Automotive security

www.hcltech.com

Whitepaper

TABLE OF CONTENTS

Abbreviations

CAN	Control Area Network
NFC	Near-field Communication
LIN	Local Interconnect Network
ECU	Electrical Control Unit
MOST	Media Oriented System Transport
GPS	Global Positioning System
UNECE	United Nations Economic Commission for Europe
WP.29	Working Party 29 (World Forum for Harmonization of Vehicle Regulations)
ISO	International Organization for Standardization
SAE	Society of Automotive Engineers
CI/CD	Continuous Integration (CI) and Continuous Delivery (CD)

Overview

The traditional cars were designed with the assumption of an isolated in-vehicle network. The security of those cars was often related to physical aspects. This changed when connected vehicles were introduced. They come with convenient and safety-related features to assist drivers in controlling the vehicles. However, their connectivity attracts many malicious actors, which results in an increasing number of attacks on connected cars. Automotive security has therefore evolved from preventing physical threats to tackling cybersecurity attacks. Besides, advanced software on cars --- similar to mobile applications --- can introduce security vulnerabilities as well as privacy concerns to car users, which weren't the case in traditional cars. This paper looks at the attack motivation, security, and privacy of connected vehicles. Ongoing solutions to improve the security and privacy of the automotive domain are also discussed.

Business Challenges

Modern cars are now equipped with multiple sensors and plenty of useful, advanced features that are enabled by software. This provides drivers with convenience and safety support. Such advancements come with a cost – namely, the security and privacy of car users. Security and privacy of modern cars now mean more than physical theft and tinted windows. While traditional cars already have (in-) vehicle communication networks, they were built with the assumption of being isolated, without a remote connection. Modern cars now have different remote features such as keyless entry, remote ignition, over-the-air updates, and many more. This opens different attack surfaces to in-vehicle communication channels (via NFC, Bluetooth, and cellular, etc.). Modern cars tend to be vulnerable to different attacks [1, 2]. Attackers could arbitrarily manipulate a car's speed [3] and unlock cars [1]. Attackers could also access the vehicle's control area network (CAN) and manipulate the in-vehicle communication [2].

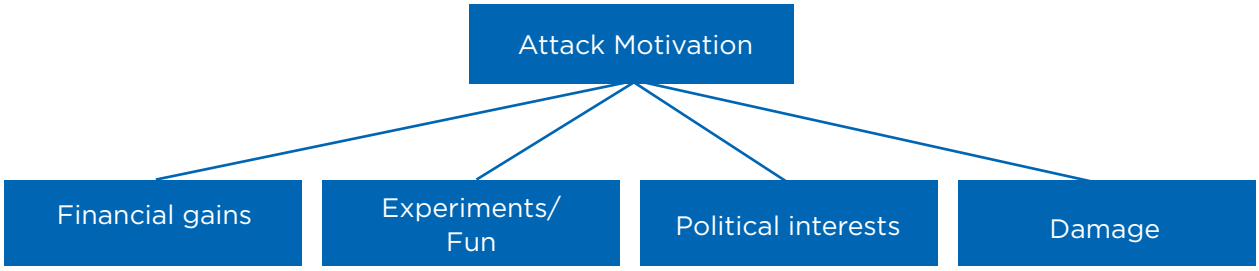
The backbone of the advancement in modern cars is the electrical control unit (ECU). ECUs communicate with each other using a different network protocol such as control area network (CAN), FlexRay, local interconnect network (LIN), media-oriented system transport (MOST), and more recently, the Ethernet. ECUs can be divided into the following subsets:

- **Powertrain:** Related to engine and transmission control
- **Safety:** Related to stability control and airbag deployment, etc.
- **Comfort:** Related to controlling, heating, and cooling
- **Infotainment:** Similar to that of a smartphone. It provides audio, video, maps, etc., to serve the needs of users
- **Telematics:** Related to providing vehicle information, and remote diagnostic, etc.

Attackers often aim to exploit security vulnerabilities in the ECUs, the protocols that they use (e.g., CAN), and in backend services that they talk to. Unlike conventional software, the security of ECUs (in modern cars) is directly linked to the safety of car users. Therefore, security is an extremely integral part of cars nowadays.

