Designing Cost-Effective Ethernet Automotive E/E Architecture Against Security Threats
Connected vehicle attack surfaces
High level security needs
Hardware security protection
Ecosystem management
Network Partitioning for security
Hardware-secured TLS
Ethernet switching requirements
Example of secure Ethernet IVN
Cars Are Already Connected

More than 20% of vehicles sold worldwide in 2015 included embedded connectivity solutions.

More than 50% of vehicles sold worldwide in 2015 to be connected (either embedded, tethered or smartphone integration).

Every new car to be connected in multiple ways by 2025.

The new question:

• Will these cars be connected with a foundation of security in mind?
High Visibility Hacks Influencing Market Trend

• Resulting in new regulations and OEM cybersecurity specs
Increasing remote attack interfaces

- On-board diagnostic port
- Telematics
  - Wi-Fi® hotspot & long-range wireless connectivity
    - 3G, 4G, LTE
  - Bluetooth® connections (smartphones)
  - Passive entry / keyless systems
- Infotainment
  - Storage media (CD, USB, SD card)

Attack scenarios

- Safety critical (Brakes, engine control…)
- Obstructive (Instrument reading, lights, infotainment…)

- No security on CAN2.0 & limited bandwidth to implement
- Ethernet VLANs for traffic separation not security
High-Level Security Needs

- Ease of integration into existing architecture & Engine Control Units (ECUs)
- Scalable across platform models
- Flexible migration to next-generation architecture
- Common methodology across all types of In-Vehicle Networking (IVN)
- Intrusion detection and OTA updates

• Cost effective total solution!!
Attributes of Automotive Hardware Security Devices

- **Secure Key Storage**
  - Trusted Ethernet nodes with secure boot & firmware update
  - TLS key protection
  - CAN communication keys & certificates storage
  - CAN communication session key(s) storage

- **Ease of Integration**
  - Less code = lower cost
  - Minimal code updates on node microcontroller (MCU)

- **Node Authentication & Key Agreement**
  - ECU authentication & key agreement scheme
  - Encrypted and authenticated command sessions

- **Hardware Crypto Accelerators**
  - Symmetric and asymmetric algorithms
  - High quality random number generators
  - HMAC & CMAC for serial communication protection

- **Automotive Grade-1**
Unprotected Hardware Attack
Microprobe to See Internal Device Nodes and Extract Keys

• Software can NOT protect private keys!
How Keys are Protected Matters!

- **Strong Multi-Level HW Security**
  - Starts with active shield
  - Plus a multitude of environmental tampers
  - Protection modes
  - Ability to erase keys

- **Designed to Defend Against**
  - Microprobe attacks
  - Timing attacks
  - Emissions analysis attacks
  - Fault, invalid command attacks
  - Power cycling, clock glitches
Security Considerations at every Node in the Vehicle

- SAE J3061 Consider risks associated with each vehicle system
Ecosystem Management

- Protect your brand
- OEM’s can manage approved suppliers for each node
- Only approved safety critical nodes operate in the vehicle
- X.509 certificates can help in authentication genuine components
Digital Certificates

- The x.509 Digital Certificate is a **unique verifiable** form of identity for the node.
- It comprises three main components:
  - The device public key
  - A signature to enable verification of the authenticity
  - Data capturing any attributes the owner intends as part of the identity
- Certificates are standards driven forms of identity for the Internet.
Creating a Certificate (Provisioning)

1. Create a unique key pair for each participant

2. MCHP or OEM creates device certificate

3. Owner embeds certificate into device

- Remember: private keys, no matter which, must remain secret!
Monolithic Approach to Securing Ethernet

- Complex
- Flexible
- Scalable
- Common methodology
- Existing architecture
- Cost effective
- Secure

→ Impractical
→ Partition network
Partitioning Network for Security

- Separate common network security from data traffic processing

### Common Network Functions
- Physical defence mechanisms
- Secure boot & download
- Authentication
- Key management
- Ecosystem and certificate chain management

### Network Specific Processing
- Virtual LANs
- Access control
- Deep packet inspection
- Ingress / egress policing
- Intrusion detection / protection

- Optimizes security performance, flexibility and cost
- Any ECU, any architecture, any configuration, any bus
Scalable Security for IVN

- Addresses large number of ECU architectures
- Secure Boot at each node
**Software-Only TLS Authentication**

- Performs cryptographic functions in software in the device MCU
  - Requires more code space
  - Requires more processing load
  - *Houses keys in software and unsecured memory*
- Small nodes with low-end processors are too slow

- **Software-only TLS is vulnerable!**

**Device main MCU**

**Main Software Stack**

**Crypto API**

**Cipher Suite SW Module & KEYS**

- **OpenSSL**
- **wolfSSL**

**Authentication Request**
Hardware Secured TLS Authentication

- Hardware-TLS offloads cryptographic functions from the device MCU
  - Access via HW-TLS API
  - Security IC handles all computation
  - Minimal code space & computational load
  - Keys are generated & protected in secure hardware

- Keys are secure!

Device main MCU

Main Software Stack

Microchip HW-TLS API

Security IC

or

OpenSSL

wolfSSL

Authentication Request

Authentication

- Key agreement
- Key storage
Exploiting Automotive Ethernet Network Characteristics

- Fixed star / hybrid network topology
- Typically maximum eight network ports on ECU
- Applications, traffic flows are known and pre-determined
- Network configuration is static (MAC, IP addresses)
- Broadcast, multicast and unicast traffic
- Limited use of protocols
  - TCP/UDP, DoIP, PTP, SOME/IP ....

- Well-defined and bounded network
- Exploit to deploy intrusion detection / protection
- LEARN → MODEL → ANALYSE → ACT
Ethernet Switch Security Requirements

- Requires hardware features to support intrusion detection / protection
- Prevent typical attacks; spoofing, flooding, misuse / failures
- Dynamically update to adapt to changing network behavior
  - 802.1Q VLAN
  - AVB (time synchronized)
  - 802.1Qci Ingress policing and filtering (per stream per port)
  - Extensive network statistics gathering (metadata)
  - TCAM-based layer 2,3,4 deep packet inspection
    - Forward, drop, mirror
    - Time stamp
    - Count
    - Modify packet
    - Rate limit
  - 802.1x Port and MAC authentication
  - Enhanced diagnostics (harness defect detection)
  - Seamless redundancy
Come and visit us at Booth #2 😊

- Ethernet Gateway Security Demonstrator
- Ethernet AVB Streaming Demonstrator
Thank You!