Security Hardening of Automotive Networks Through the Implementation of Attribute-Based Plausibility Checks

Marcel Rumez, Jürgen Dürrwang, Johannes Braun and Reiner Kriesten

Institute of Energy Efficient Mobility
University of Applied Sciences Karlsruhe
Germany, International University Campus 3, 76646 Bruchsal
Email: {ruma0003, duju0001, brjo0002, krre0001}@hs-karlsruhe.de

***Abstract*—Future vehicles will be more and more part of the Internet of Things (IoT), providing enhanced functionalities such as autonomous driving, cloud-based functions or car-sharing features to their customers. However, this change has fundamental consequences for automotive networks and their safeguarding against unauthorized access. Based on our own research results regarding vulnerabilities in a Pyrotechnic Control Unit (PCU) and upcoming changes in automotive network architecture, we combined plausibility checks with an access control mechanism to restrict network requests in different vehicle states to prevent the exploitation of safety-critical functions. In this publication, we present our enhanced plausibility checks, which are based on vehicle attributes and trustworthy sensors. To do so, we propose moving the checks to powerful domain controllers in future automotive network architectures. Moreover, we adapt a vulnerability scoring metric from traditional Information Technology (IT) to determine the originality of the sensor values. As a result, we are hardening the security against unauthorized access.**

Keywords–Automotive Safety and Security; Vehicular Attacks; Plausibility Checks; Vehicle Networks

I. INTRODUCTION

Modern automobiles consist of more than 50 Electronic Control Units (ECUs), which contain a total of up to 100 million lines of code to control safety-critical functionality. This fact combined with the close interconnectivity of automotive ECUs and an increasing number of interfaces to the vehicle's surroundings, broadens the attack surface of modern vehicles. The feasibility of such attacks has been investigated and already demonstrated by several groups of researchers [2] [3]. Additionally, attacks via access to the internal vehicle network that can cause life-threatening injuries have also been demonstrated in the past [4] [5].

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 [6]. Additionally, manufacturers implement the ability to execute software updates outside of car workshops, in order to fix problems within a short time [7]. These interfaces potentially provide means to remotely exploit vulnerabilities, obtain access to the in-vehicle network and control critical systems from a distance [8] [9].

Especially, with the remote exploitation of the Jeep Cherokee [8], 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. Having already proven the remote exploitability of a vehicle, they used 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), from broadcasting its own messages on the bus. This was done to enable them to send their own 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 the vehicle. For this purpose ECUs mostly use bus messages to derive the current state of the vehicle. Unfortunately, these messages are typically not protected from malicious modifications.

Our 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. The safety critical unit is a Pyrotechnic Control Unit (PCU), which offers the functionality to deploy attached airbags via vehicle diagnostics. This special use case scenario arises from the necessity of deploying airbags before a car can be crushed during its End of Life (EOL) recycling process. 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 inside a standard [10], suggesting a weak algorithm to ensure authentication. Furthermore, no fundamental plausibility checks with available hard-wired sensors have been used, which we recommended in an earlier paper [1] and expand upon in this paper so that they can be used for future automotive architectures. Thus, we consider it as reasonable that this weakness scales over several manufacturers. This vulnerability has since been submitted to the Common Vulnerabilities and Exposures database and can now be accessed under its identifier CVE-2017-14937 [11]. To determine the existence of the vulnerability in vehicles a Metasploit Hardware Bridge module was created [12]. The module can check the availability of the functionality combined with the weak algorithm in a PCU.

To prevent such issues, authenticity and integrity of bus

messages have to be ensured and therefore cryptographic methods can be applied. The AUTomotive Open System ARchitecture (AUTOSAR) members have already recognized the necessity of the mentioned security goals for future on-board communication. For this reason, they have standardized the Secure Onboard Communication (SecOC) module [13], which includes authentication mechanisms on the level of Protocol Data Units (PDUs). The specification does not recommend a specific method for creating a Message Authentication Code (MAC), but rather defines the payload of a secured PDU with a freshness value and an authenticator for protecting against replay attacks and unauthorized manipulation of the message.

