ALC class - Proposal for minimum assurance requirements

Certification Body - Spain.
14th International Common Criteria Conference.

Luis M. Fernández
Outline

- Proposal to enforce ALC SARs for EAL2 certifications
- Reuse of ALC class efforts applying Site Certification procedures
- Supply chain security assurance within ALC class
Current Situation

Vision Statement

- The general security level of general ICT COTS certified products needs to be raised without severely impacting price and timely availability of these products.
- The level of standardization has to be increased by building Technical Communities (TC) developing collaborative Protection Profiles (“cPPs”) and supporting documents, in order to reach reasonable, comparable, reproducible and cost-effective evaluation results.
- The existing application of STs and PPs still applies, but its CCRA mutual recognition should be limited to EAL 2.
**Current Situation**

Security Assurance Requirements for ALC class in EAL 2 certifications

<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance Family</th>
<th>Assurance Components by Evaluation Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EAL1</td>
<td>EAL2</td>
</tr>
<tr>
<td>ALC_CMC</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ALC_CMS</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ALC_DEL</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_DVS</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_FLR</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_LCD</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ALC_TAT</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Current Situation

- EAL 2 ALC class components
  - ALC_CMC.2
    - TOE & CI labeled with unique reference.
  - ALC_CMS.2
    - Configuration list composed of the «parts» of the TOE and for each developer must be identified.
  - ALC_DEL.1
    - Method of delivery to the TOE consumer. Secure delivery from developer.
**ALC Proposal**

- Component rearrangement for EAL2 evaluations according to the Vision Statement.

<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance Family</th>
<th>Assurance Components by Evaluation Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC_CMC</td>
<td>1 4 3 4 4 5 5</td>
</tr>
<tr>
<td></td>
<td>ALC_CMS</td>
<td>1 4 3 4 5 5 5</td>
</tr>
<tr>
<td></td>
<td>ALC_DEL</td>
<td>1 1 1 1 1 1 1</td>
</tr>
<tr>
<td></td>
<td>ALC_DVS</td>
<td>1 1 1 1 2 2</td>
</tr>
<tr>
<td></td>
<td>ALC_FLR</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_LCD</td>
<td>1 1 1 1 2 2</td>
</tr>
<tr>
<td></td>
<td>ALC_TAT</td>
<td>1 2 3 3</td>
</tr>
</tbody>
</table>
**ALC Proposal**

**ALC_LCD.1**
- Development and maintenance process within an overall management structure in the TOE Life-Cycle

**ALC_CMC.4**
- Automatic production of TOE
- Authorized changes to CI
- CM plan and CMS

**ALC_CMS.4**
- Implementation representation for the whole TOE
- Security flaws and resolution status

**ALC_FLR.1**
- Methods for dealing with all types of flaws encountered

**ALC_DVS.1**
- Site visit
- Assessment of security procedures
  - Physical
  - Logical
  - Personnel
- Confirm Evidence

12/09/2013
www.ccn.cni.es
Outline of security improvements within the proposal

- Specific Life-cycle definition for the TOE
- TOE produced by automated means
- TOE fully identified (source code level) and managed
- Development site(s) security measures evaluated
- Procedures to address security flaws
You might think

- "This proposal increases the workload for CC certifications"
- "Too much effort for this assurance level"

There is a possible answer.

Re-use the evaluation results.

This is not a new idea. There is already a tool to use:

- CCDB-2007-11-01 Site Certification
Site Certification

- Site Certification process according to CCDB-2007-11-01
  - TOE independent CC certification to confirm that a specific development environment fulfills the CC requirements regarding ALC class.
  - These evaluation activities can be reused in a TOE evaluations later on.
  - Based on activities and procedures defined in the Life-cycle (ALC_LCD) and the claimed attack potential.
Site Certification

Site A
- Technical Community
- SmartCards
- Mobile Devices
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.5
  - ALC_DVS.2
  - ALC_TAT.2
  - ALC_FLR.1

