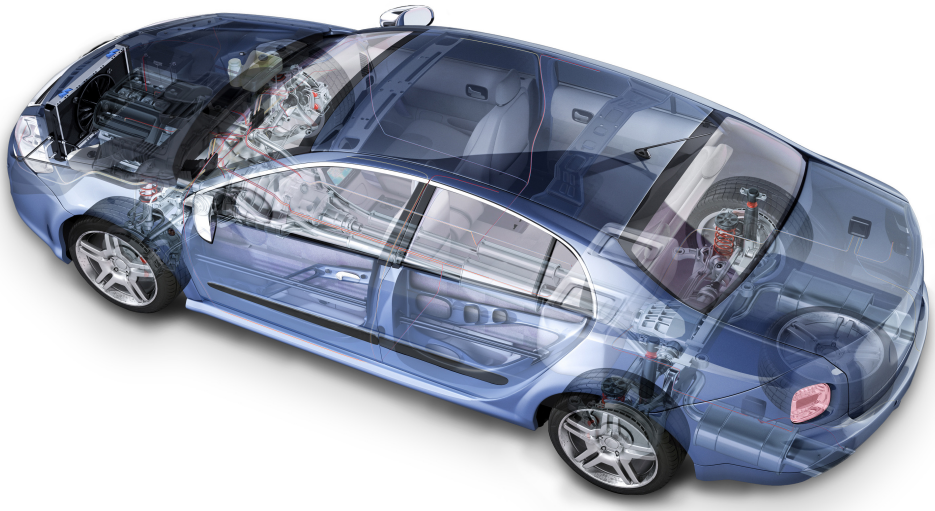
EVALUATION OF LIGHTWEIGHT TPMS FOR AUTOMOTIVE SOFTWARE UPDATES OVER THE AIR

Richard Petri, Markus Springer, Daniel Zelle, Ira McDonald, Andreas Fuchs, and Christoph Krauß

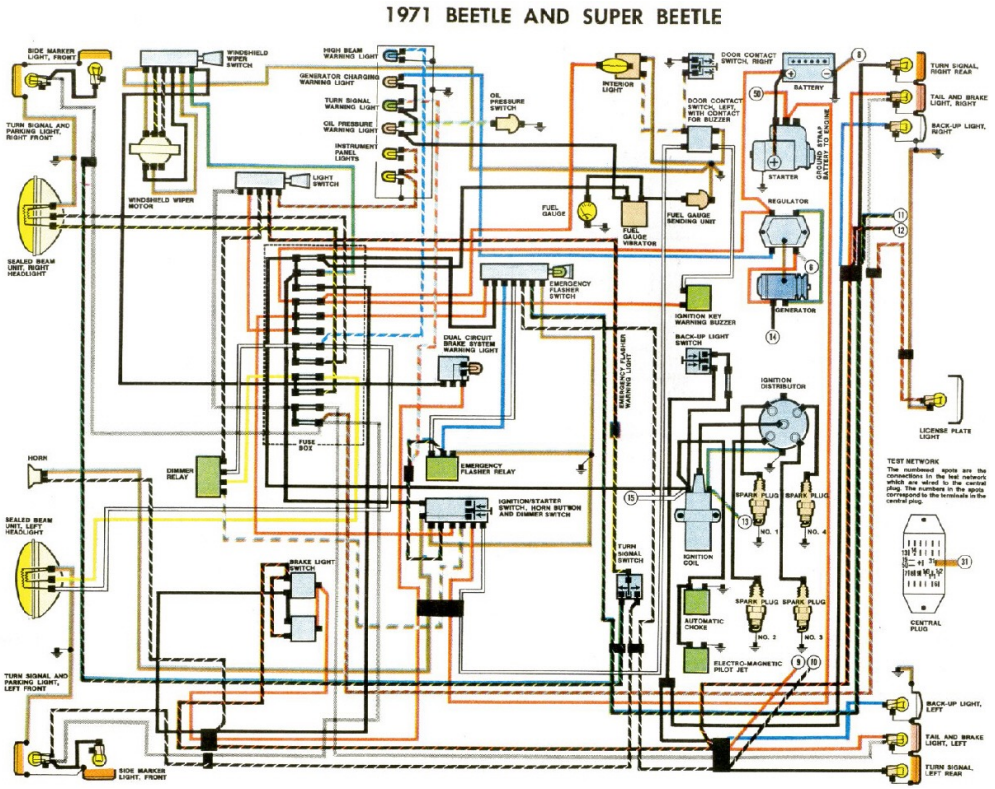


OVERVIEW

- Automotive Security
- TPM Architectures
- TPM for Automotive
- Software Updates (over-the-air) using TPM

