NEXT GENERATION OF AUTOMOTIVE SECURITY: SECURE HARDWARE AND SECURE OPEN PLATFORMS

André Groll, Jan Holle
University of Siegen, Institute for Data Communications Systems
{andre.groll,jan.holle}@uni-siegen.de

Marko Wolf, Thomas Wollinger
escrypt GmbH – Embedded Security
{marko.wolf,thomas.wollinger}@escrypt.com

ABSTRACT

This technical paper gives a short overview about the OVERSEE project, an European research project developing a new in-vehicle application and communication platform with an overall budget of about 4 M€ started in January 2010. The OVERSEE project will provide an open in-vehicle information technology (IT) platform and corresponding internal and external communication interfaces for downloading and execution of OEM applications as well as third party applications – similar to application stores known from mobile smart phones – in a safe, secure, and very flexible manner. Thus, OVERSEE will lower the barriers, that means, the costs and risks, for realizing new vehicular applications by providing a rich and standardized vehicular runtime environment, while dependably enforcing the security and reliability of the underlying information technology.

INTRODUCTION AND MOTIVATION

Modern vehicles are an integral part of the daily life in industrial nations while the amount of vehicles and the vehicle miles travelled per year are still continuously increasing. For the future of automotive transportation, there are – from the European perspective – at least two major goals. First, the number of fatalities and injuries on the road is still too high and has to be reduced further in a significant manner. Second, the use of vehicles is part of the most of our economical and ecological challenges, and hence has to be as efficient as possible with regard to the emission of CO_2, consumption of fossil fuels and the use of vehicular infrastructures [2].

Reducing the number and severity of car accidents together with a reduction of vehicular emissions can be achieved by the application of intelligent traffic management solutions that are mostly based on wireless communications between cars (V2V) and wireless communications between cars and their surrounding infrastructures (V2I). The central perquisites for the successful deployment of such V2X communication systems are reliable, well-defined vehicular communication interfaces as well as reliable vehicular information security measures against malicious encroachments during the communication and against malicious encroachments on the communications endpoints.

First, already existing V2I applications, such as the infrastructure-based e-tolling systems (e.g., *Toll Collect*) as well as the upcoming automatic emergency call system (e.g., *eCall*) use their own proprietary and closed information technology (IT) platforms (e.g., so called on-board units) or simply rely on the availability and correctness of communicated information. However, instead of adding more and more unprotected proprietary in-car boxes and communication interfaces for every new V2X application, we propose an open standardized in-vehicle application platform, which could help to share available IT resources and necessary communications periphery while providing adequate information security. Moreover, new applications can hence access IT resources (e.g.,

head-unit display, GPS signals) and can apply security mechanisms (e.g., cryptographic accelerators, hardware security), which would otherwise be virtually unaffordable.

In the following sections, we shortly describe the approach of the OVERSEE project. OVERSEE is a European research project with an overall budget of about 4 M€ started in January 2010 developing exactly such an in-vehicle application and communication platform. The OVERSEE project hence will provide an open in-vehicle IT platform and corresponding internal and external communications interfaces for downloading and execution of OEM applications as well as third party applications – similar to application stores known from mobile smart phones – in a safe, secure, and very flexible manner. Thus, OVERSEE will lower the barriers, that means, the costs and risks, for realizing new vehicular applications by providing a rich and standardized vehicular runtime environment, while dependably fulfilling the strong information security and information technology reliability requirements.

SECURE OPEN PLATFORMS AND HARDWARE SECURITY ANCHOR

Today, every new automotive project implies the development of a new and project-specific Electronic Control Unit (ECU), which causes immense costs and additional risks. Furthermore, currently there is no universal device available that is able to connect vehicle internal and external networks in a secure and standardized way (e.g., for downloading tolling information or transmitting diagnosis information). This gap, the high costs, and additional risks impede the development of new products and services that could be helpful to make vehicular traffic safer and more efficient. Hence, future innovative automotive applications require an open and secure vehicular IT application platform.

