Vehicular Security Hardware

The Security for Vehicular Security Mechanisms

Marko Wolf, escrypt GmbH – Embedded Security

Embedded Security in Cars Conference (escar), Hamburg, November 18th, 2009

The work is co-financed by the European Commission through the 7th framework program.
The need for vehicular security
Possible attacks in a vehicular environment

- **Steal** the vehicle or a valuable component
- **Circumvent** restrictions in hardware or software functionality (e.g., speed locks, feature activation, software updates)
- **Manipulate** financially, legally, or warranty relevant vehicular components (e.g., toll devices, digital tachograph, chip tuning)
- **Spy on** manufacturer's expertise and intellectual property (e.g., counterfeits, industrial espionage)
- **Violate** privacy issues (e.g., contacts, last trips)
- **Impersonate** (e.g., electronic license plate)
- **Misuse** external communication (e.g., disturb, misuse, harm)
- **Harm** passengers, destroy OEM’s reputation (e.g., safety attacks)

✨ Strong need for reliable security mechanisms!
The security of security mechanisms
Why applying standard solutions won’t work

- Beyond “standard attacks” ..
  - Insider attacks
  - Offline attacks
  - Physical attacks

- Many different attackers and attacking incentives

- Many different attack points

- Vehicular IT is client/server, embedded and mobile world

♫ Standard security solutions won’t work!
The security of security mechanisms
Trust in security mechanisms

- **Organizational attacks** (e.g., social engineering) can be prevented by well-thought security processes, secure infrastructures and organizational security policies.

- **Logical attacks** (e.g., cryptographic weaknesses or weak APIs) can be prevented by a secure well-thought security system design and adequate security protocols.

- **Software attacks** (e.g., weak OS mechanisms or malware) can be prevented by reliable software security mechanisms (e.g., secure init, secure RTEs) and the application of hardware security mechanisms that protect & enforce security of software mechanisms.

- **Hardware attacks** (e.g., security artifacts manipulations/read-out, physical locks, side-channels etc.) can be prevented by hardware tamper-protection measures.
Vehicular Security Hardware
What security hardware can help

- **Protects** software security mechanisms by
  - Providing a trustworthy *security anchor* for upper SW layers
  - *Secure generation, secure storage, and secure processing* of security-critical material shielded from all pot. malicious SW

- **Prevents** hardware tampering attacks by
  - Applying *tamper-protection* measures

- **Accelerates** security mechanisms by
  - Applying *cryptographic accelerators*

- **Reduces** security costs on high volumes by
  - Applying highly optimized special circuitry instead of general purpose hardware
Security Requirements
- High level: creation, storage, management & processing of security artifacts (e.g., keys, certificates, random numbers), authentications schemes, secure “timer” (e.g., clock, counter)...
- Low level: symmetric engine, asymmetric engine, hash function, TRNG, secure storage...
- Physical level: Physical coupling, tamper-evidence, tamper-resistance, tamper-response, and side-channel resistance

Functional Requirements
- Latency and band width
- Memory, space, and performance
- Interface compatibility, security updates
- Physical stress...

Other requirements
- Costs
- Patents and export restrictions
- Certification reg. safety (IEC 61508, SIL etc.) and security (e.g., FIPS 140, Common Criteria)
Vehicular Security Hardware
What is the current situation?

- **Proprietary** and **single-purpose** hardware security solutions in vehicular environments, for example:
  - Immobilizer
  - Digital tachograph
  - Toll Collect OBU

- General-purpose hardware security modules for **non-automotive** environments, for example:
  - IBM cryptographic coprocessor
  - Cryptographic smartcards
  - Trusted Platform Module
  - Mobile Trusted Module

.createFromEmail“Are where any solutions for vehicular security HW?”
E-safety Vehicle Intrusion proTected Application
EVITA project objectives

- Powerful ECU security hardware extension that: “.. aims at designing, verifying, and prototyping an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise.”