Automotive Networks

- Back then: No software, no bugs, no CAN, no C2X, …



Fraunhofer SIT

Automotive Networks

- Back then: No software, no bugs, no CAN, no C2X, …
- Now: 60-100 ECUs of all shapes and sizes
- Complex On-Board Networks
  - CAN, LIN, …
  - 802.11p
  - GSM, LTE
  - Bluetooth, WLAN

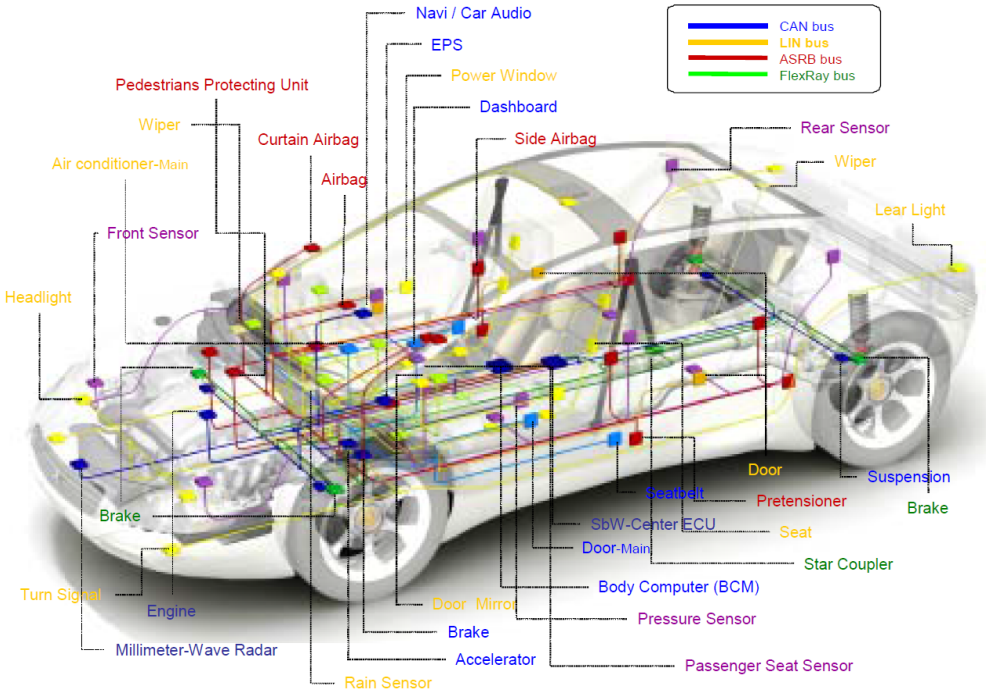


Image Credit: http://www.flexautomotive.net/EMCFLEXBLOG/post/2015/09/08/can-bus-for-controller-area-network
Image Credit: http://www.vw-kaeferclub.com

Attack Vectors

- Digital Radio
  - Wireless Keys
  - Internet / Backend
  - C2X
  - Wireless sensors
  - DAB+
- Removable Storage, WLAN, Bluetooth
- Security Challenges
  - Authenticity
  - Authorization
  - Privacy
  - Integrity / Tuning Protection

