Automotive Connectivity, Cyber Attack Scenarios and Automotive Cyber Security

Roland E. Haas[1] and Dietmar P. F. Möller[2]
[1]QSO Technologies, 16 Bachammal Road, Cox Town, Bangalore-560005, India,
[2]Clausthal University of Technology (TUC), Institute of Applied Stochastic and Operations Research,
Erzstr. 1, D-38678 Clausthal-Zellerfeld, Germany,
E-mail: reh@qso-technologies.com, dietmar.moeller@tu-clausthal.de

I. Abstract

The Automotive industry is changing rapidly, as classical automotive engineering and information and communication technologies (ICT) converge. Digitization, new mobility concepts, e-mobility, and autonomous driving require a permanent connection with the Internet and transform the car into a very complex cyber-physical system. However, with this connectivity the car becomes vulnerable to cyber attacks. It is very important to understand the threat scenarios underlying the mega trends that are changing the industry. The paper gives a brief overview of the main drivers of this change and discusses some of the major cyber security threats arising in the world of connected cars focussing on three important areas where cyber attacks can happen - e-mobility, car sharing and automated valet parking. Fortunately, there are various cyber security measures that can help to protect the connected car. We briefly discuss some of the main approaches.

II. Introduction

The Automotive industry is currently undergoing an enormous change process. For many years innovations came in steadily, continuously and - most importantly - with a certain degree of predictability. The innovations were mainly focussing on the following areas:

- Optimization of the internal combustion engine (ICE)
- Optimization of transmission and gearbox
- Active and passive safety (e.g., crashworthiness)
- Infotainment solutions and telematics
- Automotive electronics and Automotive software technologies
- Digitization of the product development and manufacturing processes

The innovations in Automotive electronics were possible by the introduction of sophisticated bus systems, software architectures (e.g., AUTOSAR = Automotive Open Software Architecture), a rapidly increasing computing power (e.g., multi-core architectures) in the ECUs (Embedded Control Units) and were mainly driven by new use cases in active safety and infotainment. Major innovations also focussed on digital product engineering and digital manufacturing. The introduction of sophisticated CAD and PLM systems (Product Lifecycle Management) allowed for efficient collaboration among distributed engineering teams. The methodologies of digital manufacturing enabled the engineers to simulate and optimize complex manufacturing processes, even complete factories, before they were actually built. This saved money and avoided costly changes in later phases of the product creation process.

III. Challenges for the Automotive Industry

Today several mega trends have appeared nearly simultaneously. Each one has the potential to disrupt the industry and challenges established value chains, cooperation models and supply systems:

- Digitization
- Connectivity (Connected Cars)
- Electromobility
- Car sharing and new mobility concepts
- Autonomous driving

1) Digitization: While the Automotive industry has been very innovative regarding the deployment of digital methods and computer simulation in engineering and manufacturing, it has been slow in embracing the smartphone revolution and the digital customer connect. This area is dominated by large IT specialists like Google and Apple who have created an ecosystem of services around the smartphone. The automotive industry is catching up and experiments with digital channels to communicate directly with their customers. This effects all aspects of the value chain - from early interaction with customers in product strategy to sales and after sales. The latter allowing problems to be detected early on which means that customers can be directed to the right garage to fix the problems before something happens. Automotive OEMs are now investing heavily in these new fields and are creating new positions like the one of a chief digital officer (CDO) in VW or BMW.

2) Electrification of Powertrain: Electrification of the powertrain is an area which is particularly challenging as the automotive OEMs typically control and own a large part of the ICE value chain. An electrical vehicle has about 30 per cent lesser parts than its ICE counterpart and the supply chain is fundamentally different. A large part of the cost is defined by the battery pack which is often

978-1-5090-4767-3/17/$31.00 ©2017 IEEE

supplied by new players. The electric motor does not need a sophisticated transmission system like its ICE counterpart. Power electronics, packaging, cooling of E/E devices and an intelligent management of power distribution are important competitive differentiators.

