Security Aspects for Software OTA
Axel Freiwald
Infineon Technologies
23.6.2016
All OEMs Will Implement Software OTA As Soon As Possible

› **Motivation:**
  Save on recalls caused by software bugs

› **Evolution not Revolution:**
  Implement into vehicle’s network with as little changes as possible

› **Challenge:** Cyber Security
SW OTA Security Threats

› Cloud connections are typically active all the time and thus OTA interfaces are potentially accessible for hackers.

› SW OTA services provide doors for attacks to permanently endanger the operation of vehicles. Typical examples: Functional changes, Tuning, Trojans

› Already the potential to attack vehicles is threatening Tier1s, OEMs and politicians.
Equal Basics for both flows to update ECUs via OBD or OTA:
- Precondition: for both flows the new software version must be officially released and meet all legal requirements (Fahrzeugfreigabe)
- ECUs receive the commands and service packs via their bus interfaces i.e. in UDS format.
- The onboard functions for updating software are handled by i.e. the Secure FLASH Bootloader
- Restrictions:
  - Only parts of the code can get updated. i.e. the secure FLASH Bootloader itself is excluded.
  - If multiple ECUs are being updated at the same time, it must be assured that all updates together are executed successfully. Partially updated vehicles are not released and are not allowed to drive.

Differences OTA to OBD updates:
- With OBD updates the external diagnostics tool acts as the update server. With OTA the central update services must get implemented inside of the vehicle.
- Some functions are additionally excluded with OTA especially those which might be needed during the update for process execution or for safety reasons (electric parking brake, door control, ...)
- The update flow must be power fail prove. Long update times are especially vulnerable for power fails.
Evolutionary Software OTA Flow
From Software Development to Vehicle Reboot

Transport via Internet

Over The Air – Telematics unit TCU
› Receive and decrypt from secure wireless protocol

Download service pack
› Check OEM authenticity
› Setup encryption services
› Service pack stored in vehicles central storage
› Verify data
› Unpack for ECUs

Updating the vehicle i.e. using UDS
› Start UDS programming session
› Send service packs to ECUs in small blocks using UDS protocol (UDS, ISO 14229-1:2013)

Update inside ECUs: Secure Flash Bootloader and HSM
› Erase Flash
› Decrypt and unzip blocks (end to end protection)
› Write new code into Flash
› Update and verify signatures (HASH)

Reboot the vehicle with new SW versions
› Exit update mode
› Restart all ECUs within the car

Generate and release new Software version

Service pack at OEMs update server

Formatting for Update Handling

Copyright © Infineon Technologies AG 2016. All rights reserved.
Protection and Safety Responsibilities for OEMs and Tier1s

Well Suited Security Measures are to be Installed for Using SOTA

Tier1 targets: ECU-IP protection and safety responsibility

OEM targets: vehicle protection and safety responsibility

vehicle level:
Secure Update Service

ECU level:
Secure Flash Boot Loader

Certificates

Encrypted SW
Secure HASH

End to End Protection Required
Typical Security Principles

Security is a system requirement

› The whole trust zone must be secured from all sides
› Keys and passwords must get especially protected

- Extra trust zones for key storage and key management
- All parties involved with key handling are requested to have same security levels. OEMs’ and Tier1s’ challenge: production and service
Secure SW OTA Front End
Security Elements and Formatting

**Step 5: Over The Air**
- Update download is established by Provision of authentication and encryption services
- File of service pack is formatted and encrypted for wireless data transport

**Step 4: Service pack into update server**
- For updating multiple ECUs in one operation all individual UDS service packs of all effected ECUs are integrated to one package
- Service pack is signed with OEM signature
- Service pack is loaded into update server as one file

**Step 3: UDS Formatting**
- Individual service pack is wrapped to get handled by the protocol of the Unified Diagnostics Services (UDS, ISO 14229-1:2013)

**Step 2: Formatting for Secure Flash Bootloader**
- chop - zip – encrypt – sign with keys and signatures from Tier1
- ECU specific individual service pack

**Step 1: Engineering**
- New software version for ECU
- Verified and released
Abstracted Vehicles Network
HW Elements For Secure Software OTA