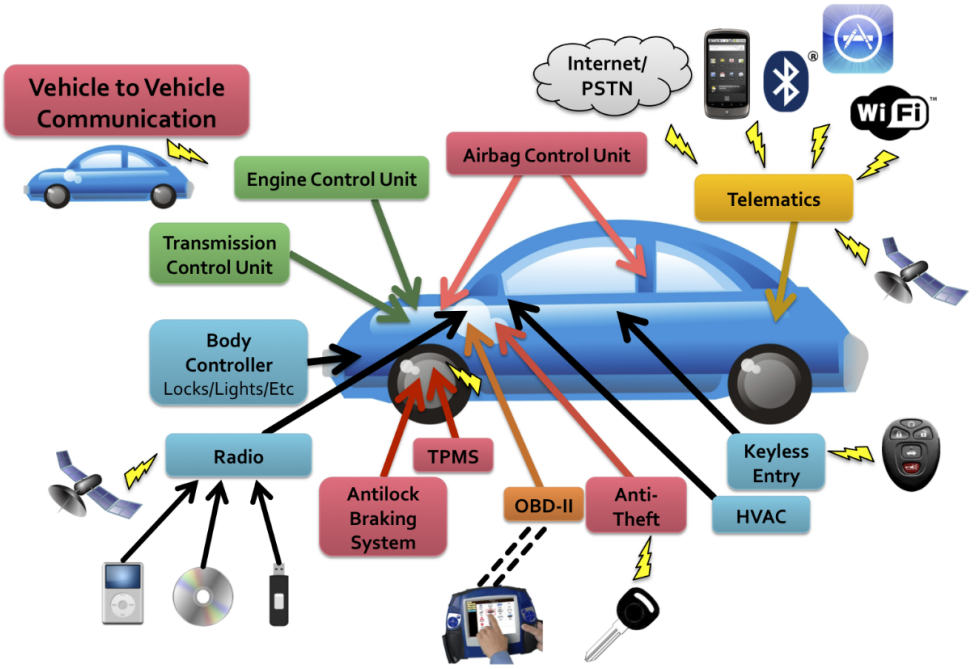
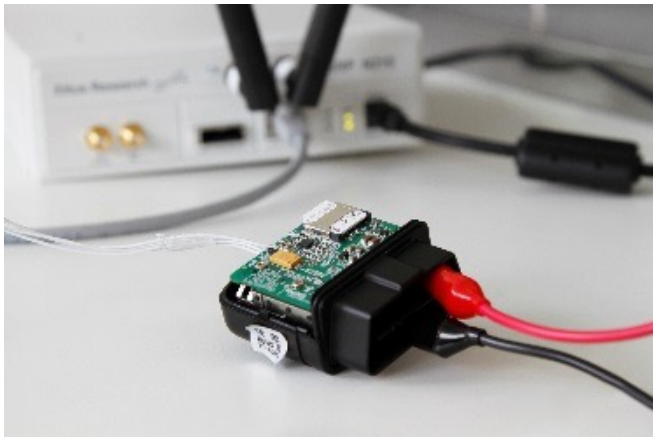


Image Credit: Checkoway et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces USENIX Security Symposium, 2011

Example Attack

- Connected OBD-II Devices *for Consumers* (Car Tracking, Insurance, …)
- System only uses Client Authentication of the dongle
- GSM Base station can be faked easily
- Attacker fakes the Backend, take over Device, **send Messages over OBD-II Port**