Secure Open Platform means the platform provides protected and standardized (e.g., compatible with existing legacy operating systems) runtime environments for the simultaneous and secure execution of multiple OEM and also non-OEM applications with secure access to vehicle-internal IT resources in particular to vehicle internal and external communication networks. The interfaces of that platform have to be standardized and public in order to enable the development of vehicle independent "plug & play" applications even by third party providers. This would reduce the amount of ECUs needed in a vehicle and thus save costs for vehicle productions. Furthermore, fewer devices will save weight, maintenance efforts and hence increase the efficiency of vehicles.

Realizing virtualization technologies together with a reliable resource control management on (powerful) ECUs allows the parallel – but strongly isolated – execution of several ECU applications on a single platform and hence allows for a noticeable more efficient and more flexible utilization of the always scantily hardware resources [3]. Moreover, the application of virtualization technologies prevents that neither an accidental malfunction (IT safety/IT reliability) nor a systematic manipulation (IT security) of one application should either affect or compromise any other application executed in parallel. Virtualization inherently enforces a strong resources management and enables the efficient and reliable sharing of available hardware resources and (communication) periphery.

Hardware Security Anchor is needed to enforce the security of (software) security functions and secret information (e.g., cryptographic keys) by placing them into physically protected hardware devices. Thus, secret information or security functions are protected against compromise or circumvention by (accidental or malicious) software manipulations or most kind of malware. Moreover, the hardware security component acts as autonomous security anchor that enables the reliable verification of any (security-critical) software before its first execution (e.g., at the bootstrap). Finally yet importantly, hardware security modules can apply special cryptographic hardware accelerators to increase the performance of the underlying cryptographic operations, for instance for fast encryption/decryption, to take most of the cryptographic load from the main application processor. The use of automotive capable, cost-effective hardware security modules [1] acting as physically protected low-level security anchor in combination with software security

components that realize high-level security functionality (e.g., device encryption, access control) provides the necessary protection against application failures and malicious encroachments.

PLATFORM ARCHITECTURE

Figure 1 gives an overview of the OVERSEE platform consisting of the standardized runtime environments connected to various internal and external communication interfaces. The efficient virtualization solution enables a flexible sharing of the hardware resources together with a strong mutual isolation of applications and a strong access control on resources, services, and data. Hence, an OVERSEE application can securely access internal ECU networks (e.g., CAN), in-vehicle communication interfaces (e.g., Bluetooth) and wireless short-range communications (e.g., Wi-Fi) as well as selected wireless long-range networks such as UMTS or GSM/GPRS if authorized by the underlying access control mechanism. To enforce the security of (software) security functions and secret information, the OVERSEE platform applies an automotive-capable hardware security anchor that enforces the protection of the virtualization environment and central security functionality and data; and may act as cryptographic accelerator as well.

