Plausibility Checks in Electronic Control Units to Enhance Safety and Security

Martin Ring and Reiner Kriesten

University of Applied Sciences Karlsruhe
76133 Karlsruhe
Germany
{martin.ring|reiner.kriesten}@hs-karlsruhe.de

Frank Kargl

Ulm University
89069 Ulm
Germany
frank.kargl@uni-ulm.de

Abstract— **Modern vehicles include a large number of Electronic Control Units interconnected by different bus systems. Attacks on these critical infrastructure elements have increased significantly over the last years, particularly since remote exploitation is possible due to increased wireless connectivity from the cars to the outside world. Many of these attacks exploit available standard communication protocols and diagnostic services implemented in cars that are often mandatory. Such services allow, for example, the activation of headlights or the turning of the steering wheel via the parking assist functionality. These services must be sufficiently secure, such that they can only be triggered when it is safe to do so, e. g., when the car is parked or driving at low speed. The validation mechanisms to determine a safe state are mainly plausibility checks, which currently often only utilize the vehicle speed, reported via the Controller Area Network bus, as an input parameter. In this paper, we motivate the need to base plausibility checks on other input values, which may be more authentic and reliable. Specifically, we propose the use of immanent signals for plausibility checks, i. e., signals derived from hard-wired sensors, which are harder to manipulate. In this paper, we propose some specific implementations of plausibility checks with immanent signals and argue how they would protect from current attacks on cars found in literature, we also discuss how the same idea may be applied to other areas, such as Industrial Control Systems.**

Keywords–Automotive Security; Vehicular Attacks; Plausibility Checks.

I. Introduction

Modern cars can be regarded as highly complex cyber physical systems. These systems are composed of up to 100 microprocessors (called Electronic Control Units (ECUs)) with up to 100 million lines of code [2]–[4]. Failures of such systems can have catastrophic consequences and come in two flavors, safety failures can be induced by a systematic or random malfunction, while security failures are induced by a malicious entitiy. These failures make the automotive systems prone to attacks. Since the introduction of bus systems to cars they were vulnerable to attacks, but these required a physical connection (e. g., car theft). With the recent introduction of ever more wireless interfaces, these attacks and many more can now be performed by remote hackers [5]. Remote attacks alone typically have little to no direct effects on the safety of cars, as they target communication units. Only combined with flaws in the internal networks can safety risks arise. Joe Weiss and the NIST share this viewpoint in that for Industrial Control Systems (ICSs) and critical infrastructures at large the principle of CIA should be replaced by AIC, thus making attacks on the availability of a system the most critical attacks, followed by attacks on its integrity and lastly its confidentiality [6]. Miller and Valasek come to the conclusion that multi stage attacks are now a realistic problem in the automotive world and argue that their work "shows that simply protecting vehicles from remote attacks isn't the only layer of defense that automakers need" [7]. A defense in depth security approach is required. One significant part of such an approach are plausibility checks, which we proposed in an earlier paper [1] and that we want to amend in this publication. In earlier publications [5], [7]–[10], most critical attacks able to compromise the safety of a car were limited to low speeds. These limitations stem from existing plausibility checks in ECUs that try to prevent the execution of the requested service in an unsafe state, like at higher speeds. However, these plausibility checks only rely on the speed of the vehicle as reported to ECUs via internal networks which can, again, be attacked. In this paper, we introduce a novel approach for enhanced validity checks that does not suffer from attackers that have infiltrated internal networks.

In the following, we will first give an introduction to plausibility checks and outline the requirements for the used signals, followed in Section II-B by an extensive overview of vulnerabilities found in cars till today. Section III then describes our approach for advanced plausibility checks and the assessment process to determine suitable functions to safeguard. Next, Section IV discusses the security of our approach and its applicability to cars and other domains like ICSs, and finally, Section V concludes this paper with an outlook.

II. State of the Art

A. Plausibility Checks

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 whether all prerequisites to safely execute a function are met. All checks discovered so far use the speed of the car as a signal to check against [7], [11]. All but one ECU (the Antilock Brake System (ABS)/Electronic Stability Control (ESC)-ECU) obtain this information from an internal bus

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

TABLE I. Qualitative severity rating scale [30].

