Software and Supply Chain Assurance Forum

TPM for Automotive
SAE J3101 defines HW Security

- Hardware Protected Security Environment
  - Offers at least one mechanism of security implemented by hardware support
  - Offers resilience against arbitrary execution of software within a system
- Secure Keystore
- Authenticated Boot
- Authenticated Software Flashing
- Authenticate messages in the vehicle
- Broadcast/Multicast Authentication
- Secure Storage
- Access to Private Data
- etc...

TPM as a HW RoT

- Root of Trust for Measurement (RTM)
- Root of Trust for Reporting (RTR)
- Root of Trust for Storage (RTS)
- Establish a basis of trust – belief that a device will behave in an expected way
- TCG uses cryptographic methods to attest identity of the device and its expected behavior, both of HW and SW
- The TCG’s method for attestation is to use a key associated with the hardware to sign one or more values that represent the software
Defense in Depth

The Interconnected Car

Components associated with physical control of the vehicle
Components associated with safety
Components associated with entertainment and convenience

Software and Services
- Over-the-Air Updates
- IDPS / Anomaly Detection
- Network enforcement
- Certificate Management Services
- Antimalware and remote monitoring
- Biometrics
- Fast cryptographic performance
- Device identification
- Isolated execution
- (Message) Authentication
- Virtualization

Hardware security building blocks
- Platform boot integrity and Chain of Trust
- Secure Storage (keys and data)
- Secure Communication
- Secure Debug
- Tamper detection and protection from side channel attacks

Security features in the silicon, for example Memory Scrambling, Execution Prevention, etc.

Analog security monitoring under the CPU
Vehicle Assets (by ENISA)

**BODY CONTROL**
ECUs and sensors: instrument cluster, climate control, door locking...
Dashboard display, air conditioning, lights, direction/warning signals, doors, windows, seat belts, motorized/heating seats...

**INFOTAINMENT CONTROL**
ECUs and sensors (Head unit Audio/video, navigation, telephone)
External media/drives/phone content...
Infotainment subnetwork (e.g. MOST)
Ad-hoc internal networks (e.g. Bluetooth, WiFi...)

**COMMUNICATIONS CONTROL**
Gateways ECU with Telematics and communications
External communication networks

**DIAGNOSTIC AND MAINTENANCE SYSTEMS**
OBD II ports
Aftermarket dongles
Garage or maintenance equipment

**POWERTRAIN CONTROL**
Engine, transmission...
ECUs and sensors: engine control, transmission control, speed control / gear control, driving support (ABS), power train sensors...

**CHASSIS CONTROL**
ECUs and sensors: steering control, airbag control, braking systems, ADAS systems...
Steering, brakes, airbag, embedded cameras, rearview mirrors, windshield wiper...

Protocols:
- CAN, LIN/SAE/J2602, RF...
- MOST, Bluetooth, WiFi...
- 3G, WiFi...
- CAN, FlexRay, RF...

Services:
- Door lock, air conditioning, seat belts...
- Entertainment (audio/video)
- Driving services: traffic information, maps...
- Additional services (fleet management, chronotachygraph, geofencing...)
- Powertrain control
- Telematics and communications
- Drive- or brake-by-wire, lane assist, collision control...
- Tire Pressure Monitoring Systems

Legend:
- Components
- Networks

©2017 Trusted Computing Group
Vehicle Threats (by ENISA)

**DAMAGE / LOSS (IT ASSETS)**
- Loss of information in the cloud
- Loss of (integrity of) sensitive information
- Damage caused by a third party
- Loss from DRM conflicts
- Information leakage

**PHYSICAL THREATS**
- Fault injection / glitching
- Side channel
- Access to HW debug ports

**FAILURES / MALFUNCTIONS**
- Failures / malfunctions of devices or systems
- Failures or disruptions of the power supply
- Software bugs
- Failures / malfunctions of parts of devices
- Failures or disruptions of communication links
- Failures or disruptions of main supply

