Privacy and Data Protection for Drivers
A Contribution from the EVITA project

Dr. Timo Kosch
BMW Group Research and Technology
Hanauerstr. 46
80992 München, Germany

SEVENTH FRAMEWORK PROGRAMME

Project partners

Project Motivation: Use Cases

Car2Car

Car2NearField

Car2TrafficInfrastructure

Car2MobileDevice

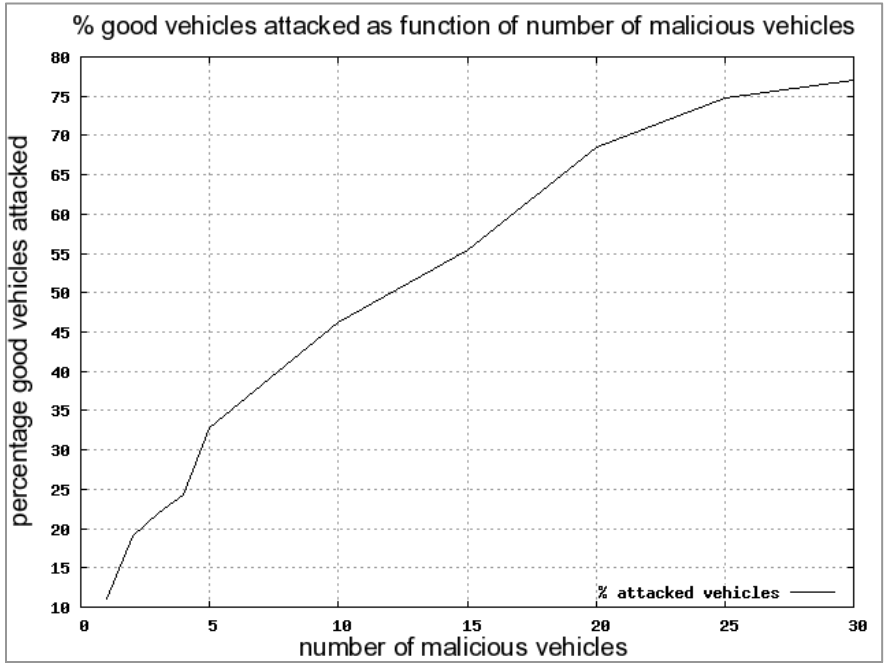
Car2Home

Car2CustomerPortal

Car2Enterprise

Threats

- **Simulation**
  - Simulation of 400 honest/good vehicles
  - Variable number of attackers randomly put in scenario
- **Results**
  - 3 attackers have hit already ≈ 20% honest/good vehicles
  - 10 attackers are able to interfere ≈ 50% of honest/good vehicles



Project Scope: Focus on in-vehicle systems

- The attacks on *external* communication:
  - must be prevented or
  - at least be detected and contained,
  - so that fake messages injected into the (wireless) communication infrastructure are properly identified and eliminated before influencing eSafety applications.

- Attacks on *in-vehicle* system infrastructure
    - via physical access or
    - via wireless interface
  - must be prevented or
  - at least be detected and contained,
  - so that fake messages are properly identified and eliminated before influencing applications.

Project Scope: Focus on in-vehicle systems

- Targeting requirements of eSafety eSecurity WG and C2C-CC
- Research on a secure on-board architecture:
  - Safeguard future cooperative eSafety applications
  - Tampering with cars can cause impact on other cars
- Software is not secure enough for tomorrow's cooperative eSafety applications:
  - Looking for appropriate SW and HW measures for ensuring security
  - Finding a suitable solution using SW and HW security
  - Research on architecture (centralized vs. distributed)
  - Defining overall security architecture for cooperative vehicles
- Defining hardware co-processor:
  - Secure on-board and V2X communication
  - Secure storage and processing of secret material
  - Hardware security anchor
  - High throughput only possible with hardware acceleration