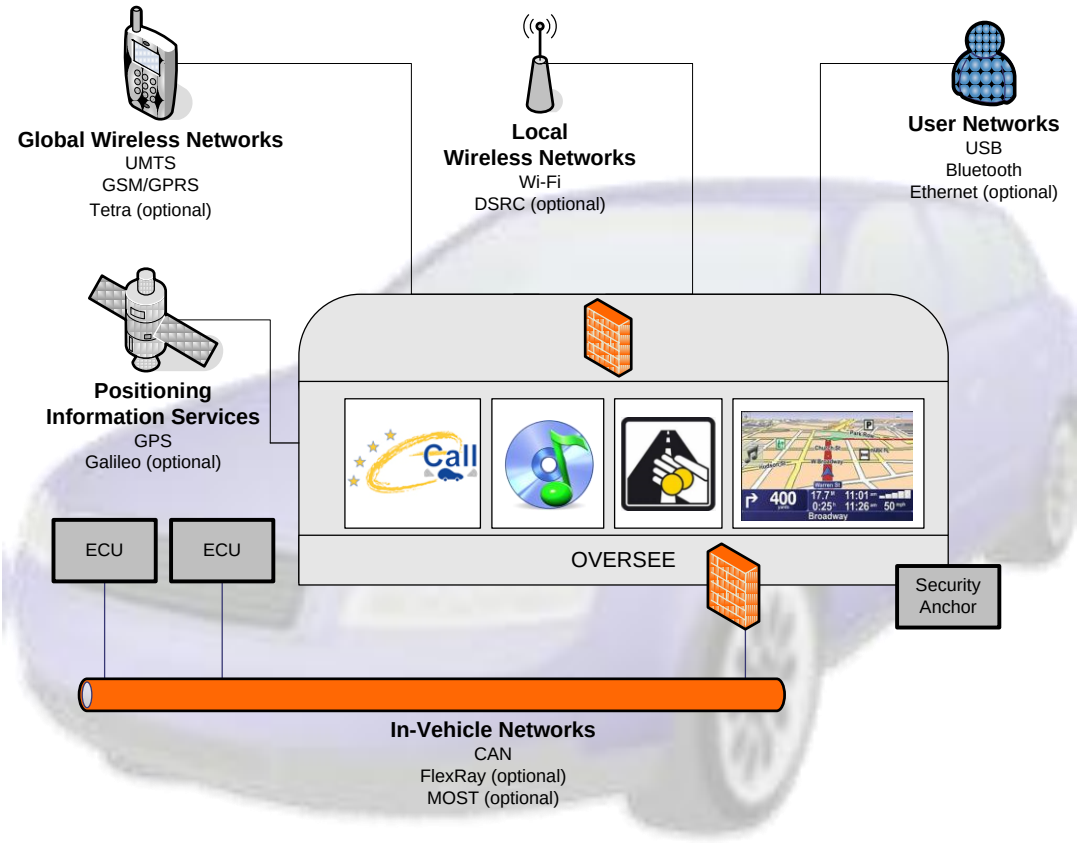

Figure 1: OVERSEE platform approach

Automotive Hardware Security Module

To ensure the security of (software) security functions and secret information, OVERSEE applies an automotive capable hardware security module (HSM). The HSM acts as autonomous hardware security anchor that secures generation, storage and processing of security-critical information (e.g., cryptographic keys) by physically shielding it from all potential malicious software. It enables also the reliable measurement (authentic boot) and/or validation (secure boot) of any (security-critical) software before its first execution (e.g., during the bootstrap). In order to restrict even hardware tampering attempts, the HSM would apply appropriate tamper-protection measures such as special coatings or sensor grids. Ideally, the HSM includes also hardware cryptographic accelerators that beats the performance of most software solutions and can provide significant CPU offload.

Table 1 provides a short comparison of potential automotive hardware security modules as provided by the EVITA project [1], the HIS consortium [6], the Trusted Computing Group [5] together in comparison with a usual smartcard. While the HIS Secure Hardware Extension (SHE) is "only" a symmetric cryptography-enabled ECU protection solution, the TCG TPM/MTM approach has no protected symmetric cryptography included.

In order to cover the different (security) functional and protection requirements as well as the different cost constraints, the EVITA project provides three different HSM classes. It hence enables a holistic security architecture (cf. Figure 2) where all modules are capable to interact securely with each other while efficiently meeting the strong cost, security, and functional requirements.

HSM / Feature	**EVITA full**	**EVITA medium**	**EVITA light**	**HIS SHE**	**TCG TPM/MTM**	**Usual smartcard**
Bootstrap integrity protection	Authentic and/or secure	Authentic and/or secure	Authentic and/or secure	Secure	Authentic	None
HW crypto algorithms (incl. key generation)	ECDSA,ECDH, AES/MAC, WHIRLPOOL/ HMAC	ECDSA,ECDH, AES/MAC, WHIRLPOOL/ HMAC	AES/MAC	AES/MAC	RSA, SHA-1/ HMAC	ECC, RSA, AES, 3DES, SHA-x & more possible (but seldom in parallel on chip)
HW crypto acceleration	ECC,AES, WHIRLPOOL (FPGA/ASIC)	AES (ASIC)	AES (ASIC)	AES (ASIC)	None	None
Internal CPU	Reprogrammable firmware & hardware (FPGA)	Reprogrammable firmware	None	None	Preset	Reprogrammable firmware
RNG	TRNG	TRNG	PRNG w/ external seed	PRNG w/ external seed	TRNG	TRNG
Counter	16x64bit	16x64bit	None	None	4x32bit	None
Internal NVM	Yes	Yes	Optional	Yes	Indirect (via SRK)	Yes
Internal clock	Yes w/ external UTC sync	Yes w/ external UTC sync	Yes w/ external UTC sync	No	No	No
Parallel access	Multiple sessions	Multiple sessions	Multiple sessions	No	Multiple sessions	No
Tamper protection	Indirect (passive, part of ASIC)	Indirect (passive, part of ASIC)	Indirect (passive, part of ASIC)	Indirect (passive, part of ASIC)	Yes (mfr. depended)	Yes (active, up to EAL5)