**NEFARIOUS ACTIVITY / ABUSE**
- Denial of service
- Malicious code / software activity
- Manipulation of hardware & software
- Manipulation of information
- Unauthorized access to information system / network
- Compromising confidential information
- Identity fraud
- Abuse of information leakage
- Unauthorized use of administration of devices & systems
- Unauthorized use of software
- Unauthorized installation of software
- Abuse of authorizations
- Malicious software
- Remote activity (execution)

**THREATS**

**UNINTENTIONAL DAMAGES (ACCIDENTAL)**
- Information leakage or sharing
- Erroneous use or administration of devices and systems
- Using information from an unreliable source
- Unintentional change of data in an information system
- Inadequate design and planning or lack of adoption

**ADVANCED PERSISTENT THREATS**

**NETWORK OUTAGE**

**EAVESDROPPING / INTERCEPTION / HIJACKING**
- Interception of information
- Replay of messages
- Interfering radiations
- Man in the middle / session hijacking
- Network reconnaissance and information gathering
- Repudiation of actions

**LEGEND:**
- Threats perceived as significant by 230% answers
- Threats perceived as significant by 53% answers
Why do you need HW Security?

<table>
<thead>
<tr>
<th>Basic Cryptography</th>
<th>Key Management</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Hash (SHA2, SHA3)</td>
<td>Key Derivation Function (KDF)</td>
<td>Compression/Decompression</td>
</tr>
<tr>
<td>Message Authentication Code (CMAC, HMAC, GMAC)</td>
<td>Secure Key and Certificate Storage</td>
<td></td>
</tr>
<tr>
<td>− Generation</td>
<td>− Access Management</td>
<td></td>
</tr>
<tr>
<td>− Verification</td>
<td>− Import/Export Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Generation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Update</td>
<td></td>
</tr>
<tr>
<td>Signatures</td>
<td>Key exchange protocols</td>
<td></td>
</tr>
<tr>
<td>− Generation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Number Generation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption/Decryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Symmetric (CBC, CTR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Asymmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− ECC (P-256, NIST, SEC2, Brainpool)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Clock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Time stamping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Validity check for key data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mirrorlink Phone Connectivity
(Google Android Auto, Apple Carplay)

USB/WiFi

CAN Test-Bench

Ethernet Diagnostics

AUTOSAR CSM Translation Stack

Hypervisor

TSS

Dedicated Security Core

TPM

Example from Mentor Graphics with HW Security Core and TPM overlay
Automotive E/E Trends
TPM Practical Applications

• A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys.

• An ECU that incorporates a TPM can create cryptographic keys and encrypt them so that they can only be decrypted by the TPM (binding a key).

• Certificates can be installed or created; the RSA private key for a certificate is bound to the TPM and cannot be exported.

• Running software can use the boot measurements of the operating system start state to prove the integrity of an ECU.

• The TPM has several Group Policy settings that might be useful in certain scenarios such as authorization.

• Because the TPM uses its own internal firmware and logic circuits to process instructions, it does not rely on the operating system, and it is not exposed to vulnerabilities that might exist in the operating system or application software.
TPM 2.0 Software Stack (TSS)

TPM is a dedicated hardware that:

- Protects a unique platform identity (TPM)
- Verifies software integrity before software is loaded (TPM)
- Protects network integrity (TNC or Trusted Network Connect)
- Protects data integrity and confidentiality (SED or Self-Encrypting Drive)
TPM Main Functions
Why TPM?

• Trusted computing is cyber defense technology that can be used to protect data, platforms and networks
• Trusted computing technologies are actively evolving, with new standards and new products regularly entering the market
• Major hardware manufacturers and software vendors support trusted computing off-the-shelf
• Trusted computing products can offer a cost-effective path to improved compliance and security

TCG has the TPM Automotive Thin Profile specification and is working on the TPM Automotive Rich Profile specification which will satisfy underlying SAE J3101 requirements and provide security foundation for protecting vehicles.