Security Hardening with Plausibility Checks for Automotive ECUs

Jürgen Dürrwang, Marcel Rumez, Johannes Braun and Reiner Kriesten

Institute of Energy Efficient Mobility
University of Applied Sciences Karlsruhe
Germany, International University Campus 3, 76646 Bruchsal
Email: {duju0001, ruma0003, brjo1015, krre0001}@hs-karlsruhe.de

***Abstract*—The automotive industry relies increasingly on computer technology in their cars, which malicious attackers can exploit. Latest published attacks have further shown an increased attack surface by adding wireless interfaces to vehicle on-board systems. Most of these attacks are based on spoofing or sending tampered bus messages, which we were able to reproduce over the last years as well. We found additional vulnerabilities with the same attack vector in cars of international Original Equipment Manufacturers (OEMs). The discovered vulnerabilities can be dangerous to life while the driver doesn't have any possibilities to prevent them. Based on this knowledge we developed an approach to prevent such attacks on Electronic Control Unit (ECU)-level. In this publication, we introduce a new type of countermeasure to reduce the attack surface of vehicles with less or no overhead. Therefore, we concentrate on plausibility checks in a new way, by employing hard-wired signals to determine the operational state of the car. As a result, we are hardening the security against attacks on legitimate functions.**

Keywords–Automotive Safety and Security; Vehicular Attacks; Plausibility Checks.

I. INTRODUCTION

Modern automobiles consist of more than 50 ECUs, which contain and implement a total of up to 100 million code lines to control safety-critical functionality. This fact, combined with the close interconnectivity of automotive ECUs, opens up new possibilities to attack these systems which impair the safe operation of the vehicle. The feasibility of such attacks has been investigated and already demonstrated by several groups of researchers [1] [2]. Additionally, attacks via access to the internal vehicle network, that can cause life-threatening injuries have also been demonstrated in the past [3] [4].

Furthermore, car manufacturers tend to equip their cars with more entertainment and comfort features using wireless connectivity. One example is the detection of traffic obstructions by using Car-2-X communication to process traffic or general environmental information provided by an ad-hoc network. In the same way, providers of car-sharing, car-rental and other fleet based services use cellular networks for the communication with their backbone. Additionally, manufacturers implement the ability to execute software updates outside of car workshops, in order to fix problems within a short time [5]. These interfaces potentially provide means to remotely exploit vulnerabilities, obtain access to the in-vehicle network and control critical systems from a distance [6] [7].

Especially, with the remote exploitation of the Jeep Cherokee [6], Miller and Valasek showed that physical access through an On-Board Diagnostics (OBD)-Connector is not mandatory any more. One year after the remote exploitation of the Jeep they provided an update on what is possible in car hacking. This time the experts didn't use a remote connection for their attacks, but a direct connection to the internal car network via the OBD-connector. The fundamental approach was to stop an ECU which is connected to the Controller Area Network (CAN) in order to send spoofed messages to another in-vehicular subscriber. As a result, they were able to execute different functions, e.g., deceleration of the vehicle or activating the parking assistant in an inappropriate driving condition. To prevent such misuses, ECUs typically use plausibility checks to validate the requested function with the state of vehicle. For this purpose ECUs use bus messages to derive the current state of the vehicle. Unfortunately, these messages are typically not protected from malicious modifications.

Additionally, our actual research has discovered a weakness in a safety critical component due to the fact, that this component provides diagnostic functions for a special use case. Unfortunately, these functions are available during the regular operation of the vehicle, potentially leading to life-threatening injuries. The discovered weakness is based on a requirement, suggesting a weak algorithm to ensure authentication. Moreover, this requirement is proposed by a standard. Thus, we consider it as reasonable, that this weakness scales over several manufacturers.