Project Scope: Complementary Security Activities

SEVECOM — Secure vehicular Communication

EVITA — In-vehicle Security Hardware

PRECIOSA — Privacy for ITS Communication

COMSafety — Consolidation

CAR 2 CAR Communication Consortium — Harmonization

ETSI — Standardization

Field Test Preparation

PRE-DRIVE C2X

Project Objectives

- Modular, (cost-) efficient security for:
  - In-vehicular devices: sensors, actuators, ECUs with
  - HW and SW architecture securing SW applications based on the HW modules
- in order to:
  - enforce ECU software protection against SW attacks
  - plus optional selected HW attacks depending on the level of HW tamper protection
  - provide ECU HW/SW-configuration attestation (reliable proof of setup)
  - support/process ECU to ECU communication protection
  - support/process V2X communication and privacy protection
- based on:
  - hardware based security anchors
  - software security layer, mechanisms and API specification
  - that make use of HW security module BUT can also be built completely in SW

Project Structure

Dissemination and external interfaces
- **Open specifications**
- **Liaison with related initiatives in the field of eSafety**

Goals

Security Requirements Analysis	Secure On-board Architecture Design	Security Architecture Prototyping	Validation & Demonstration
• Use cases • Threat & risk Assessment • Legal aspects	• Trust model • Software/ hardware partitioning • HW security module design • SW security design & protocols • Model-based verification	• Based on FPGAs and software • Partial model-based code generation • Code validation & test	• Prototypical integration in vehicular environment • Showing safety applications based on V2X communication

Milestones

- **M1 (Q1 2009):** Risks & Requirements available
- **M2 (Q4 2009):** Security & Trust Model available
- **M3 (Q2 2010):** Secure On-board Architecture & Protocol Specification available
- **M4 (Q4 2010):** Model based Verification available FPGA Prototype & SW framework available
- **M5 (Q2 2011):** Final validation & Demonstrator available

Key Results of the 1st year

WP1000 Liaison Activities

- CAST Workshop in Darmstadt
- Working on Hardware Security strategy with HIS
- Planned Liaison Workshop November 5th/ Wolfsburg

WP2000 Security Requirement Engineering

- **Use Cases:**
  - Categorization into 6 fields
  - Detailed formal information flow
- **Threat and Risk Analysis:**
  - Threat identification based on attack trees
  - EVITA concept for risk assessment, based on
    - severity of an attack (based on ISO 26262)
    - probability of success (ISO/IEC 15408 & 18045)
  - **Security Requirements:**
    - Formal and Semi-formal description