3) Autonomous Driving: Autonomous driving is another topic which is emerging as a game changer. Advanced driver assistance systems have been around for a couple of years, providing assistance functions like blind spot detection, night vision, adaptive cruise control, lane change assistance and driver's drowsiness detection, just to name a few. These systems are evolving into more and more sophisticated assistance functions that are capable to steer the car independently for a couple of seconds. High-definition maps are necessary that not only show a 2-dimensional map of the environment but also provide information about the third dimension, e.g., the road side borders, walls and obstacles. All major OEMs are working on autonomous driving as a strategic field. The challenge is to tweak the algorithms in such a way that safety and reliability is guaranteed under all circumstances. Also the hand over between machine and human is a very critical procedure. Full autonomous driving is still sometime away but it will come and we see the first applications in autonomous trucks, logistics and ride sharing.

Automated Valet Parking (AVP) is an area which is quickly becoming popular. The idea is that the car finds its parking space and maneuvers autonomously without the driver having to sit in the driver's seat to supervise. This is particularly attractive for car sharing where dropping off the car can be time consuming (finding a space for parking and aligning the car with the parking slot). Daimler and Bosch will introduce such an autonomous parking functionality for Car2Go in 2018 [18]. As the maximum speed in such a scenario is rather low the safety and legal constraints can be handled much easier than in full autonomous driving.

4) Car sharing and new mobility: The Internet has seen a wave of sharing business models and these have carried over to the automotive industry. A well known example is *Airbnb*. Car ownership is now being challenged by the access to mobility - being able to use whatever means to go from A to B in the most convenient and fastest way. Lots of different concepts have emerged. OEMs are offering car sharing services like Car2Go or Drive Now. They allow users to pick a car somewhere in the city, drive it from one location to another and drop it off at any public parking lot, which is especially useful for one-way trips.

5) Connectivity: The early beginnings can be traced back to telematics approaches for e-call and other means. However, more sophisticated applications were lacking the necessary bandwidth. Today the GSM connection bandwidth is there to support even the most complex use cases. The car is connected to back-end systems and other cars and can exchange large volumes of data. This has enabled completely new use cases in emergency, location-based services, parking, predictive maintenance, usage based insurance (UBI) and many more [11].

All of these new application areas and services have one thing in common: They rely on connectivity to optimize the eco-system and to manage the complex interactions between car and environment.

However, connected devices are vulnerable to cyber attacks and this is especially true for the connected car [20], [25], [26]. With the threat of new players emerging who could eat into the market share of the established players, time to market is very important. And all this happens while OEMs and first tiers have to build up the knowledge how to deal with software-intensive highly connected cars. A modern car is, indeed, one of the most complex cyber-physical systems available today.

IV. Cyber security and the connected car

The lack of experience with software-intensive, highly connected cars and the high pressure on time-to-market are ideal platforms for hackers to exploit vulnerabilities. That is why cyber attacks are taken very seriously and a string of public hacks and vulnerabilities have alerted OEMs and customers alike [15], [13], [14], [10], [21].

Classical IT security is based on the following objectives [9]:

- Authentication
- Confidentiality
- Integrity
- Availability/Reliability
- Non Repudiation

These objectives also apply to the connected car. Connected cars expose different cyber attack surfaces that can be exploited to breach security by gaining unauthorized access to critical systems (e.g., remotely unlocking the car by masquerading the key), eavesdropping on the communication between the car and other communication partners (smartphone, back-end servers, cars, infrastructure, etc.), altering information, denial of service attacks or breach of transactions (e.g., billing) [19].

We will briefly discuss some measures to improve the cyber security in connected cars in section VIII. Naturally, this can necessarily be only a brief overview as our focus is attack scenarios and vulnerabilities.

V. Cyber Attacks on E-cars

Electromobility opens up new attack vectors as many use cases are enabled by connectivity. For example, it is key to know the exact charging level of the battery for planning the next trip. As of today the charging infrastructure is no where comparable to the availability of gas stations, a trip has to be planned carefully and information about the next charging point is very important. Some OEMs (e.g., Tesla) have come up with new business models that include a lifetime charging for their vehicles (see [17] for a discussion on this topic). Tesla is also very active in quickly closing cyber security issues [22], [16]. Electric cars have to balance the power even more carefully than combustion engine cars. This means that the electric loads have to be watched and minimized. Integrating

all sorts of information sources, e.g., the weather, traffic conditions, drive terrain (flat, hills, etc.) can help to reduce the power consumption. If, for example, in summer it is known that the driver enters an area with lots of clouds, the AC can be configured to shut-off or reduce cooling output just a little earlier, thereby helping to save valuable battery charge. If one goes shopping it is important to know which retailer offers charging points (preferably with fast charging capabilities). This information should be displayed on the map and provides valuable input for the navigation system. When using a charging point the question is how to bill for the electricity? This is typically done cashless through a billing gateway. The car uses a M2M protocol to

- authenticate itself to the charging point,
- monitor the charging,
- report any issues and finally
- end the charging process.

