Rev. March 19, 2015

TRUSTED COMPUTING GROUP™

Trusted Computing Group and Automotive Security
March 2015

Q. How is Trusted Computing Group (TCG) involved in automotive security?
A. TCG and its members, many of which are established suppliers of system-on-chip (SoC) technologies and other components for the auto market, believe that several TCG specifications and technologies are well suited to addressing some fundamental security issues inherent in today's connected vehicles.

Q. Why would cars need security technology that has been more often found in the past in PCs and similar devices?
A. Today's cars basically are computers on wheels – most have more than 100 processors, each with its own OS, firmware, and applications. Most of these are connected on closed industrial control networks; increasingly, some other processors are connected to the wider world via cellular modems and Wi-Fi. The variety of systems and networks has created a complex group of small computers that are potentially vulnerable to remote and local attacks, hacks, and malware.

Q. What is TCG's role in helping secure these systems in cars?
A. Several years ago, TCG formed the Embedded Systems (EmSys) work group. The EmSys work group decided to focus initially on two key security vulnerabilities in cars: (a) transmission of data between the factory or third parties and vehicles; and (b) integrity of the embedded electronic control units (ECUs) in vehicles that control the car's operation, much like a small PC with memory and processing power along with firmware and application software.

Q. What specific TCG technologies could be applied to ECUs?
A. The Trusted Platform Module (TPM) and Trusted Network Connect (TNC) protocols can be applied to ECUs just as they have already been widely deployed in PCs, tablets, and mobile phones. TPM and TNC protocols could:

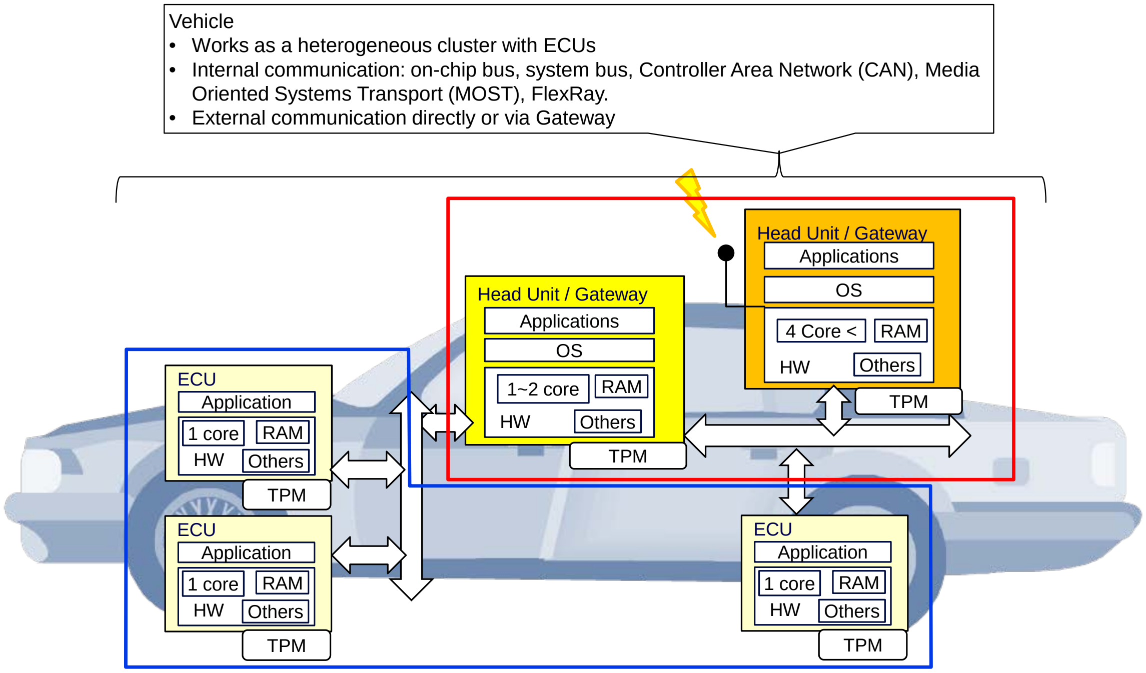
1. Measure and report on the integrity of firmware and software used in the ECU
2. Create, store, and manage cryptographic keys in the ECU
3. Provide attestation and assurance of identity of the ECU
4. Support secure firmware and software updates in the ECU
5. Provide anti-rollback protection and secure configuration memory for the ECU

Q. In the past, TPMs were built into PCs, tablets, and mobile phones that have more physical space, a larger bill of materials, and larger power budgets. How could TPMs fit into the auto electronics market, which has significant constraints on all three of these design factors?

