

CC approaches to the certification of the components of a system when the system certification is not possible

V.Bagini, F.Guida, C.Majorani, R.Menicocci, M.Orazi

FUB-OCSI

Summary

- **Preliminary assumptions**
- **System evaluation issues**
- **Alternative approaches to system evaluation**
 - TOE composition
 - CCDB-2007-09-01
 - Cross evaluation of components
 - Vertical Assurance Packages (just a taste)
 - Additional activities on Operational Environment (just a taste)
- **Metrics to evaluate the approaches (just a taste)**

Preliminary assumptions

- The system of interest has a known number of components
- Each component is completely specified from both a functional and a security point of view
 - A description of the Security Objectives of both the system and its environment is available
- For some reasons the certification of the system as a whole is not practicable
 - Next slides will try to clarify such reasons

System evaluation issues (1/6)

- Issue I: The evaluation activities could have to be performed at different times to fulfill development needs
 - Some components could require to be developed before others

System evaluation issues (2/6)

- Issue II: The evaluation activities could have to be performed at different times to reduce evaluation cost
 - Some components could have already been evaluated and the developer would like to reuse the evaluation results for system evaluation (Issue IIa)
 - The evaluation of the whole system (waiting for all the components to be developed and available at the time of system evaluation) could require more time than the system life cycle, making the results of system evaluation useless (Issue IIb)

System evaluation issues (3/6)

- Issue III: Detail level of evaluation evidences available for different components could differ because of lack of cooperation between entities involved in development processes (this issue can be solved evaluating each component to the assurance level that can be achieved with the evaluation evidence available for the component, see Issue V)

System evaluation issues (4/6)

- Issue IV: Detail level of evaluation evidences available for different components could differ because of lack of cooperation between entities involved in evaluation processes (in case one of the components of the system has been evaluated with an assurance level adequate to the assurance required by system evaluation)

System evaluation issues (5/6)

- Issue V: Different components of the overall system could require different evaluation assurance level
 - The system could have to fulfill different rules corresponding to different assurance levels for separate domains of functions or Security Objectives: instead of evaluating the whole system to the highest level of assurance required, the developer/sponsor could search solutions for differentiating the assurance provided by every single domain of functions or Security Objectives

System evaluation issues (6/6)

- Issue VI: Implementations of system components could be not available altogether in the same evaluation facility

Alternative approaches to system evaluation (1/2)

- TOE composition (CC supported approach)
- CCDB-2007-09-01 *Smart Card evaluation supporting document* (CC supported approach)
- Cross evaluation of components
 - Performing two separate evaluations (preferably with the same assurance level) of components A and B where a single evaluation is based on the approach of putting component B in the Operational Environment of component A and vice versa

Alternative approaches to system evaluation (2/2)

- Vertical assurance packages
 - Previous works
 - Challenging the concept of one evaluation per level, Nils Tekampe, 8ICCC, Rome 2007
 - Effective evaluations outside the EAL framework: Vertical Assurance Packages and Profiles, J.Emilio Rico 10ICCC Tromsø 2009
- Additional activities on Operational Environment

TOE composition

- TOE composition: the ACO class
- TOE composition purposes
- Input required by ACO activities
- Composition issues
- Feasibility

TOE composition: the ACO class (1/2)

- Specifies SARs that are designed to provide confidence that a composed TOE will operate securely when relying upon security functionality provided by previously evaluated SW,FW or HW components
 - ACO requirements focus analysis on interfaces between components
- In a composed TOE one component (dependent) relies on the services provided by another component (base)

TOE composition: the ACO class (2/2)

- Composed TOE evaluations are performed under the assumption that the sponsor of the composite evaluation is the same of the dependent component evaluation

TOE composition purposes

- Gain confidence in the security functions of a TOE that is the combination of two or more successfully evaluated components without
 - having to re-evaluate the composite TSF
 - any further development
- Dependent component developer does not have access to the type of information necessary to perform an evaluation of both the dependent and base components at EAL2 or above

Input required by ACO activities (1/2)

- Dependent component evaluation evidences
- Base component
- Base component interfaces (TSFI and not TSFI required by dependent component to provide its security functions)
 - specifications
 - test documentation

Input required by ACO activities (2/2)

- Base component guidance documentation
- Residual vulnerabilities in the base component, as reported during the base component evaluation (this is required for the ACO_VUL activities)

Composition issues (1/2)

- Composed TOE evaluated with Composition Assurance Packages (CAP) are not easily comparable between each other and to TOE evaluated using the EAL packages
- Stepwise composition has not been analyzed (see CCPart3, Annex B §611)
- The base component documentation required by CAP evaluations is not always completely available to the dependent component developer

Composition issues (2/2)

- According to the current CCRA Web site, no CAP certification has been issued and no supporting documentation for CAP evaluations is available
- The maximum attack potential for CAP evaluation is Enhanced-Basic

Feasibility

- TOE composition approach can be taken when system evaluation is not practicable because of any of the following issues :
 - Issue I, if the base component is developed before the dependent component
 - Issues IIa and IIb, if the base component is evaluated before the dependent component
 - Issue IV, if the dependent component developer is also developer/sponsor of the composite evaluation (CCPart3 par.17 §472)

