Security for Autonomous Vehicle Networks

Aifen Sui
Huawei Technologies Duesseldorf GmbH
Munich Germany
aifen.sui@huawei.com

Gordon Muehl
Huawei Technologies Duesseldorf GmbH
Munich Germany
gordon.muehl@huawei.com

2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT) | 978-1-7281-9045-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICEICT51264.2020.9334354

***Abstract*— Autonomous driving is developing rapidly with the progress of AI. But due to the evolution of automotive E/E architecture and interaction of vehicle-to-everything, security threats are also increasing rapidly. In this paper, we try to identify the technical challenges and the core issues of securing Autonomous Vehicles and the networks, make an analysis of the mainstream standards and industry best practices, and furthermore highlight some research areas.**

***Keywords*— Security, Autonomous Vehicle (AV), Vehicle-to-everything (V2X)**

I. INTRODUCTION

Autonomous driving helps to improve performance and reduce the number of driving-related accidents and crashes and is developing rapidly with the progress of AI. SAE International (the Society of Automotive Engineers) recommended a taxonomy of driving automation for on-road vehicles: from level 0 no driving automation to level 5 full automation [1]. Partially automated systems (SAE L2) are the mainstream products today. Highly automated driving (SAE L3 and higher) target to release human from more and more driving tasks and Autonomous Vehicle (AV) usually refers to Level 3 and above. The six levels of driving automation are summarized in Table I [2].

TABLE I. SIX LEVELS OF DRIVING AUTOMATION

Level	*Automation*	*Steering Cruise*	*Environ-ment Monitoring*	*Fall-back Control*	*Driving Modes*
0	Non	H	H	H	N/A
1	Supportive	H,S	H	H	Some
2	Partical	S	H	H	Some
3	Conditional	S	S	H	Some
4	High	S	S	H	Some
5	Full	S	S	S	All

(*S:* SYSTEM, *H:* HUMAN)

When the autonomy level gets higher, the security risks is also escalated. In [3], common practices and emerging technologies for autonomous driving are thoroughly studied from high level system architectures to the core functions. The available datasets and ADS development tools are also summarized. In [4] the authors provided a systematic study on the security threats regarding sensors, in-vehicle systems and in-vehicle protocols, and furthermore summarized the corresponding defense strategies. In [5] the authors presented a Taxonomy of security attacks and defense for Autonomous Vehicles.

In this paper, we try to present from other views like E/E (Electrical / Electronic) architecture, software and V2X aspects. In chapter II we try to identify the technical challenges and the core issues of securing Autonomous Vehicle networks. Then an analysis of the mainstream standards and industry best practices is given in Chapter III. In Chapter IV potential security technologies including secure E/E architecture, secure V2X and secure perception are highlighted. Finally conclusion is drawn in chapter V.

II. SECURITY CHALLENGES

By integrating various sensors, autonomous vehicles interact more with the environment when compared to traditional ones. Meanwhile the E/E architecture, software and networks are also evolved to enable autonomous features. As a consequence new security challenges are also introduced.

A. E/E architecture evolution

Most of vehicle features are aided or enabled by electrical / Electronic components and the underlying Electrical /Electronic (E/E) architecture. Continental AG presented in IEEE802 Plenary 2019 about the evolution of Automotive E/E Architecture and its impact on the network [6], which also represents the mainstream opinion about E/E architecture evolution. The evolution involves hardware, software, networking and etc., e.g. more and more functions are exposed to external, core functions are centralized into only a few computing nodes. Due to the huge changes, existing security design is not applicable any more.

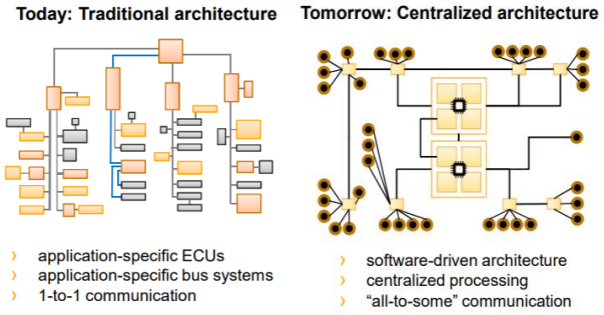

Fig. 1 Automotive E/E architecture Evolution

B. Adversarial AI

Autonomous driving is an important application areas of artificial intelligence (AI). AI enables a vehicle to percept the environment, position itself and make path planning. Datasets, methods and challenges for Object Detection for autonomous driving are summarized and analyzed in [7]. Autonomous vehicles are exposed to Adversarial scenarios especially at perception stage.

C. Vehicles connected to everything

Vehicle-to-everything (V2X) allows vehicles to communicate with other vehicles, road side units or others. V2X helps a vehicle to obtain information from around, get computing capacity from cloud, and etc. How to set up the trust among communication parties, how to protect the privacy, are still hot topics in both academic and industry.

