

Monitoring Common Criteria for Smart Security Devices

10th ICCC

Tromsø, 22-24 September 2009

ISCI-WG1

Convenor : Françoise Forge

Agenda

- History
- Contribution to CC
- Next steps
 - Minimizing Cost & Time factors
 - High level & confidence dilemma
 - keeping confidence with less reporting
 - Formalizing good practices
- Conclusion
 - CC “sustainable” improvement
 - ISCI next tasks

History- Eurosmart initiative

- Eurosmart,
 - International non-profit association founded in 1995 in Brussels
 - 24 companies of the Smart Security industry (smart card manufacturers, semiconductors, terminals, issuers)
 - Promotion and standardization of smart secure devices and smart secure systems
 - Harmonization of security evaluation schemes
- ISCI created by Eurosmart
 - To define, support and promote a universal framework for security evaluation and certification methods, tools and procedures, based on internationally accepted standards.
 - Fair, high quality, comparable, standardised evaluations.
 - To involve all actors within the evaluation process, with the goal to improve smart card evaluation time & cost
 - To provide supporting documents to guide smart card evaluations

History- Motivation

- Smart security device is a small but complex product
 - 2 pieces built separately by different manufacturers, evaluated as a whole.



- with fast evolution
 - From smart cardto smart security devices



- Evaluation strategy and methodology needed
 - Multi parts composite evaluation
 - Minimize evaluation cost overhead
 - Answer to short time to market



ISCI International Security Certification Initiative

History- ISCI contributors

- Two working groups
 - WG1 for methodology
 - WG2 - known as JHAS for technical issues (attack potential & vulnerabilities)
- ISCI-WG1 contributors
 - Smart card manufacturers, developers, Issuers, IC manufacturers



- Evaluation laboratories



- Certification Authorities



Contribution to CC- main achievements

- Kickoff meeting November 2003
- Started straight with the monitoring of CC V3
 - Commenting draft proposals till publication of CC V3.1 in July 2006
 - Supporting ALC class revision
 - Supporting **Site Certification** process definition (reuse of certified ALC evidences) developed by BSI, reviewing and commenting final supporting document (CCDB-2007-11-001)
- Developed the Vulnerability Analysis Grid to support French banking cards organization in their risk analysis
- Supporting and advising on any CC evaluation issues reported to the group (interpretations , protection profiles...)
- Updating CC supporting document, creating new ones...

Contribution to CC– supporting documents (1)

- Application of Attack potential to smart cards 2-7(JHAS)CCDB-2009-03-001 (Mandatory)
 - Defines known attack paths for smart cards , attack quotation table and vulnerability analysis rating. Regularly updated
- Composite Product evaluation for smart cards and similar devices 1-0 CCDB-2007-09-01 (Mandatory)
 - Defines Developer and evaluators task for composite evaluations
 - Compliant with CC V2.3 and CC V3.1
- ETR template for composition 1-0 CCDB-2007-09-02 (Mandatory)
 - Defines mandatory information to put in an ETR that will be used in composite evaluation
- Application of CC to IC 3-0 CCDB-2009-03-002 3-0 (Mandatory)
 - Reviewed and updated for CC V3.1

Contribution to CC– supporting documents (2)

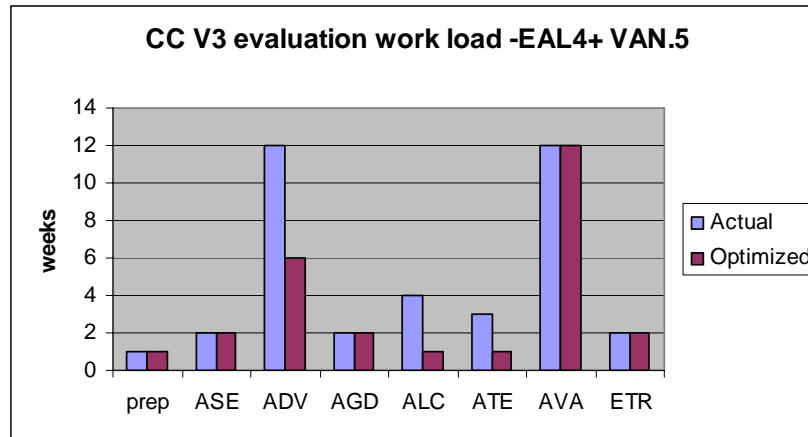
- Security Architecture (ADV_ARC) – for smart cards and similar devices
 - Final version completed January 2008
 - Released as JIL trial supporting document
 - Collecting feedbacks from CC V3.1 evaluations
 - Updated version for release to CC supporting document beginning 2010
- Reviewing “site visit” proposal from JIL
 - Objective is to define consistent approach that should be followed by evaluations labs, and Certification bodies when performing actions relating to site visits.
 - ISCI-WG1 proposed to have a ‘best practices’ approach rather than requirements too close from implementation.
 - Review next version by Q4 2009

