My Connected Car Is Under Attack: "TPM" , "TPM" HELP ME

Jeevan Visvesha
ANI technologies private limited
Bangalore, India
jeevan.visvesha@olacabs.com

Abstract— **Raising trend in connecting vehicle prompts us to answer how secure they are. They are no less than a massive computer. There are around sixty to eighty Electronic Control Unit (ECU) in the vehicle. Modern automotive technologies are required to enhance the consumer in-car experience which at the same time expands the attack surface, opening up a host of new vulnerabilities. Presence of around eighty ECUs additionally mandates for secure in-vehicle communication between the vital ECUs, that is not existent in present vehicles. Telematics Control unit (TCU) is commonly utilized in vehicles to act as sort of a gate in uplinking any vehicle information to Infrastructure and downlinking files from Infrastructure to vehicle. There are a lot of complexities involved with building connected system. Solutions for a portion of the complexities present us with imperative issues like identification and authentication, which may be of high impact. The paper can provide answers to following queries: How TPM helps in moving towards a secure authentication with the infrastructure? How TPM helps in securing the Uplinking and OTA communication? How ECU to TPM communication can be secured?**

Keywords- TPM; V2I; OTA; Secure protocol; Authentication

I. INTRODUCTION

Evolution from a traditional vehicle to connected vehicle has introduced crucial changes. The Original Equipment Manufacturer (OEM) has invested huge amounts of money on connected vehicles to boost the client comfort in driving, diagnosing, prognostic maintenance, driver assisted systems, drive patterns, vehicle tracking systems, automated controls and different luxury functionalities. Beside plain edges of connected vehicles, it exposes for many attack surfaces. However, the industry failed in predicting, understanding and addressing to the security dangers and vulnerabilities identified with associated vehicle.

As a result of lack of security in existing vehicle protocol, ton of attacks is found from sniffing the messages to flashing the malicious software configuration file, thereby affecting the critical features of the vehicle. The effect of which can be as little as sniffing sensitive data spillage to as large as human life harm. This vulnerability becomes abundant larger whenever a new device is added because of the lack of robust device identification and authentication.

This paper proposes the thought of security through Trusted Platform Module (TPM) to give resistance against the attack vectors and recognize and authenticate the ECUs securely [12][13].

The TPM that is integral part of the solution is a kind of Hardware Security Module (HSM). It is a worldwide standard for a Secure crypto processor, a devoted microcontroller intended to secure hardware through integrated cryptographic keys [8].

The paper consists of following four sections. Section II portrays the issue existing in the present usage. Section III displays the solution to mitigate the attack surfaces. Section IV provides the conclusion and future work.

II. PROBLEMS IN EXISTING CONNECTED VEHICLE

This section quickly portrays on the issues that are existing in the current connected vehicle usage. These issues result in a huge harm.

A. Device Identification

Identifying any TCU in a connected vehicle plays a significant role in processing the received information and taking an applicable call on functionalities. However, in present connected vehicle scenarios, identification of TCU is occurring on entities that are susceptible to sniffing and counterfeiting.

When exchanging sensitive information or issuing some software configuration file to device, it is constantly important to recognize a specific device. Presently in several TCUs, the identifiers which are utilized are International Mobile Equipment Identity (IMEI), printed sequential number on device, which can be easily read. TCU vendors additionally will in general utilize only a gradual sequential number which can be effectively anticipated. Similar identifiers can be utilized in counterfeited TCUs so as to act like an authentic device as mentioned in [1][2][7] on counterfeiting electronic components.

B. Device Authentication

The Authenticity of a device plays a significant role, because it is intended to validate its identity and only authorized devices are connecting to the network securely. Present TCU manufactures are accustomed to simple

 ISBN: 978-1-61208-720-7

authentication mechanism to ease the method and reduce processing complexity.

The present generally utilized strategy for authentication varies from simple token based or user name and password to relatively secure X.509 certificate based authentication. These authentication strategies are sufficiently dependable as long as this sensitive information's are stored in a secured memory in the Server and device.