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 the general approach, but rather that it relies only on the speed of the car, which is received by spoofable bus messages that can be sent by any host with access to the network segment in most current automobiles. If no network separation is present, the signal can basically be sent by any node 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 integrity protected. The modern approach [12] applies cryptographic protection, e. g., with Keyed-Hash Message Authentication Codes (HMACs), to achieve these goals. However, this type of message protection is hardly found in current production vehicles. The maximum security offered is the use of alive counters and simple checksums.

B. Attacks on Automobiles

In order to efficiently implement security measures, it is necessary to understand the problem in detail. For this reason, we conducted an extensive literature research that resulted in 22 published sources describing attacks on automobiles [5], [7]–[9], [11], [13]–[29]. In these 22 sources, a total of 87 attacks were found and classified according to CVSS v. 3 [30]. In the following, we present our results from an analysis and categorization of these attacks. The detailed analysis can be found in [31].

The Common Vulnerability Scoring System (CVSS) is widely accepted as the standard taxonomy to rate software vulnerabilities and is used, e.g., in the Common Vulnerabilities and Exposures (CVE) database. We classified all attacks according to the CVSS v. 3, limiting classification to the *Base Metrics*. These metrics reflect the vulnerabilities of the tested systems. The CVSS offers five severity ratings represented in Table I with their associated CVSS scores. Additional metrics are *Temporal Metrics* and *Environmental Metrics*. A *Temporal Metric* is used to classify the maturity of the available exploits, ranging from no available proof of concept to publicly available scripts ready to be used. *Environmental Metrics* are used to measure the impact to a shareholder if a vulnerable item is failing / compromised.

Figure 1 depicts the severity ratings of all examined attacks. Probably most noticeable is the fact that only one attack has a low severity. This is the attack on the WiFi pre-shared key (PSK) in a Mitsubishi [20]. This attack only compromises the confidentiality of the system. 28% of all attacks have a medium, 40% a high and 31% a critical severity rating.

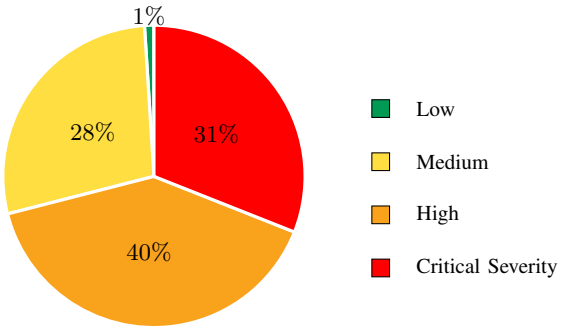

Figure 1. Severity ranking of of Vulnerabilities

Figure 2 gives an overview of the combinations of affected protection goals. The bar on the left shows all attacks that compromise a single protection goal, either confidentiality, integrity or availability (combined 26.4%). The middle bar represents the attacks that compromise a combination of two safety goals (combined 49.5%), while the right side bar represents the percentage of vulnerabilities that compromise all three protection goals (24.1%). 28% of the found vulnerabilities have a severity rating of medium, and all combinations of compromised protection goals can be found in this class. A high severity rating is determined for 40% of the found vulnerabilities. In this severity class, no attacks on the integrity of the system or the combination of confidentiality and integrity are included. 31% of all found vulnerabilities are critical, the highest severity class according to CVSS v. 3. In this class, the vulnerabilities are a combination that affect either all three protection goals (8% of all vulnerabilities) or the combination of integrity and availability (23% of all vulnerabilities). Another interesting fact is that no attack that required user interaction resulted in a critical vulnerability.

Finally, we want to investigate the attack vectors used in these attacks. The CVSS offers a distinction between four attack vectors: network, adjacent, local and physical. If a vulnerability is exploitable by network it is often referred to as *remotely exploitable*, the vulnerable component thus needs a network access and the attacker attacks through OSI layer 3. A component exploitable over an adjacent network has a network connection, but the connection only has a short range, e. g., WiFi or Bluetooth. Is a vulnerability exploitable only by local access, then the attack uses local read/write/execute commands or utilizes the user. If the vulnerability is exploitable through a physical connection, then this connection can be only brief, e. g., *evil maid attack*, or it can be a persistent connection [30].