- Prevent or at least detect malicious malfunction of in-vehicle e-safety applications

- Detect manipulated information from external entities

- Design and verify a ECU security architecture, including
  - ECU hardware security extension
  - ECU software security components
  - Corresponding (e-safety) security protocols

- Implement, demonstrate and validate ECU security architecture for practicability
**Objective:** Automotive capable security hardware ("automotive TPM") for enabling a vehicular security architecture protecting e-safety V2X communications (e.g., emergency break, eCall)

**Program:** FP7-ICT-2007 of the European Community (EC)

**Partners:** BMW, Bosch, Continental, escrypt, EURECOM, Fraunhofer, Fujitsu, Infineon, Institut TELECOM, KU Leuven, MIRA, TRIALOG from Belgium, France, Germany, Sweden, UK

**Duration:** 36 months (July 2008 – June 2011)

**Total cost:** 6 million €

**Further information:** [www.evita-project.org](http://www.evita-project.org)
E-safety Vehicle Intrusion proTected Application
EVITA ECU security architecture

- E-safety application layer
- Security layer
- Microkernel and basic software layer
- Microcontroller abstraction layer
- Microcontroller hardware layer
- Security hardware

Funded by the EU
E-safety Vehicle Intrusion proTected Application
EVITA microcontroller security extension

Microcontroller (schematic)

Flash  CPU  SRAM

Co-Processor
System control

Interface
Interface
...

Crypto control

FPGA Prototype (schematic)

Interface
System control

Crypto control

future integration

Reuse of existing IP
New development, but based on existing know-how
Prototype specific development

Work plan

- 2008: Security requirements analysis
- 2009: Secure on-board architecture design
- 2010: Reference implementation in SW & HW
- 2010: Prototyped-based demonstration (lab car)
- 2011: Publication as open specification
ECU Trusted Module (ETM)
Enabling a holistic vehicular sec. architecture

EVITA security extension in every ECU? Surely not!

- Standardized, minimized ECU hardware security module
  - Protect simpler less security-critical ECUs such as sensor & actuators
  - Prevent software attacks and some hardware attacks (e.g., root artifacts)
  - Capable to interact securely w/ higher level security HW (e.g., EVITA)

- Vehicular equivalent to TCG’s “Mobile Trusted Module (MTM)”
  - Hardware/software co-design for maximum on compatibility & flexibility (e.g., pure chip, hardware anchor + support software, pure software)
  - Secure boot for integrity protection
  - Protected (root) security artifacts processing and storage
  - Secure (in-vehicle) communication (Int. + opt. Auth./Conf.)
  - Unique ECU identification
**Security requirements**

- Non-detachable connected with ECU hardware
- Minimal immutable core root of trust code
- Minimal internal non-volatile memory for storing root security artifact(s)
- Isolated security processing environment, e.g.,
  - Additional parallel environment (e.g., dedicated RAM and μC)
  - Physical isolation mechanism (e.g., ARM TrustZone)
  - Strictly logical isolated environment (e.g., microkernel)
- Security enabled ECU processor and software stack
- Only standardized, established security algorithms (e.g., NIST, FIPS, BSI)
- ...
Other requirements

- Physical stress resistance and other functional demands (latency etc.)
- Compatibility with other (higher-level) security modules and security mechanisms and with existing ECU microprocessor architectures
- Standardized security classification according to the individual requirements to enable comprehensive flexible architectures, e.g.,
  - **Security level I**: Pure software application
  - **Security level II**: Key security artifacts shielded
  - **Security level III**: All security functionality shielded
  - **Security level IV**: Tamper-protection
- Open and patent free specifications for cost-effective OEM-wide application
Strong Vehicular Security Architectures
Coupling ETM and EVITA enabled ECUs

- Powerful EVITA extension in 2 - 4 central multi-purpose ECUs
  - Central gateway
  - Immobilizer
  - Engine control
  - Front/rear module

- Small ETM in less, but security-critical client ECUs
  - Critical sensors: e.g., wheel, acceleration, pedal sensors
  - Critical actuator: e.g., breaks, door locks, turn signal indicator
  - Critical small ECU: e.g., GPS module, lighting, clock

Secure cooperation of small ETM and powerful EVITA security extensions allows to create a cost-effective, flexible, and holistic vehicular security architecture.
Standardized security hardware is **essential** for the security of vehicular security mechanisms.

Vehicular security hardware helps **preventing** almost **all** software attacks and many physical attacks.

Automotive proof security hardware (or even standards) **currently not available** (neither low-level nor high-level).

However, open **ETM** and **EVITA** prototypes could be **promising opportunities** to act as effective, trustworthy and cost-effective hardware security anchors in vehicular environments.
escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum
info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211

Dr.-Ing. Marko Wolf
Senior Engineer
mwolf@escrypt.com

Dipl.-Psych. Katrin Mannheims (MBA)
Geschäftsführerin
kmannheims@escrypt.com

Dr.-Ing. Jan Pelzl
Geschäftsführer
jpelzl@escrypt.com

Dr.-Ing. Thomas Wollinger
Geschäftsführer
twollinger@escrypt.com

Dr.-Ing. André Weimerskirch
CEO USA
aweimerskirch@escrypt.com