Security in Connected Cars

Mushabbar Hussain

Abstract This article provides an overview about the probable security threats in modern automotive systems, and possible counter measures to safeguard the vehicle from potential attacks. This paper attempts to describe few prominent use cases in the automotive context and potential threats associated with each of them, followed by possible security mechanisms to provide a secure environment. The main focus of this paper is to discuss about the security threats in connected cars and possible security solutions to counter the attacks. Further this article briefly discusses about hardware cryptographic solutions and the advantages of hardware security for realizing real-time solutions. Finally provides a realtime illustration of how security concepts can be applied to automotive usecases. The paper concludes by highlighting the importance of having security built into the products right from the concept phase.

Keywords Cybersecurity · Connected cars · Automotive security · Key management · V2X communication · HSM

Introduction

The classic cars were much simpler, and so was the electronics in them. The components of a classic cars were discrete and unconnected to each other, they were more of a closed systems without much interaction with the external world. With advances in technology, the modern automotive systems have become more sophisticated, more software-intensive, more complex, and highly connected systems making them highly vulnerable to security attacks. A modern automobile can have up to 80 embedded microcontrollers on board running tens of millions of lines of code within them. The embedded ECU's control almost every function of the car

M. Hussain (✉)
KPIT Technologies, Sarjapura Outer Ring Road, Bangalore 560103, India
e-mail: mushabbar.hussain@kpit.com

C. Andreescu and A. Clenci (eds.), *Proceedings of the European Automotive Congress EAEC-ESFA 2015*, DOI 10.1007/978-3-319-27276-4_24

including safety-critical vehicle applications such as braking, engine control, steering, airbag functions, navigation systems etc. Therefore security attacks are not just limited to disclosure and loss of sensitive data but also affect the safety critical functions of the car.

Recent studies and Experiments conducted by Independent research organizations from EUROPE/US (Checkoway et al. 2015) have demonstrated that once a hackers gain access to the in-vehicle network of the car, could control everything; from controlling the acceleration, to applying/releasing brakes, playing songs of their choice, locking/unlocking the doors. These experiments have demonstrated that security plays an important role in automotive systems because security threats might not only cause nuisance and disclose of sensitive data but also affect the safety critical functions of the car. This mean without security there is no safety.

Security Threats in Connected Cars

A connected (or autonomous) car is a driverless car or self-driving car which is capable of sensing its environment and navigating without human input. Autonomous cars are fully connected vehicles that use a combination of wireless technologies (such as radar, lidar, GPS) and advanced sensors (stereo cameras and long- and short-range RADAR) for its operation. These cars are expected to have a permanent connection to the Internet and to the cloud for fetching various kinds of information such as current road situation, weather conditions, or the parking situation at the destination. Benefits of autonomous cars include zero accidents, reduced traffic violations, productive commute time, elimination of human errors, improved energy efficiency (Silberg and Wallace 2014).

In order to operate in real time, autonomous cars may use wireless technologies to communicate with the grid, the cloud, with other vehicles (V2V) and to infrastructure (V2I). An enormous amount of data will becomes available on the air. This essentially means that someone—a hacker, terrorists, and unauthorized parties can have means to capture data, alter records, instigate attacks on systems and track every movement of vehicle. The hackers can gain access to the vehicle sensors that control airbags, breaking systems, door lock operations and virtually control or disable the car. They could provide false information to drivers, use denial-of-service attacks to bring down the in-vehicle network, illicitly reprogram the ECUs with a malware and even can download incorrect navigation maps to mislead the driver. Therefore, system security will undoubtedly become a paramount issue which the automakers need to address before putting the autonomous cars on the road (Fig. 1).

The current automobiles today are not quite capable to detect and prevent hackers from gaining access to the vehicle network, detecting and rejecting malicious commands injected into the ECU (Barry and Philpot 2011).

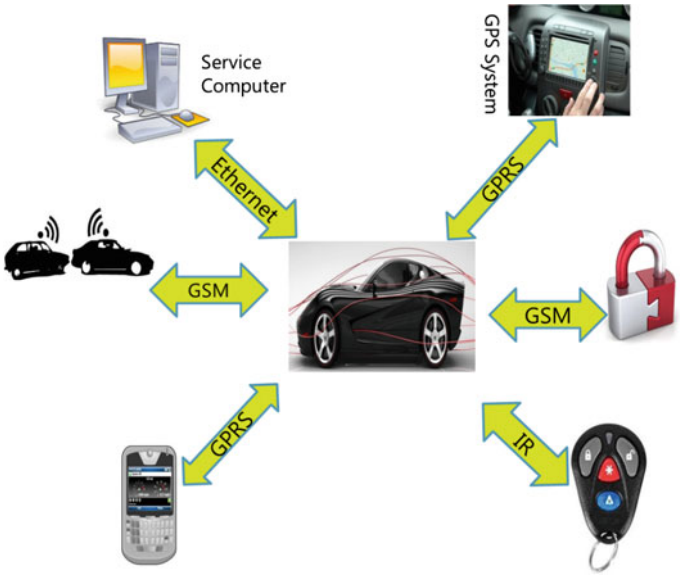

Fig. 1 Typical vehicle network of a modern vehicle

Here are some of the security threats to modern automobiles:

