Plausibility Checks in Automotive Electronic Control Units to Enhance Safety and Security

Martin Ring, and Reiner Kriesten

University of Applied Sciences Karlsruhe
76133 Karlsruhe
Emails: {martin.ring, reiner.kriesten}@hs-karlsruhe.de

Abstract— **Automobiles nowadays consist of multiple Electronic Control Units (ECUs) and bus systems. Attacks on these critical infrastructure elements have increased a lot over the last years, especially since remote exploitation is possible due to wireless connectivity. Most of these attacks targeted standard services implemented in cars. These services, e. g., allow the activation of the headlights or turning of the steering wheel via the parking assist. All these services have to be secured so they can only be executed when it is safe to do so. These checks for a safe state are plausibility checks, which nowadays only utilize the vehicle speed. In this paper we motivate the need for other values that have to be authentic and integrous. We want to utilize immanent signals, derived from hard wired sensors, for each ECU that utilizes plausibility checks.**

Keywords–Automotive Security; Vehicular Attacks; Plausibility Checks.

I. INTRODUCTION

Modern automobiles feature a myriad of cyber physical systems. These systems are composed of up to 100 microprocessors (called ECUs) with up to 100 million lines of code [1]–[3]. These systems are prone to attacks. Since the introduction of bus systems to cars they are vulnerable to attacks that require a physical connection (e. g., car theft). With the introduction of wireless interfaces, these attacks and many more can now be performed from the basement of hackers [4]. Thus the most acclaimed attacks on automotive networks nowadays have been remote attacks. These attacks alone have little to no effect on cars, only combined with flaws in the internal networks security risks can arise. Miller and Valasek come to the same conclusion and argue that their work "shows that simply protecting vehicles from remote attacks isn't the only layer of defence that automakers need." [5]. An defense in depth concept is necessary. One part of such a concept are the proposed plausibility checks in this paper. In earlier publications [4]–[8] a lot of the attacks able to compromise the safety of a car were limited to low speeds. These limitations stem from plausibility checks in ECUs that try to determine if the execution of the requested service is safe. These plausibility checks only rely on the speed of the vehicle. With this paper, new approaches for such checks will be introduced.

In the following, we will first give an introduction to plausibility checks and outline the requirements for the used signals. Section III then describes the method for advanced plausibility checks and the assessment process to determine suitable functions to safeguard. Next Section IV gives an evaluation of our method and its applicability, and finally Section V concludes this paper.

II. STATE OF THE ART

As researchers noticed in their attempts to compromise cars, most of the time the last barrier to safety critical functions is a plausibility check. These are simple checks that verify if the prerequisites to execute a function safely are met. All found checks use the speed of the car as a signal to check against [5]. All but one ECU (the Antilock Brake System (ABS)/Electronic Stability Control (ESC)-ECU) obtain this information from a bus system. The check only determines if the speed is below a predetermined threshold. This threshold is usually 5 mph or 8 kph depending on whether the country uses imperial or metrical units, respectively. Above these thresholds, ECUs change their internal state to one with very limited triggerable functions. The problem with this mechanism is not its principle function but that everything depends on the speed of the car, which is received by bus messages and can thus be sent by any host in the same subnet in current automobiles. If no network separation is present the signal can basically be sent by any host in the network even by ones plugged in externally.

In order to provide the necessary protection, the signals used for plausibility checks have to be authentic and integerous. The approach used nowadays and presented in a recent publication [9] is the applications of cryptographic functions to ensure that these preconditions are met. A possible way to ensure the authenticity and integrity of a message is the use of an Keyed-Hash Message Authentication Code (HMAC). This type of message protection can not be found in production vehicles nowadays. The maximum security offered is the use of an alive counter and a simple checksum.

III. ADVANCED PLAUSABILITY CHECKS

As stated before, plausibility checks can be applied as part of a defense in depth concept to prevent attacks on safety critical functions. Figure 1 shows the method that can be used to determine if our proposed checks can be used for a certain application.