To prevent such issues, authenticity and integrity of bus messages has to be ensured and therefore cryptographic methods can be applied. A typical approach for this is the application of a Keyed-Hash Message Authentication Code (HMAC) on salted messages. This type of cryptographic measure ensures the desired protection goals, with an acceptable need of computational performance, which is a fundamental constraint in the automotive domain. Nevertheless, there are existing drawbacks when using HMACs. In particular, the increasing bus load when attaching an HMAC on each message. Furthermore it requires an extensive key management. Accordingly to the constraints in the automotive domain like restricted bandwidth and power, a trade-off between protection level and required resources is necessary. Unfortunately, this often leads to a non-implementation of necessary security measures. In this paper, we propose an approach of using local ECU signals, in addition to the information which the ECU receives from bus systems, to perform plausibility checks. In detail, the contributions of this paper are the following:

Problem: Spoofing and tampering of bus messages in vehicular networks can lead to safety critical situations. To prevent these situations, message authenticity and integrity have to be ensured. Therefore, cryptographic measures can be

 ISBN: 978-1-61208-573-9

used, but they are often not applicable due to the fundamental constraints in the automotive domain. **Solution:** Apply plausibility checks with local ECU signals to verify data integrity without cryptography. Our **Contribution:** A novel approach for plausibility checks with local or directly measured signals for hardening security in the automotive domain. Moreover, the approach to secure safety-critical functions with plausibility checks hardens security with minimal integration effort in the typical automotive engineering process.

The paper is structured as follows: Section II summarizes the related work in the area of automotive security measures, followed by our approach in Section III, which is divided in methodology and its applicability. Furthermore, we propose a way to locate suitable signal sources inside vehicles that are necessary for our approach. This is followed by an application example that should be able to prevent the published exploitation of a passenger vehicle. In Section IV we give a short summary of our work and present an outlook on how our approach could be combined with other security measures in Section IV.

II. Related Work

Automotive manufacturers, suppliers and other organizations have already recognized the necessity for security mechanisms in the automotive domain. For this reason, a cyber security alliance was founded in the USA. The major objective of the Automotive Information Sharing and Analysis Center (AUTO-ISAC) [8] is to enhance cyber security awareness and the coordination for the automotive domain. Moreover, the alliance is providing best practices for organizational and technical security issues to support the developing process of their members. An additional effort was initialized by the Society of Automotive Engineers (SAE) with the J3061 guidebook [9], summarizing recommended security practices that can be applied in the automotive domain. Unfortunately, the guidebook gives no concrete reference implementations for possible measures.

A more comprehensive approach for security in cars is presented by Gerlach et. al. [10]. They propose a multi-layer security architecture for vehicular communication which implements different measures. In particular, they propose digital signatures with certificates as methods for providing authentication, integrity, and non-repudiation of the received messages. Due to the underlying asymmetric cryptography, high-performance ECUs or ECUs with additional Hardware Security Modules (HSMs) are needed. They further consider an application of cross-layer plausibility checks [10] as meaningful. Therefore, they establish a single instance in the vehicle which collects information from any existent source in the car. The instance is called plausibility checking module and creates its own independent view of the current vehicle state. If deviations from normal operation are detected, the instance reacts by triggering a warning. Unfortunately, the proposed instance is not implemented in each ECU, hence triggered counteractions or warnings have to be transferred over the unsecured bus again.

An additional approach is presented by Dhurandher and his researchers [11]. They propose an application of reputation and plausibility checks for Vehicular Ad Hoc Networks (VANETs). In particular, their proposed algorithm is able to detect and isolate malicious nodes by the use of sensors. Although they present an efficient and effective algorithm, the approach is designed for wireless nodes and their unique characteristics. Unfortunately, a concept for adaptation to in-vehicle networks is not given.

III. Approach

We consider an application of plausibility checks as additional protection mechanism as meaningful, if the relevant functions are able to change the physical state of the vehicle. This is partly explained by the fact that for these type of functions sensor values are already exist. As a result, our approach is applicable for a great set of functions and in particular for almost all safety-related functions. To decide if a function can be protected by our approach, some requirements have to be met. We define these requirements in the following and we further present an application example. Therefore, we divide our approach into two parts: (1) required steps to validate if the selected function can be protected by a plausibility check (see Figure 1) and (2) a reference implementation for plausibility checks with local ECU signals. Finally, we give an application example which is explained in Section III-C).

A. Applicability of Plausibility Checks

To validate if plausibility checks are applicable, a few requirements have to be checked beforehand. For this purpose, we define and highlight them as selection steps in Figure 1.