- Inducing forged traffic into the in-vehicle network
- Downloading of malicious applications into the ECU
- Gaining access to ECU resources by launching a brute force attack on the system
- Illegal Odometer Tuning
- Tuning/Manipulation protection
- Attack on Tire Pressure Monitoring System (TPMS)
- Inducing forged traffic into a navigation system
- Breaking Antitheft systems such as central locking, immobilizers
- Corruption of rewriteable flash memory
- Execution of unauthorized commands

The security system inside autonomous vehicle shall ensure:

- Technology in a self-driven car works 100 % of the time without compromising on the safety-critical functionality.
- Internal as well as external communication interfaces are properly secured
- Enable Secure software download
- Detect and prevent malware from running on the ECU's
- Enable secure access to secret keys and confidential data
- Electronic immobilizer;
- Software and hardware integrity
- Protection from theft and forgery

Realization of Security Solutions in Automotive Systems

In this section provides a general overview of some of the important automotive features, and discuss about possible security measures that can be applied to make the vehicle functions secure from cyber attacks (Fig. 2).

Main Automotive Usecases

- **Target Authentication**
  Target authentication involve authentication of entities and communication partners before allowing access to its internal resources. For ex, authentication of entities requesting read/write access to ECU internal data—ex, diagnosis testers, remote clients
- **Secure Communication**
  The system shall ensure authenticity and integrity of the data communicated over internal/external interfaces. Ex: Secure OnBoard, Secure Off-Board communications
- **Secure Boot**
  The objective of the secure boot is to ensure the integrity of code/software stored in the flash has not been compromised. Secure boot validates the flash contents by computing the digital signature of the flash software component and compare it with the pre-configured value. Popularly implemented with the help of hardware security peripheral

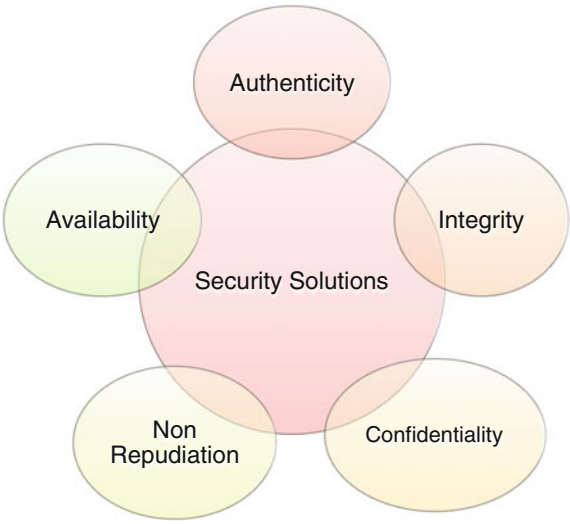

Fig. 2 Security elements of interest

- **Secure Flashing**
  Secure flashing helps to prevent malicious content from getting flashed on the ECU. Secure Software flash-loaders employ security mechanisms such as application authentication (using MAC, Digital Signatures), application integrity check (using CRC, hash) to ensure the authenticity and integrity of software being flashed into the ECU memory
- **Key management functions**
  Key management is the management of security keys in a cryptosystem. This involves key generation, exchange, storage, use, update, deletion of keys. It includes technology, policies and procedures for managing all the cryptographic keys—symmetric and asymmetric
- **V2X Communication**
  V2X (Vehicle-to-Vehicle or Infrastructure) communication involves exchange of information between vehicles, with the roadside infrastructure (ex traffic signals, warning signs), with remote systems such as e-call center, with the GPS systems etc. V2X plays an important role in the development of Intelligent Transport System (ITS) and connected cars.
- **Secure Storage**
  Secure storage of confidential data such as secret seeds, keys, keying material, security logs, and configuration/calibration data

In order to secure the vehicles from cyber-attacks, the system shall implement appropriate security mechanisms based on software and hardware cryptography. The security system must ensure that data is protected during its transit, while it is stored & accessed, and have mechanism in place to ensure both unauthorized (malicious hackers) and unintended modifications do not go undetected.