Table 1: Comparison of automotive capable hardware security modules as provided by the EVITA project [1], the HIS consortium [6], and the Trusted Computing Group [5] together in comparison with a usual smartcard.

In order to meet also the strong performance requirements for securing V2X communications, the EVITA full module includes also high-performance standardized elliptic curve arithmetic together with a hardware-accelerated hash function. However, all EVITA modules provide at least AES-based symmetric cryptography, protected random number generation and a secure tick counter that can become securely synchronized internally with coordinated universal time (UTC).

The EVITA HSM approach particularly applies and extends the ideas of Trusted Computing (e.g., authenticated boot) with meaningful extensions. A striking example are the so called "use_flags"

together with their individual authorizations. These “use_flags” are key usage restrictions that can be set for each key during creation. Thus, a certain symmetric key can be used for MAC verifications, but not for MAC generations. Moreover, each “use_flag” can have (but do not necessarily have to) individual transport restrictions (e.g., internal only, migratable) together with individual authorizations (e.g., password, bootstrap references or combination of both). More details can be found in [7].

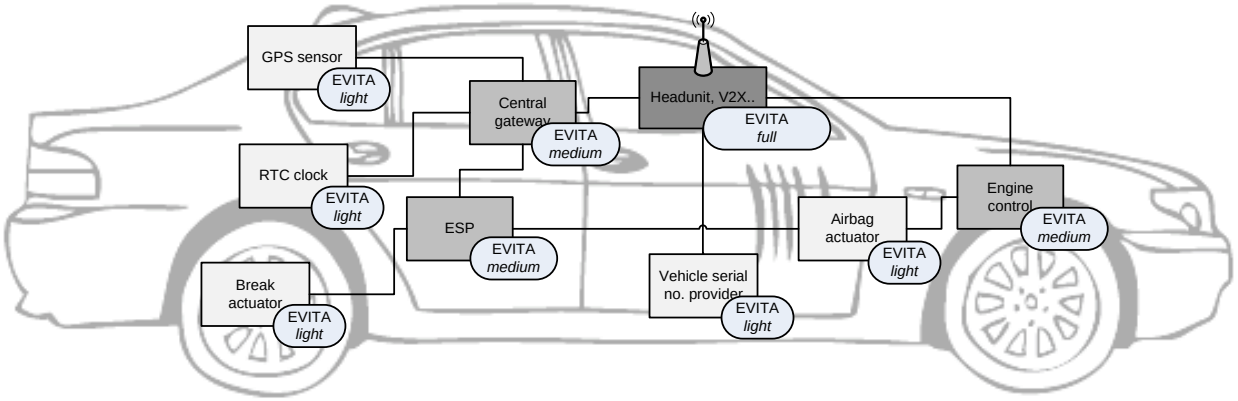

Figure 2: Efficient, cost-effective, flexible, and holistic in-vehicle EVITA HSM deployment regarding the different cost, performance constraints and functional requirements.

Secure Software Runtime Environment for Applications

The other main objective of OVERSEE is to provide secure runtime environments for automotive applications. Therefore, in Figure 3 a draft for the architecture of the OVERSEE platform is shown and the main architectural components are described below.