Figure 3 shows the distribution of attack vectors for attacks on automobiles. Most vulnerabilities can be exploited by an adjacent network, for example by having access to the local Controller Area Network (CAN) network. If a malicious host is part of the local network, other hosts can be exploited. Another example is the attack on the Bluetooth implementation described in [9]. Network exploitable vulnerabilities make up 5.7 % of all possible attack vectors, an example is the exploitation of the 3G network stack described in [9] or the remote unlocking and start of cars described in [27]. Local exploitable vulnerabilities account for 15 % of all vulnerabilities.

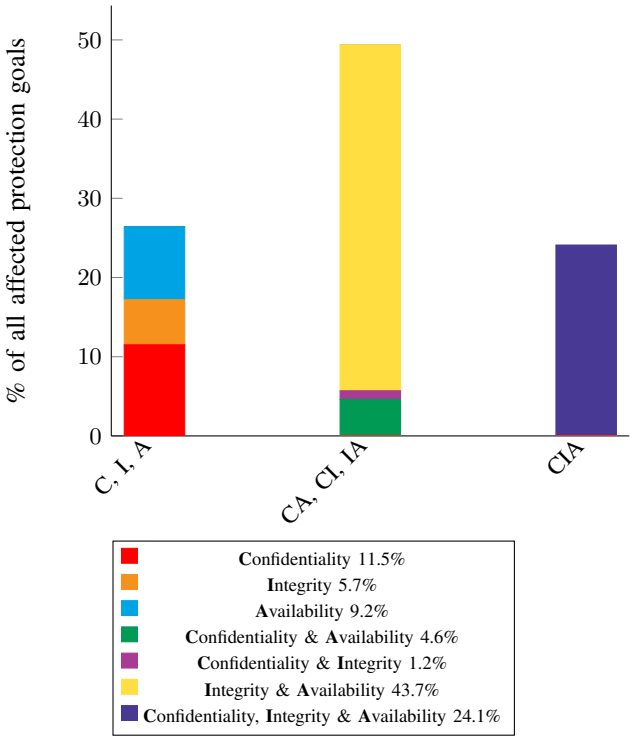

Figure 2. Overview affected protection goals

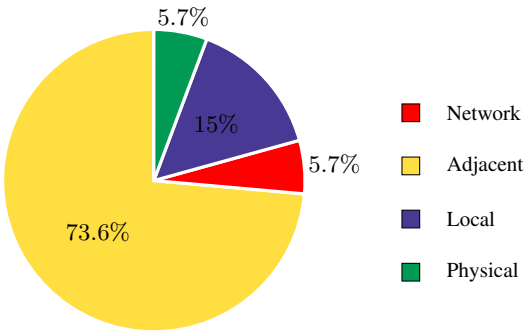

Figure 3. Distribution of attack vectors

Examples for locally exploitable vulnerabilities are, e. g., the attacks on keyless access systems described in [17], [21], [29].

Physical access was only necessary in 5.7% of all attacks, examples for such attacks are, e. g., the attack on the accelerator message in a Toyota or the dumps of the ROM of Ford ECUs in [8].

In conclusion, many of the attacks found during our literature survey rely on spoofing of messages and manipulating safety critical state (64.4%). Some attacks could only be conducted at low speeds due to simple plausibility checks being in place. However, [7] has already highlighted that such simple plausibility checks could be rendered ineffective and can be bypassed by spoofing messages that simulate a safe state, e.g., low speed. We thus conclude that more advanced and more secure plausibility checks would be required to provide better protection from such attacks. In the next section we want to present such plausibility checks.

III. Advanced Plausibility Checks

As stated before, advanced plausibility checks can be applied as part of a defense in depth concept to prevent attacks on safety critical functions. The main idea is that plausibility checks need to be based on more tamper-resistant input, because CAN messages are too easy to manipulate. In the absence of strong cryptographic protection of CAN networks in most cars, we can still resort to directly attached sensors, even if these only provide indirect evidence of the vehicles state. If, e. g., an ECU controls the steering aid and automatic steering, steering angle and forces allow it to determine whether the vehicle is driving at high speed or not, without relying on potentially spoofed remote information.

In order to allow a systematic development of such advanced plausibility checks, we have designed a systematic methodology that is shown in Figure 4 and allows to determine if our proposed approach is applicable for certain applications.