Here are some of the crypto services that help in realization of security solutions in automotive systems:

- Digital Signature generation/verification
- Message Digest generation/validation
- MAC generation/verification
- Random Number generators
- Data Encryption/Decryption based on Symmetric and Asymmetric keys
- Secure Hash

Security Solutions can be Realized by Both Hardware and Software Crypto Mechanisms

In order to harden ECUs against security attacks, security mechanisms (to prevent successful manipulation of software, data, keys and keying material) must be rooted in hardware (Fig. 3).

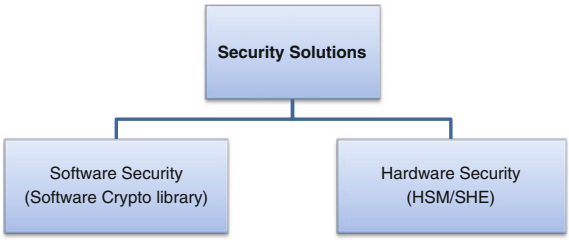

Fig. 3 Security solutions broadly level classification

Hardware security solutions are realized with the help of hardware security peripherals such as HSM (Hardware Security Module) based on EVITA, and SHE (Secure Hardware Extension) based on SHE specifications. EVITA and SHE are major security initiatives in the auto industry that define security standards, EVITA specification targets both Hardware & Software solutions

Introduction to SHE/HSM

SHE/HSM are on-chip security peripherals embedded within an automotive MCU. HSM/SHE are dedicated security modules specifically developed and designed for security use-cases. They are designed to move cryptographic functions from SW to HW domain (The Evita Project) (Fig. 4).

SHE/HSM usually provides a fixed set of cryptographic services to the application layer. The basic cryptographic services can be used to realize complex automotive security use-cases

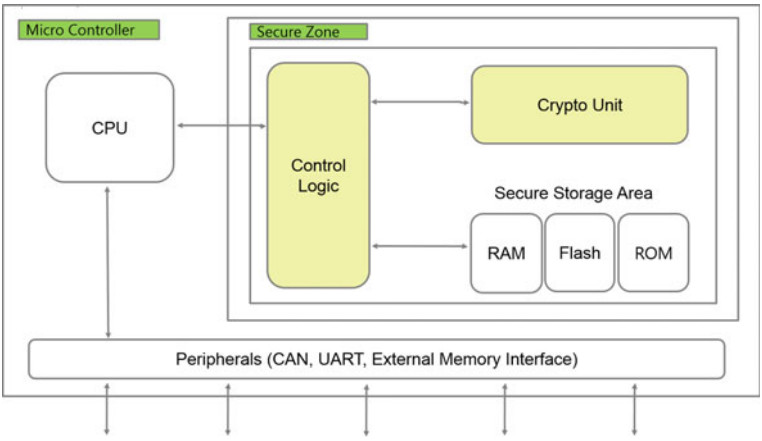

Fig. 4 Simplified logical structure of a hardware security peripheral

Main Features/Functions:

- Symmetric key Encryption based on AES-128
- CMAC generation & verification
- Random number generation for secure generation of cryptographic keys
- Application/Boot loader verification
- Secure storage of secrets keys and keying material
- On-chip Flash/ROM read-out protection against unauthorized access

Advantages of SHE/HSM:

- Onboard secure cryptographic key generation
- Onboard secure cryptographic key storage and management
- Offloading application servers for complete asymmetric and symmetric cryptography.
- Hardware acceleration

A Sample Case Study

In this section we look at practical use case of a Secure Bootloader in the automotive context and see how security concepts can be applied to make the software download more secure (Fig. 5).

Main features of a Secure Flash loader:

- **Application Authentication**: To ensure the authenticity of data downloaded to the ECU (verify that software originated from known source)
- **SW Integrity check**—Verify that the SW has not been altered during transit
- **Secure Boot**: Software authenticity verification during ECU start-up
- **Secure Access**: Ensures that only authorized Testers can unlock the ECU to perform critical tasks such as application flashing, vehicle diagnostics etc.
- **Secure Storage**: For secure storage of ECU confidential data such as secret seed/keys, keying material (Fig. 6).

Illustration of Application Authentication

To enable application authentication and integrity check, signature of the application software is computed (ex, using CMAC, RSA-2048) and attach to the software that is downloaded.

