Vector Cyber Security Solution

Embedded Software, Services and Tools
Agenda

- Introduction
  Security Mechanisms for Embedded Automotive Systems
  Services
  Vector Tools in the Context of Security
  Summary
Cyber Security does not start or end with Cryptography

- Asset Definition
- Threat and Risk Assessment
- Derivation of Security Goals
- Security Architecture Design
- Technical Security Concept Design
- Secure Implementation of Nominal Function and Security Mechanisms
- Security Validation
- Penetration Testing
- Fuzz Testing
- Functional Security Testing

Supporting Processes
Introduction

Vector Security Solution

Embedded Software

Services

Tools
Introduction

- **Security Mechanisms for Embedded Automotive Systems**
  - Services
  - Vector Tools in the Context of Security
  - Summary
Security Mechanisms for Embedded Automotive Systems

Layered Security Concept (Logical View)

Associated Security Concepts

- Secure communication to services outside the vehicle
- Intrusion detection mechanisms
- Firewalls
- Key Infrastructure / Vehicle PKI
- Synchronized secure time
- Authenticity of messages
- Integrity and freshness of messages
- Confidentiality of messages
- Key storage
- Secure boot and secure flash
- Crypto library
- HW trust anchor (HTA)
Security Mechanisms for Embedded Automotive Systems

Security Mechanisms allocated in Example Architecture

- **Firewall**
- **Key Infrastructure**
- **Crypto Primitives**
- **Monitoring / Logging**
- **Hypervisor**
- **Intrusion Detection / Prevention**
- **Secure On Board Com.**
- **Secure Off Board Com.**
- **Download Manager**
- **Secure Flash/Boot**
- **Secure Synchronized Time Manager**

- **Central Gateway**
- **Connectivity Gateway**
- **Diagnostic Interface**
- **Instrument Cluster**
- **Head Unit**
- **DSRC**
- **4G LTE**
- **CU**
- **Laptop**
- **Tablet**
- **Smartphone**
- **Smart Charging**
- **Powertrain DC**
- **Chassis DC**
- **Body DC**
- **ADAS DC**
MICROSAR 4.3ff and FBL Security Modules

Security Mechanisms for Embedded Automotive Systems

KeyM¹

Application

RTE

OS
SYS
POLM¹
KSM¹
CSM
CRYIF
CRYDRV(SW)

MEM
DIAG
SLOG¹

COM
SECOC
FWM¹
IDSM¹
CAN
CANFW¹
CANIDS¹
SCANTSYN¹

Microcontroller
Hardware Trust Anchor (HTA)

FBL Application

HIS Security Module
Runtime Protection
Update Authorization
Secure Update Manager
Sec. Bootmanager (HSM)

¹ Extensions for AUTOSAR

Vector Standard Software
Future Security Modules
Cryptographic Functions with and without HW-Support

- **Crypto Service Manager – CSM**
  - SWC use CSM through RTE
  - BSW/CDD use CSM by inclusion
  - Asynchronous operation possible
  - Callback indicates application

- **Crypto Interface – CRYIF**
  - Provides standard interfaces for specific cryptographic functions

- **Crypto Driver – CRYDRV**
  - Implementation of cryptographic functions
  - CRYDRV (SW): Usage of SW-libraries
  - CRYDRV (HW): Usage of resources and capabilities of HW-Trust Anchors (SHE, HSM, TPM,...)
Secure on board Communication

- **SecOC sends & receives secured PDUs**
  - SecOC can use security hardware acceleration via CSM
  - RTE-interface

- **Secured PDUs are protected against**
  - Spoofing
  - Manipulation
  - Replays

- **Authentication:**
  - MAC or
  - Signature
Security Mechanisms for Embedded Automotive Systems

Management of Cryptographic Material (Keys, Certificates)

- **Key Manager (KeyM)**
  - OEM specific implementation
  - Handles Key/Certificate update
  - Key Generation
  - Certificate Verification
  - Provides Key Material to application components

- **Key Storage Manager (KSM)**
  - Stores Key Material
  - Abstraction to Secure Hardware
  - Verifies Integrity and Authenticity of Cryptographic Material
  - In case of NvM storage, Keys can be encrypted and authenticated by checksum
  - Decryption and verification on initialization or on request
  - Propagates Keys to BSW
Firewalls and Intrusion Detection Systems

- **Firewall Manager - FWM**
  - CAN Firewall – CANFW
  - Ethernet Firewall - ETHFW

- **Intrusion Detection System Manager – IDSM**
  - CAN Intrusion Detection System – CANIDS
  - Ethernet Intrusion Detection System - ETHIDS
Agenda

