Security Concerns for Automotive Communication and Software Architecture

Huafeng Yu
Toyota InfoTechnology Center
465 Bernardo Avenue, Mountain View, CA 94043
Email: huafeng.yu@us.toyota-itc.com

Chung-Wei Lin
Toyota InfoTechnology Center
465 Bernardo Avenue, Mountain View, CA 94043
Email: cwlin@us.toyota-itc.com

***Abstract*—Cyber security concerns in the automotive industry have been constantly increasing as automobiles are more computerized and networked. Recent successful hacks of modern vehicles demonstrate the big security concerns for automotive systems. However it is still very hard and even impossible to predict what kinds of security issues will happen. In this paper, we present the automotive security concerns from several different and fundamental points of view: communication, system and software architecture. We first discuss different security concerns related to communication media and protocols, such as CAN bus and Ethernet. We then consider concerns for automotive architecture: general system architecture and AUTOSAR-based architecture. For each view, we summarize the open questions and challenges in the design of secured automotive systems. In spite of addressing security concerns with very specific solutions, we promote a system-level security design approach considering both communication and software architecture. This requires to consider the security issues and design from an architecture and systems engineering points of view.**

I. Introduction

Integrated security solution is one of the major missing pieces in the current design and production of automobiles. Security concerns in the automotive industry are becoming a major issue as automobiles are more connected and software-controlled. However, in modern vehicles, security has been considered in only several devices, such as immobilizers, which is not enough. Recent reports on vehicle hacking involve various systems in many models from different OEM's [9], [22]. A series of successful hacking activities against current car models show the lack of system-level security consideration in vehicle design, which lead to concerns at US political level [18].

Dissimilar to safety or performance aspects of a vehicle, vulnerability related to auto security is generally very hard and even impossible to predict. So solutions to specific vulnerability are generally not enough. To address different kinds of hacks, we need to analyze the automotive security concerns both at the system level and architecture level to ensure a secure vehicle system considering different aspects such as confidentiality, integrity, authentication, and access control [24] under the constraints, like performance, cost, and power consumption.

In this paper, we present the automotive security concerns from several different points of view: communication, system and software architecture. We first discuss different security concerns related to communication media and protocols, such as CAN (Controller Area Network) bus and Ethernet. We then consider concerns for automotive architecture: general system architecture and AUTOSAR-based (AUTomotive Open System ARchitecture) architecture. For each view, we summarize the open questions and challenges in the design of secure automotive systems.

II. Communication

A. Communication Protocols

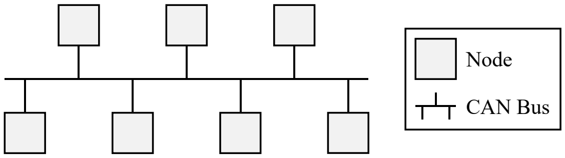

Fig. 1. All nodes are connected to the CAN bus without a host.

Currently, the most used in-vehicle communication protocol is the Controller Area Network (CAN) [3]. The CAN protocol is based on a bus, and all nodes are connected to the CAN bus without a host as shown in Fig. 1. All nodes sample every bit at the same time to support bit-wise arbitration for contention resolution and transmission, where the priority of each message is uniquely static. The data field of a frame (a frame is an instance of a message) is 8-byte long in the conventional CAN protocol, and it is 64-byte long in the CAN with Flexible Data-Rate (CAN FD) [4]. The data rate is up to 1 Mbps with connection lengths below 40 meters, and it decreases as connection lengths increase. The CAN protocol is popular for automotive systems due to low cost and simple design. Besides, certain timing models [6] can be applied to provide timing guarantees which are necessary for automotive systems.

The Ethernet is considered to be the next-generation in-vehicle communication protocol for automotive systems because of its high bandwidth and well-developed technologies. All nodes are connected through one or more Ethernet hubs or switches as shown in Fig. 2. The Ethernet is theoretically based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD), but switches can process and forward frames to appropriate ports to reduce the number of collisions.

978-1-4673-9955-5/16/$31.00 ©2016 IEEE

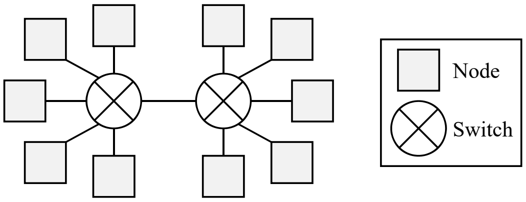

Fig. 2. All nodes are connected through one or more Ethernet hubs or switches.