OpenBTS™

Hardware Security Modules

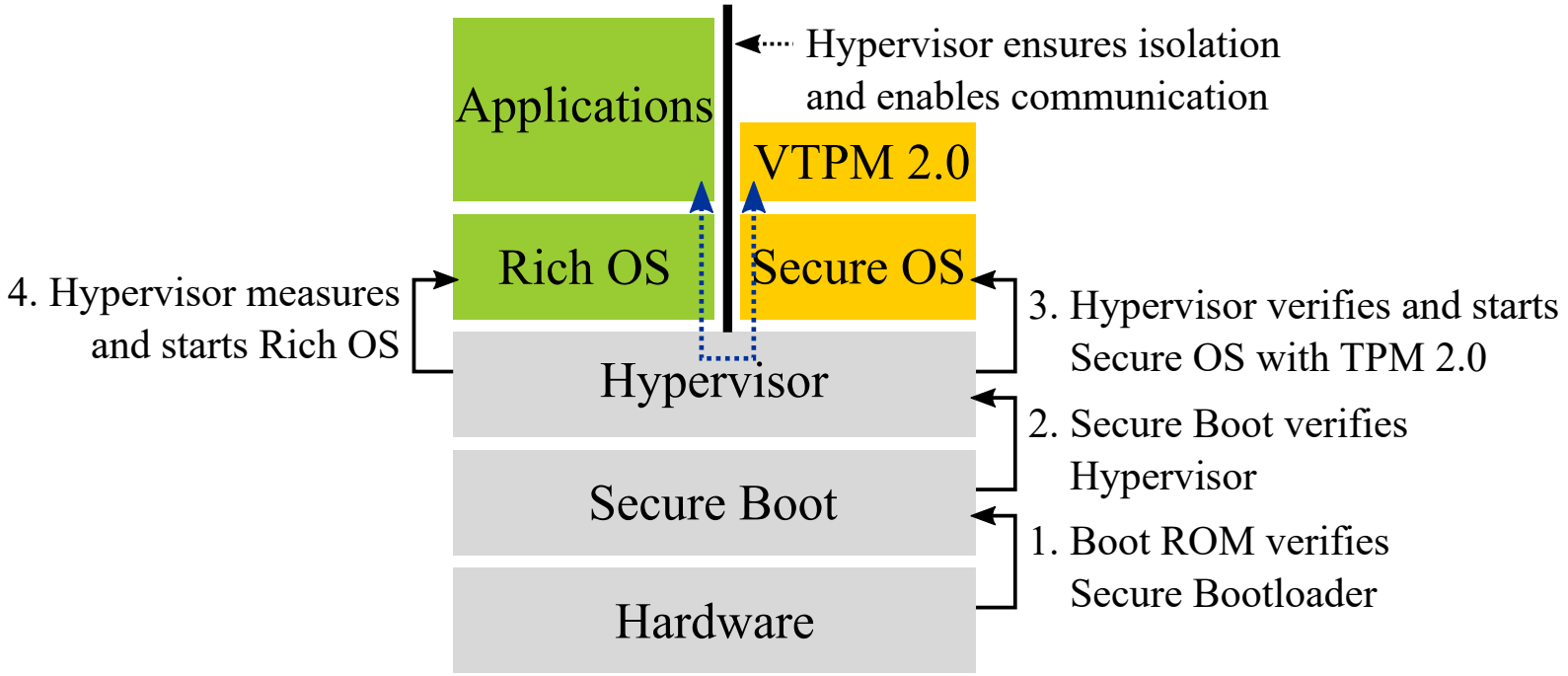
- Pure software approaches to security can't meet all requirements
  - Bugs are inevitable
  - Software based access authentication will fail eventually
  - Internal networks can’t be trusted either
- Hardware Security Modules (HSM) offer strong additional defence
  - Create, store, and use cryptographic material securely
  - Decoupled, applications never touch keys
  - Offers a root of trust, essential for recovery
- Usually implemented as discrete chips or on an SoC

TPM

- TPM is an established standard HSM in the PC context
- Provides Roots of Trust for Storage, Reporting and Measurement
- TPM 2.0 is a complete rewrite of 1.x
- Much more flexibility
  - Large range of Cryptographic Methods (extendable)
  - Enhanced NV memory, such as monotonic counters
  - Enhanced Authorization: Flexible policies can be defined and enforced for functions

TPM Architectures

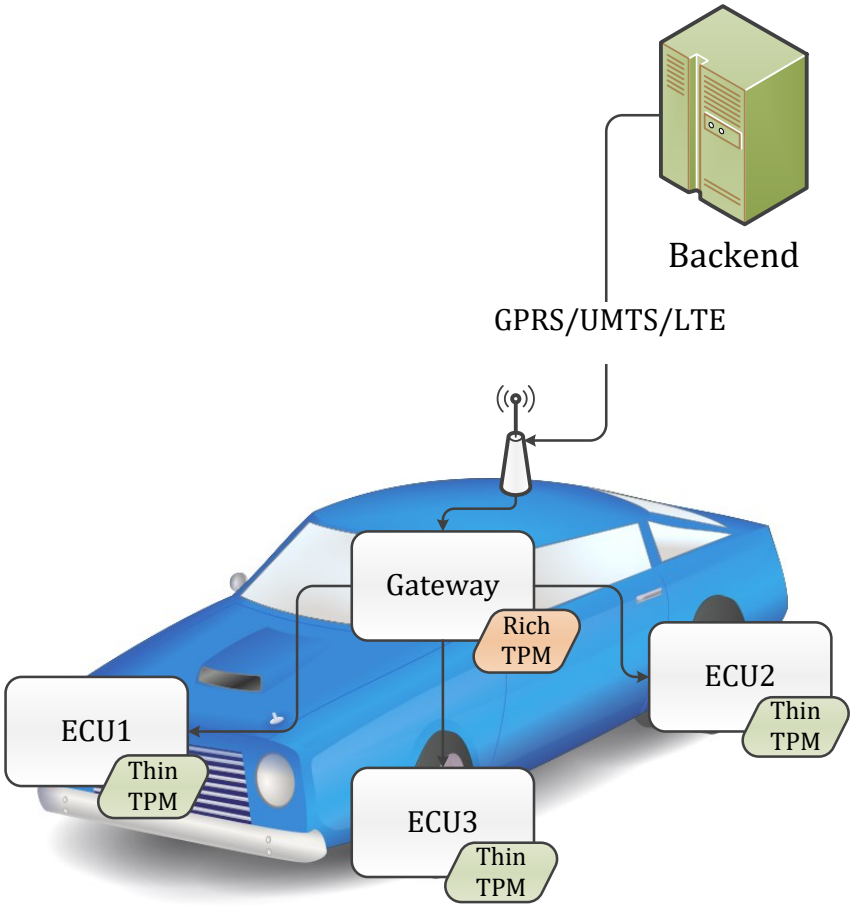
- TPM 2.0 doesn't have to be implemented as a discrete chip
- "Mobile Common Profile" allows very flexible implementation: "Firmware TPMs"