Contribution to CC -CCV4 monitoring

- 9th ICCC presentation: CC works!
 - Developer's defined protection profiles, technology oriented guidance, optimization of previous evaluation reuse (site certification)
 - No dramatic change as it costs to adapt process, but simplification with clear benefits in terms of cost and time reduction for same level of security.
- CCV4 CCDB working groups
 - Meaningful reports (Canada)
 - Smart card customers (banks, governments) require details vulnerability analysis and test results.
 - information being confidential, only reference is provided in the public ETR ; confidential documents are provided to our customer under NDA.
 - Predictive assurance (Germany)
 - Smart card manufacturer currently use faster re-evaluation process, with previous results, using change tracking tools, security impact analysis
 - Defining the threshold for self re-evaluation depends on product type

Next steps – Minimizing Cost & Time factors

- Analyzing evaluation work load
 - Proportional to level of evaluation and complexity of product
 - More documentation, more evaluators analysis and reporting
 - Recent study* showed possibility to reduce the total workload for smartcard evaluation including AVA.VAN5 up to 30% by optimizing the use of CC (dedicated assurance packages, dedicated CEM refinements)



- Evaluators have all information they need to assess confidence in high security but spend a lot of time on reporting to Certification Authority.

* Thales-CEACI & Gemalto

Next steps- High level & confidence dilemma

- CC methodology aims ensuring **comparability** between evaluation results, **repeatability** and **objectivity** of the results,
- To achieve this, precise rules have been developed ,
 - CEM precisely defines evaluators work units but too precisely the way the results/inputs have to be recorded
 - Higher level confidence requires more information that evaluator shall examine/check to determine that information is complete and accurate.....
 - Evaluator has to provide precise tasks results through reporting
- Removing reporting would compromises the CC properties of confidence, comparability and repeatability of results
- How to minimize the costly reporting, without altering those properties?

Next steps- keeping confidence with less reporting (1)

- CC requires information , not necessarily paper documents
 - ADV and ATE represents the bigger part of information to check
 - The required information usually exist (functional specification, code with comments, test script, test campaigns..).
 - Developers often write paper documentation out of source code, with errors checked by evaluator who requires corrections.... The infernal circle!
- When getting to huge amount of information is it really possible for an evaluator to look at every thing and check 100%?
 - ADV_IMP.1 allows sample to gain confidence that all the information needed [] has been supplied.
- Why not extending sampling to other tasks?
- What are the conditions allowing to keep confidence, repeatability and comparability ?

Next steps- keeping confidence with less reporting (2)

- What can be done on ADV?
 - Functional specification, high level TOE design and source code with comments at the minimum (should) exist;
 - Dedicated tools exist, allowing traceability of security requirements, generation of documentation out of the source code (e.g. Javadoc), others allow analysis of specific information
 - Further confidence can be gained using static/dynamic source code analyzer*
- What efforts are required?
 - Developers shall use tools & techniques ensuring repeatability and reusability of information (a matter of quality of development),
 - Evaluators will need to be trained on TOE and tools usage, but then easily assess they have all information required.
 - Assurance criteria & CEM could be modified to allow different forms of documentation when tools give confidence in a secure development

* High efficient evaluations: CCN presentation 8th ICCC Rome 2007

Next steps- keeping confidence with less reporting (3)

- What can be done with ATE?
 - Test plans, scripts, scenario, test campaigns, test coverage matrix and test results (should) exist,
 - Developer uses standard or dedicated tools that are usually shared with evaluators,
 - Evaluator can perform sampling to gain assurance on test completeness, replay partially campaigns, modify parameters for the Independent Testing....
- What efforts are required
 - Developers shall use tools & techniques ensuring repeatability and reusability of test information
 - Evaluators will need to be trained on test tools usage
 - Assurance criteria & CEM could be modified to allow different forms of test results documentation and assess usage of specific tools giving confidence in the completeness of test .

Next steps- Formalizing good practices

- Good practices are already currently used
 - ALC class evaluation is minimized with the reuse of former evaluation results. Site Certification Process, formalizes this reuse.
 - Implementation of change tracking, Security Impact Analysis allows fast re-evaluation.
 - Modular design avoids rechecking 'unchanged parts' from a previous evaluation.
 - Sharing development and test tools with evaluator is also common practice
- Formalizing the good practices and allowing more evidences check and sampling, reduce the evaluator work load

Conclusion - CC “sustainable” improvement

- The information required by the CC exist when a quality development process is used,
- Developers do the job, the information exist and should be made available to evaluators ,
- Assessment of information completeness and accuracy, should be achieved using methodology and tools, ensuring repeatability.
- ISCI is in favor of CC ‘sustainable’ improvement
 - No dramatic change that will cost in updating present process
 - No additional criteria that would lead to other constraints
 - But upgrading the methodology, opening to usage of tools and evidences to provide the comparability and repeatability of information as require by the criteria.

Conclusion –ISCI next tasks

- Efficiency of guidance has been proven in CC evaluation optimization for smart cards.
- ISCI will continue on the successful trail with developers, evaluators, Certification Authorities
 - Identifying the different techniques suitable to ensure secure development and testing repeatability
 - Defining acceptable possible solutions with all partners
 - Developing the solution and formalizing in guidance
 - Submitting to JIL and CCDB

Thank you !

Questions ?