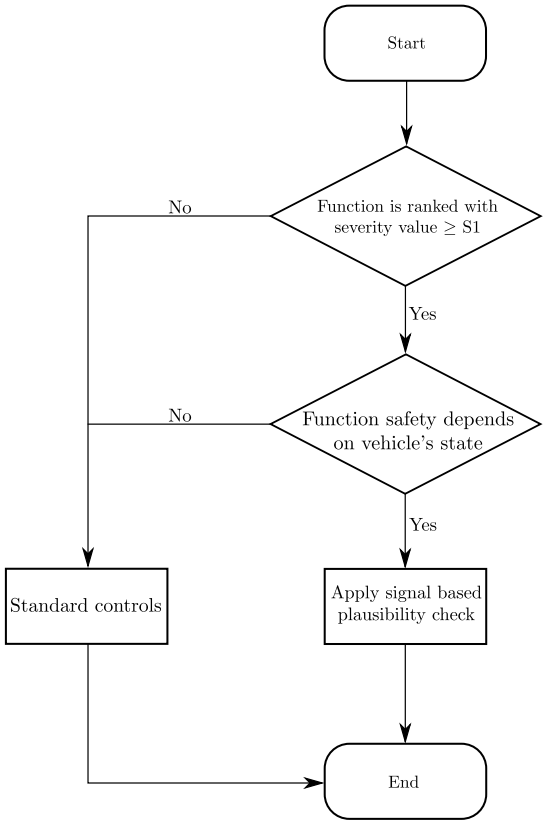

Figure 4. Methodology for applying plausibility checks

Before 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 [32]. The objective of this analysis is the identification and classification of the hazards of an item ("a system that implements a function at a vehicle level" [32]). 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 4. The next necessary decision is to determine whether the function in question depends on the state of the vehicle.

In addition to a Hazard and Risk Analysis for the identification of *safety* risks, the overall evaluation of *security* risks is performed in a Threat Analysis and Risk Assessment (TARA) at the beginning of an automotive project [33]. Several approaches can be taken into account in order to conduct existing vulnerabilities and attacker models, e. g., starting from the entry points of possible attacks into a system. Figure 5 shows a high-level description of possible entry points for an individual ECU.

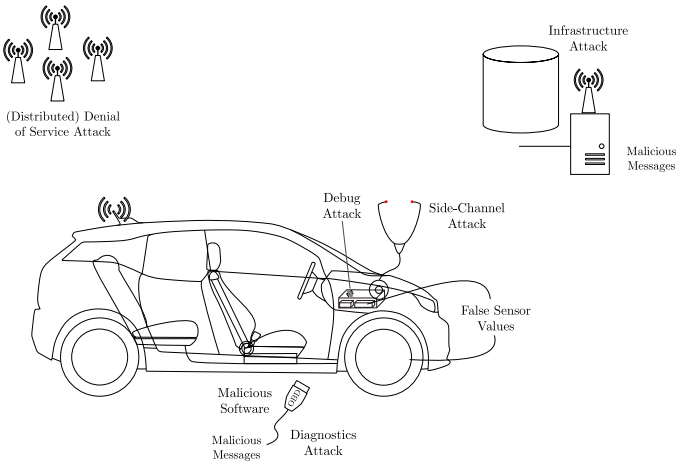

Figure 5. Possible entry Points to an ECU

The implementation of a simple plausibility check with speed evaluation is attractive to attacks, which are launched by the use of a counterfeit speed value on the on-board bus system, combined with an issuing of an (authenticated) diagnostics service request from an off-board tester unit or a wireless connection endpoint in case of diagnostics-over-the-air service possibilities. Hard-wired sensor values of an ECU are by nature resistant to protocol attacks. Thus, their use in an overall ECU security concept can be seen as complementary approach in order to derive a reliable decision on a safe state.

When the requirements as described above and pictured in Figure 4 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 their integrity should be guaranteed. These protection goals can be met by applying cryptographic functions, e. g., using HMAC [12]. 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, unless the network was planned with security in mind. If security was not a priority, or even considered during development, the necessary computational power and secure storage could be absent. This absence of relevant hardware could make a complete overhaul of the network necessary to improve security. Another point against cryptographic measures is that it is still possible to circumvent these functions by attacking other components, which is not possible when using hard-wired sensors for plausibility checks. In the next paragraphs we want to present a possible solution with a practical example based on the attacks by Miller and Valasek [7].