Site B
- Technical Community
- SmartCards
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2
  - ALC_DEL.1

Site C
- Technical Community
- SmartCards
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2

Site D
- Technical Community
- SmartCards
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2

Analysis

Certificate check

Splicing (reuse)

ST Conformance Claim (cPP)

TOE ALC_LCD.1

TOE Certificate

12/09/2013

www.ccn.cni.es
There is a problem: Minimum assurance requirements for Site Certification according to CCDB-2007-11-01:

- Minimum assurance requirements
  - ALC_CMC.3
  - ALC_CMS.3
  - ALC_DVS.1
  - ALC_LCD.1

- Current EAL2 components
  - ALC_CMC.2
  - ALC_CMS.2
  - ALC_DEL.1

- ALC proposal components
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DEL.1
  - ALC_DVS.1
  - ALC_LCD.1
  - ALC_FLR.1

This proposal makes compatible the Vision Statement with Site Certification processes and supporting documents.
Site Certification

Benefits

- For the TOE consumer
  - Security assessment of the whole TOE life-cycle
  - Supply chain assurance (as we’ll see later)

- For the TOE developer
  - Maximum reuse of ALC class documentation
  - Obtain an additional Certificate to certify Development Site Security (similar to ISO 27000 approach)
  - Flexibility: combine certified sites in different countries decreasing ALC class evaluation efforts.
Supply Chain and ALC proposal

- The Council of Supply Chain Management Professionals defines supply chain management as follows:
  - "Supply Chain Management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. […]"

- All these activities are closely related to the TOE Life-Cycle as defined in CC

- Current components → Supply Chain Security
Supply Chain and ALC proposal

- TOE might be composed of different components and parts developed by different entities in different tiers.

- CC considers the TOE as a whole and takes into account each part, so security assessment considers security maintenance processes for each component.

ALC proposal components supply chain coverage

- ALC_LCD.1 - provides definitions and procedures of phases on the development and security maintenance of the TOE. Documents should provide information about:
  - Where each phase takes place? → Site
  - Who is responsible of each phase? → Organization
  - What activities are carried out in each phase (inputs/outputs)? → Policies
  - How these activities are considered by each actor? → Processes
Supply Chain and ALC proposal

- Once this information is provided, all the other ALC components deeply address security issues related to the supply chain in each phase.
ALC Proposal & Vision Statement

- Refinements to ALC components within iTCs and CPP.
  - iTC can refine ALC requirements and components to better fit them with different technologies.
  - ALC supporting documents aligned with technologies in the scope of a specific iTC.
  - Site Certificate recognition agreements between Schemes in iTC.

Technical Communities

- Life-cycle definition
- CI identification measures
- CI Confidentiality & Integrity measures
- Minimum Site Requirements
ALC Proposal & Vision Statement

Some ideas for refinements to ALC components in TC and cPP.

- Development & manufacturing phases
- Actors, roles and responsibilities
- Common Policies and Processes

- Procedures to identify and track CI and TOE components
- Integrity control measures

- Flaw remediation processes to address Supply Chain flaws.
ALC Proposal & Vision Statement

- Refinements to ALC components in TC and cPP.

  - Protect TOE integrity delivery to consumers
  - Traceability in the Supply Chain.

  - Minimum site requirements
  - Protect TOE CI integrity in internal deliveries (subcontractors and development sites).
  - Accountability and traceability of CI
  - Rules to reuse Site Certificates depending on the technology area.
ALC Proposal & Vision Statement

Alignment with the vision statement

- Component Rearrangement
- Enhance Security
- Reuse CC ALC class components
- Minimize time and efforts
- Site Certification

CCMC Vision Statement
Conclusions

Compatible with Site Certification

Enhance Security

Supply Chain Security Assessment

Reuse of Results

ITC & cPP oriented

ALC proposal
Contact Information

- **E-mail**: organismo.certificacion@cni.es
- **Web Site**: www.oc.ccn.cni.es
References