PROJECT

EVITA

E-safety Vehicle Intrusion proTected Applications

Funding: European (7th RTD Framework Programme)

Duration: Jul 2008 - Dec 2011

Status: Complete with results

Total project cost: €5,890,309

EU contribution: €3,825,993

Call for proposal: FP7-ICT-2007-2

CORDIS RCN : 87605

Background & policy context:

Future 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. Examples of such applications are local danger warnings and electronic emergency brakes. While these functionalities inspire a new era of traffic safety, new security requirements need to be considered in order to prevent attacks on these systems. Examples of such threats are forced malfunctioning of safety-critical components or the interference with the traffic flow by means of fake messages.

Objectives:

Secure and trustworthy intra-vehicular communication is the basis for trustworthy communication among cars or between cars and the infrastructure. Therefore, the objective of the EVITA project was to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle.

By focusing on the protection of the intra-vehicle communication, EVITA complemented other e-safety related projects that focus on the protection of the vehicle-to-X communication.

Furthermore, it is desirable to have a standardised solution for secure automotive on-board networks. This is because:

- this will reduce technical barriers arising from companies developing different solutions independently;
- all over the world, the automotive industry faces similar security problems;
- standards enable third-party semiconductor manufacturers to independently start chip development and production.

Methodology:

Starting from identifying the necessary industrial use cases regarding assembly and field maintenance and compiling profound scenarios of possible threats, the overall security requirements are defined. On this basis a secure trust model will be compiled and a secure on-board architecture and protocol will be specified, verified, validated and, lastly, demonstrated. EVITA will release the architecture and protocol specification as an open standard.

The work plan is as follows:

1. Security requirements analysis

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

2. 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 will be designed. The security functions will be partitioned between software and hardware. The root of trust will be placed in hardware security modules that may be realised as extensions to automotive controllers or as dedicated security controller chips.

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

3. Implementation

   For prototyping, FPGA's will be used to extend standard automotive controllers with the functionality of cryptographic coprocessors. The low-level drivers for interacting with the hardware will be partially generated from UML models.

   For even faster prototyping, the security functionality will also be implemented purely in software. An API will be 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 will be validated to ensure its correctness.

4. Prototype-based demonstration

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

   Releasing t

Parent Programmes:

FP7-ICT - Information and Communication Technologies

Institute type: Public institution

Institute name: European Commission

Funding type: Public (EU)

Lead Organisation:

Frauenhofer Geselschaft Zur Foerderung Der Angewandten Forschung E.v.

Address:
Hansastrasse 27C
80686 MUNCHEN
Germany

Organisation Website:
http://www.fhg.de

EU Contribution: €908,065

Partner Organisations:

Mira Limited

Address:
WATLING STREET
NUNEATON WARWICKSHIRE
CV10 0TU
United Kingdom

Organisation Website:
http://www.mira.co.uk

EU Contribution: €126,750

Fujitsu Semiconductor Embedded Solutions Austria Gmbh

Address:
Freistadter Strasse
4040 Linz
Austria

EU Contribution: €91,451

Robert Bosch Gmbh

Address:
Robert-Bosch Platz
70839 Gerlingen-Schillerhoehe
Germany

Organisation Website:
http://www.bosch.com

EU Contribution: €272,011

Fujitsu Services Ab

Address:
Rosenlundsgatan
11891 Stockholm
Sweden

EU Contribution: €123,894

Imarine Deniz Teknolojileri Ve Arastirmalari Sanayi Ve Ticaret Anonimsirketi

Address:
GOZTEPE MAH. GOKSU EVLERI MENEKSE SOK. B237B ANADO EYKOZ
34815 ISTANBUL
Turkey

Organisation Website:
http://www.infineon.com

EU Contribution: €245,265

Continental Teves Ag & Co. Ohg

Address:
GUERICKESTRASSE 7
60488 FRANKFURT AM MAIN
Germany

Organisation Website:
http://www.continental-corporation.com

EU Contribution: €130,300

Institut Mines-Telecom

Address:
37-39 RUE DAREAU
75014 PARIS
France

Organisation Website:
http://www.institut-telecom.fr

EU Contribution: €250,282

Trialog

Address:
25 Rue Du General Foy
75008 Paris
France

EU Contribution: €234,225

Eurecom

Address:
Route Des Chappes 450 Campus Sophiatech
6410 Biot
France

EU Contribution: €304,762

Katholieke Universiteit Leuven

Address:
Oude Markt
3000 Leuven
Belgium

Organisation Website:
http://www.kuleuven.be

EU Contribution: €159,720

Fujitsu Semiconductor Europe Gmbh

Address:
Pittlerstrasse
63225 Langen
Germany

EU Contribution: €17,598

Bayerische Motoren Werke Ag

Address:
Petuelring 130
80809 MUNICH
Germany

Organisation Website:
http://www.bmwgroup.de

EU Contribution: €260,950

Escrypt Gmbh

Address:
WITTENER STRASSE 45
44789 BOCHUM
Germany

EU Contribution: €700,720

Technologies:

Technologies:

Safety systems
In-vehicle technologies for navigation and safety

Development phase: Research/Invention

Key Results:

The EVITA project results have been distributed through a variety of communication channels to ensure broad utilisation. All project deliverables have been published as open specifications on the project website, so the entire automotive industry may benefit from the project results. Furthermore, workshops were held in August 2009 in July 2010. A Final Workshop, including live vehicle demonstrations, took place in November 2011.

In a broad sense, by helping to reduce road transport problems, the EVITA results are intended to benefit the society as a whole. Other beneficiaries of the project results are the industries that have to cope with communication security problems, likewise to that in the automotive sector. For example: similarly complex communication networks are embedded in airplanes, power stations, house control systems and remote maintenance systems.

Technical Implications

The development of a cost-efficient HSM (Hardware Security Modules) in the EVITA project will help many embedded applications to efficiently improve their security.

Policy implications

The EVITA project strove to establish a standard for secure automotive sensor/actuator networks and to assure a broad utilisation of the EVITA results in the automotive industry. The impact will be multiplied as soon as vehicle manufacturers and electronics suppliers take up on the developed secure architecture specification and protocols.

Other results

The EVITA project has specified hardware and software interfaces. The hardware interface provides the application software with access to the HSM (Hardware Security Modules) functionality. It is asynchronous, almost completely multi-session capable and partly also multi-threading capable. Based on the secure on-board architecture, secure on-board communications protocols have been designed, supporting the security requirements and enabling the specified use cases.

Documents:
EVITA: Project Summary (Final report)

STRIA Roadmaps: Cooperative, connected and automated transport

Transport mode: Road transport

Transport sectors: Passenger transport, Freight transport

Transport policies: Safety/Security

Geo-spatial type: Other