ECU Side:

- ECU re-computes the signature of the downloaded software: S'
- Compares computed signature(S') with the attached signature(S)

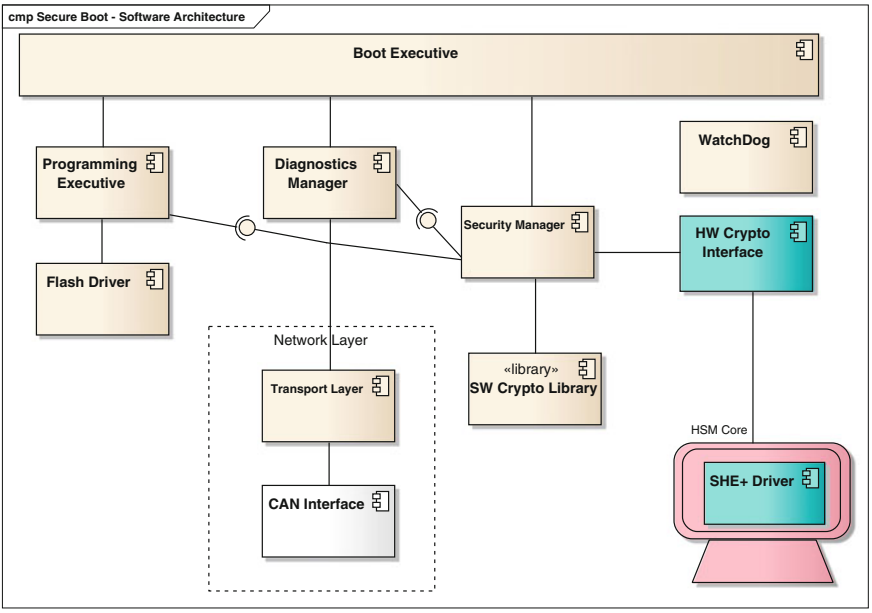

Fig. 5 Secure bootloader architecture

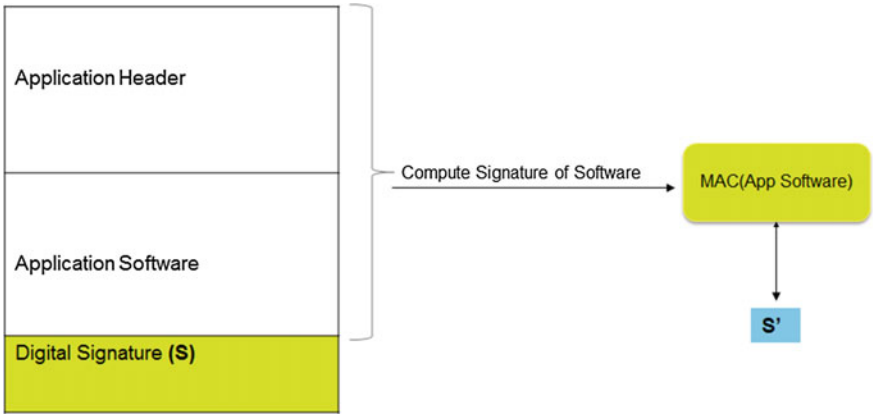

Fig. 6 Application authentication example

- If S = S' → application is authentic

The above example illustrations demonstrates how security concepts can be applied to verify the authenticity and integrity of software before flashing them into the ECU.

Conclusions

With modern automotive systems getting connected to the internet, the security is no more an optional feature. In the last decade, the automobile industry has been focusing more on improving safety aspects of the car and this decade the focus would be to build more secure and safer vehicles. As the security threats can endanger life of the passengers designing more secure products is an absolute necessity.

Building secure products cannot happen overnight, it should start from the early days of software development life cycle. Security should be built into the design and into the code. Developers should start designing and implementing security based on threat analysis results of their systems, address the vulnerabilities (security holes) in a phase wise manner. Lastly consider industry standards such as NIST (National Institute of Standards and Technology), ENISA(European Union Agency for Network and Information Security), FIPS(Federal Information Processing Standards), EVITA, SHE, in building crypto/security solutions rather than going with proprietary security mechanisms

Currently many organizations are involved in doing research related to security in connected cars. Most of the research has focused on identifying the security problems and only to a lesser extent towards presenting solutions. Much remains to be done. One of the greatest challenges in adding security to the connected car would be to adapt the security solutions to the very high safety requirements, under the constraints of very limited hardware, software and power resources.

References

Barry K, Philpot C (2011) Can your Car be hacked? http://www.caranddriver.com/features/can-your-car-be-hacked-feature

Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S (2015) Comprehensive experimental analyses of automotive attack surfaces. University of California, San Diego; Koscher K, Czeskis A, Roesner F, Kohno T University of Washington

Digital signature. http://en.wikipedia.org/wiki/Digital_signature

Information security. http://en.wikipedia.org/wiki/Information_security

Potlapally N (2008) Secure embedded system design. http://palms.ee.princeton.edu/PALMSopen/dissertations/Nachiketh_Potlapally_phdthesis.pdf

Silberg G, Wallace R (2014) Self-driving cars: the next revolution. https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf

The Evita project. http://www.evita-project.org/objectives.html