Vehicular On-board Security: EVITA Project

C2C-CC Security Workshop

5 November 2009 VW, MobileLifeCampus Wolfsburg

Hervé Seudié

Corporate Sector Research and Advance Engineering

Robert Bosch GmbH

Outline

1. Project Scope and Objectives
2. Security Requirement Analysis
3. Hardware Security Modules as security anchor
4. Software Architecture
5. Summary & Outlook

Project Scope (1): Focus on in-vehicular systems

- Securing the *external* car2X communication:
    - Via wireless interface

  – Goals: Prevention from attacks, Detection from attacks, Containment of attacks

- Securing the *in-vehicular* system infrastructure
    - via physical access
    - via wireless interface

  – Goals: Prevention from attacks, Detection from attacks, Containment of attacks

Project Scope (2): Focus on in-vehicular systems

– Targeting requirements of eSafety, eSecurity WG and C2C-CC

– Research on a secure on-board architecture:
  – Protection of high critical eSafety applications
  – Defining overall on-board security architecture for cooperative vehicles

– Software is not secure enough for tomorrow's cooperative eSafety applications:
  – Looking for appropriate SW and HW measures for ensuring security
  – Finding a suitable partitioning of SW and HW security

– Defining hardware co-processor:
  – Secure storage and processing of secret material
  – High throughput only possible with hardware acceleration

Project Scope (2): Complementary Security Activities

SEVECOM — Secure vehicular Communication

EVITA — In-vehicular Security Hardware

PRECIOSA — Privacy for ITS Communication

COMeSafety — Consolidation

CAR 2 CAR — Harmonization

ETSI — Standardization

Field Test Preparation (PRE-DRIVE C2X)

Project partners

BMW Group Research and Technology

BOSCH

Continental

escrypt Embedded Security

EURECOM Sophia Antipolis

Fraunhofer SIT

Fraunhofer ISI

FUJITSU

infineon

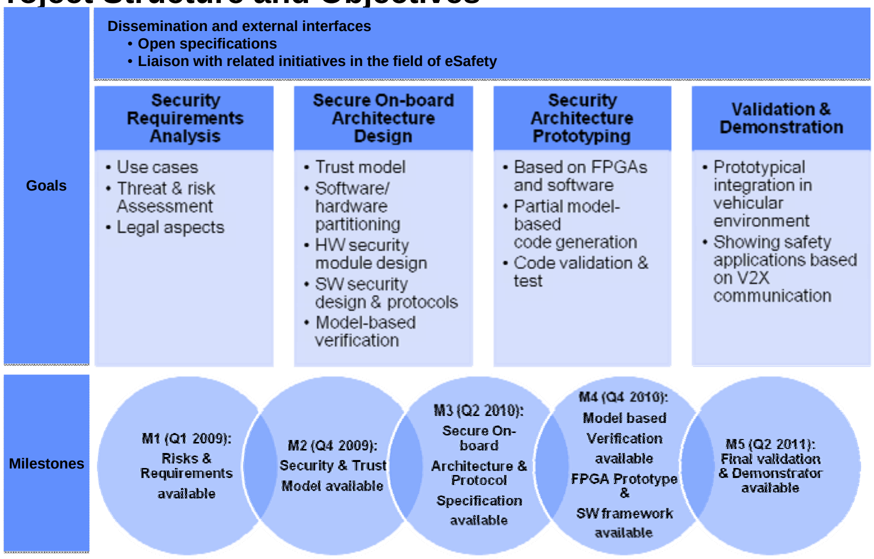
KATHOLIEKE UNIVERSITEIT LEUVEN

MIRA

TELECOM ParisTech

TRIALOG

Project Structure and Objectives



Security Requirement Analysis

- **Use Case Categories**
  - Car2MyCar, MyCar2Car, Car2I, I2Car
  - Nomadic Devices, USB Sticks, MP3
  - Aftermarket Components, Diagnosis

- **Risk and Threat analysis**
  - **Risk** associated with an attack is a function of:
    - **severity** of impact (i.e. harm to stakeholders)
    - **probability** of successful attack
    - for safety-related risks, **controllability** of hazardous situations needs to be considered
  - Not possible to quantify severity and probability in many applications

➔ need to relate severity and probability to attack trees resulting from security threat analysis

