Non-Interfering Composed Evaluation

Igor Furgel, Viola Saftig, Tobias Wagner
T-Systems International GmbH
{Igor.Furgel|Viola.Saftig|Tobias.Wagner}
@t-systems.com

Kevin Müller
Airbus Group Innovations
Kevin.Mueller@airbus.com

Reinhard Schwarz
Fraunhofer IESE
Reinhard.Schwarz@iese.fraunhofer.de

Axel Söding-Freiherr von Blomberg
OpenSynergy
Axel.vonBlomberg@opensynergy.com

ABSTRACT

§1 In this document an extension of the concept for the evaluation of a Composed TOE is presented. This approach, namely the Non-Interfering Composed TOE, is based on the traceable property of the non-interference of two certified TOEs.

CCS Concepts

Systems security • Software and application security

Keywords

security composition; security evaluation and certification; Non-Interference; Separation kernel; MILS (Multiple Independent Levels of Security); Virtualization; Hypervisor.

1. Introduction

§2 In Common Criteria, Version 3.1 [1-4], the assurance class *Composition* (ACO) and *composed assurance package* (CAP)[1] are defined to evaluate a TOE composed of two already certified TOEs that can be identified as one Base TOE and one Dependent TOE (jointly referred to as Component TOEs). To perform an evaluation of the Composed TOE, the interactions between the Base and the Dependent TOEs are analysed relying on additional high-level information (functional behaviour and interaction at external interfaces) provided by the developer of the Composed TOE. The evaluator of the Composed TOE possesses only high-level information about the Composed TOE itself and of the Base and the Dependent TOEs. The evaluator of the Composed TOE can analyse and assess the Composed TOE at most at an assurance level that enables a verdict for the TOE's resistance to attacks by an attacker with at most Enhanced-Basic attack potential (CAP-C, roughly comparable to EAL 4).

§3 Following the ACO methodology, the evaluator also has to perform a vulnerability analysis for each concrete Composed TOE in the rigour as required by the chosen CAP (CAP-A to CAP-C) [3]. Therefore, it is not possible to exchange, for example, the Dependent TOE without re-performing this vulnerability analysis completely. This disadvantage emerges due to the absence of a proof that a Component TOE has a limited functionality within defined execution boundaries. For example, using the compositional methodology of ACO, it is required to show that the Component TOEs do not overwrite each other's memory.

In order to avoid or to significantly mitigate these issues of the ACO, we evolved an evaluation methodology for the *Non-Interfering Composed TOEs*.

[1] CAP is based on the assurance components defined in ACO.

2. Terminology

§4 In the following, the term "*interaction*" implies the allowed communication of two certified Component TOEs according to a given information flow policy inside the Composed TOE as described in the Security Target of the Composed TOE.

In contrast, "*interference*" implies any communication or influence on a Component TOE that is not explicitly authorized by the certified security policy for this Component TOE as laid down in its related Security Target. An example of such interference is one Component TOE bypassing the security policy of the other Component TOE due to improper use of externally visible interfaces (e.g. APIs or implicitly existing interfaces) or invalid modification of environmental properties (e.g. using a bypass via a directly mapped device).

Both – interaction and interference – may also include communication with the environment of the Composed TOE.

§5 "*Non-Interference*" between Component TOEs means that the execution of one Component TOE does not undermine the certified security policy of the other Component TOE as it is defined in the related Security Target specification. In particular, non-interference demands for each Component TOE that its complete internal state is well defined and well-known at any time regardless of the processing status and condition of the other Component TOE. Note that non-interference does not presume the total absence of interactions between TOE components, see §4 above.

3. Non-Interfering Composed Evaluation

§6 The extended evaluation of a Non-Interfering Composed TOE is based on the idea that non-interference between the Component TOEs can be evidently demonstrated. The non-interference property of the Component TOEs shall be verified during the dedicated evaluation processes of each Component TOE, since the corresponding evaluation facilities possess the entire range of information about each Component TOE. The evaluator of the Component TOE shall be able to produce the required evidences, which are below described in detail, by performing a non-interference analysis.