In advance to this assessment, a hazard and risk analysis has to be conducted. This analysis is part of every automotive development lifecycle and demanded by the functional safety standard ISO 26262 [10]. The objective of this analysis is the identification and classification of the hazards of an item ("a

 ISBN: 978-1-61208-515-9

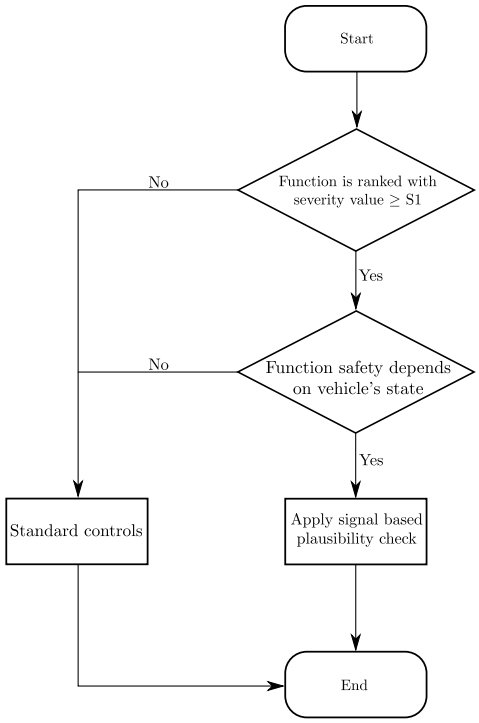

Figure 1. Methodology for applying plausibility checks

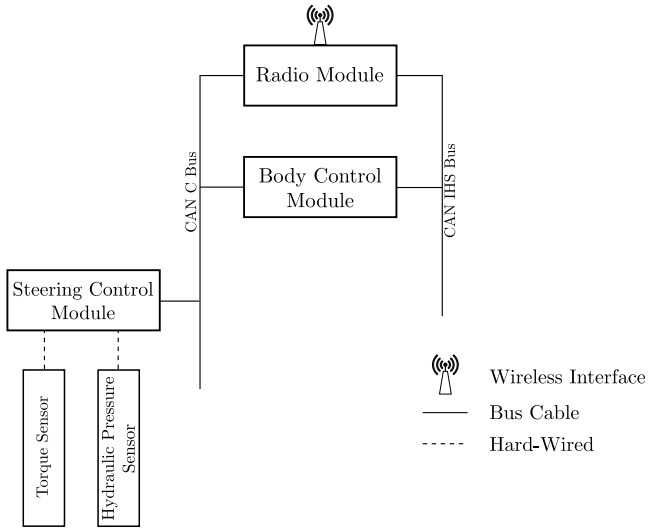

Figure 2. Sub-architecture of a Jeep Cherokee 2014 [4]

system that implements a function at a vehicle level" [10]). Such an item could, e. g. , be the airbag. In addition, safety goals related to the prevention and mitigation of the found hazards have to be drafted. For each hazard, an Automotive Safety Integrity Level (ASIL) has to be calculated. The inputs for this calculation are the expected loss in case of an accident (*severity*) and the probability of the accident occurring (*exposure and controllability*). For this contemplation only the severity as the consequences of a malfunction are considered. With levels from S 0 to S 3, functions with a severity equal or above S 1 (light to moderate injuries) are deemed meaningful. These considerations are embodied by the first decision in the design structure chart pictured in Figure 1. The next necessary decision is to determine if the function in question depends on the state of the vehicle.

When these requirements are met, advanced plausibility checks should and can be used to safeguard functions. As mentioned before, inputs to these plausibility checks have to be authentic and integrous. These protection goals can be met by applying cryptographic functions, e. g. , using HMAC [9]. This type of cryptographic measure ensures the desired protection goals with an acceptable demand for computational performance. Nevertheless there also exist a few drawbacks using HMACs. In particular the key management and reduced bandwidth on the bus by attaching an HMAC to each message are problematic. Is there another method to ensure the needed protection goals without the drawbacks of HMACs? To answer this question we took a deeper look into automotive architectures like the one presented in Figure 2.