C. Firmware/Software update or Configuration file change

Firmware Over The Air (FOTA)/Software Over The Air (SOTA) is an approach used to update software/firmware of any ECU over the air. This feature helps in upgrading or performing diagnostics without taking the vehicle to the Service station. Any malicious software update result in a huge devastation to the system in the vehicle. It very well may be as basic as change of vehicle parameters to complex as remotely accessing or controlling the vehicle mentioned in [3][4][10].

The current industry updating or providing configuration push over the air is actualized on Cyclic Redundancy Check (CRC)/checksum mechanism. An assailant can make his own malicious file with appropriate determined CRC/checksum. There is no validation on the device whether or not the configuration files are from the trustworthy server, that has to be addressed in an exceedingly secure method

D. Probable implementation mistakes in correct usage of TPM

We may have seen solely advantage and secure part of using TPM. Are there any Attack areas for the TPM? Indeed, we do have if TPM is not utilized in the right manner.

Regardless of the reality, we know the active attack on TPM is possible, yet hard to perform and requires expensive devices. A passive attack is still possible with modest and simple strategies.

We realize that TCU microcontroller is connected to TPM through I2C/SPI lines. As these TPM cannot do bulk encryption, these secret keys should be shared to microcontroller when required. These lines can be sniffed to fetch the sensitive data and keys [5][7].

III. MITIGATION

This section clarifies the proposed flow for mitigating issues which was referenced in the previous segment. Our plan is to principally touch upon the secure integration of TPM to the prevailing ECU

A. Device identification

- Each TPM is a unique. Master ID will be burnt during the manufacturing process which cannot be read or altered by anyone
- Changing the master ID is equivalent to changing into new device.
- Keeping this Master ID as seed, a key pair is generated known as EK_pub and EK_priv (EK = Endorsement Key) [12]
- Another set of Key is generated after ownership is claimed on TPM. This is Storage Root Key (SRK). using this, SRK_pub and SRK_priv is generated.
- EK is specific to device and SRK is specific to owner
- Microcontroller will have its own manufacture ID (µC ID)
- Secure uploading of all µC ID, EK_pub and SRK_pub is done to the server which is referred as inventory list as shown in Figure 1.

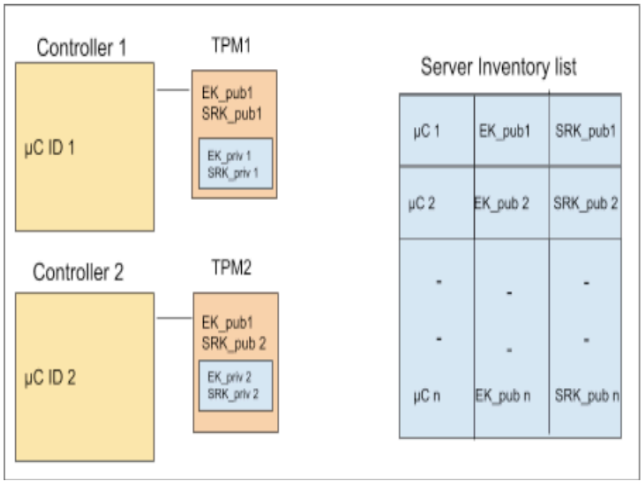

Figure 1. Device identification

B. Device Authentication

Device authentication is the most important mechanism in any of the connected world, where the server wants to identify the device and also device wants to identify the server, thereby mitigating the two entities impersonating each other.

a) Initiation step
- Device with a TPM first connects to the server and requests to initiate for authentication
- Server_pub key is pre-stored in TCU during provisioning process.
- The device shall generate a Random number known as "Nonce".
- The Nonce and µc ID are encrypted and sent to the server as shown in Figure 2. $Encrypt_{server\_publ}$[Nonce + µC ID]