D. *Complex software and OTA update*

Automotive software are becoming extremely complex. A modern high-end car may contain around 100 million lines of code, and the number is still increasing. Software update has been a pain point for OEMs for a very long time. To improve update efficiency and speed new business to market, Over-the-air (OTA) update mechanism is introduced to automotive industry for firmware and software update. But lots of attacks have been reported to exploit weakness in software update mechanism.

E. *Safety first consideration*

For automotive, safety is always the first principle for system design. ISO 26262 [8] is a risk-based safety standard. It provides guidance for developing and validating safety of automotive systems. In ISO 26262 ASIL (the Automotive Safety Integrity Level) is defined to quantify the severity of a hazard, probability of exposure and controllability of the situation. Although there are similarities between security and safety in aspect to hazard and risk definition, the analysis methods are very different. When designing and implementing security in automotive, safety should always be the first principle. It's a big difference from IT security design.

Safety will not be discussed further in this paper. We will focus on E/E architecture, V2X, and AI related topics.

III. Analysis of Standards and Industry Best Practices

To secure autonomous vehicles, lots of standards and industry communities are developed. In this chapter, we introduce and analyze three important standards as examples, from aspects of automotive engineering, V2X and automotive software respectively.

A. *ISO/SAE 21434 for automotive engineering lifecycle*

ISO/SAE 21434 standard [9, 10] addresses cybersecurity with respect to the engineering of electrical and electronic (E/E) systems in vehicles. It will cover all stages of vehicle lifecycle from design to decommissioning, and apply to all electronic systems, components, software and external connectivity. It's the most important dedicated security standard for automotive.

Fig. 2 shows an overview of the standard structure. Fig. 3 is an example workflow for security engineering together with product engineering.

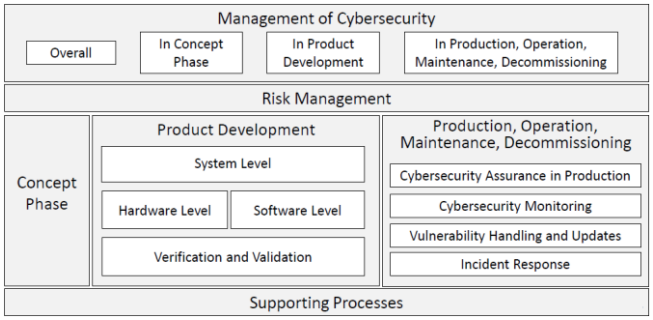

Fig. 2 ISO/SAE 21434 – Overview of Structure

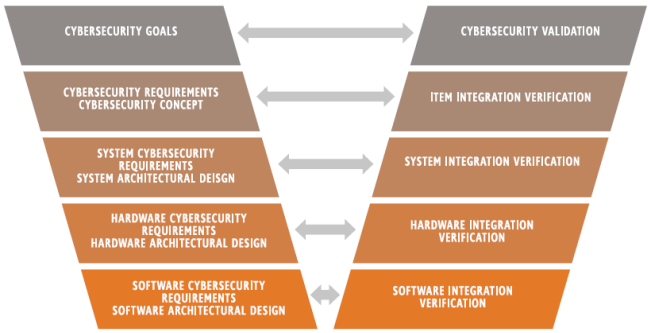

Fig. 3 Example workflow for cybersecurity in product development

B. *5GAA for Vehicles to Everything*

V2X enables the interaction among vehicles, infrastructure, pedestrians and etc. [11] To secure V2X, the fundamental problem is how to establish trust in this ecosystem, that means to develop, standardize and implement Security Credential Management Systems (SCMS).

5G Automotive Association (5GAA) is one of the most important organization to define the Security Credential Management Systems for automotive. 5GAA was established by key players in automotive and telecommunications industries and aims to develop future connected and automated vehicle solutions. 5GAA [12] has simplified the existing V2X credential management systems by EU [13] and US [14], and therefore to be more practical in real use scenarios.

5GAA also defines other security mechanisms, like Misbehavior Detection (MBD) for identifying misbehavior within the V2X network.

C. *Autosar for automotive software*

AUTOSAR (AUTomotive Open System ARchitecture) is a worldwide de facto automotive middleware standard. Its members cover vehicle manufacturers, suppliers, automotive electronics vendors, semiconductor companies and etc. [14] Autosar defines Classic Platform for traditional vehicle functions and Adaptive Platform for high-computing functions. As shown in figure 4, the Adaptive Platform provides several security functions, like IAM (Identity and Access Management), Crypto and secure on-board communications.