Figure 2 represents a part of a Jeep Cherokee 2014 network architecture which was the target of the latest attacks of Miller and Valasek on a car [4], [5]. The figure shows different ECUs and gateways that are interconnected by bus systems. Furthermore, some hard-wired sensors are apparent delivering relevant information about the state of the vehicle. This information can be used to derive ECU immanent signals for plausibility checks without the need for cryptographic algorithms.

ECU immanent signals should be used for plausibility checks whenever possible. These signals can be signals produced in the ECU, like the regulated torque in the engine ECU that is calculated by adding up all the torque demands of the engine auxiliaries and the driver requirement. The other possibility for such signals are hard-wired sensor signals like the rotational speed sensors for the ABS / ESC ECU. With the help of Figure 3 we want to show how an immanent signal of an ECU can be used to make a plausibility check for a requested function. The latest hacks applied on the Jeep [5] jammed the signal of another ECU that normally would have been used to make the plausibility check. In this case the plausibility check would verify if the car is in reverse and slower than 5 mph. The check for the driving direction is not easily possible but we can check for the speed constraint. We can assume a known level of hydraulic pressure in the steering system because we have a hard-wired sensor for this signal to the Steering Control Module (SCM). This module also evaluates the signal of the torque sensor. With this information we can determine the speed of the car within small limits. With the help of the information in Figure 3 it is possible to determine the speed of a car. As a small example we will show the determination of the threshold for the steering torque for the conditions the Jeep has to meet to execute the steering angle change. With a supposed threshold of 20 kph for the Jeep and an assumption of 20 bar for the hydraulic pressure brings us to the conclusion that a steering moment of more than 2.9 Nm is equivalent to a speed above the defined threshold and thus the execution of the requested function has to be refused. An implementation according to this technique would have prevented the attack on the steering system as described in [5]. Such immanent signals can be found and utilized on almost any safety critical ECU in a car. Only if such signals are not existent signals from other ECUs should

be used. As mentioned before these signals have to fulfill some preconditions, namely being integrous and authentic. Only if these prerequisites are fulfilled, such bus signals can be used for plausibility checks of functions with a severity value of S 1 or above.

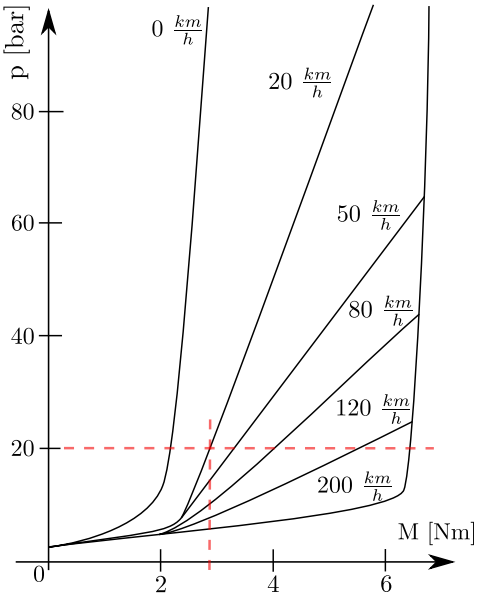

Figure 3. Plot of steering moment dependent on hydraulic pressure and vehicular speed [11]

The other attacks presented in the latest release of Wired [5] are more problematic as they use legitimate messages to request certain functions. The *slamming on the car's brakes* is a standard function that is executed while the driver presses the switch for the electronic parking brake. While pressing the switch the pump for the ABS / ESC system gets activated and provides the pressure to engage the brakes of the car. Such a brake maneuver is comparable with an emergency braking. As Miller and Valasek were able to request and execute this function it is reasonable to assume that the switch for the electronic parking brake is directly connected to the bus system of the car. The same thing can be concluded for their last attack, the unintended acceleration of the car. They used the standard function to enable Apdative Cruise Control (ACC) and then increase the target speed of the cruise control. This is possible by replaying messages of the switches embedded in the steering wheel. We were able to observe the same situation in an electric vehicle produced by a German manufacturer. Therefore, safety critical functions with an ASIL of D should not be able to be activated by bus messages. For all requests of such functions direct connections should be used (peer-to-peer); although these connections can be network connections, like Controller Area Network (CAN) or Ethernet, they should not be routed over gateways.