Introduction

Security Mechanisms for Embedded Automotive Systems

- **Services**
  - Vector Tools in the Context of Security
  - Summary
Security Studies

- Asset Definition
- Threat and Risk Assessment
- Derivation of Security Goals
- Security Architecture Design & Analysis
- Security Concept Design & Analysis
- Secure Implementation of Nominal Function and Security Mechanisms
- Security Validation
- Penetration Testing
- Fuzz Testing
- Functional Security Testing

Supporting Processes

▶ Security Studies
  - Examining customer defined security concepts
  - Proof of concept implementation of security mechanisms
  - Incident analysis
  - Performance analysis
Security Engineering

• (Interim) Security manager for system, function or ECU
• Integration of security engineering methods in customer processes
• Application of security engineering methods
• Technical consulting for security testing

Services

Security Engineering

- Asset Definition
- Threat and Risk Assessment
- Derivation of Security Goals
- Security Architecture Design & Analysis
- Security Concept Design & Analysis
- Secure Implementation of Nominal Function and Security Mechanisms
- Functional Security Testing
- Fuzz Testing
- Penetration Testing
- Security Validation
- Supporting Processes
Security Architecture Analysis & Design

- Analysis of released or future security architectures
- Support in specification
- Benchmarking of vehicle security architectures

Services

- Asset Definition
- Threat and Risk Assessment
- Derivation of Security Goals
- Security Architecture Design & Analysis
- Security Concept Design & Analysis
- Secure Implementation of Nominal Function and Security Mechanisms
- Security Validation
- Penetration Testing
- Fuzz Testing
- Functional Security Testing
- Supporting Processes
Vehicle Security Architecture Implementation

- Development of vehicle security architectures for series
- Implementation based on established standards and customer specific extensions
- Integration support
Automotive Security Training

- Onsite or offsite training in security aspects relevant for automotive
- Training modules for different goals
  - Processes & standards
  - Basic crypto concepts
  - Technical security mechanisms

Services

- Asset Definition
- Threat and Risk Assessment
- Derivation of Security Goals
- Security Architecture Design & Analysis
- Security Concept Design & Analysis
- Secure Implementation of Nominal Function and Security Mechanisms
- Functional Security Testing
- Fuzz Testing
- Penetration Testing
- Security Validation
- Functional Security Testing
- Fuzz Testing
- Penetration Testing
- Security Validation
- Security Concept Design & Analysis
- Secure Implementation of Nominal Function and Security Mechanisms
- Supporting Processes
Agenda

Introduction
Security Mechanisms for Embedded Automotive Systems
Services

▶ Vector Tools in the Context of Security

Summary
Vector Tools in the Context of Security

Overview

Services

Embedded Software

Tools
Vector Tools in the Context of Security

Challenges for Testing

- Increasing integration of security mechanisms in current and new architectures
- New challenges for automotive testing
  - Testing of security
  - Testing despite security
Automotive Security Testing

- **Functional security testing**
  - Test of security related functions for correct behavior and robustness

- **Vulnerability scanning**
  - Test for known security vulnerabilities

- **Fuzzing**
  - Try to find new vulnerabilities of an implementation by sending malformed input to target system
  - Good benefit-to-cost ratio.

- **Penetration testing**
  - Highly individual & creative testing of the whole system (SW+HW) performed by a “smart human tester”
  - Based on many years of “hacking” experience
Fuzz Testing with CANoe

**Benefits**

- Highly integrated solution (no need to configure via command line)
- GUI is familiar to automotive testing engineers
- Fuzzer configuration can handle automotive specific data types
- Is offered in package with technical consulting for security testing
Testing despite Security

Testing of nominal functions regardless of security mechanisms

- **Confidentiality**
  - "But I need to be able to read any message for debugging purposes"

- **Authenticity / Freshness**
  - "But I need the system to accept data from my log file in order to replicate the problem!"

**Complexity drivers**

- Different types of cryptographic keys
- Security protocols
- Different security architectures
- Different processes / backends
Vector Tools in the Context of Security

Enabling Analysis and Test of Secured Networks

- **Benefits**
  - Highly integrated solution (no need to adapt existing tool chains)
  - Provides consistent interfaces for different tools and security sources
  - Security source plugins can be developed by customer or ordered as a development service
Agenda

Introduction
Security Mechanisms for Embedded Automotive Systems Services
Vector Tools in the Context of Security

Summary
Vector Security Solution

Summary

Services

Embedded Software

Tools
For more information about Vector and our products please visit

www.vector.com

Author:

Dr. Eduard Metzker

Vector Informatik GmbH