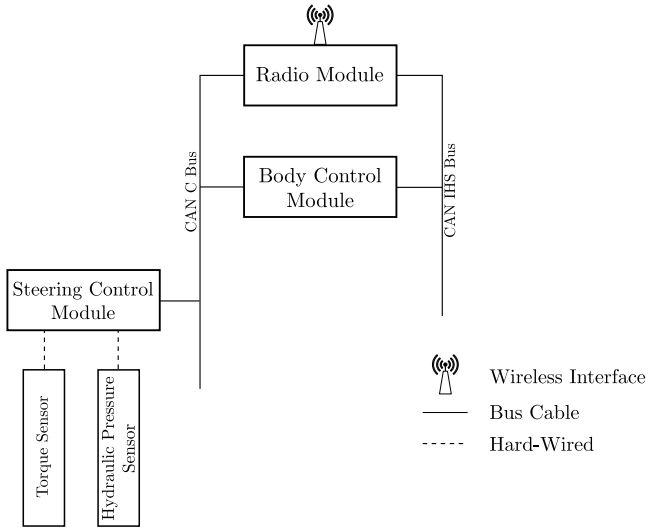

Figure 6. Sub-architecture of a Jeep Cherokee 2014 [5]

Figure 6 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 [5], [7]. The figure shows different ECUs and gateways that are interconnected by bus systems. Furthermore, some hard-wired sensors are present, 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 protection.

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, such as the rotational speed sensors for the ABS / ESC ECU. With the help of Figure 7 we want to show how an immanent signal of an ECU can be used to make a plausibility check for a requested function. This example is based on the latest hacks of Miller and Valasek. On their Jeep Cherokee [7] they spoofed the speed signal of the ABS-ECU that normally would have been used by the Steering Control Module (SCM) to make a plausibility check. In this case, the plausibility check would verify whether 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 SCM. This module also evaluates the signal of the torque sensor. With the help of the information in Figure 7 it is possible to determine the speed of a car within small limits.

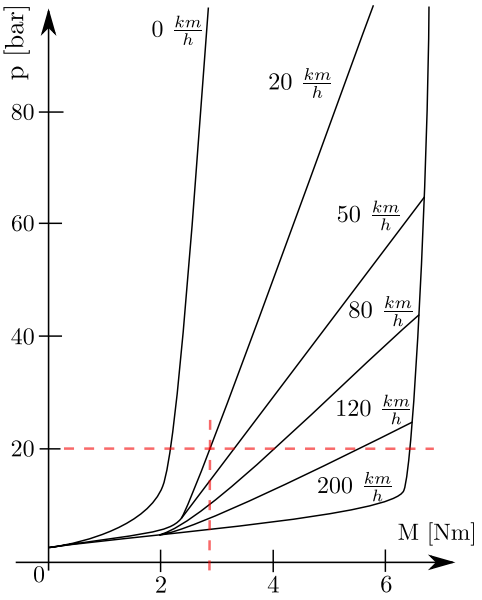

Figure 7. Plot of steering moment dependent on hydraulic pressure and vehicular speed [34]

As an example, we will show how to determine the threshold for the steering torque up to which a safe execution of safety critical functions is permissible. For easier visual evaluation we suppose a threshold of 20 kph for the safe state of 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.

A plausibility check like described here would have easily prevented the attack on the steering system as described in [7]. Our analysis indicates that such immanent signals can be found and utilized in almost any safety critical ECU in a car. We argue that signals from other ECUs should only be used, if local sensor signals are not available and if remote information is cryptographically protected. As mentioned before, input to plausibility checks has to fulfill some preconditions, namely being integrous and authentic. Only if these prerequisites are fulfilled, such bus messages can be used for plausibility checks of functions with a severity value of S 1 or above.

To conclude this section we want to present some limits for this method and ways to prevent them. The other attacks on the Jeep Cherokee [7] 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 when the driver presses the switch for the electronic parking brake. While pressing the switch the pump for the ABS / ESC system is activated and provides the pressure to engage the brakes of the car. Such a brake maneuver is comparable with 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 can be concluded for their last attack, the unintended acceleration of the car. They used the standard function to enable the 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 CAN or Ethernet, they should not be routed over gateways.

IV. Discussion

A. Automotive Systems

To demonstrate the broad applicability of our proposed method, we now discuss other examples of instances where plausibility checks with immanent signals can be used. First, we further evaluate the examples in Section III. After these examples, other published attacks on safety critical functions (lighting, engine, gearbox, brakes and suspensions [5], [8], [10], [16]) and the possibility to apply plausibility checks with ECU immanent signals are evaluated. Finally, we provide a discussion of how a our approach can also be applied to other fields, like ICSs.