The key here is a seamless integration of all players involved - car, infrastructure provider (including park space operator), municipality, energy company and billing service provider.

The identity has to be checked for billing purposes and in order to configure the charging process. An attacker could try to masquerade as a proper user and disrupt the authentication process in various ways. If there is no strong authentication, the key or password could be hijacked and used for a re-play attack.

Electric cars rely on connectivity to communicate all sorts of parameters, like level of charge, battery health status, etc. and sport all features of a modern connected car like smartphone remote control, location aware services, connected parking and so forth.

If the connectivity is disrupted by a denial-of-service attack or the car is hacked to gain access to critical internal systems this could have severe consequences.

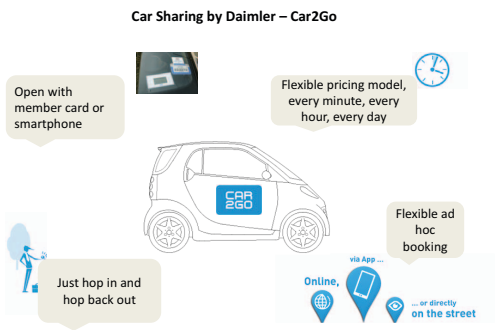

Figure 1. Car2Go concept

VI. Cyber Attacks on shared cars

Car sharing relies on a direct link between the car and backend servers. This is established by a GSM connection. The car will continuously report its position and some key operational data to the backend server. When the car is dropped off, its final position is locked. The user reports the condition and the log-off procedure is being initiated which carefully checks if the car is still in the limit of the area where it should be operated. If everything goes well the cars will be ready for the next user to pick it up (see fig 1 and 2).

There are multiple attack scenarios on car sharing providers such as:

- Spoofing of GPS signals to redirect the car
- Attack on the GSM communication between head unit (HU) to back-end server
- Hacking user accounts to get access to personal data
- Attack on the smart card for filling the tank
- Denial-of-Service (DoS) attacks on the head unit

In the early days of Car2Go the user could only open the car with a special card that contained an RFID tag. The RFID tag authenticates itself to a reader device mounted behind the windscreen. This woke up and activated the head unit, sent the RFID information to the backend server (via the GSM connection of the telematic control unit (TCU)) and, if everything was ok, opened the door of the car. A second level of identity proof required the user to key in a 4-digit-PIN number (two factor authentication). RFID tags typically use a simple challenge-response authentication based on a *nonce* sent from one partner to the other. This potentially could be used to masquerade as a proper user and get unauthorized access. This is why the second line of defense, using a PIN number, is still important to prevent unauthorized access. Today the car can also be opened with a smartphone. This requires a communication between smartphone to back-end as well as back-end to car. Multiple attack scenarios are possible [19], [26].

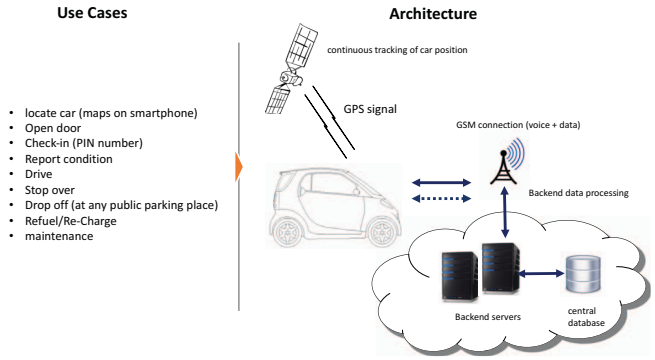

Figure 2. Car2Go architecture

Also new features like over the air update (OTA) of software open up further possibilities for severe attacks. With the introduction of new valet parking functionality for car sharing the potential attack surfaces have become even larger. We will discuss valet parking attacks in the next section.