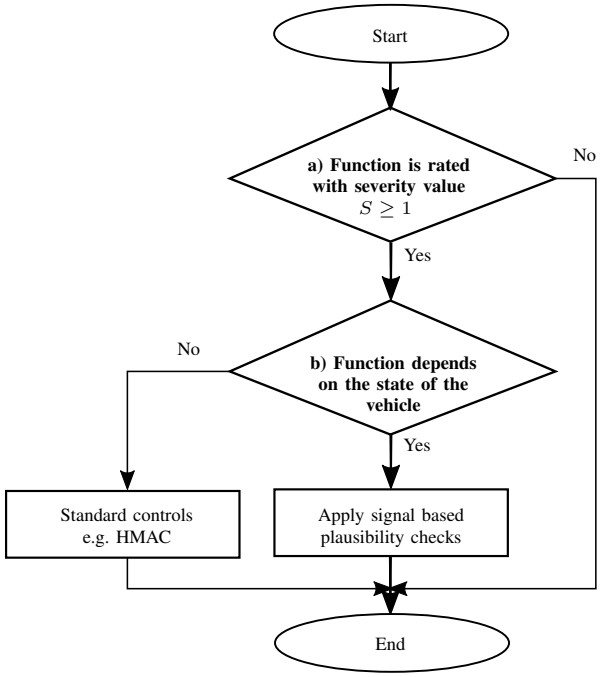

Figure 1. Methodology for applying signal based plausibility checks.

Figure 1 shows the required steps to identify functions that are applicable for plausibility checks. Before we can validate *Step a)*, a hazard and risk analysis has to be performed. This is a demand of the functional safety standard ISO 26262 [12]. The aim of the analysis is to identify potential hazards of a function. Furthermore, for each hazard a so-called Automotive Safety Integrity Level (ASIL) based on three values is calculated. One of these values is defined as severity, describing the possible impact of the malfunction related to the selected function. Thus, we consider a selection of functions able to

cause hazards with a severity value greater or equal to S1 as meaningful. In particular, a severity value of $S \geq 1$ implies injuries of vehicle occupants [12] and must be prevented. If the function is rated with $S \geq 1$, the next step is to check, if the selected function has dependencies on the vehicle state (moving or standing still, etc.) as shown by *Step b)* in Figure 1. If plausibility checks are not applicable, but the function is rated with $S \geq 1$, we deem an application of standard security controls to be mandatory.

B. Plausibility Checks with Local ECU Signals

To guarantee that signals used for plausibility checks can not be maliciously modified or sent, we have to implement protection mechanisms. In particular, we have to ensure the authenticity and integrity of the used signals. Therefore, we could apply the already mentioned cryptographic methods with all their drawbacks. Instead, we chose another way to ensure the protection of the information assets without the afore mentioned drawbacks. To explain the approach we take a closer look into automotive architectures like the one presented in Figure 2.

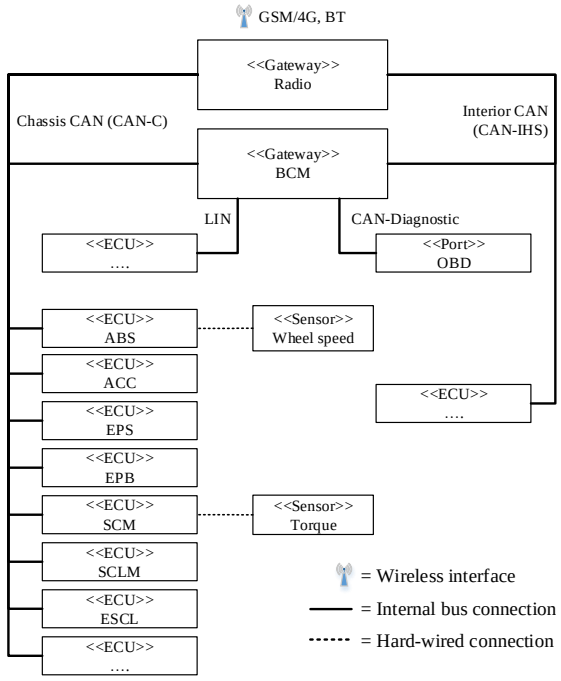

Figure 2. Part of the electrical architecture of a Jeep Cherokee 2014, based on the work of Valasek et. al. [6]. As diagram notation we use the UML4PF profile extension [13].

