Enhanced Security Functionalities with Android Devices inside Vehicles

PhD thesis - Summary
for obtaining the Scientific Title of PhD in Engineering from
Politehnica University Timișoara
in the Field of Computer and Information Technology
by
Eng. Tudor-Sebastian Andreica
PhD Supervisor: Prof. Bogdan Groza
June, 2024

The past few decades have seen significant changes in the automotive industry with regards to electronics. The traditional mechanical components used in vehicles have gradually been replaced by software-based solutions. More and more components are now equipped with processors that run software programs, making them more versatile, such as the ability to support multiple communication protocols and provide diagnostic capabilities. Recent developments in technology have had a significant impact on the automotive industry, including the emergence of electric and hybrid vehicles, autonomous cars and connected cars. These advancements are expected to shape the future of the industry, making it more sustainable and efficient.

An automotive head unit is the central control system for in-vehicle entertainment and various other functions, such as car driving modes, activation and deactivation of Advanced Driver-Assistance Systems (ADAS) features, climate control, seat heaters and 360-degree camera display. Modern head units are the successor of the car radios which have been installed in vehicles since the 1920s for entertainment purposes. Advancements in the following decades included the introduction of 8-track tapes and cassette tapes in the 1960s, followed by the introduction of the CD player in 1984. At the beginning of the 21st century, vehicle audio systems began to accommodate modern digital storage media such as USB drives and memory cards. In addition, the scope of head units was broadened to include other functionalities such as navigation, telematics and remote diagnostics. Modern head units are equipped with high-performance CPUs, large memories and modern operating systems like Android. They feature a display screen and user interface controls, such as rotary controllers and touchscreens. Besides classic features like AM/FM radio, CD and DVD playback, the head units also support Bluetooth, Wi-Fi, cellular connectivity, GPS navigation and are used to control several car functions. Furthermore, modern head units offer advanced applications such as Apple CarPlay and Android Auto, which allow drivers to connect their smartphones to the car's infotainment system and control music, navigation and other apps running on the smartphones through the head unit's interface. Overall, the automotive head units play an important role in providing entertainment and connectivity features to both drivers and passengers, while also serving as a central control center for other important functions of the cars. However, due to their robust computational capabilities and connectivity, head units can also be used in security applications, the main topic addressed by the research in this thesis. Figure 1 shows the PNI A8020 head

Fig. 1. The PNI A8020 Head Unit (used in several research papers of the author)

unit, one of the two head units used in the experimental setups from several works included in this thesis.

Along with the benefits of the new functionalities added to modern vehicles, including the aforementioned head units, there are also side effects that need to be considered. Twenty years ago, cybersecurity was not a concern within the automotive industry. However, with the integration of new features and technology in vehicles, it has now become a critical subject as technological advancements can also open doors to various security attacks. In recent years, there have been numerous cybersecurity incidents and studies that have raised concerns and created awareness in the automotive industry. Some of these are suggested below:

- In 2015, Miller and Valasek, two cybersecurity researchers, successfully carried out a remote hack on a Jeep Cherokee. They were able to gain control of the vehicle's systems, including steering and brakes [1]. This incident, which was reported by Wired magazine, prompted a recall of 1.4 million vehicles by the manufacturer [2].
- Tesla vehicles, well-known for using some of the most advanced technology in the automotive industry, have also been the subject of several cybersecurity attacks. Nie et al., researchers from the Keen Security Lab of Tencent, were able to carry out two remote attacks on different Tesla models in 2016 [3] and 2017 [4]. They were able to compromise various in-vehicle systems, such as the Instrument Cluster (IC), Central Information Display (CID) and Gateway, gaining access to the CAN bus to inject malicious CAN messages at their will.
- According to an article published by Wired magazine [5], a study conducted by the Munich-based automobile club Allgemeiner Deutscher Automobil-Club (ADAC) evaluated the vulnerability of dozens of cars to *radio amplification attacks* that can extend the range of a driver's wireless key fob without their knowledge, allowing an attacker to open and even

start the car. The study found that 24 different vehicles from 19 different manufacturers were all susceptible to this type of attack.

The occurrence of these incidents highlights the importance of implementing robust cybersecurity measures in the automotive sector. It also emphasizes the ongoing efforts of both researchers and hackers to discover and exploit vulnerabilities in modern vehicles. Therefore, it is crucial for automobile manufacturers and suppliers to continually invest in cybersecurity research and development to keep pace with emerging threats.