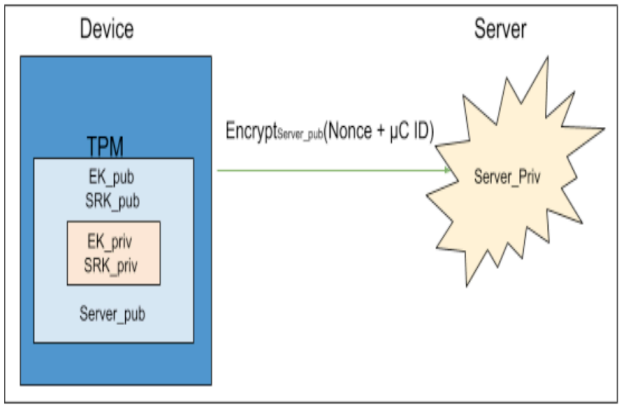

Figure 2. Initiation flow

b) Challenge Flow

- The server now decrypts the received value using Server_priv key.
- Once it decrypts, the Server will generate the Auth Validator (a random string) shown in Figure 3.1.
- Using the µC ID, it fetches the mapping of EK_pub and SRK_pub from the server inventory list.
- Now the Nonce + Auth Validator is signed using Server_priv and encrypted 1st using EK_priv and then using SRK_priv.
- This data is sent to the device as shown in Figure 3.2

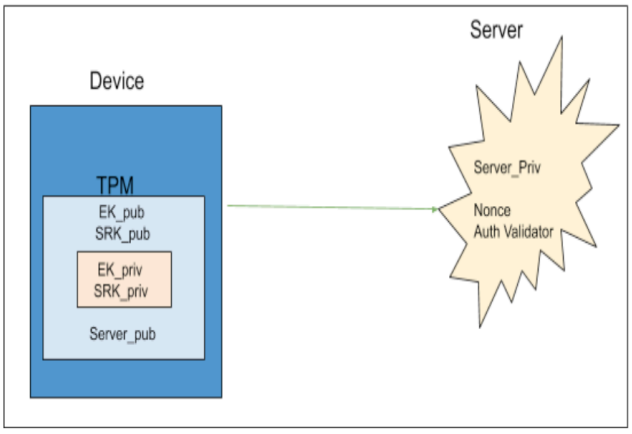

Figure 3.1. Challenge Flow

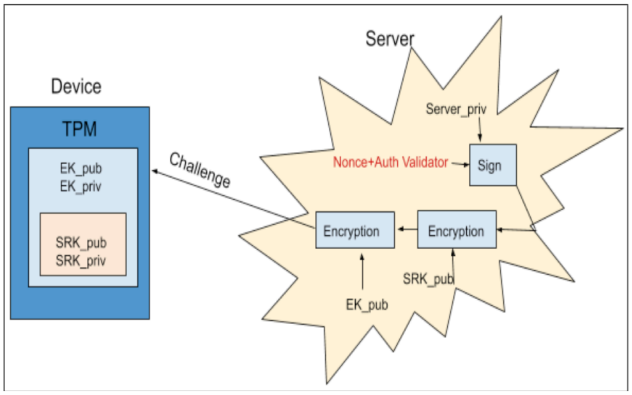

Figure 3.2. Challenge Flow

c) *Verification flow*

- The encrypted nonce is decrypted first using EK_priv and then with SRK_priv to prove the ownership.
- The signed value is verified using Server_pub key to authenticate whether it has come from a trusted server.
- Once signature is verified, The obtained Nonce is verified with the nonce which was generated during the initialisation flow.
- Once Nonce matches, the Auth validator is stored in the TPM secure memory as shown in Figure 4.