VII. Cyber threats to Automated Valet Parking

Automated Valet Parking (AVP) introduces several new cyber attack threats mainly due to the need of vehicle-to-infrastructure (V2I) communication and the necessary modifications to the park house infrastructure. Daimler and Bosch will launch an automated valet parking feature for Car2Go in 2018 [18].

AVP functions are vulnerable to various cyber attacks:

- Cyber attackers could try to steal the car or gain unauthorized access to critical systems of the vehicle
- Attacks could also directly effect the sensors (blinding and confusing camera sensors, relaying or spoofing signals, etc.)

Furthermore, autonomous features potentially increase the consequences of an attack as the human driver can not oversee all situations and - if necessary - interfere in time. Park house management systems often use a Window PC as the central control hub. If the operating system is not patched properly - or worse - support has expired (e.g., in the case of Windows XP) this can be a serious threat. Malware could spread through the USB port or the network and could compromise the attached subsystems, including actuators and sensors. In such a scenario vehicles could receive false signals and could end up in the wrong place. Also, the in-house position guidance system could be disturbed and rendered useless for path planning.

VIII. Cyber security and mitigation of cyber attacks

Modern vehicles are fully connected and are prone to cyber attacks as they expose a complex attack surface [12], [3]. Encryption should be used to keep all communication between the car and the outside world confidential. There are various ways to do this, e.g., one can use Transport Layer Security (TLS) for Vehicle-to-Internet communication.

Intrusion detection systems (IDS) can help to detect attacks by filtering the data streams of the connected car [1], [2], [4], [6], [5]. They are capable of classifying data streams (inside and outside the car) into normal or abnormal (i.e. potentially malicious). IDS systems are based on nonlinear pattern recognition algorithms. A popular and well known way to implement them is to use an artificial neural network.

Strong authentication is necessary to avoid unauthorized access, infringement of data privacy and masquerading of devices.

There are different choices to enforce a strong authentication between the car, backend servers and Internet of Things (IoT) devices like:

- Public-Private Key Infrastructures (PKI)
- Trusted Platform Modules (TPM)
- OpenAuth 2.0 authentication
- Pre-shared keys with a challenge-response protocol and symmetric encryption, etc.

Threat intelligence is a very important area too. Cyber security companies constantly track known attacks and disseminate this knowledge to OEMs and first tiers. Attacks, vulnerabilities and exploits can be visualized by means of a dashboard [23] like the one used by classical IT security tools.

The topic of Automotive Cybersecurity is currently in the focus of both the popular press as well as the automotive industry and the scientific community. A good overview of the current trends, challenges and research areas is given in [12], [24], [25], [26], [8], [19].

IX. Summary and Conclusions

The Automotive industry is changing rapidly - electromobility, digitization, autonomous driving, and new mobility services are challenging established business models and value chains. All of these concepts rely on connectivity with high bandwidth connections between the car, IT back-end systems and IoT infrastructures. The time-to-market pressure is a challenge. Customers want to connect their latest gadgets to the car (smartphone, smart watch, etc.). The high demand for connectivity exposes various attack surfaces which can be exploited by black hackers and cyber criminals. In this paper we have looked at three use cases of connectivity and their cyber security consequences - e-mobility, car sharing and a special case of autonomous driving - automated valet parking. We discussed the cyber attack surfaces and some possible attack scenarios. Fortunately, the car is not defenseless. Cybersecurity processes, methods and tools, many of them well known in the information and communication technology (ICT) sector, can also be deployed in the field of connected cars. We briefly discussed authentication, intrusion detection and threat intelligence as ways to counteract cyber attacks. However, like in the ICT world, cyber security is a moving target where hackers will constantly explore new ways to exploit vulnerabilities and car manufacturers must be careful and prepared to fight them off.

References

[1] Fallstrand, D. and Lindstrom, V. (2015) Automotive IDPS: Applicability analysis of intrusion detection and prevention in automotive systems. [Online]. Available: http://publications.lib.chalmers.se/records/fulltext/219075/219075.pdf

[2] Vestlund, C. (2009) Intrusion Detection Systems in Networked Embedded Systems. [Online]. Available: https://www.ida.liu.se/ TDDD17/oldprojects/2009/projects/026.pdf

[3] La Vinh, H. and Cavalli, A. R. "Security attacks and solutions in vehicular ad hoc networks: a survey", *International Journal on AdHoc Networking Systems (IJANS)*, vol 4, no. 16, pp. 1-20, 2014.