Attack Motivation

Given the car's value, the most common motivation for attacks is theft. While car theft has been happening since the beginning of its history, the recent advancement of new features in modern cars introduces different 'theft' surfaces such as keyless entry, remote start, etc. Further, as modern cars are equipped with many useful yet sensitive sensors, attackers also aim to obtain information that is recorded by such sensors (e.g., GPS). Sensitive information is not only provided by sensors but also by advanced software installed in modern cars. Like mobile apps, apps on cars can store user-sensitive information such as driver's information, payment information, car usage details, etc. Malicious actors can target such information for financial gains or as leveraging steps to exploit more attacks on users (cars). Attackers can also try to exploit vulnerabilities in automotive products for experiments or simply for fun. Finally, attacks on modern cars could be motivated by political reasons between different parties or different countries for their (political) interests. This aspect is similar to any other type of cyber attack. However, cars are moving targets, and most importantly, they transport humans. The safety and security of a car are therefore always linked to the safety and security of its passengers. The attacker's goal could also be to damage the car and threaten the safety of its passengers.



Potential Security Vulnerabilities

The attack surface on connected cars has become broader given their connectivity such as vehicle to infrastructure, vehicle to vehicle, vehicle to cloud, vehicle to pedestrian, and vehicle to everything. This makes car security systems and their components vulnerable to different attacks. Attacks can threaten various aspects of connected cars.

1. In-vehicle communication channels

Attackers could spoof messages, interfere with sensor signals, and manipulate keyless entry functions to physically steal cars, or spoof GPS values to misdirect car drivers. This all happens as the in-vehicle communication channel was designed to function as isolated in-vehicle networks (e.g., CAN bus protocol), where the remote connection was not considered, and the security was not built-in. However, the remote connection has now become an essential part of modern vehicles. To prevent the mentioned attacks, in-vehicle communication needs to protect the integrity, authenticity, and confidentiality, as well as the availability of messages in transit.

2. The update process

Over-the-air updates bring car experience to the next level. Particularly, car users will not have to visit car dealers for certain maintenance activities (such as software OS-related updates). This would significantly save time and reduce costs. New (versions of) features can also be added or updated to cars by means of remote updates. Bug fixes can be deployed in a similar manner to conventional software. While over-the-air update is an exciting part, it also faces certain threats. Specifically, the update can also be modified and fabricated by malicious attackers controlling the network connections. As a result, the related parties must take action to prevent potential attacks on the update process of modern cars.

3. Third-party software components

Third-party software components are not new to any software ecosystem. On the one hand, it improves the potential of modern cars by providing useful, advanced, and convenient features (infotainment, driver assistance, etc.) offered by third-party companies. On the other, it introduces new attack surfaces to modern cars. Car manufacturers need to carefully vet third-party software components either by automatic, manual, or hybrid means to prevent both intentionally malicious third-party software and benign software with security and privacy vulnerabilities.

4. Backend servers

When attackers gain access to a backend server, (s)he could deploy malicious over-the-air updates to the vehicle (or vehicle's fleet). Eventually, (s)he could control the vehicle (or even the entire fleet of vehicles). Besides, collected information that is stored on backend servers can also be stolen by malicious attackers if vulnerabilities are found. APIs for communication with vehicles must be protected using a robust protocol that only supports strong cryptographic algorithms and has access control. Audits must be regularly performed on backend servers to ensure they comply with security and privacy guidelines, regulations, and standards.

Current Solutions

1. Hardware security modules

Hardware security modules provide cryptographic functionality. They often have their own processor, memory, and hardware accelerator. Different software components in modern vehicles could use such hardware security modules to protect the integrity, confidentiality, authenticity of the information in exchanges, e.g., through encryption, hashing, etc. While hardware security modules offer huge potential to modern cars' security and privacy, they also have their own challenges. Unlike traditional desktop environments with huge computational power, the hardware security modules in the automotive domain must deliver output with minimum latency while operating in a resource-constrained environment.

2. Securing in-vehicle communication channels

The man in the middle attacks (eavesdropping, masquerading, and replay) could be avoided to a certain level by providing encryption and authentication for messages in exchanges. Researchers have proposed different solutions to secure the vehicle communication channels [4, 5, 6]. Further, intrusion detection and prevention methods are applied to the automotive domain to identify abnormal events concerning in-vehicle communication effectively. This is divided into two directions:

- Signature-based: Anomalous behaviors are defined beforehand, and anomaly detectors look for messages that exhibit similar (or identical) characteristics and flag them as abnormal.
- Anomaly-based: Normal behaviors are defined, and anomaly detectors would look for behaviors that deviate from the normal ones. This approach can detect unknown attacks on connected vehicles.

