Non-Interfering Composed Evaluation

How to Exchange Components without Re-Evaluation?

Igor Furgel, Viola Saftig, Tobias Wagner (T-Systems)
Kevin Müller (Airbus Group Innovations)
Reinhard Schwarz (Fraunhofer IESE)
Axel Söding-Freherr von Blomberg (OpenSynergy)

Contact: Igor.Furgel@t-systems.com

MILS Workshop 2016, in cooperation with HiPEAC’16, Prague

15/03/2016
Industrial use cases have shown limitations of current compositional methodologies

New Common Criteria **evaluation method** for evaluating one composed *target of evaluation* (TOE) based on two (or more) already certified TOEs

Application cases
State of the Art and Motivation

- **ACO / CAP (Composed Assurance Package)**
  - Composed certification of already certified components
  - Just conformance checks at component’s boundaries without proof of execution boundaries (no non-interference proof)
  - Up to CAP-C (attack potential: enhanced basic, i.e. EAL 4 like)
  - No conformance claim to an EAL package possible
  - Not widely applied in the real world

CCDB Composition

- Composite certification of already certified platform and non-certified application using this platform
- Using the development documents and the vulnerability analysis of platform to ensure security properties of final Composite TOE
- EAL package claim is possible
- No limitation on assurance level, i.e. EAL 7 possible
- **Drawbacks:**
  - Re-usability of evaluation results for the application is difficult
  - Effort for re-certification may be quite high
Motivation

Puzzle Composition

- Exchange a system component with interface/function-compatible one
- Use-cases
  - Product from Vendor-A is replaced by product from Vendor-B
  - Flexible in-the-field update

Definitions

a) **Component TOE**: input to the evaluation; two or more already certified products

b) **Composed TOE**: output of the evaluation; one certified final product based on the set of Component TOEs

c) **Interaction**: the allowed communication of two certified Component TOEs according to a given information flow policy inside the Composed TOE

d) **Interference**: any communication or influence on a Component TOE that is not explicitly authorized by the certified security policy for this Component TOE
New methodology based on *non-interfering* between Component TOEs

- *Interaction* between Component TOEs possible only according to a given information flow policy inside the Composed TOE

- *Interference* is *not* possible inside the Composed TOE
Idea and Principle of Non-Interference

- Execution of one Component TOE does not undermine the certified security policy of other Component TOE.
- The complete internal state of each Component TOE is well-defined and known at any time.
- *Non-interference between the Component TOEs shall be evidently demonstrated*
  - The non-interference property of the Component TOEs shall be verified during the dedicated evaluation processes of each Component TOE ➔ non-interference analysis by responsible Component TOE evaluator.

- This methodology is a *peer-to-peer* one: it treats Component TOEs in a symmetric way as equal entities from the point of view of their non-interference.
Step 1: *A priori* analysis of the Component TOEs

- *A priori* evidence of fundamental non-interference between the Component TOEs
  - This *a priori* determination is one of the principal distinctions between the new methodology and the ACO and CCDB methodologies relying on an *a posteriori* determination of the level of non-interference between the Component TOEs

- Preparing non-interfering composed evaluation
- Analysis of all possible internal states of Component TOEs
- Analysis of non-bypassability and non-tampering
- Yielding a list of non-interference requirements
  → Single Components need to be made suitable for this approach
Step 2: Evaluation of the Non-Interfering Composed TOE

- Relies on the analysis of certified non-interfering properties of the Component TOEs (see Step #1)
- Analysis of mapping between the requirements of each Component TOE with the SFRs of the other Component TOEs
- Analysis of functional interactions between Component TOEs
- Verification of the fulfilment of non-interference requirements
- If necessary (incomplete requirement matching) perform reduced vulnerability assessment
Application Case 1

- Non-Interfering Composed TOE for Base and Dependent TOE

Non-interference is shown if:

1. The Base TOE strictly and evidently separates the application from the Base TOE

2. The fulfilment of all requirements for running the application in a non-interfered way (wrt. app-certificate) can be evidently guaranteed by the Base TOE

3. The fulfilment of all requirements for running the Base TOE in a non-interfered way (wrt. base-certificate) can be evidently guaranteed by the application
Application Case 2

- Non-Interfering Composed TOE:
  - Interaction via the underlying platform
Interaction via the underlying platform

**Non-interference** is shown if:

1. The fulfilment of all requirements for executing the Component TOE 1 and TOE 2 in a non-interfered way, as imposed by their certificates, can be evidently guaranteed by the Component TOE 3 (underlying platform) and by its *concrete configuration*.