The data field of a frame is 1,500-byte long, and the data rate ranges 3 Mbps to 100 Gbps, depending on the physical layers. To further provide timing guarantees, several Ethernet extensions, such as Time-Sensitive Network [11] (former Audio Video Bridging) and Time-Triggered Ethernet [21], are proposed. Different from the conventional Ethernet, these extensions support Quality of Service (QoS) and preemption so that high-priority messages can be guaranteed to meet their corresponding deadlines. Again, this feature is necessary for automotive systems.

For Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communication, the major technology is Dedicated Short Range Communications (DSRC), also known as Wireless Access in Vehicular Environments (WAVE), which is specified in a set of standards [12]. They cover from the physical layer to the application layer, utilize IEEE 802.11p in the lower layers, and define many different perspectives including architecture, multi-channel operation, network services, security services in the higher layers. Especially, Basic Safety Message (BSM) is defined in the message sublayer (above the transport layer), and it contains time, position, velocity, direction, size, and other important information of a vehicle. More details of DSRC can be obtained in some previous works [12].

B. Security Concerns

Security has been identified as a rising issue for automotive systems. Especially, communication protocols are the interfaces for attackers to get access to systems, and those interfaces include diagnostics ports, empty ports, or wireless networks. The CAN protocol is the most popular protocol for attackers since it is widely used and there is no security protection. Hoppe *et al.* [10] discovered the weakness of the CAN protocol and controlled the operations of electric window lifts, warning lights, and airbag control systems. Koscher *et al.* [15] presented that they are able to manipulate safety-critical ECUs (Electronic Control Unit) and execute the functions of body control modules, engine control modules, electronic brake control modules, etc. Furthermore, denial-of-service attacks were also successfully performed so that inputs from the driver were ignored. Rouf *et al.* [20] studied wireless tire pressure monitoring systems and demonstrated that eavesdropping and spoofing are possible for messages sent from a tire pressure sensor. Kleberger *et al.* [14] provided an overview of in-vehicle security threats and protections.

Besides in-vehicle networks, Checkoway *et al.* [5] focused on external attacking surfaces of automotive systems and demonstrated remote exploitation through indirect physical access (CD or PassThru, a standardized programming interface for the access of diagnostic ports), short-range wireless access (Bluetooth), and long-range wireless access (cellular). A recent case [7] also showed that a vehicle was hacked through a cellular network, a specific network port, and an in-vehicle Internet-connected computer which is deployed widely in many modern models. The air conditioner, radio, windshield wipers, and even accelerator, were all taken control in this case.

There are many different types of security requirements to be achieved. They can be categorized into integrity, authenticity, confidentiality, and availability. Usually, integrity and authenticity are more important than confidentiality for automotive systems as it is extremely danger if a system is taken control by an attacker. As as result, most existing security mechanisms [8], [17], [19], [23], [25] focused on authenticating messages, and most of them utilized symmetric cryptography to compute Message Authentication Codes (MACs) so that a receiver can authenticate the identity of a sender.

C. Open Problems

Cross-Layer Security. Although many security mechanisms exist for automotive systems, they usually address security problems in certain specific layers. There may still be security concerns as a security hole in another layer still provides opportunities for attackers to make the whole system fail. A comprehensive study on cross-layer security analysis and protection is necessary for the system-level security.

Limited Resource. Due to cost and design complexity, the communication resource and the corresponding computational resource in automotive systems are usually less than those in computer network. This makes it difficult to directly apply high-overhead security mechanisms or existing security mechanisms in computer network to automotive systems. This also means, when security mechanisms are proposed, the applicability on automotive systems must be considered and verified.

Hard Design Constraint. Automotive systems have some hard design constraints. One example is the real-time deadline of a message corresponding to a safety-critical application. Similar to the problem of limited resource, even if security mechanisms have been proved to be secure, its impact on real-time deadlines and other design constraints must also be considered and verified.

Plug-and-Play Architecture. A plug-and-play architecture allows users to download or update applications in real-time, and this causes more security concerns because the applications themselves and their transmissions are possible to be vulnerable by attackers. On the other hand, the corresponding design becomes more flexible (for example, the priority assignment for messages in the CAN protocol), which raises more challenges when considering security and other design constraints together.

Unstable Connection. Security mechanisms for automotive systems should not rely on the assumption that the connection to a third-party is always available. This is by the nature that automotive systems are moving, probably with high speeds, and they may enter some regions without connections.

III. Software Architecture

In this section, we mainly consider security concerns related to automotive software architecture. First, we consider the architecture from a more general point of view, i.e., an architecture composed of sensors, ECUs, buses, and actuators; then we consider a more specific automotive standard software architecture: AUTOSAR.