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. According 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 threat scenarios, the message authenticity and integrity have to be ensured. However, channel protection alone is not sufficient if an ECU has been compromised. In this case, it is conceivable that an attacker would be able to transmit malicious payload with a valid message authenticity and integrity. Without additional checks, the receiver wouldn't be able to identify the tampered signal values of the message payload. **Solution:** Apply plausibility checks with trustworthy sensor signals as an additional security measure for cryptographic approaches to identify manipulations of received messages on ECU or domain controller level. Our **Contribution:** We present an enhanced network-based approach of attribute-based plausibility checks for future automotive networks based on our local approach for plausibility checks [1] and provide application examples to prevent two known attacks.

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 for our future work in Section V.

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) [14] 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 [15], 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 vehicles is presented by Gerlach et al. [16]. 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 [16] as meaningful. Therefore, they establish a single instance in the vehicle which collects information from any existent source in the vehicle. 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 et al. [17]. 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 already exist. As a result, our approach is applicable for a great set of functions and in particular for 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 logical steps: First, it has to be determined if the selected function can be protected by a plausibility check (see Figure 1). This is followed by a method for implementing plausibility checks depending on the vehicle's network architecture. Finally, we give two application examples, which are explained in Section III-D).

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.

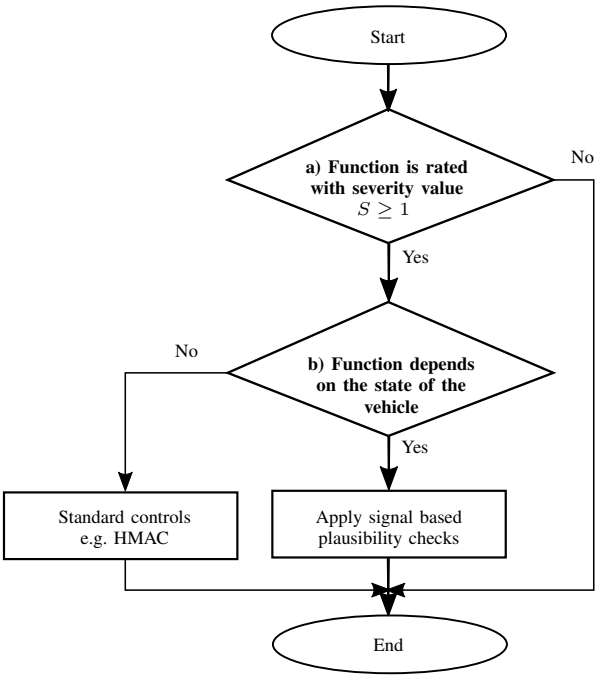

Figure 1. Methodology for applying signal based plausibility checks.

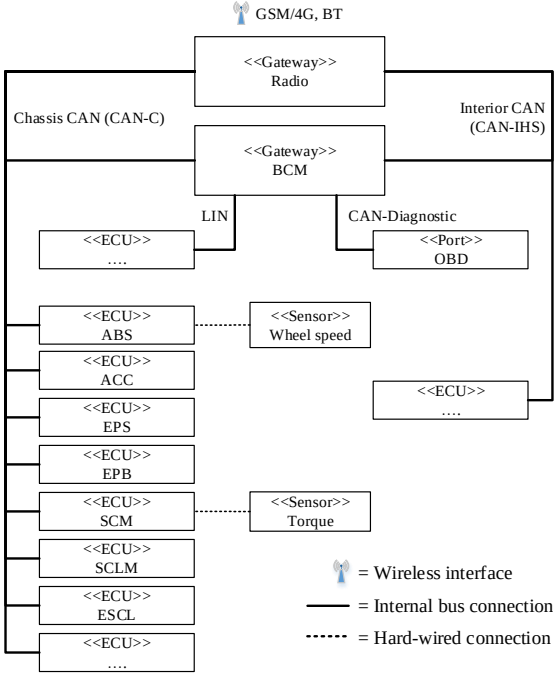

Figure 2. Part of the electrical architecture of a Jeep Cherokee 2014, based on the work of Valasek et al. [8]. As diagram notation we use the UML4PF profile extension [19].