3.1 Differences to Current Methodologies

§7 For the extended evaluation of the Non-Interfering Composed TOE, the fundamental non-interference between the Component TOEs shall be evidenced apriori for each of the Component TOE, i.e., before the extended evaluation of the Non-Interfering Composed TOE is started.

This apriori determination is one of the principal distinctions between the new methodology set out here and the ACO methodology relying on an aposteriori determination of the level of non-interference between the Component TOEs. The new methodology is fully independent of the ACO methodology.

Also the other currently applied method of the CCDB [5] for performing composite evaluation relies on aposteriori analysis of the composed system, e.g. by performing vulnerability analysis. Even if this method of *Composite product evaluation for Smart Cards and similar devices* reaches high evaluation levels (up to EAL7) the effort for re-certification after changing a system component may be very high. Additionally disadvantageous in this method is the absence of a certification scheme allowing to rely on already certified dependent Component TOEs that interact with the Base TOE to limit efforts. The new Non-Interfering Composition methodology set out here targets the reduction of the re-certification efforts since it allows the composition of already independently certified Component TOE.

§8 The evaluator of the Non-Interfering Composed TOE shall rely on these non-interfering evidences provided to him/her. Hence, the evaluator of the Non-Interfering Composed TOE possesses sufficient information (in terms of amount and rigour) for making an assessment of the Non-Interfering Composed TOE up to the highest assurance level defined by the Common Criteria (i.e., EAL 7). This enables a verdict for the TOE resistance to attacks by an attacker with even high attack potential.

The evaluator of the Non-Interfering Composed TOE can also significantly reduce his/her effort for performing additional vulnerability analysis for the Non-Interfering Composed TOE, even to zero: once the non-interfering property of the Component TOEs has evidently been demonstrated, an additional vulnerability analysis of the Non-Interfering Composed TOE shall not be necessary. In such a case, the evaluation process of the Non-Interfering Composed TOE may resemble a simple conformity verification of the fulfilment of boundary conditions (e.g. resource and timing constrains, API usage, etc.) imposed by the security certificates of the Component TOEs.

§9 For developers this apriori evaluation method transfers evaluation efforts from the step of vulnerability analysing and testing of the final aposterori composed system to efforts on analysing, assessing and testing the Component TOEs with additional focus on their non-interference properties. For an initial certification of a composed system the apriori non-interfering evaluation methodology will not reduce the evaluation efforts in total. However, it enables reusability of certified non-interfering Component TOEs for successing non-interfering composed evaluations, regardless whether these Component TOEs are composed in newer versions of the composed system (new releases of version) or in a new composed system having a different security policy definition.

§10 To demonstrate the non-interference, all (explicit and implicit) interfaces between the Component TOEs shall be clearly defined and completely and accurately described. Provided that it is possible to demonstrate non-interference, the evaluation of the Non-Interfering Composed TOE shall rely on the analysis and assessment of this non-interference property between the Component TOEs.

§11 The certificate of a non-interfering Component TOE needs to state the component's capability to take part in a non-interfering Composed Evaluation. Hence, full information necessary for a certificate-conform security composition shall be stated in the security certificates of the related Component TOE. In particular, references to AGD documents required to fulfil the operational environment needs to be clearly identified by the Component TOE's certification reports. If the System Integrator lacks information on these documents, additional work for the composition will be required (e.g. additional vulnerability analysis).

3.2 Constellations

§12 There can be different constellations, to which the new methodology is applicable as addressed here. It is to note that this methodology is a peer-to-peer one from the point of view of assurance (security), i.e. it treats Component TOEs in a symmetric way as equal entities from the point of view of their non-interference.