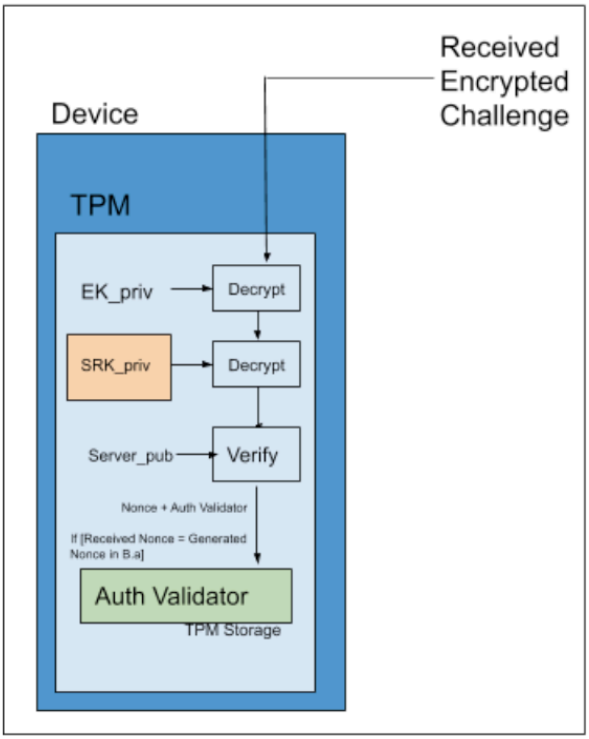

Figure 4. Verification Flow

 ISBN: 978-1-61208-720-7

As a result of the usage of Nonce, replay attack can be avoided which is the real security concern in the present industry. Auth Validator is generated by the server and same Auth Validator is shared securely to TPM. This **Auth Validator** will serve as a symmetric key for encrypting further data to the cloud, thereby solving the confidentiality of the information exchanging mutually. This Process of step a, b and c performs the mutual authentication where TCU can authenticate the server securely and server can authenticate and trust the TCU, which is non-existent in the automotive domain. Introduction of robust security mechanisms like this can provide a **new dimension of security** for the connected vehicle.

C. Firmware/Software update or Configuration file change

Any software update and configuration change must be performed securely, as the dangers were clearly referenced in the previous section. Integration of TPM with the TCU helps in doing this task securely. The serious issue in any of the crypto process is storing of the sensitive keys which are utilized for performing signing, encryption. Storing of these sensitive keys in a secure memory is a major task. In any case, TPM also provides a secure storage highlighting feature to store sensitive keys.

a) Code Signing process

- The Server will generate Server_priv key and store it securely
- The Server_pub key is encrypted and shared to TCU like how it shared Auth Validator in Device Authentication [B].
- The Server_pub is decrypted and stored in the TPM Secure memory.
- EK_pub is already available with the Server
- Now the Software or configuration file is signed using Server_priv key and encrypt the signed packet using EK_Pub of respective device and share to the device as show in Figure 5.

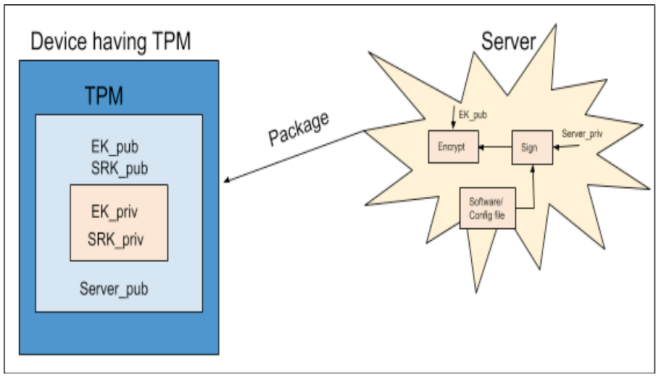

Figure 5. Code signing process

b) Verification process

- The received package is protected as it is encrypted which solves the confidentiality issue.
- This package is decrypted using device EK_priv.
- The decrypted package is verified using Stored Server_pub key. This verifies the integrity and also verifies it is from a trusted server as shown in Figure 6.

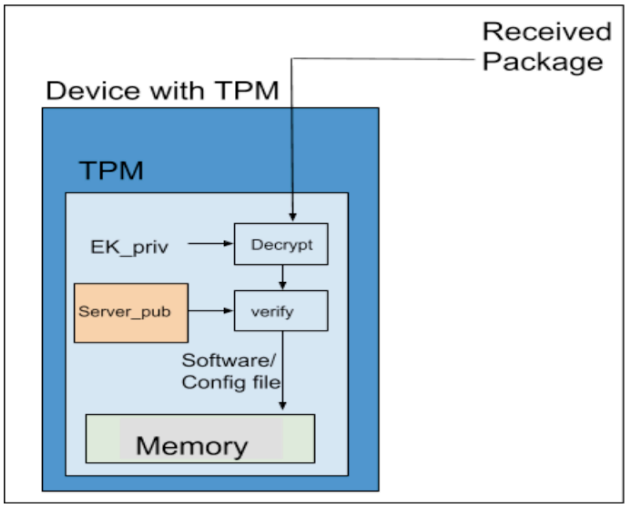

Figure 6. Verification of Package

D. Probable solution to mitigate implementation mistakes while marrying TPM to ECU

As described in the previous section, TPM can add to powerful security modules. However, if not implemented and incorporated in the correct manner, it is prone to several security risks. Below are the considerations to be taken care while marrying TPM to any critical ECU.