A. TCG and its members recognize that the market for auto electronics devices and components is different. Therefore, the EmSys work group has developed a new profile specification that is a subset of TPM capabilities for ECUs and provides key features that are integral to auto security without burdening ECUs with unnecessary features.

Q. What is this new profile of the TPM?
A. The new specification is called the **TCG TPM 2.0 Automotive Thin Profile**. It recognizes the unique performance requirements (including temperature, vibration, acceleration and others) in the auto environment; limited memory requirements; power management capability; and unique software requirements that may involve limited firmware.

The spec also recognizes the long lifecycle of an auto, which might be more than 20 years.


Vehicle
- Works as a heterogeneous cluster with ECUs
- Internal communication: on-chip bus, system bus, Controller Area Network (CAN), Media Oriented Systems Transport (MOST), FlexRay.
- External communication directly or via Gateway

Q. How would Automotive-Thin TPMs based on this spec work in cars?
A. Each ECU would have its own TPM. Significant features of Automotive-Thin TPMs include:

1. Support of resource-constrained ECUs to report their integrity and provide attestation of their configuration for reliable remote maintenance services

2. Support for storage of ECU firmware measurements, creation of integrity digests, and creation of signatures on integrity digests

3. Support for firmware updates or patches through verification of digital signatures and confirmation to a Remote Maintenance Center that an update installation has completed successfully

4. Support for secure management of cryptographic keys (creation, storage, revocation, export, import, etc.)

Q. How can you guarantee that the remote maintenance process is secure?
A. The secure update process could be implemented using the following steps:

1. Accurate remote determination of in-vehicle software and hardware configuration and integrity (via measurements performed using the TPM, securely attested by the TPM itself and verifiable by third parties, and transferred by TNC protocols)

2. Verification and logging of successful completion of intended software updates (via measurements performed using the TPM, securely attested by the TPM itself and verifiable by third parties, and transferred by TNC protocols)

3. Secure long-term storage of audit logs (created by the TPM itself) of the related update operations and TPM measurement operations (transferred by TNC protocols or secure system logging channels to network accessible SEDs or other high-reliability storage)

Q. Will there be other TPM profiles for automobiles and, if so, for what application or type of system?
A. In the future, the TCG may also develop another TPM profile for automobiles that could address enhanced security for a head unit or gateway system that could be used for management and coordination of multiple TPM-equipped ECUs in a vehicle and for securing cellular and Internet communications between a remote maintenance center or third party and the actual vehicle.

Q. What input has TCG had from the auto industry?
A. TCG's members include the world's leading automaker along with some of the world's leading auto electronics suppliers, who have been involved in creating the spec. TCG members are participating in SAE Vehicle Electrical System Security Committee and SAE Vehicle Electrical Hardware Security Task Force meetings. TCG also recently contributed a response to the U.S. National Highway Traffic Safety Administration's Automotive Electronic Control Systems Safety and Security note. TCG also is collaborating with the International Telecommunication Union Telecommunication Standardization Sector SG17 which is addressing secure software updates to cars.

Q. Where can I learn more about this new TPM profile?
A. TCG will provide a demo of the TPM 2.0 Automotive Thin Profile at the SAE World Congress, April 22. More info can be found here,
http://www.trustedcomputinggroup.org/media_room/events/189

Q. What is this demonstration?
A. The demonstration was hosted by TCG members Toyota Info Technology Center and Fujitsu and shows a secure remote firmware update for an ECU in a car using the Trusted Platform Module (TPM) for a secure hardware root of trust.

The secure update will demonstrate three key items:

1. Accurate remote determination of in-vehicle software and hardware configuration and integrity (via measurements performed using the TPM, securely attested by the TPM itself and verifiable by third parties, and transferred by TNC protocols)

2. Verification and logging of successful completion of intended software updates (via measurements performed using the TPM, securely attested by the TPM itself and verifiable by third parties, and transferred by TNC protocols)

3. Secure long-term storage of audit logs (created by the TPM itself) of the related update operations and TPM measurement operations (transferred by TNC protocols or secure system logging channels to network accessible SEDs or other high-reliability storage)

CONTACT: Anne Price,
1-602-330-6495
anne@prworksonline.com
Twitter: @TrustedComputin
https://www.trustedcomputinggroup.org