Site evaluation according to the Site Certification Process

Dr. Burkhard Grimm, Thomas Schroeder, Jan Stohner
T-Systems

9th ICCC
9th International Common Criteria Conference

Overview of the talk

- Beginning
  - Starting Re-use
  - Definition of a regular audit intervals
- Formal Re-use
  - Scheme specific process
  - Re-use by other evaluation labs possible
- Site Certification Process
  - Requirements and Evaluation tasks
- Product Evaluation
  - Evaluation process
  - Evidence during product evaluation
- Outlook

Beginning
Starting Re-use

- The evaluation of different products within the same development environment and similar development tools based on the same process description lead to the same evaluation results.
- Especially if:
  - The time interval between the two evaluations is short
  - The evaluation is applied by the same evaluation lab

- Re-use was a case by case decision between the certification body and the evaluator

Beginning
Definition of regular audit intervals

- Continuously evolving production processes and development tools limit the time of re-use.
- Evolving threats and associated constraints require new assessments not considered during the performed audit.
- No process for the handling of changes within the development environment and development process.

- Limitation of the time interval between two audits
  - Shall not be more than two years
  - Only applicable if no security relevant changes occur

Formal Re-use
Scheme specific process

- The first re-use concepts are limited to the re-use by the same lab, therefore a new process was defined
- Re-use is split in two evaluation tasks
  - Product type specific evaluation tasks
    - Evaluation of process descriptions and tools that are the same for all products of the same type. These parts can be re-used.
  - Product specific evaluation tasks
    - Evidence for a specific product that the evaluated processes and tools are used during the development. These parts are subject to the specific product evaluation.

(German scheme interpretation AIS38)

Formal Re-use

Re-use by other evaluation labs possible

- Re-use of evaluation results from one lab are reusable by another lab
  - Increasing number of evaluations
  - Usage of the same subcontractor by different developers
- Re-use approach is based on
  - Common understanding of the audit tasks of the evaluations labs
  - Common life cycle definition for similar products
  - Re-use under the same certification body

Site Certification Process
Motivation and Limits

- Evaluation of a site independent of a product
- To be used in product evaluations by multiple developers and different evaluation labs
- Type specific development/production process
  - Limitation: not any site for any product
- Constraints given by other evaluation input e.g. Protection Profiles

Site Certification Process
General Approach

- Basis: **Site Security Target (SST)** as analogon of Security Target in product evaluations
- **Splicing**
  - Combine
    - Certified Sites
    - Evaluated non-certified portions of Certified Sites
      - to meet additional ALC requirements (e.g. for a product evaluation)
    - Evaluated non-certified Sites (e.g. for a product evaluation)
- **Integration**
  - Integration of all combined Sites into a product evaluation
  - Special focus on Life Cycle Definition of the TOE involving all Sites
- Supporting Document Guidance: Site Certification, CCDB-2007-11-001, Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, Revision 1, October 2007

Site Certification Process

Site Security Target (SST)

- Defines **Security Problem Definition**
  - consisting of
    - Assets
    - Threats
    - Organisational Policies
  - to be covered by
    - Security Objectives
- **Security Assurance Requirements**
  - ALC requirements only
  - Minimum set of ALC requirements
  - Refinements for specific product types shall be included if applicable, e.g from a PP
  - Rationale that requirements meet objectives

Site Certification Process

Site Security Target (SST) (cont.)

- **Site Summary Specification**
  - Link between actual evidence of the Site and assurance requirements
  - Identification of evidence
  - Description of aspects how the Site meets the assurance requirements
  - Tracing of those aspects to the actual evidence

- **Security Assurance Requirements**
  - ALC requirements only
  - Minimum set of ALC requirements
  - Refinements for specific product types shall be included if applicable, e.g from a PP
  - Rationale that requirements meet objective

Site Certification Process
Site Security Target (SST) (cont.)

- **Assumptions**
  - Different focus than for product evaluation where assumptions cover the TOE environment
  - Vital to clearly define interfaces to the Site to be certified
    - e.g. for delivery aspects
  - Not covered by evaluation methodology in the Guidance Document
    - Prerequisite for Splicing of Sites

Site Certification Process
Evaluation Criteria

- **Guidance Document**
  - Covers
    - General Site Certification approach
    - Contents of SST
    - Evaluation of SST (AST)
- **Open Items**
  - Evaluation of ALC requirements
    - High-level: AST under Site Summary Specification of SST
    - Site audit
    - ALC report
  - Assessment of security measures (JIL document on requirements for site visits)
  - Evaluation of Assumptions

Site Certification Process

The devil is in the detail

- **Standardisation makes the difference**
  - Example mask shop
    - defined input and defined output
    - processes: product type specific (characteristics of a specific product is not relevant)
  - Example personalisation office
    - defined input and output is the finished product
    - processes: product specific (it can be checked if the site provides sufficient physical security and if the data management is appropriate but within a site certification it cannot be evaluated whether the personalisation protocol of a specific product prevents manipulation or disclosure during the personalisation, collusion with one insider)

Product Evaluation

Integration into a product evaluation

- **Site Security Target(s) must be used to check**
  - Scope of the site evaluation (coverage of tools and processes)
  - Assumptions of the site are fulfilled
    - Assumptions on required information (specifications, descriptions, delivery process)
    - Assumptions on the properties of the semi-finished product
  - Assurance requirements for the product are covered by the site evaluation(s)
- **Product specific evidence from a certified site**
  - Release certificate for the product under evaluation from the evaluated site
- **Consistency check of the over all life cycle description for the product under evaluation**

Outlook

- Site Certificates independent of product evaluations
- Evaluation and Certification that general security procedures independent of a specific product are applied
- Requirements on development environment are the same for a product evaluation and a site evaluation
- Very limited flexibility for adaption of processes at a certified site for a specific product
- Efficient re-use
- Some open items