EVITA

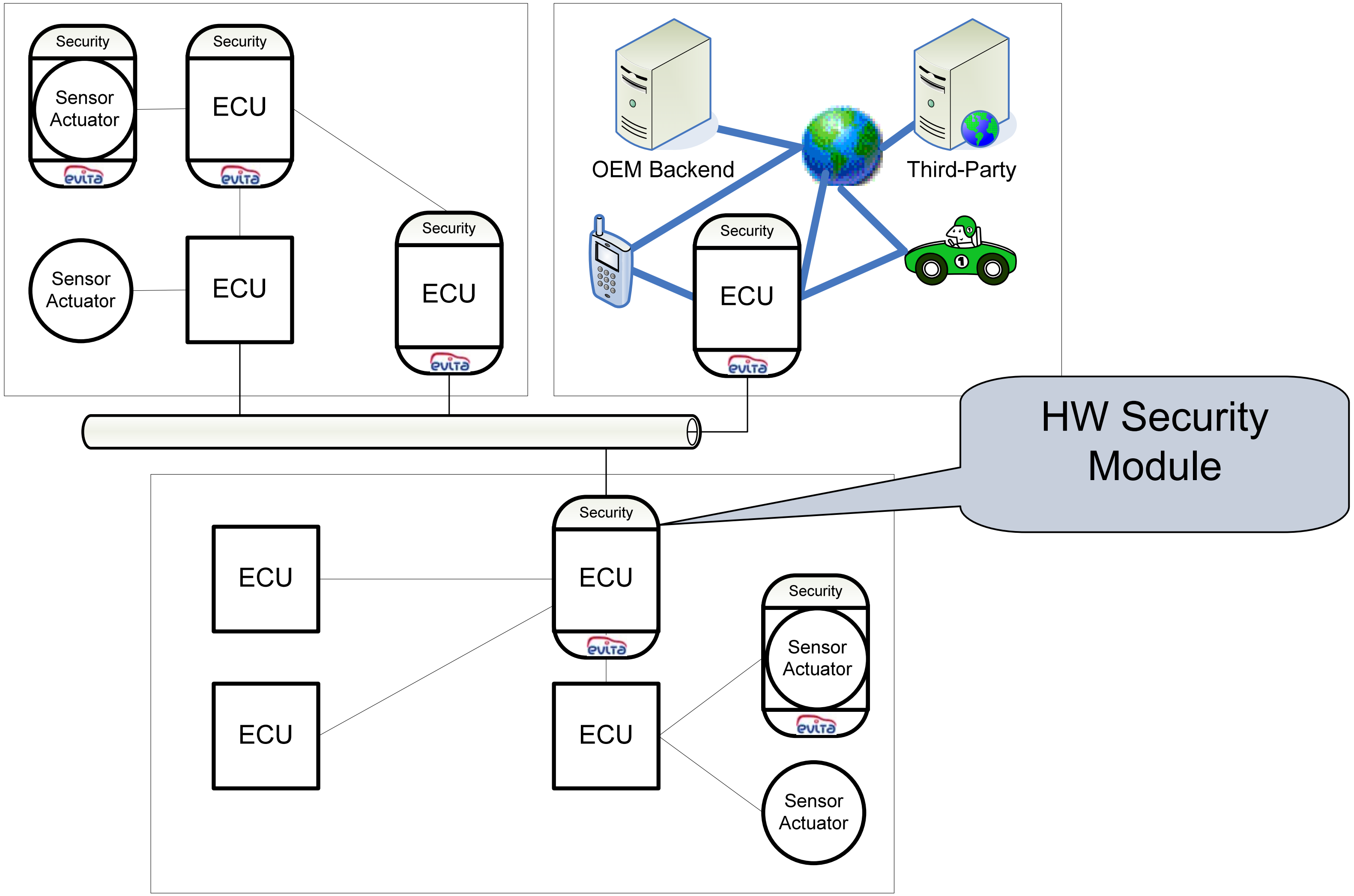
WP3000 Secure On-board Architecture Design and Verification

- First draft of Security and Trust Model:
  - Specification of a Meta-model for Trust and Security
  - Formal Security Refinement Process
- EVITA Architecture:
  - Design of a three-leveled HW architecture
  - Discussion on integration of EVITA library with AUTOSAR

WP4000 Security Architecture Implementation

- Defined and agreed on prototype hardware
- Defined and agreed on implementation tool chain