Figure 2 represents a part of the E/E architecture of a Jeep Cherokee 2014, which was the attack target of the researchers [6] [14] mentioned in the beginning. The architecture shows different ECUs and gateways interconnected by three CAN-Bus systems (CAN-C, CAN-IHS, CAN-Diagnostic), as well as one LIN-Bus. Furthermore, each wheel has a sensor measuring the wheel speed which is hard-wired to the Antilock Braking System (ABS), respectively the Electronic Stability Control (ESC). This information can be used to derive ECU local signals for plausibility checks without the need for cryptographic algorithms. In particular, these sensor values can indirectly describe the state of the vehicle. With the wheel speed sensor shown in Figure 2, we can derive whether the vehicle is moving or not. If the vehicle is on halt, all sensor values of the wheels have to be zero or vary significantly due to a spinning wheel. This hard-wired sensor type is only an example. Additionally, we can combine two or more sensor values to derive more precise information about the state of the vehicle. The important point in our approach is that an ECU with hard-wired sensors can operate as a guardian against spoofed or tampered signals. In general, it is important that a safety critical function can be additionally protected by one or more hard-wired sensor values. By adding this requirement, an attacker would no longer be able to spoof sensor values over bus messages, while ECUs can verify the plausibility of the received values. We are aware that hard-wired sensors can increase cabling efforts, if an ECU normally doesn't have access to any hard-wired sensors. However, the addition of security techniques is often tied to increased costs.

To be precise, authenticity and integrity are only ensured, if the attacker is not capable of getting access to the sensors themselves, requiring him to be in the vicinity of the vehicle. We assume that the possibility of an attacker accessing sensors is unlikely in comparison to his ability to send spoofed messages via CAN [6]. This is reasonable due to the fact that an attacker has to overcome several physical barriers, e.g. opening the hood, ECU housing or removing the wire insulation.

C. Application Example

As an example, we want to discuss the latest Jeep [14] hack, as well as the attack on the steering system which have been done. Generally, the vulnerabilities in diagnostic mode, which the researchers used for disabling the Jeep's brakes among other things, are only working if the car is in reverse and slower than 5 mph. How can we make sure, that the values received for plausibility checks are valid and not tampered with? We want to answer this question by the following examples, based on the already mentioned vulnerabilities and how our approach would prevent these hacks in the future.

In the first example, the researchers set the real ECU in a service mode causing it to stop sending messages on the bus. This step enables them to send their own messages in the name of the jammed ECU. Electric Power Steering (EPS), which can be integrated in modern vehicles, e.g., the hacked Jeep series, requires various input parameters for calculating the electric steering support. One of these control values is the velocity of the vehicle. Depending on the current speed and other parameters, the Steering Control Module (SCM) calculates the steering torque. Basically, the steering torque support is decreasing by the SCM, when the velocity is increasing. Applied to the example of the Jeep hack, we want to show the determination of the steering torque threshold, which was one of the conditions the Jeep had to meet, in order to execute the steering angle change. A request for a high torque support in vehicle speeds of 30 mph or higher is not legitimate. However, we have to ensure that the integrity of the velocity value is given, for example by a hard-wired connection of the wheel speed sensors to the SCM. For instance, by implementing our approach, we deem the execution of the function as done in the hack would have been refused during the plausibility check.

Another attack presented by Valasek and Miller [14] was the application of the car's brakes. The exploited function is normally used to activate the electronic parking brake for

 ISBN: 978-1-61208-573-9

emergency braking by pressing the parking switch for a longer amount of time. Thereupon the pump for the ABS and ESC system gets activated and provides the necessary pressure to engage the brakes of the car. In this case, our approach is not applicable because of the missing hard-wired signals. In particular, an implemented plausibility check would not be possible, because of the lack of hard-wired signals. Therefore it can not be differentiated between unintended or intended emergency braking, because we have only the information from the bus. In a case like this, where no hard-wired signal sources available we propose to check the feasibility of adding a hard-wired connection.

Our own attempts have shown, that the related safety relevant ECU mentioned in the introduction has already connected hard-wired signals. However, the existent checks do not analyse the use-case correctly. Thus, it would have been possible to increase the security level simply by using enhanced software prompts, e.g., logical *and/or* conjunctions.