§13 The first constellation is exactly one as foreseen in the assurance class ACO: there is a Base TOE and a Dependent TOE. They functionally stay in a kind of server-client relationship: the client requests for functional services and the server delivers them. The latter is usually an application, hence, in the following the term "application" will be used interchangeably with the term "Dependent TOE", cf. Figure 1:

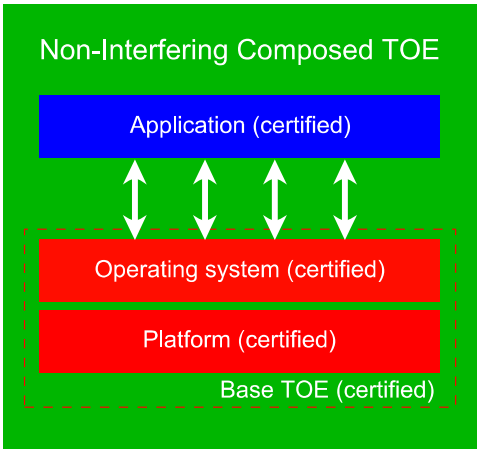

Figure 1: Sketch of a Non-Interfering Composed TOE for Base and Dependent TOEs. The composed evaluation depends on the analysis of the non-interference between the Base TOE and the application – depicted by white arrows.

For example, a certified application runs on a certified Base TOE, such as a separation kernel, including a certified hardware platform. Separation kernels provide isolated runtime environments, so-called partitions, for hosting applications. Non-interference between the application and the Base TOE is shown if:

1. The Base TOE (e.g. the separation kernel) strictly and evidently separates the application from the Base TOE – from both the Base TOE itself and the hardware platform.
2. The fulfilment of all requirements for running the application in a secure (i.e. as certified) and non-interfered way, as imposed by the security certificate of the application (incl. related AGD contributions), can be evidently guaranteed by the Base TOE.

3. The fulfilment of all requirements for running the Base TOE in a secure (i.e. as certified) and non-interfered way, as imposed by the security certificate of the Base TOE (incl. related AGD contributions), can be evidently guaranteed by the application.

§14 The second constellation is when the Component TOEs are connected with each other via an external bus:

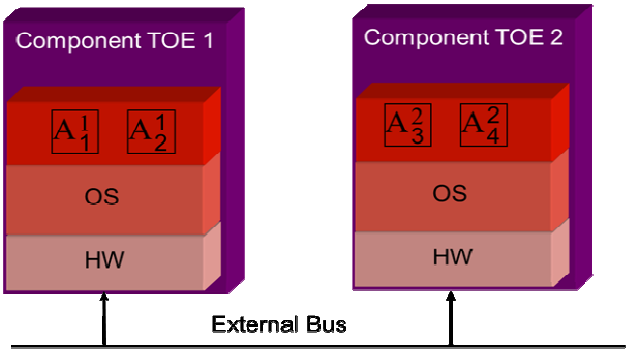

Figure 2: Sketch of a Non-Interfering Composed TOE: consisting of physically separated Component TOEs

Non-interference between the Component TOEs is shown if:

- The fulfilment of all requirements for running the Component TOE 1 in a secure (i.e. as certified) and non-interfered way, as imposed by the security certificate for Component TOE 1 (incl. related AGD contributions), can be evidently guaranteed by Component TOE 2 and vice versa.

§15 The third constellation is when the Component TOEs are executed in same run-time environment and directly interacting with each other.

Non-interference between the Component TOEs is shown if:

- The fulfilment of all requirements for executing Component TOE 1 in a secure (i.e. as certified) and non-interfered way, as imposed by the security certificate for Component TOE 1 (incl. related AGD contributions), can be evidently guaranteed by Component TOE 2 and by Component TOE 3 and vice versa, mutually for each Component TOE being part of the Non-Interfering Composed TOE N*(N-1)/2 times, where N represents the number of Component TOEs inside.

