► If the certification takes longer than expected (standard case?), a newer product version can be submitted.

► In the two-step process this is possible without limitations in the first phase only.

► If the product version is changed in the second phase, version-specific work (e.g. independent testing) has to be redone.
  ◆ Project schedule and budget are at risk.
Comparison of Efficiency

► Two certification processes are necessary to reach final goal.
► Administrative Overhead.
► A multilevel certification in only one process would reduce that overhead.

► Adoption of Multi-Level Certifications by Certification Bodies or the CC in general would help minimize the overhead and increase the efficiency of the process.
Challenge: Publication

- Certification bodies publish lists of products in evaluation.
- A Re-Certification cannot be started officially before the base certification is finished.
- At project start only the base certification will be published not indicating the targeted EAL correctly.
Wrap-up

► CC Certification processes are very time-consuming.
► If a CC certificate is finally issued, the certified version may not even be the newest product version.
► The presented approach
  ◆ leads to a significant shorter time-to-certificate,
  ◆ can be used without changing the CC certification process and
  ◆ leads to an (administrative) overhead.
► Appeal to the Certification bodies: adopt this process
Thank you for your attention!

Any Questions?

Dr. Bertolt Krüger  
SRC Security Research and Consulting  

Bertolt.Krueger@src-gmbh.de  
+49 228 2806 122

Dr. Christian Tobias  
Utimaco Safeware AG  

Christian.Tobias@utimaco.de  
+49 6171 88 1711