Virtualization is a technology that is well known from personal computers and servers in classical computer networks. Roughly spoken, it is the idea to insert an additional (software) layer − above the real hardware − which provides so called virtual machines for the execution of the applications. The virtualization layer suspends and resumes the virtual machines according to an appropriate schedule and therefore the applications obtain the impression that they are running on the machine exclusively. Since the applications are only able to call the resources that are provided by their virtual machine all resource calls would be processed by the virtualization subsystem and could hence be rejected or forwarded to the real (hardware) resources. This will lead to a strong isolation of the running applications, where no application is aware of the other executed applications – except a special secure communication channel is established. Moreover, no application is able to harm another executed application by inserting malformed code or consuming more resources than configured, even in the case the application crashes. For the virtualization subsystem the OVERSEE consortium selected XtratuM [8] which is a hypervisor especially designed for real time embedded systems and developed mainly with focus on projects in aerospace industry. The customization of XtratumM towards the use in the automotive domain will be one of the major steps within the OVERSEE project.

Standardized, open compartments are the main concept to overcome the need for a special ECU for every new developed automotive application. The compartments or to say virtual machines will be standardized and open which means that not only OEMs are able to develop applications which could be executed in the virtual machines of OVERSEE but also third party developers including open source projects. Nevertheless, the compartments will be isolated from each other (see above). Some important requirements of the compartments will be the support of real time and legacy operating systems as well as applications which will be executed directly on the "hardware" provided by the virtual machines − without the additional costs of an operating system. Since the

virtualization is transparent to the executed application or OS, almost no changes will be necessary to legacy applications or the used OS. This fact together with the possibility to develop vehicle independent applications will speed up the development of innovative automotive applications and will decrease maintenance costs.

Communication interfaces are the main facilities required by modern and upcoming automotive applications. Since the range of network interfaces − which are connected to the OVERSEE platform − could be individual configured, a generic and standardized communication interface to the networks will be provided to the applications. The network interfaces will be categorized and access rights for the different applications could be granted or even denied. This will ensure the control over the information flow and hence could be helpful to ensure especially privacy requirements. Moreover, the generic network interface will anticipate the development of automotive applications, since the details of the network access will be hidden to the application.

Firewalls are separating network parts into different security domains. Furthermore, firewalls are able to protect network interfaces of IT systems against attacks from outside and against information drain from inside – like personal firewalls in personal computers. The OVERSEE platform will apply a firewall to every connected network interface enforcing the policies of communication defined for the different applications and users of the OVERSEE platform. Moreover, because the great amount of network interfaces towards the vehicle today will be consolidated within only one single point of access – the OVERSEE platform – the overall security of communication could be easily enhanced and monitored.