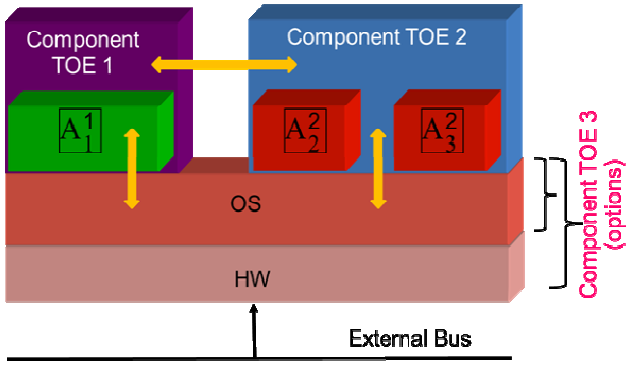

Figure 3: Sketch of a Non-Interfering Composed TOE: same execution environment and direct interaction

§16 The fourth constellation is when the Component TOEs are executed in same run-time environment and interacting with each other exclusively via the underlying platform (Component TOE 3 in Figure 4 below). A basically possible direct communication between Component TOE 1 and Component TOE 2 is excluded here by a domain separation service provided by Component TOE 3. A communication between Component TOE 1 and Component TOE 2 is established by using services and communication channels provided by Component TOE 3. The definition of the format of the communication exchange or communication protocol remains up to the Component TOE 1 and Component TOE 2:

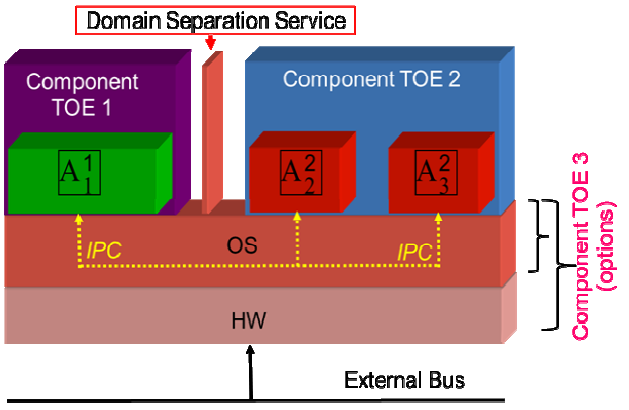

Figure 4: Sketch of a Non-Interfering Composed TOE: same execution environment and interaction via the underlying platform

Non-interference between the Component TOEs is shown if:

1. The fulfilment of all requirements for executing the Component TOE 1 and TOE 2 in a secure (i.e. as certified) and non-interfered way, as imposed by the security certificate for the Component TOE 1 and TOE 2 (incl. related AGD contributions), respectively, can be evidently guaranteed by the Component TOE 3 (underlying platform) and by a concrete configuration of the Component TOE 3.
2. The fulfilment of all requirements for executing the Component TOE 3 (underlying platform) in a secure (i.e. as

certified) and non-interfered way, as imposed by the security certificate for the Component TOE 3 (incl. related AGD contributions), can be evidently guaranteed by the Component TOE 1, Component TOE 2 and by a concrete configuration of the Component TOE 3.

Due to an effective Domain Separation Service provided by the Component TOE 3 (underlying platform), the evidence for non-interference shall be brought for each single Component TOE inside the Non-Interfering Composed TOE, i.e. merely N times.

3.3 Evaluation Steps

§17 The evaluation of the Non-Interfering Composed TOE shall rely on the certified evidence of the non-interference property between certified Component TOEs. Hence, each Component TOE shall be certified with respect to a possible future evaluation of a Non-Interfering Composed TOE. To this end, the following requirements shall be fulfilled:

- The CC security certificate of each Component TOE shall include the analysis of all its possible internal states, all its externally visible security relevant interfaces and all requirements having to be fulfilled by its operational environment to ensure the non-interference of the Component TOE. The Non-Interference Analysis of each Component TOE shall result in a specific statement including a complete list of non-interference requirements that shall be fulfilled by its operational environment. It shall be demonstrated that this list is complete and sufficient to justify that a given Component TOE cannot be interfered by its operational environment. The results of Non-Interference Analysis for each Component TOE are expected to be part of its AGD documents.

