Authors/Speaker(s): Igor Furgel (T-Systems), Nathalie FEYT & Thomas BEN (Thales Communications & Security)

Organisations: T-Systems International GmbH, Thales Communications & Security

Contact

T-Systems: igor.furgel@t-systems.com
+49 228 9841 5120 (phone); +49 228 9841 6000 (fax)
Vorgebirgsstr. 49
53119 Bonn
Germany

Thales: **Nathalie.feyt@thalesgroup.com**
& Thomas.ben@thalesgroup.com
+33 6 80 35 86 24
18 Avenue Ed Belin
BPI1414
31400 Toulouse

Title of contribution:

Security Composition with Software Platform: Integration of Hardware and Applications

Keywords:

composite evaluation & certification, hard- & software integration, smart phones, tablets, mobile devices, automotive, avionics, smart meters, embedded devices, java based products

Curriculum Vitae Igor Furgel:

Head of the Confirmation Body of T-Systems and security evaluator with the following focus:
– Development of evaluation methodology for different aspects of CC (esp. composite evaluation, vulnerability analysis and high evaluation assurance levels incl. contributions to the CC v3.1 and guiding respective evaluation methodology)
– Embedded systems in general, the Digital Tachograph system, electronic signatures
– Virtualisers and hypervisors with security domain separation
– Smart card operating systems and applications, java cards and cryptographic boxes
– Lectures of the public relevant analysing results on different conferences, seminars and workshops
– Conception and support of establishment a Common Criteria evaluation laboratory
– Performing conformity assessments and issuing conformity certificates according to German Electronic Signature Act
– Official and special training and coaching for Common Criteria (for evaluators, developers and certifiers).

Curriculum Vitae Nathalie Feyt

– Head of Thales ITSEF since 8 years
Specialised in Embedded systems evaluation in general, particularly for mobile payment security
– Lobbying for usage of CC in new markets (mobile telecom, space, avionics, automotive)
– Active Participant to the creation of a CC evaluation framework of “POI” by delivering part of JTEM CEM guidelines and attack methods
– Proposition for improvement of CC evaluation implementations (a.g. “JIL collection of developer evidence)

Curriculum Vitae Thomas BEN

Senior security evaluator (CC / Expertise) since 13 years in Thales ITSEF
– Specialised in Embedded systems evaluation in general, particularly for smart card& similar devices and space security equipments
– Representation to European space agency on the use of CC security evaluations in Space programs
– Contribution to JHAS & JTEM
– Previous ICCC presentations

Abstract:

A technical integration of a software platform (e.g. of a hypervisor, JRE or JCRE, operating system) with other components like an underlying hardware (microcontroller) and user applications is a question of their functional compatibility which is addressed in the related user manuals.

But what is about the **trustworthiness and the assurance level** of the resulting system? **How can and why should the system integrator, who puts the single items together, rely on the resulting system?**

A **secure** sharing of resources provided by a platform to several applications has been a top question for last years. In our multi-vendors world, the single parts of final IT product or system – hardware, hypervisors, operating systems, user applications - are provided by different manufacturers. Good examples for such final complex IT products are smart phones, tablets and other mobile devices, automotive, avionics, smart meters and other embedded devices, java based products.

T-Systems ITSEF has been essentially involved into the development of the CC JIL Mandatory Document ”Composite product evaluation for smartcards and similar devices” and performed numerous evaluations on embedded devices and smart cards.
Thales ITSEF has performed numerous evaluations on mobile devices (USIM or embedded SIM) for mobile payment applications since more than 3 years now, where application segregation is the main security functions asked to the operating systems constituting the software platform.

This talk considers composition approaches and methodologies facilitating experience of

- integration of software platform with hardware (composition ‘to the bottom’) – by T-System
  and
- integration of software platform (integrating the “underlying hardware”) with user applications (composition ‘to the top’) by Thales

in a **trusted** way.

Approach for the Integration of Hardware (composition ‘to the bottom’) [T-Systems]

During the talk we will consider a new approach for a **secure** integration of hardware, whereby the SW platform is assumed to be CC certified. This new approach enables a more flexible choice and exchange of hardware than just to count very concrete hardware units (microcontrollers) being suitable for a secure integration with the SW platform.
This ‘state-platform-security-properties’ approach enables the system integrator to choose between several hardware units being not only functionally suitable, but also from the point of view of security composition. This approach also fulfils two necessary conditions supporting practical usability of SW platform:

(1) flexibility ‘to the bottom’, i.e. the ability of SW platform to be integrated in several hardware platforms, and
(2) usability ‘to the top’, i.e. security certified SW platform may (and, mostly probable will) be used later on as the ‘underlying platform’ for further CC composite certifications with different applications.

Approach for the Integration of Applications (composition ‘to the top’) [Thales Communications and Security]

The next topic of the talk will be a **secure** integration of (user) applications, whereby the SW platform is assumed to be CC certified. Due to this choice, the CC certified SW platform can be used as the ‘underlying platform’ for further CC composite certifications with different applications.
If the system integrator decided to composite-certify one or several applications together with the already CC certified SW platform, the question arise, **which composite evaluation procedure and methodology shall be applied for this composite certification in order to get a recognized CC certificate?**
Since the final IT products/systems using a high secure SW platform are usually intended to secure **highly sensitive assets**, it is to assume that the targeted EAL for such a composite TOE may be quite high as well as the targeted TOE resistance may be against a high attack potential.
Currently, the CC JIL Mandatory Document ”Composite product evaluation for smartcards and similar devices” is used to obtain high level of assurance on product constituted by USIM or Javacard or Multos platforms which are embedding application segregation functions, and secure applications (a.g. mobile payment applications). Based on actual feedback on composition of applications on those platforms, we can propose to apply them with some refinements on SW platforms. Therefore, appropriate procedure and methodology can be derived and experiment by different ITSEF and pushed for potential CCDB adoption.
This methodology, once adopted, will enable including one or several applications running on a software platform into the CC composite certification.