IV. Conclusion

In this publication, we proposed a new way to implement plausibility checks for automotive ECUs. The approach is capable to ensure that signals used for plausibility checks are resilient against replay and tampering. Furthermore, the approach uses already available information, like sensor signals, to verify function requests with the actual state of the vehicle. Due to the fact, that no cryptography is needed and existent information is reused, our approach requires less performance and costs, e.g., no HSM chips, as well as no additional busload than other security measures. Additionally, we showed an example implementation of our approach, which is able to prevent a known attack. We used hard-wired sensor signals like wheel speed sensors of the ABS to ensure the integrity of the velocity signal. Furthermore, using the electric power steering ECU example, we have shown how a function is able to perform a plausibility check. This is done by a function request during runtime using characteristic values.

After doing our own research we can confirm that replay attacks can be performed with minimal effort, if bus systems like CAN are used. In combination with our findings based on a safety critical function in an ECU, which is rated with a severity value of 3, we recommend that such functions should only be executable by bus messages if they validate the plausibility of the request. Therefore, our approach recommends using at least two values received from different sources. In the best case scenario, one source is a hard-wired connection. Finally, messages for ASIL D functions should not be routed over gateways, unless there is no other way. This will prevent relaying malicious messages between different domains.

V. Future Work

The mentioned vulnerabilities show us the necessity of additional safeguards for future vehicles. This creates new challenges for the whole automotive domain, in addition to the rising amount of interconnected services. Due to this fact, we are working on a following step including distributed firewalls techniques to enhance the security level for diagnostic services and functions which can change the physical state of the car, by using Stateful Packet Inspection (SPI), as well as Deep Packet Inspection (DPI). We want to use the approach to distinguish between different sets of implemented policies depending on the requested use case, e.g., starting a diagnostic session. For validating the specific use case the internal firewalls have to check different hard-wired sensors like wheel speed or seat occupancy. Thus, the firewalls have to ensure that requested services are matching to the associated use cases based on the vehicle state. Additionally, through the use of SPI, we assume that the firewall would be able to detect anomalies, like the attack example of jamming an ECU by setting it in boot ROM mode in order to spoof its control functions influencing the vehicle movement. We are convinced that plausibility checks with local signals are hardening the security of a vehicle. Finally, we're going to publish detailed information regarding the weakness in the safety relevant ECU in the near future and contribute an enhanced approach fixing this type of issue. Additionally, the mentioned firewall techniques shall also be evaluated and flow into an additional publication.

Acknowledgment

This work has been developed in the project SAFE ME ASAP (reference number: 03FH011IX5) that is partly funded by the German ministry of education and research (BMBF) within the research programme ICT 2020.

References

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., "Comprehensive experimental analyses of automotive attack surfaces," 2011.

[2] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," black hat USA, 2014, last checked on 09.05.2017. [Online]. Available: https://sm.asisonline.org/ASIS%20SM%20Documents/remote%20attack%20surfaces.pdf

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., "Experimental security analysis of a modern automobile," Symposium on Security and Privacy, 2010.

[4] C. Miller and C. Valasek, "Adventures in automotive networks and control units," DEF CON, vol. 21, 2013, pp. 260–264.

[5] M. S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henninger, "Secure automotive on-board protocols: A case of over-the-air firmware updates," Nets4Cars/Nets4Trains 2011, 2011, pp. 224–238.

[6] C. Valasek and C. Miller, "Remote exploitation of an unaltered passenger vehicle," last checked on 09.05.2017. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

[7] A. Greenberg, "Tesla Responds to Chinese Hack With a Major Security Upgrade," last checked on 23.03.2017. [Online]. Available: https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/

[8] AUTO-ISAC, "Automotive information sharing and analysis center," https://www.automotiveisac.com/index.php, last checked on 09.05.2017.

[9] SAE, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," 01.2016, last checked on 12.04.2016. [Online]. Available: http://standards.sae.org/wip/j3061/

[10] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," in Workshop on Intelligent Transportation, 2007.

[11] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks," Systems Journal, IEEE, vol. 8, no. 2, 2014, pp. 384–394.

[12] ISO, "ISO 26262 – Road Vehicles – Functional Safety," 2011.

[13] D. Hatebur and M. Heisel, "A uml profile for requirements analysis of dependable software," in International Conference on Computer Safety, Reliability, and Security. Springer, 2010, pp. 317–331.

[14] C. Valasek and C. Miller, "CAN Message Injection: OG Dynamite Edition," last checked on 05.04.2017. [Online]. Available: http://illmatics.com/can%20message%20injection.pdf

 ISBN: 978-1-61208-573-9