A. General Automotive Architecture

A general architecture is similar to Fig. 1, where the nodes are computing units (e.g., ECUs), sensors (e.g., speed sensors, radar, LIDAR, WiFi, DSRC devices) and actuators (e.g., brake). The links between nodes can be any kind of communication media (e.g., LIN, CAN, FlexRay, Ethernet). Security concerns may occur in all these devices. For example, in [9], a LIDAR was hacked and the security researcher claimed, “I can take echoes of a fake car and put them at any location I want, and I can do the same with a pedestrian or a wall.” ECU can be updated with uncertified software for expected power or MPG (Miles Per Gallon); buses can be hacked and used to send faulty messages.

From an architectural point of view, we mainly discuss two aspects here: access points of hacking and system-level security. Regarding access point, we can easily find directly physical access to sensors, actuators and ECUs. Currently, only several critical automotive subsystems (such as immobilizers and certain ECUs) are protected by particular security mechanism. One can also access from the in-vehicle network provided by buses, like CAN, FlexRay, or Ethernet. One example is the access of CAN buses via OBD-II (On-Board Diagnostics) interface. New communication features, such as Bluetooth, WiFi, DSRC, provide another potential access point, from which hacks can be achieved remotely. The new trend of connected and autonomous cars makes security-related protection more exigent.

Architecture-based system-level security is mainly discussed from three aspects here: basic security support, hardware and software security implementation. Basic security support includes security services (e.g., libraries) that are provided for both hardware and software security implementations. Hardware and software security implementation includes modules that enable to protect specific hardware and software with particular mechanisms. Next subsection gives more details about system-level security with the standard AUTOSAR architecture.

B. AUTOSAR and Its Security Concepts

AUTOSAR [1] is an open standard dedicated to automotive software architecture. It is developed by AUTOSAR consortium, which includes participants from OEMs, suppliers, and tool vendors. AUTOSAR provides an open standardized ECU software system architecture and platform concept for the design of automotive software and user interfaces. It defines several software layers to address complexity and modularity, including Basic software (BSW), Runtime Environment (RTE), and Application layer. AUTOSAR enables a system-level solution for software integration.

The security is a relatively new addition to AUTOSAR and it mainly focuses on authentication using cryptography for secure computing and communication. The AUTOSAR architecture consists of four layers including Application Layer, Service Layer, the ECU Abstraction Layer, and Microcontroller Abstraction Layer. Fig. 3 shows an AUTOSAR Layered View with CSM (Crypto Service Manager).

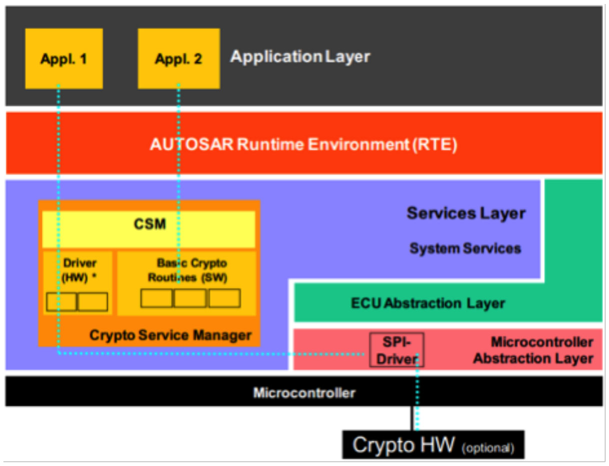

Fig. 3. AUTOSAR Layered View with CSM, extracted from [2].

- Application Layer hosts software applications running on the runtime environment to provide functions of the ECU system.
- Service Layer is used to provide basic services for application and basic software modules. That is, it offers the most relevant functionalities for application software and basic software modules.
- ECU Abstraction Layer responds to the functions of applications in Application Layer and connects to Microcontroller Abstraction Layer which is the interface to the microcontroller of the ECU.
- Microcontroller Abstraction Layer accesses on-chip MCU peripheral modules and external devices.
- Crypto Service Manager (CSM) provides cryptography services via a software library (Basic crypto routines) and/or on a hardware module (Crypto HW). The latter is defined not be read or modified by any malicious activities and can be used to store secret keys.

Even AUTOSAR provides a specific security mechanism, it still lacks sufficient support to system-level security concerns, which is still a challenge for the automotive domain [13]. In the next subsection, current open questions are summarized.