Interpretation of attack trees

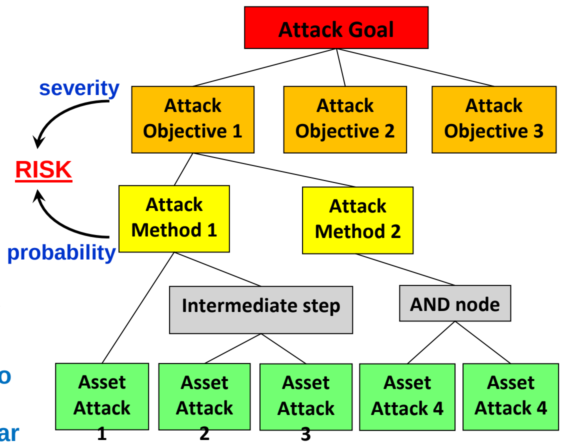
Level 0: Attack Goal
(Illegal benefit to attacker)

Level 1: Attack Objectives
(Harm for stakeholders – severity)

Level 2: Attack Methods
(Combined probability of successful attack)

Intermediate/dummy nodes

Level 3: Asset Attacks
(Attack potential – related to probability of success for specific attacks on particular assets)



Security severity classification – a 4-component vector

Class	Safety	Privacy	Financial	Operational
S0	No injuries.	No data access.	No financial loss.	No impact on operation.
S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).	Low level loss (~€10).	Impact not discernible to driver.
S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.	Moderate loss (~€100). Low losses for multiple units.	Driver aware. Not discernible in multiple units.
S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.	Heavy loss (~€1000). Multiple moderate loss.	Significant impact. Multiple units with driver aware.
S4	Fatal for multiple vehicles.	Driver identity access for multiple units.	Multiple heavy losses.	Significant impact for multiple units.

Attack potential and probability

- **Attack potential** evaluation
  - using established, structured approach from "Common Criteria"
  - applied at asset attack level
- Indicative of **attack probability** (inverse relationship)
  - numerical scale used to represent relative ranking of attack probability

Attack potential		Attack probability	
Rating	**Description**	**Likelihood**	**Ranking**
0–9	Basic	Highly likely	5
10–13	Enhanced basic	Likely	4
14–19	Moderate	Possible	3
20–24	High	Unlikely	2
≥25	Beyond high	Remote	1

Sample asset attack ratings

Attack tree node	Asset (attack)	Required attack potential		Asset-attack probability
		Value	Rating	
[6.2.2.1]	GPS (jamming)	4	Basic	5
[6.3.2.2], [9.1.1.1], [9.3.3.3],	Communications Unit (denial of service)	11	Enhanced-Basic	4
[15.1.1], [15.2.1]	In-car User Hardware Interfaces (access)	15	Moderate	3
[3.2.2.4.2.2], [4.3.2.1.2.2]	In-car Sensors (spoof)	24	High	2
[8.3.1]	Environment Sensors (flash malicious code to firmware)	41	Beyond High	1

Risk analysis – attack tree table

Sample risk analysis – attack active brake

Attack Objective	Severity (S)	Attack Method	Risk level (R)	Combined attack method probability (*A*)	Asset (attack)	Asset-attack probability (*P*)
9.1 Delay active braking (e.g. by x ms)	$S_S=0$ $S_P=0$ $S_F=0$ $S_O=2$	Delay computation	$R_S=R0$ $R_P=R0$ $R_F=R0$ $R_O=R3$	4	9.1.1.2 Chassis Safety Controller (denial of service)	2
					9.1.1.1 Communications Unit (denial of service)	**4**
		Delay data transmission	$R_S=R0$ $R_P=R0$ $R_F=R0$ $R_O=R4$	5	9.1.2.1 Wireless Communications (jamming)	**5**
					9.1.2.2 Backbone Bus (jamming)	4
					9.1.2.3 Chassis Safety Bus (jamming)	4

Prioritising security requirements

- Requirements classified in terms of security properties that they represent
  - confidentiality, privacy, availability, authenticity etc.
- Requirements mapped to use cases, attack trees and asset attacks
- Priority indicated by summary of risk analysis
  - collates results from risk assessment of all attack trees
  - organized by **asset** (*what to protect*) and **attack type** (*how to protect it*)
    - mapped to groups of security requirements
  - identifies risk levels found from attack trees and the number of occurrences
- Interpretation
  - few instances and/or low risk suggest low priority for protection
  - high risk and/or many instances suggest higher priority for protection