IV. Evaluation

To demonstrate the validity of this method in this section we present other examples of instances where plausibility checks with immanent signals can be used. First, we further evaluate the examples in Section II. After these examples other published attacks on safety critical functions (lighting, engine,

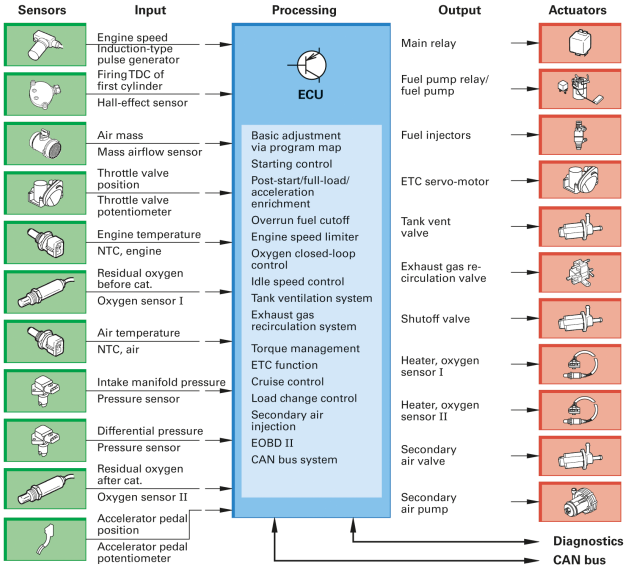

Figure 4. Engine ECU with its hard-wired sensors (green) and actuators (red) [13]

gearbox, brakes and suspensions [4], [6], [8], [12]) and the possibility to apply plausibility checks with ECU immanent signals are evaluated.

We start with the engine example. There are multiple attacks published on the engine of a car [6]–[8], [12]. Most attacks completely disable the engine and shut it down. To achieve this result standard services were used to reset the ECU, deactivate fuel injectors or initiate a flash session. Every service should use a plausibility check as the safety of its execution is widely dependent on the vehicles state. There are multiple immanent sensor values or processed signals that could be used for these plausibility checks. An extensive overview is presented in Figure 4. The easiest signal to use is the rpm-signal of the engine. If this signal is unequal zero no service that compromises the operation of the engine should be able to execute. Not necessarily forbidden should be services that help mechanics with diagnostics of the engine in a workshop, like reading out live data. Besides the aforementioned rpm-signal there are a host of other sensor signals which could be used, like the readout of the air mass sensor, exhaust temperature sensor, fuel pressure sensor and more. A processed signal that could be used is the calculated torque of the engine. This torquer is calculated by adding the demands of all auxiliaries of the engine, like the AC compressor, the alternator or the hydraulic steering pump as well as the driver demand. If this signal is unequal zero it can also be concluded that the car is in use and any execution of service that compromises the operation of the engine can be deemed unsafe.

The second and probably most critical point of attack is the braking system, which was also the target of multiple attacks [4]–[6], [12]. The executed attacks include wheel selective braking as well as disabling the braking system all together. Here it is also possible to use ECU immanent signals. All wheel speed sensors are hard wired to the ECU. Modern wheel speed sensors can determine speeds as low as

 ISBN: 978-1-61208-515-9

0.1 kph [14]. As soon as any speed is detected all safety critical services should stop their execution. However, the speed signal is not the only one that can be used, as an alternative the hard wired three-axis acceleration sensor can be evaluated. As soon as these sensors signals show any acceleration the car is not in a safe state to execute safety critical functions.