CCDB-2007-09-001

- Description of the approach
- Pros and cons against composition
- Nature of the TOE
- Cooperation between entities
- Feasibility

Description of the approach (1/2)

- CCDB-2007-09-001 *Composite product evaluation for Smart Cards and similar devices*
- Composite TOE = (at least) 2 components
 - Platform = HW* component previously evaluated and certified at some EAL (*at least partially)
 - Application = SW component (generally) not evaluated
- Security mechanisms provided by the platform (base component) are managed by the application (dependent component)

Description of the approach (2/2)

- Composition-based approach not used because
 - It does not allow direct comparison with a similar system certified after a single evaluation
 - It is not applicable if resistance to an attack potential higher than Enhanced-Basic is required
- The Composite TOE is evaluated at an EAL
 - Ad hoc refinements to some CC v2.x and v3.1 SARs are defined (the approach is applicable to each EAL)
 - The EAL of the composite TOE is assumed to be equivalent to the EAL of the platform or lower

Pros against composition

- Higher assurance may be obtained
 - EAL certification, resistance to any attack potential
- One evaluation is required instead of two
 - Only EAL evaluation of the composite TOE is needed (platform previously evaluated)
 - Composition would require EAL evaluation of the application and CAP evaluation of the system
- The evaluation process is easier to iterate
 - An evaluated composite TOE can be the platform for a new composite TOE

Cons against composition

- The CCDB-2007-09-001 approach can be applied only under some assumptions (which are not required by composition) about
 - Nature of the TOE
 - Cooperation between different entities

Nature of the TOE (1/2)

- The TOE must consist of
 - A previously evaluated and certified platform and
 - One or more additional applications
- Examples of composite TOE are explicitly considered by CCDB-2007-09-001
 - Smart card (platform = IC, application = OS)
 - Java card (platform = RE, application = applet)
 - Crypto box (platform = HW, application = specific cryptographic application)

Nature of the TOE (2/2)

- (cont.) Secure terminal containing a SAM/HSM (platform = SAM/HSM (server), application = SAM/HSM-external terminal software (client))
- Composite TOEs corresponding to different examples have been actually evaluated
- The composite TOE model could be generalized
 - Actual examples beyond the CCDB-2007-09-001 ones could be sought
 - Assumptions on the nature of the components (HW-based platform and purely SW applications) could be relaxed

Cooperation between entities (1/2)

- Some examples of documentation deliveries required by composite evaluation are the following (see CCDB-2007-09-001 for a complete list)
- The Application Developer needs all the information related to the platform security mechanisms the application has to manage
- Such information must be provided by the Platform Developer in form of a guidance or user's manual

Cooperation between entities (2/2)

- The Composite Product Evaluator and Certification Body need platform evaluation documents that are generally not (completely) public, as
 - Security Target
 - Certification Report
 - ETR_COMP (defined in CCDB-2007-09-001) compiled from the standard platform ETR
- Such documents must be provided by the Platform Evaluator and Certification Body

Feasibility

- CCDB-2007-09-001 approach can be taken when system evaluation is not practicable because of any of the following issues:
 - Issue I (different components can be developed at generally different times)
 - Issue II (the platform has already been evaluated)
 - Issue V (the assurance for the overall system can be lower than the one obtained for the platform)

Cross evaluation of components

- TOE environments in CC
- The Operational Environment (OE)
- OE-related evaluation actions
- OE issues
- A way to put a component in the OE
- Effects on the evaluation
- Cross evaluation of components issues
- Real case examination: CWA 14169
- Feasibility

TOE environments in CC

- Different TOE environments can be considered
 - Operational environment (OE) (formally defined in CC v3.1)
 - Test environment (formally defined in CC v3.1)
 - Development environment (formally defined in CC v3.1 but not of interest for this presentation)

The Operational Environment (OE)

- ***operational environment*** - *environment in which the TOE is operated* (CC v3.1)
 - Not so helpful to derive a model!
- The evaluation activities refer to the OE by means of
 - Assumptions
 - Security Objectives for the Operational Environment

OE-related evaluation actions (1/3)

- The evaluator is required to perform the following actions (we don't report hierarchical actions):
 - Check for correct description of Assumptions for OE in Security Problem Definition, if applicable (ASE_SPD.1-4)
 - Check for correct description of Security Objectives for OE and of their Rationale: (ASE_OBJ.1-1, ASE_OBJ.2-3, ASE_OBJ.2-6)
 - Check if Security Objectives for OE correctly address the dependency of SFRs, if applicable (ASE_REQ.1-9)

OE-related evaluation actions (2/3)

- Check if operational guidance describes the security measures to be followed in order to fulfill the Security Objectives for the OE (AGD_OPE.1-6, AGD_OPE.1-8) (*)
- Check if the installation procedures describe the steps necessary for secure preparation of the OE in accordance with the Security Objectives in the ST (AGD_PRE.1-2, AGD_PRE.1-3) (*)
- (*) It could be hard to complete these activities if an instantiation of OE is not available during the evaluation

OE-related evaluation actions (3/3)

- Check consistency between the Security Objectives for the OE and test environment (as provided to evaluators) during functional testing, independent testing and vulnerability assessment activities (ATE_FUN.1-3, ATE_IND.1-1, AVA_VAN.1-1, respectively)

OE issues

- The Standard CC doesn't require an instance of OE as an input for evaluation activities
 - The model of OE derivable from the OE Security Objectives couldn't be enough to perform the OE-related evaluation activities required by AGD, ATE and AVA classes
- The standard CC doesn't provide means to end user to check if its OE is consistent with the one defined in ST (through security objectives for OE!)