For example, the Non-Interference Analysis for a Component TOE may include, amongst other, an analysis of and requirements on non-bypassability – if interaction is allowed and components build on layered implementation of security services - and non-tampering of the Component TOE by its operational environment.

If a Component TOE is an operating system (OS), the Non-Interference Analysis for a Component TOE should demonstrate that the complete security separation between the Component TOE (OS) and an application is ensured by the security functional requirements (SFRs) of the Component TOE (OS)[2].

§18 The evaluation of the Non-Interfering Composed TOE shall demonstrate that the list of non-interference requirements of the Component TOE 1 can completely be mapped to the SFRs from Security Target and/or the requirements from the user guidance of the Component TOE 2, and vice versa. If it is successfully demonstrated that all Component TOEs within the Composed TOE are fully non-interfering, an additional, monolithic analysis of the Composed TOE shall not be necessary. Thus, the evaluation of the Non-Interfering Composed TOE can be confined to the evaluation of the functional interaction between Component TOEs (i.e. without a dedicated vulnerability analysis for the Non-Interfering Composed TOE), whether all security relevant conditions are fulfilled.

§19 In certain circumstances, a Component TOE adds additional assumptions to the Composed TOE. Such assumptions either shall be fulfilled by the security objectives of the other Component TOE or shall be added to the combined assumptions of the Composed TOE. Examples for the latter are dedicated hardware access, where the access to some hardware device itself is mediated by the Component TOE (OS) (e.g. memory-mapped devices), but the hardware device needs to be present in the platform (e.g. network connectors). If combined assumptions are contradictory and their fulfilment is impossible (e.g. combined timing requirements of applications), then the Composed TOE cannot be verified/certified.

§20 If demonstrated that the Component TOEs are merely partially non-interfering, additional specific integration tests shall be performed by the evaluator of the Non-Interfering Composed TOE. These integration tests shall close the "gap", if possible, and evidence non-interference for the remaining requirements/properties.

§21 The evaluation of the Non-Interfering Composed TOE should reduce the overall amount of evaluation work at the Non-Interfering Composed TOE if all components are certified in an appropriate way using the methodology outlined above.

The amount of evaluation work for individual components might increase, though, due to the need for providing the non-interference evidence (see also §9).

The proposed methodology offers some further advantages: a Component TOE (e.g., an application) can be replaced with less effort. Supplemental Component TOEs providing application services combined with the Component TOE providing the separation property (Base TOE) can be added by only evaluating the new application Component TOE using this methodology and the already existing Composed TOE. Thus, the new evaluation methodology for non-interfering Composed TOE enables a higher business flexibility for the vendors and operators of Composed TOEs.

§22 This evaluation method shall allow also a nested evaluation of a computer system. System architectures following the concept of Multiple Independent Layers of Security (MILS) employ several security functionalities organized in layers. The proper functioning of one layer may rely on the implementation of another layer. Each layer can be represented by an application. Using this evaluation methodology, an evaluated Composed TOE can operate as a Base TOE (providing, among others, the separation property) for a later certification with a different Component TOEs (usually providing application services) as long as all required non-interference properties are shown with the required assurance.

§23 The overall assurance level of the Non-Interfering Composed TOE is upper bounded by the lowest assurance level among the Component TOEs. A mandatory requirement to reach this upper bound is the availability of all documentation and additional documents stated in the certification report of each Composed TOE.

A final verdict on the assurance level of the Non-Interfering Composed TOE resides with the evaluator of the Non-Interfering Composed TOE. In case of partially non-interfering Composed TOE (cf. §20) the evaluator may determine additional vulnerabilities due to the composition that may influence the overall assurance level of the Composed TOE.