Our research shows vulnerabilities in active suspension systems. The ECUs controlling such systems also use a vast amount of sensors and signals to control the ride of a vehicle. Two possible immanent signals of such a system are acceleration sensors or sensors for the level of each wheel. If the signals of the level sensors of the car change or an acceleration unequal zero is detected it can be concluded that the car is in motion and thus safety critical functions should not be able to perform their task of, e. g. , resetting the ECU.

A way to utilize immanent signals to check the safe state of the car with immanent signals of the steering system was presented in Section III. This shows that these systems could be safeguarded in their current implementation with our method. Furthermore, these examples show that this method allows it to safeguard every ECU responsible for lateral or longitudinal behavior of a vehicle.

An instance where an odd sensor signal could be used were attacks on the headlights of cars [6], [8]. These attacks spoofed messages of the light sensor or used diagnostic messages to deactivate the headlights of a car. The sensor signal of the light sensor is evaluated in the vehicle supply system control device. This device also powers the electric fuel pump, see, e. g. , the schematic in [15]. This pump is only active when the engine is running and during a short time after unlocking the car or switching on the ignition. The signal is thus also a good indicator if it is safe to execute the inquired function. As the sensor is in the mentioned schematic hard wired to the executing ECU it can determine if the message was spoofed or issued by the correct sender.

V. Conclusion

In this paper, we have motivated the need for security plausibility checks. Such checks are already implemented but rely on bus messages of the vehicle speed which can be jammed or spoofed. As they are one crucial part of a defense in depth approach, a secure implementation is crucial.

With the use of immanent signals a secure way for plausibility checks is found. This approach can be used in modern cars without any need to change the architecture or wiring; all that has to change is the software and that can be achieved by a simple software update. We have discussed that many of the published attacks can be prevented by the presented approach.

References

[1] R. N. Charette, “This Car Runs on Code,” 2009. [Online]. Available: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

[2] G. Serio and D. Wollschläger, “Vernetztes Automobil Verteidigungsstrategien im Kampf gegen Cyberattacken,” ATZelektronik - 06/2015, 2015.

[3] SAE, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” 2016. [Online]. Available: http://standards.sae.org/wip/j3061/

[4] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle.” [Online]. Available: http://illmatics.com/Remote Car Hacking.pdf

[5] ——, “CAN Message Injection – OG Dynamite Edition.” [Online]. Available: http://illmatics.com/can%20message%20injection.pdf

[6] ——, “Adventures in Automotive Networks and Control Units,” 2014. [Online]. Available: http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf/

[7] 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.

[8] “Gehackte Mobilität,” Apr. 2016. [Online]. Available: https://www.3sat.de/mediathek/?mode=play&obj=58732

[9] K. Beckers, J. Dürrwang, and D. Holling, “Standard Compliant Hazard and Threat Analysis for the Automotive Domain,” Information, vol. 7, no. 3, 2016, p. 36. [Online]. Available: http://www.mdpi.com/2078-2489/7/3/36

[10] ISO, “ISO 26262 Road vehicles – Functional safety,” 2011.

[11] H. Felder, “Autoelektrik – Grundlagen- und Fachwissen.” [Online]. Available: http://www.fahrzeug-elektrik.de/

[12] 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.

[13] R. H. Gscheidle, Ed., Modern automotive technology : fundamentals, service, diagnostics, 2nd ed., ser. Europa reference books for automotive technology. Haan-Gruiten: Verl. Europa-Lehrmittel, 2014.

[14] “Raddrehzahlsensoren im Kraftfahrzeug Funktion, Diagnose, Fehlersuche.” Tech. Rep. [Online]. Available: http://www.hella.com/ePaper/Raddrehzalsensoren/document.pdf

[15] “STG. Bordnetz - Control Mains Power Supply.” [Online]. Available: http://www.seatforum.de/uploads/DRAFT01%5B1%5D244.jpg

 ISBN: 978-1-61208-515-9