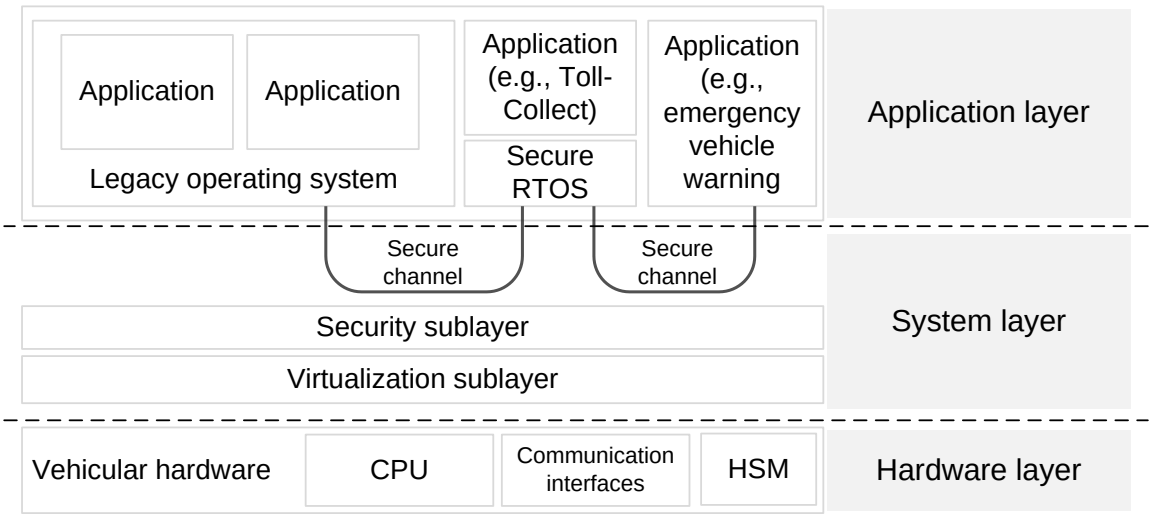

Figure 3: OVERSEE runtime architecture consisting of a hardware layer, a system layer including a security and virtualization sublayer and an application layer on top.

USE CASES

To be sure that all requirements for an open and secure in-vehicle platform would be considered the OVERSEE consortium started the project with a collection of recent and near-term automotive and especially ITS use-cases. Two of these use-cases would be briefly described below.

Parking lot reservation

The idea of a parking lot reservation system is that drivers would be able to reserve a parking lot at their destination or along their route. This would help especially drivers of heavy good vehicles (HGV) to stick to their rest periods.

A platform that should be able to serve such a parking lot application will need access to a long range communication system (e.g., UMTS), the current position (e.g., determined via GPS) and input from the driver or navigation system (e.g., destination or route and expected time of arrival).

The wide spread use of a parking lot reservation system could help to improve both efficiency of road transport – avoid time and fuel consumption for searching a free parking lot – and safety of road transport – prevent overcrowded resting places at motorways while helping drivers of HGVs to be regained for driving.

Emergency vehicle warning

A free lane for an approaching emergency vehicle will help to save the life of injured or sick people and reduce the number of accidents as well as critical situations where emergency vehicles are involved in. Sadly, especially emergency vehicles are often impeded because of drivers who were not aware of the approaching emergency vehicle. An emergency vehicle warning could help to inform drivers in front of an emergency vehicle via a warning message transmitted directly from the emergency vehicle, for instance, by the use of a DSRC (Dedicated Short Range Communication) link.

To serve such an application a platform needs access to the current position of the vehicle, a short-range ad hoc network and facilities to prove the authenticity of arriving messages. Furthermore, the upgrade of infrastructure equipment could extend the opportunities of this use-case, for instance, by switching traffic lights for the approaching emergency vehicle to green.

CONCLUSION AND OUTLOOK

In order to meet the upcoming challenges in the automotive domain especially regarding vehicular safety and traffic efficiency, quite a number of new and innovative vehicular applications and services are strongly required. To lower the barriers, that means, the costs and risks, for realizing new vehicular applications, the OVERSEE platform provides rich, standardized runtime environments including all necessary IT resources and data including mandatory information security mechanisms. Thus, OVERSEE enables the fast and secure realization of new automotive applications while at the same time protecting the vehicle and all applications executed in parallel against potential failures and even against malicious encroachments.

REFERENCES

[1] E-safety Vehicle Intrusion Protected Applications (EVITA) project, www.evita-project.org

[2] European Commission, Action Plan for the Deployment of Intelligent Transport Systems in Europe, http://ec.europa.eu/transport/its/road/road_en.htm

[3] J.Pelzl, M.Wolf, T.Wollinger, "Virtualization Technologies for Cars — Solutions to increase safety and security of vehicular ECUs", In Automotive 2008 — Sicherheit und Zuverlässigkeit für automobile Informationstechnik, Stuttgart, Germany, November 19 – 20, 2008

[4] Open Vehicular Secure Platform (OVERSEE) Project, www.oversee-project.com

[5] Trusted Computing Group, Trusted Platform Module Main Specification Version 1.2, Revision 103, July 2007

[6] Herstellerinitiative Software (HIS) Security Working Group. SHE – Secure Hardware Extension Version 1.1, October 2009

[7] E-safety Vehicle Intrusion Protected Applications (EVITA) project, Deliverable D3.2: Secure On-board Architecture Specification, March 2010

[8] XtratuM Hypervisor designed for real-time embedded systems, www.xtratum.org