- Use the TPM, which has a BGA package (pins are underneath and hard to find the pins for probing). Prefer not to use packages with exposing leads like QFN/TSSOP packages.
- The I2C/SPI lines communicating with the microcontroller must be routed through the internal layers while designing Printed Circuit Board (PCB). So making the communication lines difficult for probing as mentioned in [6].

 ISBN: 978-1-61208-720-7

IV. CONCLUSION AND FUTURE WORK

The primary focus of this paper was to provide efficient and practical solutions for some of critical threats in the connected vehicle environment, which was explained in Section II. These attack surfaces can be segregated into 2 major things, one is a physical attack and another is a remote attack. There are several researches done on the technical aspects of the security of connected cars. This study combines the existing research on the technical security aspects of connected vehicles along with the improvisation of security in connected vehicles. Usage of TPM is already proven in networking domains in enhancing the security. Recently automotive domain started using it. It is worth looking at matured domains to borrow certain technology to empower security posture in ever growing automotive world. Another research question that can be examined and is not covered in this paper is about the V2V secure communication. How do we extend this connected vehicle concept to prevent accident or enhance the safety of passenger or driver by connecting to nearby vehicle when in danger? Thus, with the current and growing awareness of the importance of hardware security, trustworthy connected vehicle systems can be deployed in the coming years.

REFERENCES

[1] J. Laidlaw, “Counterfeit hardware may lead to malware and failure”, HACKADAY, 18 June 2019.

[2] C.S Jeena, “Counterfeit threat for electronic industry on rise: plug it”, The Holography times, Volume 8, Issue 24, 2014.

[3] S. Nie, L. Liu, W. Zhang and Y. Du, “Over-the-air: How we remotely compromised the Gateway, BCM and Autopilot ECUs of Tesla cars”, Blackhat USA, August 2018.

[4] “Car Hacking Research: Remote attack Tesla Motors”, Keen Security lab of Tencent, 19 September 2016.

[5] J. Winter and K. Dietrich, “A hijacker’s guide to communication interfaces of the trusted platform module”, ScienceDirect, Volume 65, March 2013.

[6] “AN928.1 EPR32 Series 1 Layout Design guide”, Silicon labs

[7] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya Z. Ma, F. Kargl, A. Kung and J.P Hubaux, “Secure vehicular Communication Systems: Design and Architecture”, IEEE Communications Magazine, 30 December 2009.

[8] F. Kargl, P. Papadimitratos, L. Buttyan , M. Muter, E. Schoch , B. Wiedersheim T.V. Thong, G. Calandriell, A. Held and A. Kung, “Secure Vehicular Communication Systems: Implementation, Performance and research Challenges”, IEEE Communications Magazine, 25 November 2008.

[9] “Secure Vehicular Communications: Security Architecture and Mechanisms for V2V/V2I”, SeVeCom, Delivarable 2.1, 2007- 2008.

[10] S. Nie, L. Liu and Yuefeng Du, “Free-fall: hacking tesla from wireless to CAN bus”, blackhat, September 2016.

[11] T. Leinmuller, “Car2x Communication - Challenges, standardization and implementation in Europe and in the US”, 2007.

[12] J.S. Suresh and L. Jongkun, “A TPM based architecture for Secure VANET”, Indian Journal of Science and Technology, July 2015.

[13] G. Guette and O. Heen. “A TPM based architecture for improved security and anonymity in Vehicular Ad-hoc Networks”, IEEE Vehicular Networking Conference, 2009.

[14] “TPM 2.0 Library Specification”, Trusted Computing Group, 29 September 2016.

[15] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and Vulnerable : A story of Telematics Failures”, USENIX, 2015.

 ISBN: 978-1-61208-720-7