[2] If the Component TOE (OS) consists of an operating system not including a certified (hardware) platform, it should be additionally demonstrated that the underlying platform does not supply any functionality to bypass or tamper with the operating system.

4. Use Case: Avionics MILS Firewall

§24 The described evaluation method is useful to demonstrate the compositional certification of an avionic firewall function. This firewall is developed using the MILS principals. It shall filter data traffic of communication peers according to a defined information flow policy. The filtering shall be possible on different application-level protocols, such as TFTP or HTTP. The firewall shall be designed and evaluated allowing subsequent incremental modifications and addition of new application-level filters. Using the non-interfering Composed TOE methodology, the required re-certification shall be possible with decreased efforts, in particular, without the need to re-certify unchanged parts.

§25 From a system viewpoint, the firewall function uses the fourth constellation (see §16) and comprises the following Component TOEs:

a. A hardware platform (part of the certified Component TOE providing the separation property (Base TOE), red box in Figure 5)

b. A Separation Kernel (part of the certified Base TOE, red box in Figure 5) with EAL5+ (AVA_VAN.5)

c. A fundamental gateway architecture processing data traffic up to the transport layer (e.g. UDP and TCP) and deciding which filter application to apply. From the gateway viewpoint filters are “holes” in the system. These holes are filled with certified Component TOEs. The gateway architecture uses different partitions (R1, T1, R2, T2 in Figure 5) provided by the Separation Kernel to encapsulate the fundamental gateway from the filters to assure non-interference between filters and the fundamental gateway infrastructure. This basic gateway architecture is a certified Component TOE (blue dotted box in Figure 5) to EAL5+ (AVA_VAN.5, ATE_COV.3)

d. The filters being certified to EAL5 and being hosted by separate partitions (yellow boxes in Figure 5)

e. A system configuration, in particular of the Separation Kernel, defining which partitions of the certified gateway— and especially of the certified filters— are allowed to interact (white arrows in Figure 5).

§26 Figure 5 clarifies the special environmental property of a Non-Interfering Composed TOE using a Separation Kernel as a Component TOE separating other Component TOE of each other by partitions. The interaction between two partitions (blue and yellow boxes) is defined by two properties:

a. The format of the data exchange (also known as communication protocol). This communication protocol has to be implemented by the binaries running inside the respective partitions, i.e. the Component TOEs.

b. The communication channel provided between two partitions to allow interaction. This property is under exclusive control of the Base TOE. Hence, the Base TOE defines the only possible ways of interactions, allowing to prove the Non-Interference property between applications more easily.

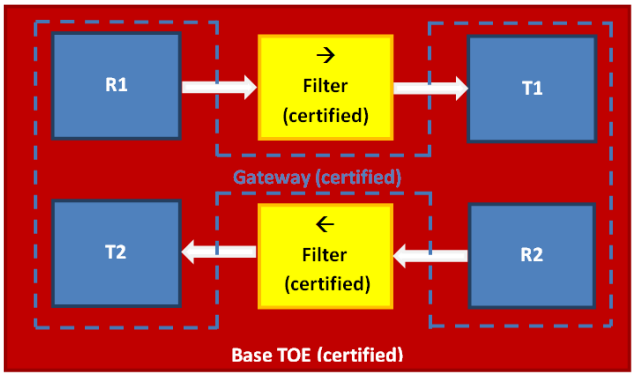

Figure 5: Non-Interfering Composed Firewall TOE

§27 For the Non-Interfering Composed TOE of the firewall function, we have to provide

a. A certification including a full vulnerability assessment for the Separation Kernel Component TOE, the gateway Component TOE, and the filters Component TOEs, independently of each other;

b. A complete list of non-interference requirements for each Component TOE;

c. A valid configuration of the Separation Kernel TOE, showing, in particular, the correct instantiation of communication channels topology as defined by the security policy of the Composed TOE for authorized interactions, showing non-overlaying memory areas to avoid interference, and showing proper configuration of devices;

d. A proof that the non-interference requirements of each Component TOE are fulfilled in the Non-Interfering Composed TOE. For the Component TOEs interacting with each other, or for Component TOE only partially non-interfering (cf. §19), an additional integration test between those Component TOEs shall show the intended behaviour of the Non-Interfering Composed TOE.

e. Due to the presented EALs of the Component TOEs in this example - EAL5+ for the Base TOE, EAL5+ for the gateway architecture and EAL5 for the filters components - the upper bound of the Non-interfering Composed TOE is EAL5.