We start with the engine example. There are multiple attacks published on the engine of a car [8]–[10], [16]. 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 such 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 8. The easiest signal to use is the rpm-signal of the engine. If this signal is non-zero, no service that compromises the operation of the engine should be able to execute. Services that help mechanics with diagnostics of the engine in a workshop, like reading out live data, may still be allowed. Besides the aforementioned rpm-signal, there are a lot 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 torque 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 be concluded that the car is in use and any execution of services that compromises the operation of the engine should be considered unsafe.

The second and probably most critical point of attack is the braking system, which was also the target of multiple attacks [5], [7], [8], [16]. 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 0.1 kph [36]. As soon as a non-zero 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.

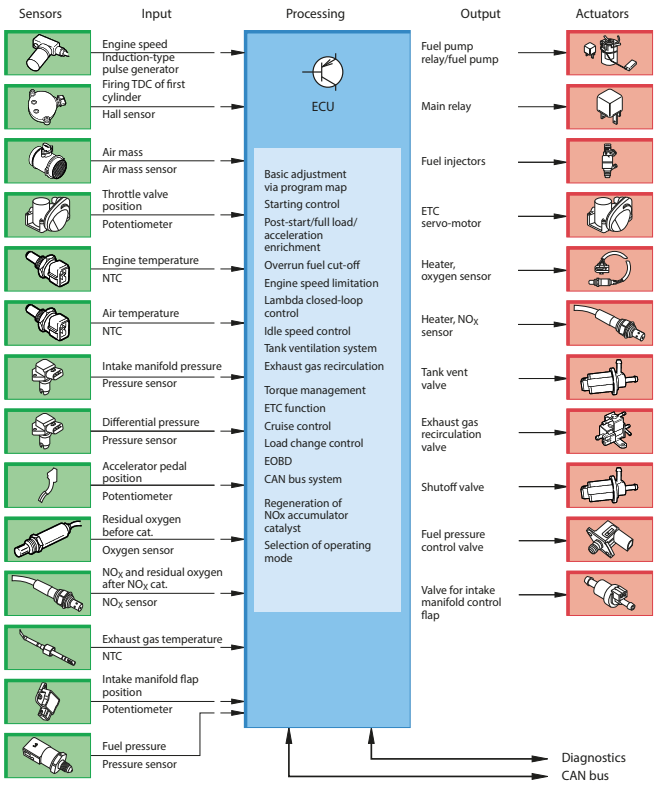

Figure 8. Engine ECU with its hard-wired sensors (green) and actuators (red) [35]

Our research also identified 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 to 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 advanced plausibility checking to ensure 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. In conclusion, the presented examples show that this method allows to safeguard every ECU responsible for lateral or longitudinal behavior of a vehicle.

This method is not limited to safeguarding the movement of the car: other safety critical aspects can be secured, like the state of the lights, this is an instance where an odd sensor signal could be used [8], [10]. Attacks on the lights of a car 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 [37]. 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.

B. *Advanced Plausibility Checks in other Domains*

We claim that a similar approach for plausibility checking can be applied to many cyber-physical systems. The security problem in such systems is often the same. Control systems rely on insecure input to trigger actions that may be put the system in danger if executed in some situations. Often, plausibility checks are applied to prevent the system from entering unsafe states, but if attackers manage to manipulate the input to the plausibility check, there is no security gain.

So, our approach on rating the trustworthiness of all input to plausibility checks and then relying only on authentic and integrity-protected input should also be applied in such systems. Examples include ICSs or Building Automation Systems (BASs).

A simple example in a BAS may be a local controller that manages the blinds of a room depending on the instructions of a central control system. Depending on weather conditions like sun or wind, the blinds may be moved up or down. Communication can use protocols like BACnet or KNX that often provide no security features.

An attacker may now inject control messages to move blinds down during strong wind, resulting in damage to the building. While the local control may also receive wind speed via the network and thus apply plausibility checks to ignore the central controller's command in case it is unsafe to lower the blinds due to strong wind, an attacker may of course also inject false wind sensor information into the network.