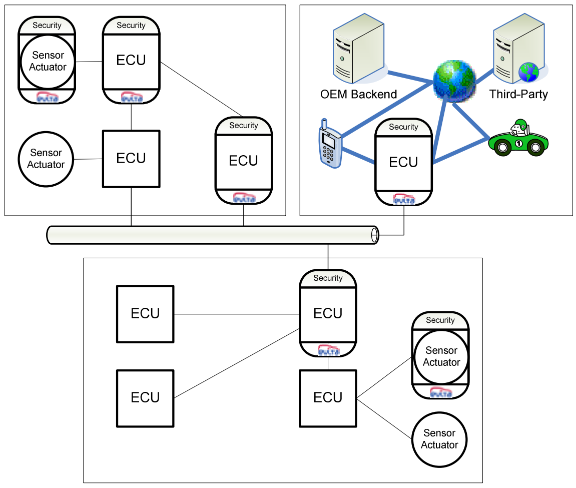
Risk-based security requirement priorities

Identified threats		Risk analysis results		Security requirements
Asset	*Attack*	*Risk level*	*Instances*	
Chassis Safety Controller	Denial of service	1 2	3 1	Authenticity_6, Availability_102, Availability_106 **Low priority**
	Exploit implementation flaws	4 5	1 1	Authenticity_1, Authenticity_2, Authenticity_3 …
Wireless Comms	Corrupt or fake messages	2 3 4 5 6 7	5 5 4 1 4 3	… Confidentiality_1, Confidentiality_2, Authenticity_101 … **Important to protect against this asset attack**
	Jamming	4 5	3 2	… Availability_107, Availability_108, Integrity_102

Vehicular On-board Architecture Requirements

- **Integrity of hardware security module:**
  - *Prevention/detection of tampering with hardware security modules*
- **Integrity and authenticity of in-vehicle software and data:**
  - *Unauthorized alteration of any* in-vehicle software must be infeasible / detectable
- **Integrity and authenticity of in-vehicular communication:**
  - *Unauthorized modification of* data can be detected by the receiver
- **Confidentiality of in-vehicular communication and data:**
  - *Unauthorized disclosure of confidential* data sent or stored must be infeasible.
- **Proof of platform integrity and authenticity to other (remote) entities:**
  - Capability to prove the integrity and authenticity of its platform configuration
- **Access Control to in-vehicle data and resources:**
  - *Enabling availability and well-defined* access to all data and resources

Basic Idea: EVITA Overall On-Board Architecture



Hardware Security Module as security anchor

- **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

Hardware Security Module: Analysis

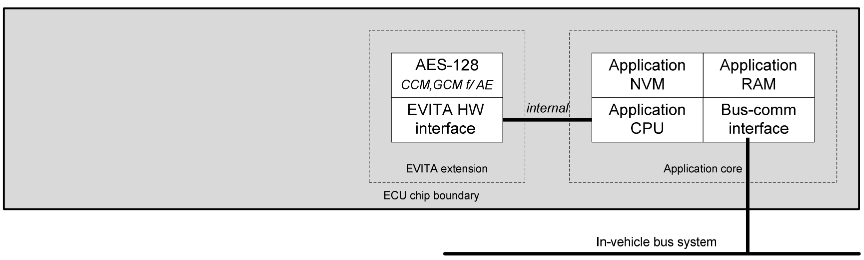
- **HSM physically separate from CPU**
  - Less secure than a single chip: connection between CPU and HSM not secure.
  - Suitable for short-term designs or low-security applications with very small production runs
  - Expensive: extra chip costs more due to the extra pins

- **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
  - 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

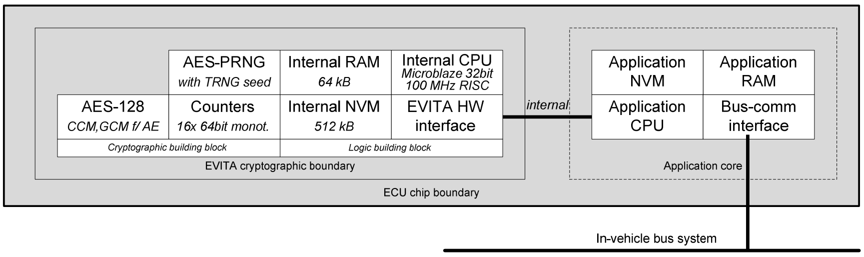
Different topologies of HSM

- EVITA light version (Sensor/Actuator level)