5. Use Case: Automotive MILS Infotainment Device

§28 The described evaluation method is useful to demonstrate the compositional certification of an automotive infotainment device. This device is developed using the MILS principals. It combines independent high-level components of different security levels, namely an Android component, an Autosar component, and, depending on customer needs, additional custom components like an Instrument cluster or Navigation component. It shall isolate the components from each other and allow only explicitly defined communication between them. At the same time it shall provide system services like graphics display, access to device interfaces or hardware resources to each component. The infotainment device shall be designed and evaluated to guarantee freedom of interference between the high-level components, without making any assumptions on the

Android component. From a user perspective, it shall be possible to install arbitrary user applications to the Android component using the connectivity interface(s) to access online services or local interfaces like USB. Using the non-interfering Composed TOE methodology, it shall be possible to introduce updates for the Autosar component and other custom components with decreased certification efforts, in particular, without the need to re-certify unchanged parts.

§29 From a system viewpoint, the infotainment device uses the fourth constellation (see §16) and comprises the following Component TOEs:

a. A hardware platform (part of the certified Component TOE providing the separation property (Base TOE))

b. A Separation Kernel (part of the certified Base TOE)

c. A Network Manager partition controlling the communication flow between the high-level components. It is a certified Component TOE.

d. A Device Service partition providing shared access to hardware resources. It is a certified Component TOE.

e. An Autosar partition being developed according to automotive grade development processes. It is designed to have exclusive access to the automotive-specific vehicle interface (e.g. CAN). It is a certified Component TOE.

f. Optional custom partitions being developed according to automotive grade development processes. If applicable, they are certified Component TOEs.

g. An Android partition that has controlled access to hardware resources which may be exclusive or shared. It is not a certified Component TOE. It is the responsibility of the underlying Base TOE to guarantee overall freedom of interference when these resources are accessed and (possibly mis-)used by the Android partition.

h. A system configuration, in particular of the Separation Kernel, defining which partitions of the certified infotainment device are allowed to interact, which hardware resources are accessible from within which partition and which functions of the separation kernel API are accessible from which partition.

§30 Figure 6 depicts the high-level architecture and clarifies the relations between the various Component TOEs (double arrows). The access permissions to hardware resources are shown with the single arrows. The following properties apply:

a. The Autosar partition has exclusive access to the CAN interface.

b. All high-level component partitions (Autosar, Android and optional Custom partitions) communicate through the Network Manager partition. There is no direct communication path between these components.

c. Shared resources are managed by the Device Service partition, which has exclusive access to the respective hardware resources. The Device Service partition controls the IOMMU which ensures separation on device level.

d. Shared device services provided by the Device Service are accessed through the Network Manager partition. There is no direct link between the Device Service partition and any other high-level component partition.

e. All hardware resources explicitly assigned to the Android partition must be controlled by the IOMMU to guarantee separation on device level.