Basic Idea: EVITA Overall On-Board Architecture



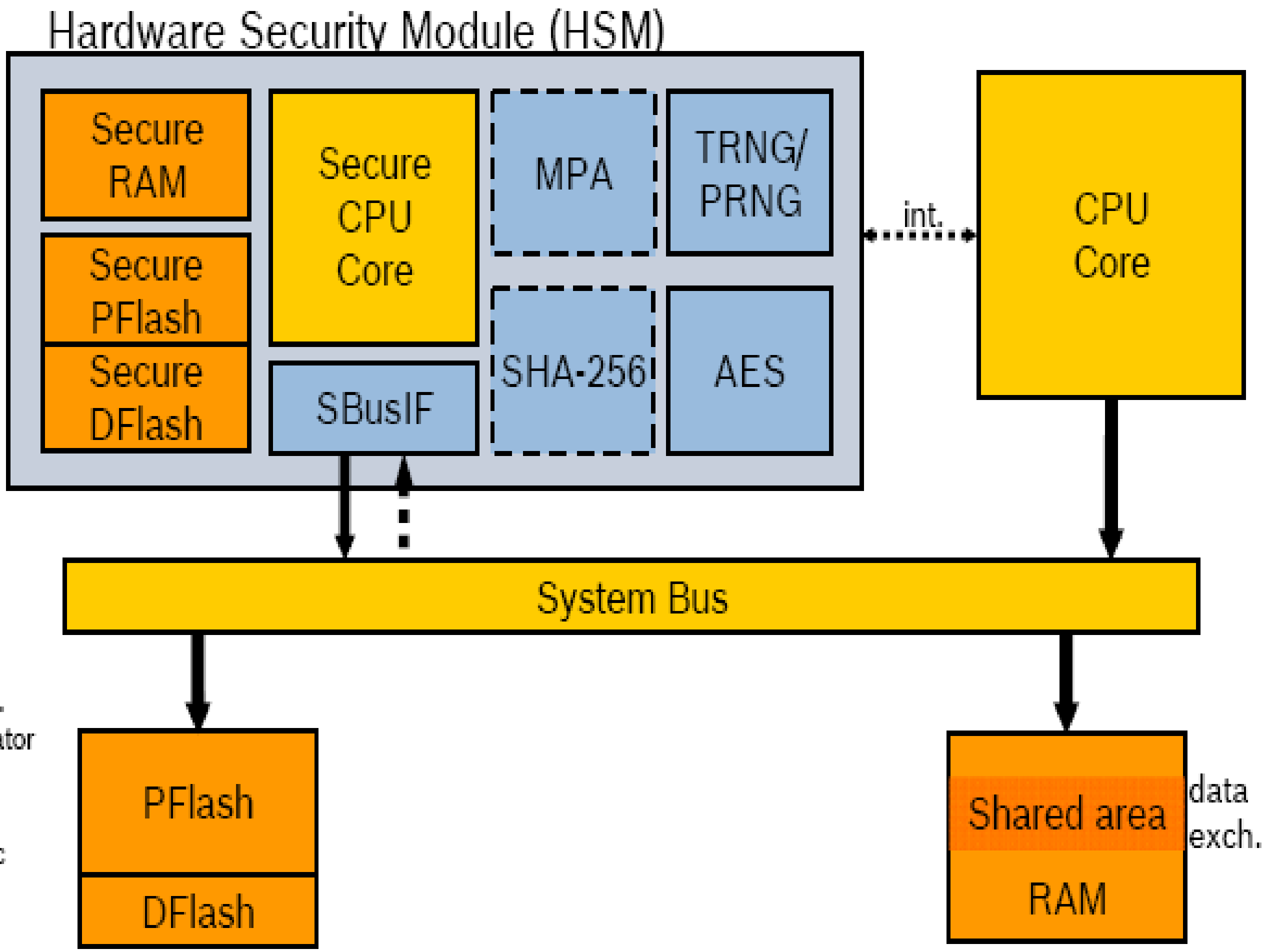
General Structure of Hardware Security Module

- Main goal
  - Providing secure platform for cryptographic functionalities that support use cases
- Features
  - Secure Storage
  - HW Cryptographic Engines
  - Secure CPU Core
  - Scalable Security Architecture
- Advantages
  - Flexibility
  - Extendability
  - Migration Path from existing SW solutions