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 must be performed. This is a demand of the functional safety standard ISO 26262 [18]. The aim of the analysis is to identify potential hazards of a function. Furthermore, a so-called Automotive Safety Integrity Level (ASIL) is calculated for each hazard based on three values. 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 S greater or equal to 1 as meaningful. In particular, a severity value of $S \geq 1$ implies injuries of vehicle occupants [18] 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, e.g., computing power, higher memory consumption, additional bus load, key management and testing of the implemented algorithms. Instead, we chose another way to check the originality of the signals indirectly 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 represents a part of the E/E architecture of a Jeep Cherokee 2014, which was the attack target of the researchers [8] [20] 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 local ECU 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 at a standstill, 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 on the bus. 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, because ECUs could verify the plausibility of the received values.

To be precise, authenticity and integrity are only ensured, if the attacker is not capable of getting access to the sensors themselves, which would require 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 [8]. This is reasonable due to the fact that an attacker would have to overcome several

physical barriers, e.g., opening the hood, ECU housing or removing the wire insulation.

C. Plausibility Checks for Future Architectures

The next generation of E/E architectures (see Figure 3) in passenger vehicles will be modified in their structure. In the future, the ECUs will be divided in different domains like powertrain, chassis or driver assistance systems. This change provides more flexibility and scalability for the manufacturers. Moreover this opens up new ways for increasing the security level. The new domain controllers are powerful with regard to their clock-rate and memory, so that Original Equipment Manufacturers (OEMs) move computing-intensive applications from legacy ECUs to the enhanced domain controllers.

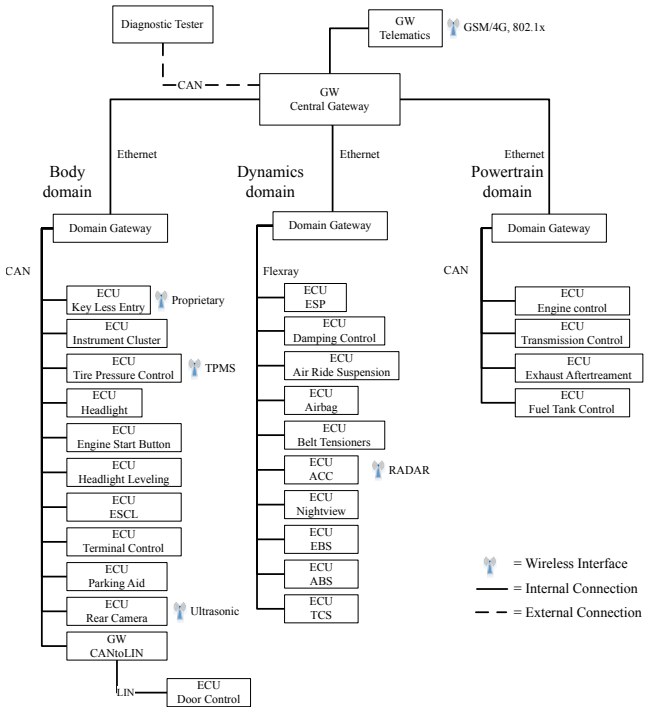

Figure 3. The next generation of E/E architectures (exemplary).

In this section we want to introduce our enhanced plausibility checks adapted to the new domain structure. Furthermore we have analyzed the latest Jeep hack [20] again and assigned the different attacks into two categories, whether the exploited function is based on diagnostic functionalities or not. The investigation has shown that five out of the seven performed attacks are based on the same approach, which sets the target ECU in Bootrom mode. This mode represents an extended diagnostic session for flash applications and requires authentication via the Security Access (SA) service. However, various research publications [21] have shown that implemented SA algorithms are often insecure. If an ECU is in Bootrom mode, it will exit the normal operation mode, e.g., stop sending CAN messages until the new firmware is successfully flashed. They exploited this functionality by setting the ECU in Bootrom mode without supplying a suitable firmware file. Therefore, the ECU is stuck in a loop and remains in this state even when the vehicle speeds up. The researcher used this attack technique for avoiding message confliction on the bus. Usually, additional injected messages typically lead to message confliction because the receiving ECU detects this anomaly and acts differently depending on the type of ECU.