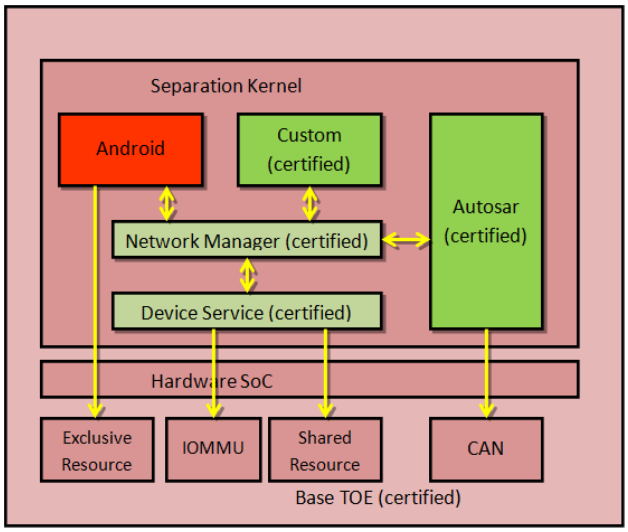

Figure 6: Non-interfering Composed Infotainment TOE

For the Non-Interfering Composed TOE of the infotainment device, we have to provide

a. A certification including a full vulnerability assessment for the Separation Kernel Component TOE, the Device Service Component TOE, the Autosar Component TOE, the Network Manager Component TOE and the optional Custom Component TOEs, independently of each other;

b. A complete list of non-interference requirements for each Component TOE;

c. A valid configuration of the Separation Kernel TOE, showing, in particular, the correct instantiation of communication channels topology as defined by the security policy of the Composed TOE for authorized interactions, showing non-overlaying memory areas to avoid interference, and showing proper configuration of device accesses;

d. A valid configuration of the Device Service TOE, showing, in particular, the correct configuration of the IOMMU to ensure separation on device level;

e. A valid configuration of the Network Manager TOE, showing, in particular, the correct instantiation of communication control elements (e.g. filters) as defined by the security policy of the Composed TOE for authorized interactions;

f. A proof that the non-interference requirements of each Component TOE are fulfilled in the Non-Interfering Composed TOE. For the Component TOEs interacting with each other, or for Component TOE only partially non-interfering (cf. §19), an additional integration test between those Component TOEs shall show the intended behaviour of the Non-Interfering Composed TOE.

6. Summary

§30 This paper presented a new methodology to perform composed security evaluations in the framework of the Common Criteria (CC). Composed evaluations take multiple already certified Targets of Evaluation (TOEs) and combine them into a new, joint TOE, the composed TOE. Firstly, this allows to split the composite TOE into multiple subsets, which might be easier and cheaper to certify as single components than in the composed TOE. Secondly, this enables reusing certified components for multiple composed TOEs in order to reduce subsequent evaluation cost.

§31 The CC presents already two evaluation methodologies to perform compositional evaluations (*Composed Assurance Package* and the *Composite product evaluation for Smart Cards and similar device)*; however both have issues regarding their usage for flexible modular systems. These issues are limitations of the highest reachable Evaluation Assurance Level (*Composed Assurance Package*), and limitations in the flexibility of the reuse of evaluation results of Component TOEs.

§32 This document presents a new composite evaluation methodology using the property of non-interference. It assumes a platform TOE can evidently operate as component to separate additional Component TOEs for each other without interference. Such a platform TOE can be a Separation Kernel, a special, certifiable microkernel often mentioned in the context of systems following the principals of Multiple Independent Levels of Security (MILS). The methodology proposes to perform an *apriori* evaluation and vulnerability assessment of the Component TOEs; this differs to other composite evaluation methodologies. Each certificate needs to state runtime requirements in order to allow a Component TOE to operate as evaluated in the Composite TOE. If all these requirements can be fulfilled by other Component TOEs, and the Component TOEs can be evidently run without interference, the final Composite TOE is certifiable without additional and expensive vulnerability assessments. This finally saves costs in subsequent certifications.

§33 Future work can be seen in the application of this methodology in a CC security evaluation. It is recommended to perform this in the environment of a high-assurance composed TOE using the design principals of MILS and running on top of a Separation Kernel. Results of such a guided and pioneering application of the methodology will gain valuable information of the practical applicability of Non-Interfering Composed Evaluations.

7. REFERENCES

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

[5] Common Criteria Development Board, Composite product evaluation for Smart Cards and similar devices, April 2012, CCDB-2012-04-001