2. The fulfilment of all requirements for executing the Component TOE 3 (underlying platform) in a non-interfered way, as imposed by its certificate, can be evidently guaranteed by the Component TOE 1, Component TOE 2 and given a *concrete configuration* of the Component TOE 3.
Separation Kernel as Base TOE

Separation Kernel
- Certifiable Operating System layer
- Separates system and processing resources
- Provides separated runtime environments to host applications
  → mandatory property to evidently proof non-interference
- Provide controlled communication between runtime environment
  → controls interactions and defines interfaces/access point to applications

MILS Architecture
- Low-criticality Partition
- Medium-criticality Partition
- High-criticality Partition

Hardware
(CPUs, memory, and devices)

Network
Actuator

Use Case: Non-Interfering Composed Firewall TOE

**Base TOE:**
Certified Separation Kernel (with HW)

**Dependent TOE 1:**
Generic Gateway (R, T)

**Dependent TOE 2:**
Specific Protocol Filters

**Challenges:**

1. Evidently secure (= certified) Composed Firewall using filter configuration A
2. Evolutionary Evaluation by enhancing filter configuration A (updates)
3. Incremental Improvement by adding filter configuration B (from the box of certified filters)

Back to the motivation

Puzzle Composition

- Exchange a system component with interface/function-compatible one
- Use-cases
  - Product from Vendor-A is replaced by product from Vendor-B
  - Flexible in-the-field update

Summary and Benefits

- Common Criteria does not currently offer a highly flexible methodology for compositional evaluation regarding:
  - Reusability of single components
  - Independent evaluation of components
  - Compositional assurance of products from different vendors

- **Non-interfering** methodology shifts effort for vulnerability assessment to component evaluation to *avoid duplication of effort* during the compositional step when performing re-evaluations (however for initial certification, efforts likely similar to CCDB composite methodology)

- Evaluation effort for **Non-Interfering Composed TOE** can significantly be reduced due to the *non-interfering property of* and the related *evidence for* Component TOEs

Summary and Benefits (cont.)

- Targets certifications of dynamic high-assurance systems

- Conformance claim to each **EAL** package is possible

- Enables a verdict for the TOE resistance to attacks by an attacker with even *high* attack potential

- A Component TOE (e.g., an application) can be replaced with less effort:
  - A supplemental application can be added to an already existing Composed TOE by only evaluating the new application Component TOE

- The new evaluation methodology for non-interfering Composed TOE enables a higher business flexibility for the vendors and operators of Composed TOEs

---

EURO-MILS CONTRACT NO: 318353

“This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 318353.”

If you need further information, please contact the coordinator:
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55   Fax: +43 4242 233 55 77
E-Mail: coordination@euromils.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.
BACKUP Slides or to be used
Sketch of a Non-Interfering Composed TOE: consisting of physically separated Component TOEs
Sketch of a Non-Interfering Composed TOE:
same execution environment and direct interaction
\((N^*(N-1)/2\) evidences)

Non-Interfering Composed Evaluation, I. Furgel, K. Müller, T. Wagner, 2\(^{nd}\) MILS -WS, Prague 2016
MILS architecture is the enabler for high-assurance compositional certification

The core is Separation Kernel

Components under certified composition
- Hardware, Separation kernel, Applications
Compositional Certification: Scenario

- MILS architecture is the enabler for high-assurance compositional certification
- The core is **Separation Kernel**
- Components under certified composition
  - Hardware, Separation kernel, Applications

- MILS architecture is the enabler for high-assurance compositional certification
- The core is Separation Kernel
- Components under certified composition
  - Hardware, Separation kernel, Applications

Compositional Certification: Scenario

T - composition
Compositional Certification: Scenario 1

- **Puzzle Composition**
  - Exchange system component with interface/function-compatible one
  - Use-cases
    - Product from Vendor-A is replaced by product from Vendor-B
    - Flexible in-the-field update

---

Diagram:

- **Low-criticality App**
- **High-criticality App**
- **New Medium-criticality App**
- **MILS Platform (Separation Kernel)**
- **Hardware (CPUs, memory, and devices)**
- **Network**
- **Actuator**