General Structure of Hardware Security Module

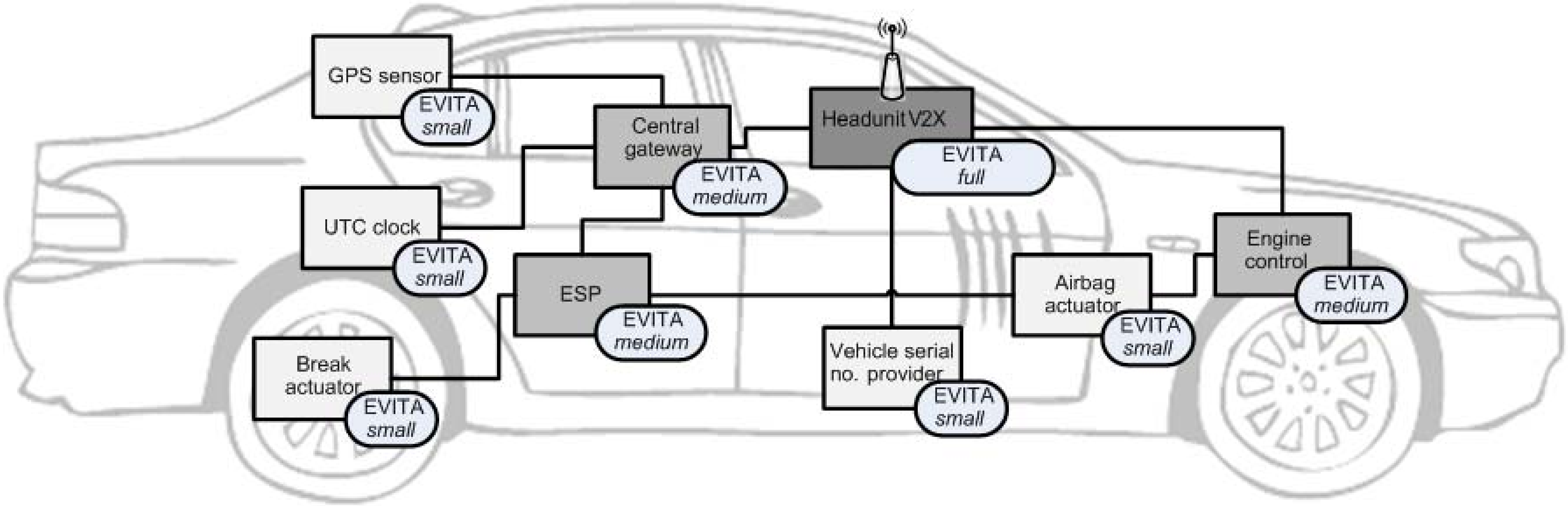
- **HSM physically separate from CPU**
  - Less secure than a single chip: connection between CPU and HSM not secure.
  - Suitable for short-term designs or low-security applications with very small production runs
  - Expensive: extra chip costs more due to the extra pins,
- **HSM in the same chip as the CPU but with a state machine**
  - More secure than external chip and more cost-effective
  - Not flexible: Hardware structure not modifiable. Automotive microcontroller life cycle is more than 20 years
  - Suitable for very high security applications with very short lifetimes
  - implementing asymmetric cryptography using this structure requires large (and inflexible) multi-precision arithmetic hardware.
  - Cryptographic applications will need to be implemented at the application CPU level: possible performance issues.
  - Changing a state machine requires hardware redesign and is very expensive
- **HSM in the same chip as the CPU but with a programmable secure core**
  - proposed solution
  - Secure and cost-effective
  - Flexible because of programmable core.
  - Usable for other industries

General Structure of Hardware Security Module



AES: Advanced Encryption Std.
RNG: Random Number Generator
TRNG: True RNG
PRNG: Pseudo RNG
MPA: Multi-Precision Arithmetic
SBusIF: System Bus Interface
PFlash: Program Flash
DFlash: Data Flash

EVITA On-Board Architecture Deployment



Next Steps in Year 2

– Finalization of Security and Trust Model

– Finalization of EVITA Security Architecture

– EVITA Security Protocols

– Model based Verification

– Implementation

Thank you for your attention.

www.evita-project.org

Benjamin Weyl
Chair WG Security & Middleware

CAR 2 CAR
COMMUNICATION CONSORTIUM

www.car-2-car.org

timo.kosch@bmw.de
benjamin.weyl@bmw.de

BMW Group
Research and Technology