Due to the fact that manufacturers move functions from single ECUs to the more powerful domain controller, we also follow this approach with our proposed plausibility checks. Furthermore, we are able to assess the trustworthiness of the request by comparing the current vehicles attributes to our security policy. In traditional IT exists a similar approach for authorization, which is called Attribute-Based-Access-Control (ABAC) [22] based on security policies in combination with different types of attributes (subject, object and environment). Generally in ABAC, the access control engine makes a decision to grant or deny any access request of a subject (entities that can perform actions on the system) to an object (function, file, variable, method) by interpreting the predefined security policy. Additionally, this model supports checks with boolean logic, e.g., "IF, THEN" statements and allows dynamic filtering due to the combination of subject attributes with environmental conditions (physical location, time, etc.).

We deem that ABAC can be adapted for an automotive Network Access Control (NAC) in combination with plausibility checks based on specific attributes, e.g., *message type, signals, device type, timing specifications*, because a lot of functions are only safety-critical when they are triggered during critical driving situations. Therefore, due to domain separation in the vehicle, we can use plausibility checks as an environmental attribute for granting access to network requests. As a result of domain controllers being connected to different networks by design, they are a prime candidate for implementing plausibility checks. For this reason, our approach is based on leveraging the most trustworthy sensor values to achieve a secure and reliable vehicle state information as an environmental attribute. To find suitable sensor values, we first have to identify all available sources, i.e., sensors in the vehicle. However, sensor sources vary wildly regarding the trustworthiness of their supplied signals.

Hence, we have decided to classify the sensor sources based on the CVSS, because this open industry standard is widely used for assessing the severity of information systems security vulnerabilities. The severity scores are based on criteria of three different metric groups [23]. We used the *Base Metrics* because their characteristics matched to the sensor sources the best. The base metric group is subdivided in *Exploitability metrics* and *Impact metrics*. For a better comprehension regarding to our sensor classification approach, we want to explain the different sub metric characteristics consecutively. The *Attack Vector (AV)* includes values how an attacker can exploit a vulnerability, e.g., is the attack target reachable via network or if physical access is needed. Furthermore, the *Attack Complexity (AC)* represents preconditions, e.g., the attacker must be man in the middle, which have to be fulfilled before an successful attack can be performed. The metric also includes the level of *Privileges Required (PR)* and whether a *User Interaction (UI)* besides an attacker is mandatory to exploit the vulnerability. The last item in this subgroup is the *Scope (S)*, which represents the ability of a vulnerability to impact other resources. The other subgroup includes the *Impact Metrics* whether an exploited vulnerability of the target component has an impact on the information assets, which are

TABLE I. Sensor Classification based on CVSS Base Metrics specification

Sensor	AV	AC	PR	UI	S	C	I	A	Score	Severity
Wheel speed	Physical	Low	High	None	Changed	None	High	High	6.5	medium
Acceleration	Adjacent	Low	High	None	Changed	None	High	High	8.1	high
Seat occupancy	Physical	Low	High	None	Changed	None	High	High	6.8	medium
ACC Radar	Network	Low	None	None	Changed	None	High	High	10	critical

specified with *Confidentiality Impact (C)*, *Integrity Impact (I)* and *Availability Impact (A)*.

We have applied the CVSS metric to some sensors of modern vehicles (see Table I) to identify the best suitable signal source for determining the current vehicle state. For our classification, we have set the scope of our investigation to determine the overall difficulty to manipulate the raw data of relevant sensors. However, as the CVSS originally comes from traditional IT some metrics have to be seen from another point of view for the automotive domain. That means, the metric PR is mapped to the required accessibility for tampering with raw sensor data from an attacker's point of view. The easiest way to manipulate raw sensor data is without any physical access or connections. In that case no specific privileges are required and the PR would be assigned with the value *None*. Furthermore, a higher degree of privileges would be, if an attacker needs any access to an physical interface, e.g., the OBD connector with partly standardized protocols, the associated PR value would be *Low*. The most difficult case from the point of view of the attacker is to manipulate raw data of in-vehicle sensors, because the protocols are mostly proprietary and the mounting position is often difficult to access. Hence, we are rating this case with the highest value (*High*). An example that some sensors can be easily manipulated from the outside has been shown in recent research with a camera mounted behind the windscreen of a car by displaying a specific graphic pattern in front of it [24]. However, to manipulate a sensor in the engine compartment an attacker would have to illegally unlock the car in order to unlock the hood latch.