3. Secure by design

Related parties must consider integrating car security devices into the development lifecycle of automotive software. This is an effective approach to minimize the cost caused by security incidents that can potentially be identified and avoided during the development phase. The secure development lifecycle considers security-related aspects in all development phases. Generally, the secure development lifecycle includes security analysis, security best practices, and testing into existing software development processes (e.g., waterfall, agile, CI/CD).

4. Regulations and standards for automotive security

To holistically tackle the issues of automotive security & privacy, relevant organizations and governments aim to make security an essential part of the automotive development life cycle. Standards and regulations for automotive security, therefore, have been introduced. Compliant cybersecurity management has, therefore, become an important goal for automotive companies.

The UN ECE WP.29 [7] and the ISO/SAE 21434 [8] require securing vehicles throughout their lifecycle. They additionally require a well-defined automotive cybersecurity management system inside the organization and thorough threat analysis and risks assessment (TARA). As their names suggest, the UN ECE WP.29 will be legally binding, while the ISO/SAE 21434 standard is becoming the norm in the industry but is not legally binding.

With UN ECE WP.29 being legally binding, starting from July 2022 onwards, newly-produced vehicle lines must obtain type approval as a sub-component of the process of vehicle type approval. Additionally, approval for system type for automotive cybersecurity will become mandatory for all vehicle 'first registrations' after July 2024. All manufacturers and suppliers are racing toward compliance with such a regulation. Rapid implementation of automotive security solutions complying with security and privacy guidelines is therefore becoming a key competitive factor.

Conclusion

Modern cars have become increasingly connected. They are also attracting a growing number of malicious actors that exploit security and privacy vulnerabilities in connected vehicles for financial, business, and political gains. This is an exciting time to see how organizations shape themselves toward securing connected vehicles and protecting car users. It is not only about building automotive products that are compliant with security and privacy regulations but also providing end-to-end cybersecurity in automotive solutions that span across the product's entire lifecycle.

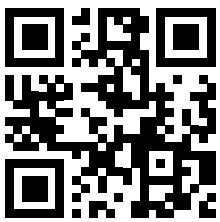
References

1. Andy Greenberg, "A New Wireless Hack Can Unlock 100 Million Volkswagens", 2016
2. Keen Security Lab., "Experimental Security Assessment of BMW Cars: A Summary Report", 2018, https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf, accessed December 2021
3. Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. IEEE Vehicular Technology Magazine, 12(2), 45-51.
4. W. Choi, K. Joo, H. J. Jo, M. C. Park and D. H. Lee, "VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2114-2129, Aug. 2018, doi: 10.1109/TIFS.2018.2812149.
5. Q. Zhang, M. Almulla and A. Boukerche, "An Improved Scheme for Key Management of RFID in Vehicular Adhoc Networks," in IEEE Latin America Transactions, vol. 11, no. 6, pp. 1286-1294, Dec. 2013, doi: 10.1109/TLA.2013.6710374.
6. N. Nowdehi, A. Lautenbach, T. Olovsson, In-vehicle CAN message authentication: an evaluation based on industrial criteria, in: IEEE 86th Vehicular Technology Conference, 2017.
7. UNECE, WP.29, https://unece.org/wp29-introduction, accessed December 2021
8. ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering, ISO/SAE, https://www.iso.org/standard/70918.html, accessed December 2021

Author Info

Cuong Nguyen

Cuong Nguyen works as an Associate General Manager in the area of cybersecurity. He obtained his Ph.D. degree from CISPA Helmholtz Center for Information Security & Saarland University. His research revolves around mobile security, embedded system security, and automotive security.



www.hcltech.com

HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on June 30, 2021, HCL has a consolidated revenue of US$ 10.5 billion and its 176,000 ideapreneurs operate out of 50 countries.

For more details contact: ers.info@hcl.com
Follow us on twitter: http://twitter.com/hclers and our blog http://ers.hclblogs.com/
Visit our website: http://www.hcltech.com/engineering-services/

WI-10322432177O153-EN00GL