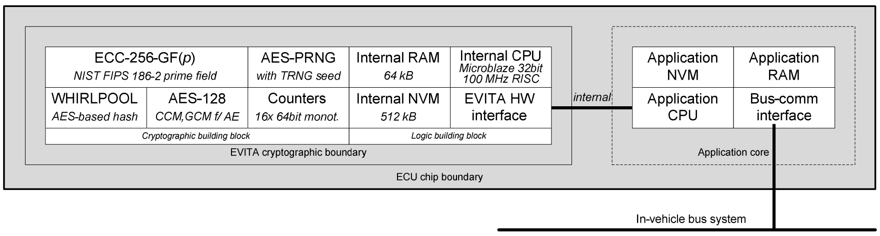
Different topologies of HSM

- EVITA Medium version (ECU Level)



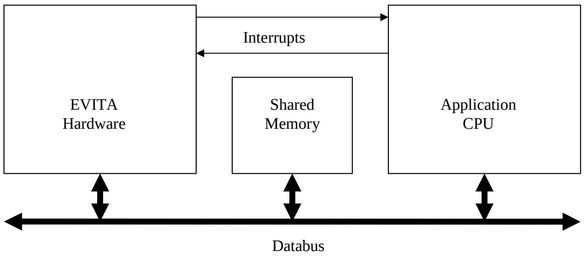
Different topologies of HSM

- EVITA Full version (ECU Level – V2X)

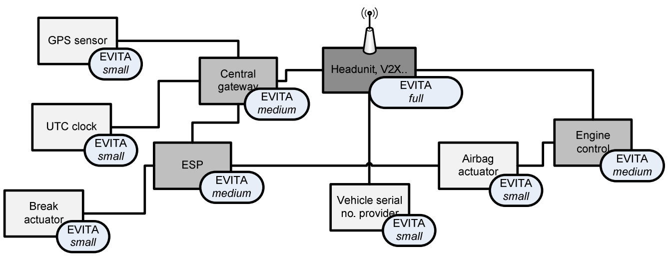


Hardware interface between HSM and application CPU

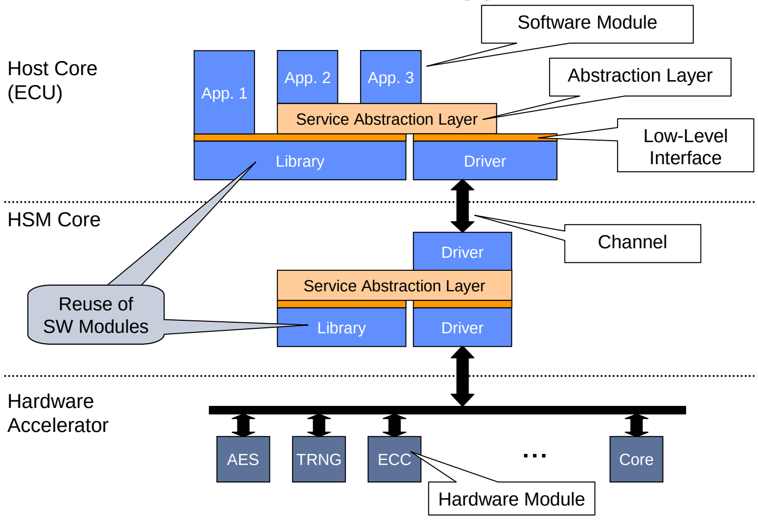
- HSM and application CPU has write/read rights for the Shared Memory
- Trigger through interrupt
- Polling optional: periodically check of the result buffer



EVITA On-Board Architecture Deployment



Software Architecture: Autosar Approach



Summary & Outlook

- **Summary:**
  - Focus on securing in-vehicular applications and components
  - Requirements analysis based on Standards: ISO 26262 & ISO/IEC (15408 & 18045)
  - Design of a three-leveled HW architecture
  - Design of a security software architecture based on AUTOSAR
- **Outlook:**
  - Open specification of soft- and hardware design and protocols: Input for standardization
  - Proof-of-concept by designing with formal methods and tools
  - Prototypical implementation using the AUTOSAR stack CUBAS from Bosch
  - Integration into a demonstrator

Thank you for your attention.

www.evita-project.org

Hervé Seudié
Robert Bosch GmbH
Corporate Sector Research and Advance Engineering
Herve.seudie@de.bosch.com