To clarify the adaptation of the aforementioned metrics, the following section contains an example rating for the radar sensor of an Adaptive Cruise Control (ACC) system. We have assigned the value *Network* for the attack vector, because the sensor can be manipulated from the outside without any physical access. The attack complexity is low, because with no additional security measures, a manipulation of the sensor values can be performed very easily. Furthermore, no specific privileges or additional user interactions are required so that both metrics are rated with the value *None*. Due to the fact that an attack would have an impact on all distributed functions in the network, which are using these sensor values, we classified the scope with *Changed*. Looking now at the information assets, which are also included in the classification scheme, we deem that a successfully performed attack leads to a complete loss of the integrity as well as the availability. However, the confidentiality remains unaffected, because current in-vehicle communication is not encrypted.

The final score of the CVSS serves the purpose of comparing different signal sources that provide the same information. Furthermore, the metric provides a textual rating of the numerical score (see Table II). Based on this we have decided to set a rating limit for selecting a suitable sensor to a maximum value of 8.9 (High). For example, the score for the ACC radar sensor with the highest CVSS rating of 10.0 would be out of range to be used for sensor-based plausibility checks. Furthermore, it is recommended to select sensors with the lowest rating score, if more than one sensor for determining the same physical vehicle state is available.

In addition to finding suitable sensors for plausibility checks in domain controllers the CVSS supports another important feature in terms of rating trustworthiness in raw sensor data. A lot of research activities are focused on transmission security, e.g., protection of CAN messages. But what happens when an attacker manipulates the raw data of the corresponding sensors? Applying cryptographic measures afterwards, e.g., for the on-board communication are unable to detect this type of modified values discretely. At this time, the data is already manipulated. Before implementing complex protection mechanisms for network data, we should verify the raw sensor data first by applying plausibility checks in the first step of sensor data processing, e.g., through sensor fusion. To find which sensor should be additionally secured, the performed rating of the CVSS can be reused.

TABLE II. Qualitative Severity Rating Scale [23]

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

D. Application Example

1) Local-based Plausibility Checks: As an example, we want to discuss the latest Jeep hack [20], as well as the attack on the steering system which have been performed. 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, which explain how our approach would prevent these hacks in the future.

In the first example, the researchers set the real ECU in Bootrom Mode, causing it to stop sending messages on the bus. This step enabled 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

TABLE III. Extract of a Security Policy and corresponding Filtering rules for Domain Gateways

No.	Security Policy	Filtering rule
1	No driving operation, e.g., if an ECU is in Bootrom-Mode	Block all driving relevant requests
2	No extended diagnostic session while vehicle is moving	Block all diagnostic requests with SID 10 Sub-Function 02, if vehicle speed >= 6 mph
3	No diagnostic requests regarding End-of-life activation of pyrotechnic devices, while vehicle is moving	Block all diagnostic requests with SID 10 Sub-Function 04, if seat occupancy ! = 0 or vehicle speed >= 6 mph or seat buckle ! = 0

the velocity of the vehicle. Depending on the current speed and other parameters, the Steering Control Module (SCM) calculates the necessary 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 that 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 [20] was the application of the car's brakes. The exploited function is normally used to activate the electronic parking brake for 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 only have the information from the bus. In a case like this, where no hard-wired signal sources are available, we propose to check the feasibility of adding a hard-wired connection. The feasibility is given if the implementation effort of additional hard-wired connections is less than the implementation effort of a comparable cryptographic measure. Considering the mass-production of sensors in contrast to the effort of the selection, implementation, and testing of cryptographic measures, we consider additional hard-wired connections as less costly.

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 analyze 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.

2) Network-based Plausibility Checks: Due to the change in future automotive architectures, we want to present an enhanced approach, how local plausibility checks can be adapted in future domain controllers to harden the security at the network level. In the redesigned methodology (see Figure 4), we have created several steps to achieve sensor-based plausibility checks that could be used in this new architecture. First we have to define insecure and prohibited vehicle states for different use cases and define a security policy based on those. The policy is generally written from the point of view of the object, which conditions have to be fulfilled for granting or denying access to a subject. Table III shows such an exemplary security policy, which includes several rules depending on different vehicle state attributes. After defining the policy, it is necessary to analyze the vehicle architecture to identify possible sensors for subsequent plausibility checks. The following step of sensor classification by applying the CVSS metric is mandatory to ensure the highest resilience against tampering of the sensor values. As we have already mentioned before, we recommend to select sensors based on the rating results. Moreover, it is recommended to select sensors of different domains to increase the trustworthiness even more. The next step should also be done carefully, because the transmitted sensor data within the network, e.g., via CAN, constitutes the trust anchor for the plausibility checks and therefore must not be manipulated during the transmission between sensor source and domain controllers. In detail, the authenticity and integrity of the selected sensor values must be ensured, e.g., by using the SecOC Module of the AUTOSAR standard. By securing only the specific information that is used in the plausibility checks later on, the approach tries to be as lightweight as possible.