A way to put a component in the OE

- The TOE overview describes how the TOE A interacts with the component B included in the OE (B can be defined in the TOE overview or in an additional ST section (e.g., terminology))
- In the Assumptions the component B is declared to be in the OE of the TOE A
- The component B is in charge of some Security Objectives for the OE of the TOE A

Effects on the evaluation (1/3)

- All the evaluation activities that must take into account the OE should consider the component B present in the OE of the TOE A
- For this purpose the characterization of B should be completed by SFRs and such SFRs are also useful to put constraints in component B evaluation

Effects on the evaluation (2/3)

- A link between the respective STs of A and B (logical connection) must be established (e.g., by means of suitable PPs)
 - To allow cross evaluation of A and B it should be assured that
 - Security objectives (and requirements*) for the TOE in the ST of A include Security Objectives (and requirements *if included) for the OE attributed to A in the ST of B (and vice versa)

Effects on the evaluation (3/3)

- Presence of B during the evaluation of A (and vice versa)
 - The evaluation of A cannot be performed using an already evaluated B if the evaluation of B requires an already evaluated A
 - A correct (and possibly partial) implementation of B could be sufficient
 - Correctness of the implementation should be assured by suitable tests (if such tests must be performed during the evaluation of A, suitable evaluation activities must be introduced)

Cross evaluation of components issues

- This approach misses the assurance that the evaluation could provide on the effects or real interaction between components A and B
- This approach requires a deeper analysis

CWA 14169 (1/3)

- *Secure signature-creation devices (SSCD) EAL 4+*
- 3 Types of SSCDs
 - SSCD Type 1: Key pair generation
 - SSCD Type 2: Signature creation
 - SSCD Type 3: Key pair generation and Signature creation
- For each SSCD Type a PP that conform to CC v2.1 has been evaluated

CWA 14169 (2/3)

- In the Type 1 PP, Type 2 SSCD is part of the OE and vice versa
- Type 1 and 2 PPs establish a link between conformant STs
 - Security objectives (and requirements) for the TOE in the Type 1 PP include Security Objectives (and requirements) for the OE attributed to the Type 1 SSCD in the Type 2 PP (and vice versa)

CWA 14169 (3/3)

- By consequence, cross evaluation of Type 1 and 2 SSCDs is possible
 - The cross evaluation approach is used by SSCD designers who decide to employ dedicated devices for (resource-consuming) key pair generation (see *CWA15355 Guidelines for the implementation of Secure Signature-Creation Devices*)
- Type 1 and 2 SSCDs are separately evaluated (both at EAL 4+)

Feasibility

- The cross evaluation of components can be taken when system evaluation is not practicable because of any of the following issues:
 - Issue I
 - Issues II and IV, if the components are logically connected (see before)
 - Issues III and V, if it is acceptable to evaluate the components at different levels
 - Issues VI, if it is sufficient to have only a partial representation of B in environment of component A

Vertical Assurance Packages (VAP)

- The main idea is to apply different assurance packages to different domains in the same TOE
- The domain can be related to
 - Security Objectives
 - Security Functional Requirements
 - Security Functions
- The VAP approach could address the issue of different package of assurance required by different components of the whole system

VAP, Open Issues

- Is still not mature
- Would the VAP-based evaluation be recognized by CCRA ?
- Require deeper inspection

Feasibility

- VAP approach can be taken when system evaluation is not practicable because of any of the following issues:
 - Issues I, IIa and IIb, if there is a one-to-one correspondence between system components and functional domains and if there are no dependencies between domains
 - Issue V

Additional activities on OE

- Performing evaluation activities on OE (if applicable) and/or on support HW/FW/SW defined in TOE overview:
 - Known vulnerability analysis or
- No assurances provided for OE security functions

Feasibility

- The Additional activities on OE approach can be taken when system evaluation is not practicable because of any of the following issues:
 - Issue I
 - Issues III and IV, if the component for which the evaluation evidences aren't available is the one outside the TOE
 - Issue V, if the additional activities fulfill the assurance requirements stated in the rules

Metrics to evaluate the approaches

- To define some kind of distance between a selected approach and the optimal solution (canonical certification of the system as a whole), at least the following aspects should be taken into account
 - Amount of evaluation activities to be performed
 - Number and significance of identified potential vulnerabilities
 - Completeness of functional and penetration tests to be performed