**OPTIGA™ TPM**
Central trusted anchor for the vehicle

**HSM within AURIX™**
Trusted anchor for ECUs
Secure Elements For SOTA At ECUs
Two Essential Building Blocks

HSM* Module: Trusted Anchor At ECU
› Secure Boot & Integrity check
› Authentication
› Encryption / Decryption
› Key Management

Secure Flash Bootloader: Update client services using UDS
› Initiate update process
› Erase old SW version
› Load single SW blocks
› Decrypt & check integrity
› Unzip & perform signature check
› Rewrite
› Verify completeness of service pack
› New HASH key to HSM for secure boot
› Confirm execution to backend

AURIX™ HSM offers the strong isolation and crypto agility required for SOTA

*) Hardware Security Module
AURIX™ Hardware Security Module
A consequent security enhancement

Secure Platform

Hardware Security Module (HSM)

› A highly flexible and programmable solution
› AES128 HW accelerator matching performance for automotive protocols
› Crypto- and Algorithm Agility by Software
› AIS31 compliant True Random Number Generator (TRNG) with high Random Entropy over Lifetime
OPTIGA™ TPM
Trusted Platform Module

› Temper proof design and architecture: CC EAL4+ certified
  - Individual private key by hardware
  - Unlimited number of asymmetric / symmetric keys
  - Certified true random number generator TRNG: AIS31

› TPM use case in vehicles: Main trusted anchor for the vehicle
  - Asymmetric cryptography in authentication services
  - Central generation, storage, and processing of individual keys for the vehicle including production and service
  - Flexible Authorization mechanisms to protect against duplication/misuse

› TPM use case in SOTA process:
  - Mutual authentication of vehicle with OEMs servers
  - Key generation (SHA) for update OTA
The downtime of the vehicle during a remote software update creates new responsibilities and control tasks

1. The driver must accept that he cannot use the vehicle during the update
2. The driver must ensure that the vehicle does not move: i.e. engine off, parking brake on, etc.
3. It must be ensured that the vehicle has enough electric battery power
4. The vehicle's update system must be able to detect the fulfillment of all requirements from above by sensors or drivers' input of acceptance respectively

The shorter the down time the less critical is a remote update
Correlation between downtime and EE architecture
Example of updating 4MB of Code – classical approach

1. Bus-Transfer (4MByte)
   Usable Date Rate
   1) **FlexRay** (10MBit/s): ca. 300 KByte/s
      ca. 13,6s
   2) **CAN-FD** (2MBit/s): ca. 88,5 KByte/s
      ca. 47,4s
   3) **CAN** (500kBit/s) : ca. 16,8 KByte/s
      ca. 250s
   4) **Ethernet** (100MBit/s): ca. 5-10 MByte/s
      ca. 1 s

2. Processing & Reprogramming inside ECU (4MByte)
   AES-128 Hash: ca. 0,16s and
   + Erase\(^5\): ca. 8s and
   + Programming: ca. 4s

---

1) 50% Dynamic segment usage
2) "ISO CAN FD", 64 Bytes data field, 2 MBAud, 50% bus load
3) "Classical CAN", 8 Bytes data field, 500 kBaud, 50% bus load
4) Bandwidth depending on used protocol e.g. UCP or TCP/IP
5) AURIX™, 65nm generation
Three topology proposals to minimizing the downtime of one ECU

**Topology 1: Update from Central Storage**

- Downtime: Mins (CAN), Secs (Ethernet)
- State of the art today
- No cost adder

**Topology 2: Update from Local Storage**

- Downtime: Secs
- Products available today
- Medium to small cost adder

**Topology 3: Doubled Embedded Flash**

- Downtime: None
- Products under evaluation, not available today
- High cost adder
Summary

Software Over The Air is an opportunity for lower costs and new revenues

Security is essential, on product and process level
- HSM has the programmability and asymmetric crypto required for Secure Flash Bootloader
- TPM offers certified product and process security

Network architecture and topology are key to limiting vehicle downtime
- A smooth migration path is possible today without significant cost impact

Infineon has the key building blocks today for SOTA and will continue to evolve through next generations
Part of your life. Part of tomorrow.