After these steps, the preconditions for the sensor-based plausibility checks are complete. They can be used for specific message filtering in the domain controllers by deriving fine-grained filtering rules with boolean logic from the defined security policy in combination with the selected sensor attribute values. The rules should include more than one sensor value for determining a precise vehicle state. The best-case scenario would be the integration of the two of three principle referred to the sensor sources. However, it will not always be possible to find more than one sensor source for each defined vehicle state.

At this point, we want to depict an example, how these enhanced plausibility checks can be used to complicate specific attack techniques. In the mentioned Jeep hack, Miller and Valasek have often applied the same trick by setting a specific ECU in Bootrom Mode. After that, they were able to send their own spoofed CAN messages to alter the vehicle movement. By applying our approach this method would not have been possible, because the domain controllers are able to check the actual vehicle state via a state table, e.g., if an ECU is currently in a diagnostic session, before they route inter-domain messages. As a consequence, the domain controllers block all messages for triggering driving relevant functions. Furthermore, the domain controllers are also able to verify, if specific sensor values match to the current vehicle state. Besides blocking the relevant functions we suggest to record this event for a forensic process and we further suggest to place the vehicle in fail-safe mode if the requested function is rated with a severity value $\geq$ 2. This is reasonable due

to the fact that an attack could be started with the intent to injure the passengers. The fail-safe mode allows the driver to continue using the vehicle, but encourages him to visit the workshop. The workshop is then able to search for the source of the malicious request, e.g., attached OBD devices.

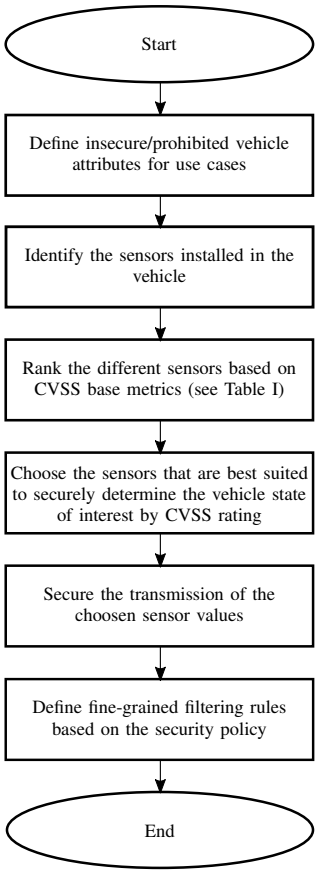

Figure 4. Process for deriving filtering rules based on trustworthy sensors and the defined security policy.

IV. Conclusion

In this publication, we proposed a new way to implement plausibility checks for automotive ECUs as well as a new approach to increase the security level in future architectures by enhanced network-based plausibility checks. Both approaches are capable to ensure that signals used for plausibility checks are resilient against replay and tampering. Based on the two approaches, we also want to divide the conclusion into two sections:

1) Local-based Plausibility Checks: The local approach uses already available information, like sensor signals, to verify function requests with the actual state of the vehicle. Due to the fact that our local approach uses no cryptography and existent information is reused, our approach tries to be as lightweight as possible to keep additional busload to a minimum. However, the approach is not suitable to secure all functions on ECUs, because at least one hard-wired sensor source should be available. Furthermore, we showed an example implementation of our plausibility approach, which is able to prevent a known attack. For this case we used hard-wired sensor signals like wheel speed sensors of the ABS to ensure the integrity of the velocity signal. The other example was focused on the electric power steering ECU.