C. Open Questions

Computing Performance and Resource Consumption. From an architectural viewpoint, the biggest concern is not the implementation of different security algorithm or mechanisms, but the performance and resource consumption. Automotive domain always in a high competitive market, and the cost is always one of biggest constraints, which will eventually limit the application of best security solutions.

New Hardware Devices. New hardware devices, sometimes help to increase the performance of the system, e.g., multicore, GPU, then performant security mechanism can be implemented. But new hardware also give new challenges, e.g., LIDAR, radar, camera. With these new hardware device, more security concerns emerge, e.g., delay the data transmission from camera can make the autonomous vehicles make wrong decisions on its environment.

Computing Platform Concern. Next generation vehicle systems provide a potential performant computing platform, where large amount of private data are produced and stored. So security concerns include not only controlling the vehicle, but also accessing private or protected data, or even controlling the auto platform to attack others.

Integration Concern. Different security mechanisms and algorithms or even platforms will be designed and implemented in the automotive systems. How to integration all these security implementations will be a big challenge. Another challenge is to integrate security with other aspects, such as safety [16].

IV. Conclusion

In this paper, we present the automotive security concerns from several different points of view: communication, system and software architecture. We first discuss different security concerns related to communication media and protocols, such as CAN bus and Ethernet. We then consider concerns for automotive architecture: general system architecture and AUTOSAR-based architecture. For each view, we summarize the open questions and challenges in the design of secure automotive systems. In conclusion, we promote a system-level security design approach considering communication and software architecture. This requires to consider the security issues and design with a dedicated systems engineering methodology, which is adapted to automotive systems engineering.

References

[1] AUTOSAR, "Automotive open system architecture v4.2.2.", 2015.

[2] AUTOSAR, "AUTOSAR: specification of crypto service manager v4.2.2.", 2015.

[3] Bosch, CAN Specification (Version 2.0), 1991.

[4] Bosch, CAN with Flexible Data-Rate White Paper (Version 1.1), 2011.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," *USENIX Conference on Security*, pp. 6–6, 2011.

[6] M. Di Natale, H. Zeng, P. Giusto, and A. Ghosal, "Worst-case time analysis of CAN messages," *Understanding and Using the Controller Area Network Communication Protocol*, pp. 43–65. Springer, 2012.

[7] A. Greenberg, "Hackers remotely kill a Jeep on the highway—with me in it," Wired, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] B. Groza, S. Murvay, A. Van Herrewege, and I. Verbauwhede, "LiBrA-CAN: a lightweight broadcast authentication protocol for Controller Area Networks," *International Conference on Cryptology and Network Security*, pp. 185–200, 2012.

[9] M. Harris, "Researcher hacks self-driving car sensors," *IEEE Spectrum*, Sep. 2015.

[10] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—practical examples and selected short-term countermeasures," *International Conference on Computer Safety, Reliability, and Security*, pp. 235–248, 2008.

[11] IEEE, IEEE Standard for Local and Metropolitan Area Networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks, IEEE Standard 802.1AS-2011, 2011.

[12] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[13] D. Kim, E. Song, and H. Yu, "Introducing Attribute-Based Access Control to AUTOSAR," *SAE World Congress 2016*, doi:10.4271/2016-01-0069, 2016.

[14] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," *IEEE Intelligent Vehicles Symposium*, pp. 528–533, 2011.

[15] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," *IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.

[16] C.-W. Lin, and H. Yu, "Cooperation or Competition? Coexistence of Safety and Security in Next-Generation Ethernet-Based Automotive Networks," *ACM/EDAC/IEEE Design Automation Conference (DAC)*, to appear, 2016.

[17] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the Controller Area Network communication protocol," *ASE International Conference on Cyber Security*, pp. 344–350, 2012.

[18] E. Markey, "Tracking & hacking: security & privacy gaps put American drivers at risk," 2015.

[19] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, "Lightweight authentication for secure automotive networks," *IEEE/ACM Design, Automation and Test in Europe*, pp. 285–288, 2015.

[20] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," *USENIX Conference on Security*, pp. 21–21, 2010.

[21] SAE, Time-Triggered Ethernet, SAE Standard AS6802, 2011.

[22] D. Schneider, "Jeep hacking 101," *IEEE Spectrum*, 2015.

[23] A. Van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth—a simple, backward compatible broadcast authentication protocol for CAN bus," *Workshop on Embedded Security in Cars*, 2011.

[24] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: embedding security in vehicles," *EURASIP Journal on Embedded Systems*, p. 16, 2007.

[25] R. Zalman and A. Mayer, "A secure but still safe and low cost automotive communication technique," *ACM/IEEE Design Automation Conference*, pp. 43:1–43:5, 2014.