Our approach would now search for local sensors data that may be used for advanced plausibility checks. For example, one may add a force-sensor to the blinds, to determine whether there is a strong wind drag and then decide to move the blinds in a safe state, i. e., up.

While researchers have studied intrusion detection and prevention for ICSs [38] and BASs [39], advanced plausibility checking and the consideration of reliability of input is not well studied so far, and should be considered as a field for future research.

V. Conclusion

In this paper, we have discussed the need for advanced plausibility checks to secure automotive systems from advanced attacks that have been recently demonstrated. While basic checks are already implemented in existing vehicles, they rely on bus messages of the vehicle speed, which may be forged, e. g., by the use of jamming or spoofing techniques. As these validations are one crucial part of a defense in depth approach, a more secure implementation is crucial.

With the use of immanent signals derived from hard-wired sensors a more secure way for plausibility checks can be found. We have discussed how this approach can be used in various functions of modern cars without any need to change the ECU or communication architecture; all changes depend on improved software realizations of the plausibility check and rely only on already available sensor input. We have shown that many of the recently published attacks could have been prevented by the presented approach. As discussed with

building automation, similar approaches can be found in many other cyber-physical-systems.

For future work, we see a big potential in integrating remote and local input for plausibility checks. One should provide a trust rating for input to plausibility checks and determine plausibility of a system state based on these trust ratings. Furthermore, prospective future networks [40] are planned based on virtual servers, with this approach the hard wired sensor signals are not as easy to use as shown in this paper and has to be adapted.

REFERENCES

[1] M. Ring and R. Kriesten, "Plausibility Checks in Automotive Electronic Control Units to Enhance Safety and Security," in VEHICULAR 2016, 2016, accessed: 04.05.2017. [Online]. Available: https://thinkmind.org/download.php?articleid=vehicular_2016_1_30_30035

[2] R. N. Charette, "This Car Runs on Code," 2009, accessed: 12.02.2016. [Online]. Available: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

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

[4] SAE, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," 2016, accessed: 12.04.2016. [Online]. Available: http://standards.sae.org/wip/j3061/

[5] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," 2015, accessed: 13.03.2017. [Online]. Available: http://illmatics.com/Remote Car Hacking.pdf

[6] J. K. Weiss and S. N. Katzke, "Industrial Control System (ICS) Security: An Overview of Emerging Standards, Guidelines, and Implementation Activities." National Institute of Standards and Technology, Tech. Rep., accessed: 13.03.2017. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/ACSAC-presentation-v2.pdf

[7] C. Miller and C. Valasek, "CAN Message Injection – OG Dynamite Edition," 2016, accessed: 13.03.2017. [Online]. Available: http://illmatics.com/can message injection.pdf

[8] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," 2014, accessed: 13.03.2017. [Online]. Available: http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf/

[9] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, and Others, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," 2011.

[10] "Gehackte Mobilität," Apr. 2016, accessed: 14.06.2016. [Online]. Available: https://www.3sat.de/mediathek/?mode=play&obj=58732

[11] M. Ring, J. Dürrwang, F. Sommer, and R. Kriesten, "Survey on Vehicular Attacks – Building a Vulnerability Database," in ICVES, ser. IEEE International Conference on Vehicular Electronics and Safety (ICVES), vol. 2015. IEEE, 2015, pp. 208–212.

[12] 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, accessed: 02.09.2016. [Online]. Available: http://www.mdpi.com/2078-2489/7/3/36

[13] Keen Security Lab of Tencent, "Car Hacking Research: Remote Attack Tesla Motors," 2016, accessed: 13.03.2017. [Online]. Available: http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[14] T. Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," feb 2016, accessed: 13.03.2017. [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[15] R. Verdult, D. F. Garcia, and B. Ege, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer," Supplement to the 22nd USENIX Security Symposium (USENIX Security 13), 2015, pp. 703–718, accessed: 13.03.2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/verdult

[16] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447–462, accessed: 13.03.2017. [Online]. Available: http://dx.doi.org/10.1109/SP.2010.34

[17] R. Verdult, D. F. Garcia, and J. Balasch, "Gone in 360 Seconds: Hijacking with Hitag2," Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), 2012, pp. 237–252, accessed: 13.03.2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/verdult

[18] B. Howard, "Hack the diagnostics connector, steal yourself a BMW in 3 minutes," in ExtremeTech, jul 2012, pp. 3–7, accessed: 13.03.2017. [Online]. Available: http://www.extremetech.com/extreme/132526-hack-the-diagnostics-connector-steal-yourself-a-bmw-in-3-minutes

[19] K. Poulsen, "Hacker Disables More Than 100 Cars Remotely," Wired, 2010, accessed: 13.03.2017. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/

[20] D. Lodge, "Hacking the Mitsubishi Outlander PHEV hybrid — Pen Test Partners," 2016, accessed: 13.03.2017. [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

[21] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme," Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008, vol. 5157, 2008, pp. 203–220.