TPM Profiles

- The Full TPM Specification is rarely needed
- TPM 2.0 can also be defined in profiles
- We looked at the “Automotive Thin Profile” of TPM 2.0
  - Extremely lean profile, removes most features, but Asym. Crypto still available
  - Still supports Remote attestation and authentication
  - (Unoptimized) TPM Simulator implementation is about 35% smaller in TPM Thin Profile
  - Impact for SoC/Chip implementations is hard to predict
- EVITA specification has a similar approach with Light, Medium, Full

Automotive Application of TPMs



Software updates over-the-air (SOTA)

- Updating Software/Firmware of ECUs "over-the-air" instead of in the repair shop during maintenance (or during a recall)
- Idea: Connected ECU loads firmware update package via network (GSM, LTE, …) and installs at opportune time, avoiding expensive recalls
- Numerous challenges:
  - Technical: heterogenous environment (components, Car models, configurations), reliability (failure recovery, integrity)
  - Security: authorisation and authenticity, downgrade protection, confidentiality
  - Legal: liability

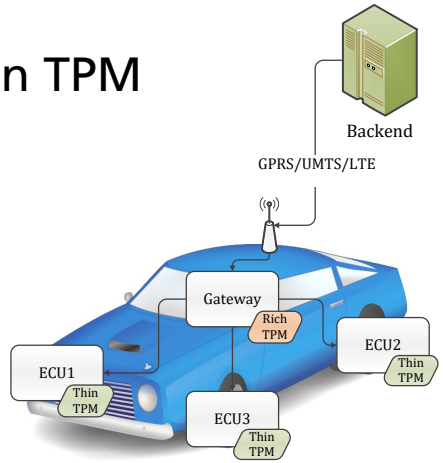
Previously: Secure Update with TPMs

- Headunit Demonstrator for TPM
- IP and Privacy Protection
- TPM Contains decryption Key for Data (Maps, Personal Data, …)
- Measured Boot ensures, Keys only become usable for Authorized Software

- Keys bound to OEM Signed “Ticket” describing valid boot image (Version number, Measured Boot PCR Hash,…)
- Monotonic Counter provides Rollback Protection, if lower version is installed, Ticket becomes invalid

Authenticated Updates with Automotive Thin TPM

- Automotive Thin TPMs can perform Quotes, but no Signature verification (optional feature)
- Assuming the aforementioned System Architecture, Authenticated Updates can be performed
- Idea: Gateway with Rich TPM assists
  - Gateway receives and verifies update Packages
  - Opens an Authenticated Channel to ECU with Thin TPM



Liability

- TPMs are a root of trust for measurement
- Important Liability Issues
  - What Software (and/or which version) was installed?
  - Validity of Logs/Reports?
- Thin TPM support this with the Quote (Attestation) Function
  - Platform Configuration Registers (PCRs) cryptographically record the software state
  - TPM can attest to the PCR values *remotely*
  - Backend will request a Quote with a nonce, to verify which version is installed (e.g. after an update)

Conclusion

- Hardware based Root of Trust is an important building block for secure interconnected systems
- TPM offers comprehensive functionality to support many applications, such as a secure update
- The modular/flexible TPM 2.0 Standard allows cost-effective HSM
- Even lightweight TPMs can offer security enhancements