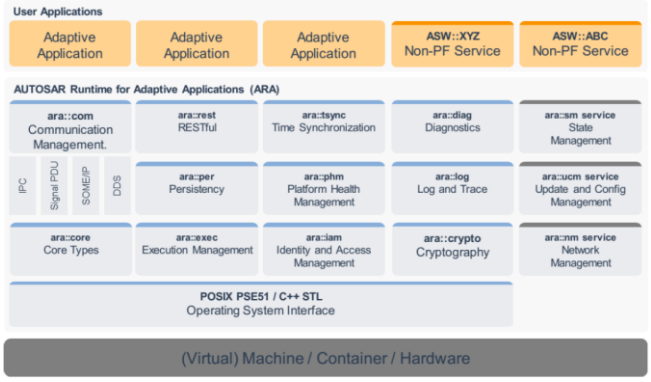

Fig. 4 Autosar Adaptive Platform architecture logical view

IV. Security Technologies

A. Secure new E/E architecture

As discussed above, automotive E/E architecture is evolving into software driven zonal architecture. It involves a re-design of network topology, hardware and software. Therefore a key problem is how to isolate the zones inside a vehicle and how to isolate the vehicle from external. Another important topic would be secure OTA (over-the-air) update mechanism, which is a key element for business success for OEMs.

B. Secure V2X communication

As discussed in chapter III, how to establish trust among communication parties is a fundamental problem. Another important topics for V2X would be IDS (Intrusion Detection System), which has been an important security element for network traffic.

C. Secure perception and positioning

Spoofing is one of the most critical threats to sensors. Multi-Sensor-Fusion is commonly recognized as an effective way to anti-spoofing [15]. This topic relies highly on AI progress.

V. Conclusion

Due to the automotive E/E architecture evolution, interaction of vehicle-to-everything and progress of AI, autonomous driving has developed rapidly, meanwhile security threats increases dramatically as well. In this paper we analyzed the technical challenges and standards for securing autonomous vehicles. Secure E/E architecture, secure V2X and secure perception are highlighted as important areas to address the above challenges.

References

[1] Automated Driving: Levels of Driving Automation, chart of "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles". Standard J3016, SAE International. Accessed: Jun. 2018. [Online]. https://www.sae.org/standards/content/j3016

[2] A. Chattopadhyay, K. Lam, Y. Tavva, Member, "Autonomous Vehicle: Security by Design", IEEE Trans. on Intelligent Transportation Systems, 2020

[3] E. Yurtserver, J. Lambert, A. Carballo, K. Takeda, "A Survey of Autonomous Driving: Common Practices and Emerging Technologies", IEEE Access, Vol. 8, 2020, pp. 58443-58469

[4] K. Ren, Q. Wang, C. Wang, Z. Qin, X. Lin, "The Security of Autonomous Driving: Threats, Defenses, and Future Directions", Proceedings of the IEEE (Volume: 108, Issue: 2, Feb. 2020), pp. 357 – 372

[5] V. Thing, J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences", 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 15-18 Dec. 2016

[6] H. Zinner, J. Brand, D. Hopf, "Automotive E/E Architecture evolution and the impact on the network", IEEE802 Plenary, March 2019, 802.1 TSN, https://ieee802.org/1/files/public/docs2019/dg-zinner-automotive-architecture-evolution-0319-v02.pdf

[7] D. Feng, C. Haase-Schuetz, L. Rosenbaum, H. Hertlein, C. Glaeser, F. Timm, W. Wiesbeck, K. Dietmayer, "Deep Multi-modal Object Detection and Semantic Segmentation for Autonomous Driving: Datasets, Methods, and Challenges", IEEE Transactions on Intelligent Transportation Systems, Feb. 2020

[8] ISO 26262-1:2011 Road vehicles — Functional safety

[9] ISO/SAE DIS 21434: Road vehicles — Cybersecurity engineering. ISO/SAE International, 2020.

[10] H. I. Akram, "Bridge the Cybersecurity Gap in Automotive - The upcoming ISO/SAE 21434 and its implicaitons for automotive cybersecurity engineering", white paper from Matrickz Magnificence in Technology, https://www.matrickzacademy.com/whitepaper-download-main1597125775036

[11] V. Sharma; I. You; N. Guizani, "Security of 5G-V2X: Technologies, Standardization, and Research Directions", IEEE Network (Vol. 34, Issue: 5, September/October 2020)

[12] 5GAA Automotive Association white paper, 5GAA Efficient Security Provisioning System, Feb. 2020

[13] European Commission, Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), vol. Release 1.1, 2018.

[14] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn and R. Goudy, "A Security Credential Management System for V2X Communications", IEEE Transactions on Intelligent Transport Systems, vol. 19, no. 12, pp. 3850-3871, Dec. 2018.

[15] Z. Wang, Y. Wu, Q. Niu, "Multi-sensor Fusion in Automated Driving: A Survey", IEEE Access, Vol. 8, 2020, pp. 2847-2868