[22] T. Hoppe, "Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware: eine methodische Analyse im Spektrum von Manipulationen und Schutzkonzepten," Ph.D. dissertation, 2014.

[23] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." IACR Cryptology ePrint Archive, vol. 2011, 2011, accessed: 13.03.2017. [Online]. Available: http://dx.doi.org/10.3929/ethz-a-006708714

[24] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study," Proceedings of the 19th USENIX Conference on Security, 2010, p. 21, accessed: 13.03.2017. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929848

[25] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks – Practical examples and selected short-term countermeasures," Reliability Engineering & System Safety, vol. 96, no. 1, 2011, pp. 11–25, accessed: 13.03.2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0951832010001602

[26] D. Spaar, "Sicherheitslücken bei BMWs Connected-Drive," feb 2015, accessed: 13.03.2017. [Online]. Available: https://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html

[27] D. Bailey and M. Solnik, "Theft via text: Cars vulnerable to hack attacks," aug 2011, accessed: 13.03.2017. [Online]. Available: http://www.cbsnews.com/news/theft-via-text-cars-vulnerable-to-hack-attacks/

[28] Y. Burakova, B. Hass, L. Millar, and A. Weimerskirch, "Truck Hacking: An Experimental Analysis of the SAE J1939 Standard," 10th USENIX Workshop on Offensive Technologies (WOOT 16), aug 2016, accessed: 13.03.2017. [Online]. Available: https://www.usenix.org/conference/woot16/workshop-program/presentation/burakova

[29] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock It and Still Lose It – on the (In)Security of Automotive Remote Keyless Entry Systems," in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 2016, accessed: 13.03.2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

[30] CVSS Special Interest Group, "Common Vulnerability Scoring System," 2016, accessed: 13.03.2017. [Online]. Available: https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf https://www.first.org/cvss/calculator/3.0

[31] M. Ring, "Angriffsklassifikation," 2017, accessed: 13.03.2017. [Online]. Available: http://www.mmt.hs-karlsruhe.de/downloads/IEEM/Angriffsklassifizierung.ods

[32] ISO, "ISO 26262 Road vehicles – Functional safety," 2011.

[33] M. Dowd, J. McDonald, and J. Schuh, The art of software security assessment : identifying and preventing software vulnerabilities. Upper Saddle River, NJ: Addison-Wesley, 2007, accessed: 13.03.2017. [Online]. Available: http://www.gbv.de/dms/ilmenau/toc/515753645.pdf

[34] H. Felder, "Autoelektrik – Grundlagen- und Fachwissen," accessed: 24.08.2016. [Online]. Available: http://www.fahrzeug-elektrik.de/

[35] 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.

[36] "Raddrehzahlsensoren im Kraftfahrzeug Funktion, Diagnose, Fehlersuche." Tech. Rep., accessed: 15.08.2016. [Online]. Available: http://www.hella.com/ePaper/Raddrehzalsensoren/document.pdf

[37] "STG. Bordnetz - Control Mains Power Supply," accessed: 15.08.2016. [Online]. Available: http://www.seatforum.de/uploads/DRAFT01%5B1%5D244.jpg

[38] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in scada systems," IEEE Transactions on Industrial Informatics, vol. 7, no. 2, May 2011, pp. 179–186.

[39] M. Caselli, E. Zambon, J. Amann, R. Sommer, and F. Kargl, "Specification mining for intrusion detection in networked control systems," in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, Aug 2016, pp. 791–806. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/caselli

[40] C. Meineck, "Ethernet network-security for on-board networks," in Vector Cyber Security Symposium, 2016, accessed: 04.05.2017. [Online]. Available: https://vector.com/portal/medien/cmc/events/commercial_events/vses16/lectures/vSES16_05_Meineck.pdf