[4] Alheeti, K. M. A., Gruebler, A., and McDonald-Maier, K. D. "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars", in *Sixth International Conference on Emerging Security Technologies (EST)*, Braunschweig, pp. 86-91, 2015.

[5] Simon Haykin, *Neural Networks and Learning Machines*, 3rd ed. New Jersey, USA: Pearson Education, 2008.

[6] Shieh, Shiuhpyng W. and Gligor, Virgil D. "A pattern-oriented intrusion-detection model and its applications. Research in Security and Privacy", in *IEEE Computer Society Symposium*. pp. 327–342, 1991.

[7] Scarfone, Karen and Mell, Peter. (2007, February) Guide to Intrusion Detection and Prevention Systems (IDPS). [Online]. Available: https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps
[8] Poulsen, Kevin. (2010, March) Hacker disables more than 100 cars remotely. [Online]. Available: www.wired.com/threatlevel/2010/03/hacker-bricks-cars
[9] Intel Security. (2015) Intel Security White Paper Automotive Security Best Practice. [Online]. Available: https://www.mcafee.com/de/resources/white-papers/wp-automotive-security.pdf
[10] Greenberg, A. (2013, July) Hackers Reveal Nasty New Car Attacks-With me Behind the Wheel. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/766c84cb228c
[11] Vembo, D. (2016, June) Connected Cars, Architecture, Challenges and Way Forward. [Online]. Available: http://www.sasken.com/sites/default/files/Sasken_Whitepaper_Connected_Car_Challenges_0.pdf
[12] Mahaffey, Kevin. (2015, August) The New Assembly Line: 3 Best Practices For Building (secure) Connected Cars. [Online]. Available: https://blog.lookout.com/tesla-research
[13] McMillan, Robert. (2011, March) With Hacking, Music Can Take Control of Your Car. [Online]. Available: http://www.computerworld.com/article/2506755/security0/with-hacking–music-can-take-control-of-your-car.html
[14] Miller, Charlie, and Chris Valasek. (2015, August) Remote exploitation of an unaltered passenger vehicle. [Online]. Available: http://illmatics.com/Remote
[15] IET. (2015) Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles. [Online]. Available: http://www.theiet.org/sectors/transport/documents/automotive-cs.cfm
[16] Brisbourne, Alex. (2014, February). Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? [Online]. Available: http://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/
[17] Stewart, Jack. (2016, November) As Tesla grows up, it gives up on free charging. [Online]. Available: https://www.wired.com/2016/11/tesla-grows-gives-free-charging/
[18] Telematics News. (2015, September) Daimler, Bosch and Car2Go develop automatic parking. [Online]. Available: http://telematicsnews.info/2015/09/15/daimler-bosch-and-car2go-develop-automatic-parking/
[19] Symantec IoT Team. (2015) Building Comprehensive Security Into Cars. Technical Report. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/building-security-into-cars-iot_en-us.pdf
[20] Miller Charlie and Valasek Chris. (2014). A Survey of Remote Automotive Attack Surfaces. [Online]. Available: https://www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf
[21] Markey, E. J. (2015, July) SPY Car Act of 2015, 114th Congress (2015-2016). [Online]. Available: https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info
[22] Kim Zetter. (2015, August) Researchers Hacked A Model S, But Tesla's Already Released A Patch. [Online]. Available: https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/
[23] Argus Cybersecurity. (2017, May) Protecting Cars, Trucks and Commercial Vehicles from Hacking - an Overview. [Online]. Available: https://argus-sec.com/car-hacking/Argus-sec.com
[24] Kevin Mahaffey. (2015, September) Here Is How To Address Car Hacking Threats. [Online]. Available: https://techcrunch.com/2015/09/12/to-protect-cars-from-cyber-attacks-a-call-for-action/ TechCrunch
[25] Olivia Solon. (2015) From Car-Jacking to Car-Hacking: How Vehicles Became Targets For Cybercriminals. [Online]. Available: https://www.bloomberg.com/news/articles/2015-08-04/hackers-force-carmakers-to-boost-security-for-driverless-era
[26] Roderick. Currie. (2015) Developments in Car Hacking. [Online]. Available: https://www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607