15 April, 2011

EVITA

E-Safety Vehicle Intrusion Protected Applications

European Commission
Information Society and Media

Project Objectives

The objectives of EVITA – a project co-funded by the European Commission – are to design, to verify, and to prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise. Thus, EVITA provides a basis for the secure deployment of electronic safety aids based on vehicle-to-vehicle and vehicle-to-infrastructure communication. Focussing on on-board network protection, EVITA complements other e-safety related projects that focus on protecting the communication of vehicles with the outside.

At a Glance

Project Coordinator:

Fraunhofer Institute for Secure Information Technology (Germany)

Partners:

BMW Research and Technology	(Germany)
Continental Teves AG & Co. oHG	(Germany)
escrypt GmbH	(Germany)
EURECOM	(France)
Fraunhofer ISI	(Germany)
Fujitsu Semiconductor	(Germany/Austria)
Infineon Technologies AG	(Germany)
Institut Télécom	(France)
Katholieke Universiteit Leuven	(Belgium)
MIRA Ltd.	(UK)
Robert Bosch GmbH	(Germany)
TRIALOG	(France)

Duration:

42 months (July 2008 – December 2011)

Total Cost:

6 million €

Programme:

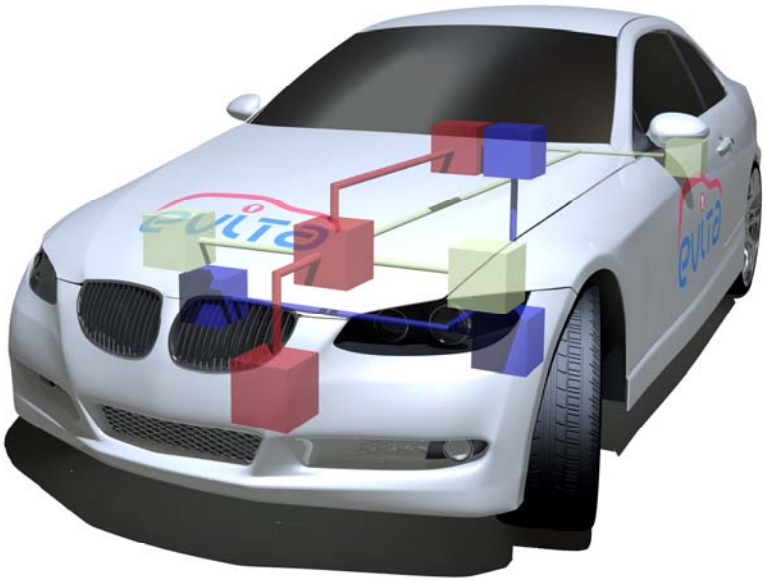
FP7-ICT-2007 of the European Community

Contact:

Dr.-Ing. Olaf Henniger, Fraunhofer SIT
Rheinstraße 75, 64295 Darmstadt, Germany
Email: olaf.henniger@sit.fraunhofer.de
Tel.: +49 6151 869 264
Fax: +49 6151 869 224
URL: http://evita-project.org

Background

Automotive safety applications based on vehicle-to-vehicle and vehicle-to-infrastructure communication have been identified as a means for decreasing the number of fatal traffic accidents in the future. Examples of such applications are local danger warnings and electronic emergency brakes. While these functionalities herald a new era of traffic safety, new security requirements need to be considered in order to prevent attacks on these systems.



A modern car may be equipped with up to 70 embedded ECUs (electronic control units) for a diversity of functions. The ECUs are connected via various vehicular buses (e.g. CAN, MOST, LIN), forming a complex distributed system. So far, there has been little incentive and opportunity for tampering with automotive networks. This changes with the advent of new vehicular communication interfaces. There are various threats, such as forced malfunctioning of safety-critical components or the interference with the traffic flow by means of fake messages.

Approach

Security Requirements Analysis

Starting from relevant use cases and security threat scenarios, security requirements for automotive on-board networks are specified. Also legal requirements on privacy, data protection, and liability issues are considered.

Secure On-Board Architecture Design

Based on the security requirements and the automotive constraints, a secure on-board architecture and secure on-board communications protocols are designed. The security functions are partitioned between software and hardware. The root of trust is placed in hardware security modules (HSMs) that should be realised as extensions to automotive controllers.

In order to ensure that the identified security requirements are satisfied, selected parts of the secure on-board architecture and the communications protocols are modelled using UML and automata and verified using a set of different but complementary model-based verification tools.

Implementation

For prototyping, FPGAs are used to extend standard automotive controllers with the functionality of cryptographic co-processors. The low-level drivers for interacting with the hardware are partially generated from UML models.

For even faster prototyping, the security functionality is also implemented purely in software. An API is defined so that applications on top of this API can use the cryptographic functions regardless of whether they are provided in hardware or software. All developed code is validated to ensure its correctness.

Prototype-based Demonstration

The secure on-board communication is deployed inside a lab car demonstrating e-safety applications based on vehicle-to-X communication. Cryptographic methods ensure the integrity and authenticity of information exchanged within the vehicle and protect ECUs against theft, tampering, and unauthorised cloning.

Releasing the automotive hardware security modules for deployment in cars on public roads requires further implementation and testing efforts, which are out of scope of this project.

Dissemination of Results

In order that the entire automotive industry may benefit from the project results, the secure on-board architecture and communications protocol specifications are published as open specifications.

The EVITA project partners liaise with related initiatives in the fields of e-safety and embedded security to achieve multilateral synergies.

For further information:

Information Desk
European Commission – Information Society and Media DG
Office: BU31 01/18 B-1049 Brussels
Email: infso-desk@ec.europa.eu
Tel.: +32 2 299 93 99
Fax: +32 2 299 94 99
URL: http://europa.eu/information_society