2) Network-based Plausibility Checks: In our enhanced network-based approach for future architectures, we moved local plausibility checks to the more powerful domain controller for filtering inter-domain network traffic based on the actual vehicle state. In order to determine the actual vehicle state, we need trustworthy sensor information. For this reason, we presented a methodology to select suitable sensors by adapting the CVSS metric for an automotive severity assessment. Furthermore, we adapted a NAC approach from traditional IT, which allows dynamic and context-aware access control with security policies based on specific attributes, e.g., vehicle speed or diagnostic session. By analyzing the mentioned Jeep hack again, we examined and explained the Bootrom vulnerability, which enabled the involved researchers to exploit several functions. With the recommended state table and proposed enhanced plausibility approach, this kind of attack would not have been possible. Moreover, the vulnerability found during our own research activity, present in different ECUs that can lead to the detonation of pyrotechnic charges, would be blocked by checking the security policy in the domain controller. Due to the fact that in future architectures a variety of sensor signals will be protected by default, this leads to the assumption that the overhead for the network remains unchanged as well as that no additional wiring is required. We are currently working on evaluating the whole network traffic with respect to latencies and memory requirements to address this open gap.

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 a PCU, which is rated with a severity value of 3, we recommend that such functions should only be executable by bus messages as long as the plausibility of the request can be verified. 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.

V. Future Work

The mentioned vulnerabilities show us the necessity of additional safeguards for upcoming vehicles. In the future the amount of interconnected services will continue to increase and the vehicle can be seen as a part of the IoT. That means current network design paradigms will also change from static signal-oriented approaches to service-oriented communication for achieving more flexibility regarding to software updates and upgrades during the whole vehicle life-cycle. This will also allow to swap out functions in the cloud for reducing the computing power requirements in vehicle ECUs or for providing more customer functionalities and creates new business cases for OEMs as well as third-party providers due to the introduction of vehicle Application Programming Interfaces (APIs). This creates new challenges for the whole automotive domain with focus on communication security. Due to this fact we are working on dynamic, distributed and scalable firewall techniques to address authorization regarding service-oriented architectures. In detail we want to enhance the presented sensor-based approach with focus on an ABAC automotive

policy framework and their evaluation in respect to timing and safety constraints.

ACKNOWLEDGMENT

This work has been developed in the projects SAFE ME ASAP (reference number: 03FH011IX5) and AUTO-SIMA (reference number: 13FH006IX6) which are partly funded by the German ministry of education and research (BMBF) within the research programme ICT 2020.

REFERENCES

[1] J. Dürrwang, M. Rumez, J. Braun, and R. Kriesten, "Security Hardening with Plausibility Checks for Automotive ECUs," in VEHICULAR 2017, 2017, vol. 6, pp. 38–41. [Online]. Available: http://www.thinkmind.org/download.php?articleid=vehicular_2017_2_40_30053

[2] 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.

[3] 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

[4] 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.

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

[6] J. C. Norte, "Hacking industrial vehicles from the internet," last checked on 12.02.2018. [Online]. Available: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

[7] 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.

[8] 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

[9] 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/

[10] ISO, "ISO 26021 Road vehicles – End-of-life activation of on-board pyrotechnic devices," 2009.

[11] "CVE-2017-14937," last checked on 10.01.2018. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14937

[12] Rapid7, "Tesla Responds to Chinese Hack With a Major Security Upgrade," last checked on 07.02.2018. [Online]. Available: https://www.rapid7.com/db/modules/post/hardware/automotive/pdt

[13] AUTOSAR, "AUTOSAR 4.3.0 – Specification of Module Secure Onboard Communication," 2016.

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

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

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

[17] 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.

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

[19] 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.

[20] 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

[21] M. Ring, T. Rensen, and R. Kriesten, "Evaluation of Vehicle Diagnostics Security: Implementation of a Reproducible Security Access," Secureware, vol. 2014, 2014.

[22] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control – Definition and Considerations," 2014, last checked on 12.01.2018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

[23] CVSS Special Interest Group, "Common Vulnerability Scoring Group v3.0 - Specification Document," last checked on 08.01.2018. [Online]. Available: https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf

[24] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "Deceiving Autonomous Cars with Toxic Signs," last checked on 21.02.2018. [Online]. Available: https://arxiv.org/pdf/1802.06430.pdf