Research objectives. The main objective of this thesis is to enhance vehicular security using Android devices, such as head units and smartphones, which have become ubiquitous within modern automobiles. More specifically, the thesis aims to achieve the following objectives:

1) Investigate the potential of pairing-based cryptography in automotive security applications, using both Android devices and in-vehicle units;
2) Propose a secure vehicle access control system based on identity-based and group signature schemes using modern Android smartphones;
3) Develop a smartphone-based solution for securing vehicle-to-vehicle communication using identity-based cryptography;
4) Propose efficient intrusion detection systems for the CAN bus, with a focus on deploying them on Android-based devices (such as head units or even smartphones).

Major contributions In this thesis, the use of Android devices, which offer more extensive processing and connectivity capabilities compared to regular ECUs, is explored for several vehicular security applications. The main contributions of this thesis can be summarized as follows:

1) Evaluation of several pairing-based libraries on Android devices and automotive microcontrollers, as well as a discussion of four possible automotive use cases for these cryptographic blocks [6];
2) A proposal for a secure smartphone-based vehicular access control system that relies on a mixed Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), using modern cryptographic techniques such as identity-based and group signatures to ensure security and privacy. A proof-of-concept implementation is also presented to demonstrate deployment feasibility [7];
3) Exploring the feasibility of securing vehicle-to-vehicle communication using identity-based cryptography from license plate recognition by conducting experiments for license plate reading using smartphones [8];
4) Evaluation of several binary classifiers as candidates for IDS in terms of detection accuracy on CAN and CAN-FD datasets collected from real vehicles [9];
5) A proposed IDS solution that consists of a locally installed IDS instance on Android head units in each vehicle and a centralized cloud-based IDS that processes data from multiple vehicles This solution also includes intrusion reporting with Threat Analysis and Risk Assessment (TARA) according to ISO/SAE 21434 [10].

These contributions of the author are reflected in a series of publications in relevant ISI journals and conferences. In [6], the author explores the applications of pairing-based cryptography in several automotive scenarios. The author evaluated two software libraries that contain cryptographic schemes relying on pairings, on both Android devices and in-vehicle microcontrollers. Furthermore, this work briefly discusses four automotive scenarios that could benefit from pairings as security solutions. The pairings serve as the basis for modern cryptographic techniques such as identity-based and group signatures, which were proposed by the author as

solutions to secure the smartphone-based vehicular access control system presented in [7]. The car access control system proposed in [7] relies on a role-based access control policy mixed with attributes to ensure security and privacy. The security protocol suite comprises modern cryptographic blocks, including identity-based and group signatures, as well as regular asymmetric and symmetric primitives. The work also includes a proof-of-concept implementation on Android devices that demonstrates the feasibility of the proposed solution. The protocol supports different communication technologies, such as NFC, Bluetooth and Wi-Fi, and was tested using several smartphones, aftermarket Android head units and a real-world in-vehicle controller. In [8], the author proposed a security solution for vehicle-to-vehicle communication. In this approach, license plates are used as unique identifiers to derive public keys for an identity-based scheme that enables vehicles to establish a secure communication channel. Several experiments, consisting of license plate reading using modern smartphones, were conducted to demonstrate the feasibility of the proposed approach. Additionally, the execution speed of the proposed cryptographic primitives was evaluated on the smartphones from the setup, showing that modern Android devices can manage these more demanding cryptographic algorithms. The author also contributed to the security of in-vehicle networks by proposing solutions for intrusion detection systems in [9] and [10]. In [9], the author evaluated various binary classifiers to detect intrusions and proposed a two-stage IDS for the CAN bus. The proposed IDS was evaluated in real-time using a setup consisting of automotive and Android devices, with CAN datasets collected from real vehicles. In [10], a more advanced IDS approach was proposed, designed to run on both Android head units and cloud-based applications. While the locally-installed IDS runs in each vehicle, the cloud-based IDS operates with CAN data coming from groups of vehicles and is updated with the latest types of attacks. Additionally, the classification results of the cloud-based IDS are further analyzed by an incident management team following the ISO/SAE 21434 guidelines and the outcomes are stored on the Blockchain for transparency and traceability.

Besides the previous topics which form the main body of this thesis, the author has also contributed to several other researches in the area of in-vehicle security. In [11], the author evaluated the state of uninitialized SRAM in several automotive microcontrollers. Uninitialized SRAM provides a unique pattern on each device due to physical imperfections and can be successfully exploited in security mechanisms such as fingerprinting or the extraction of cryptographic keys by using both the affinity toward some fixed state and the deviation from it. The author's research in [12] presents a low-cost solution for wireless automotive keys with rights sharing capabilities based on the MSP430 microcontroller. Another contribution is the evaluation of the security algorithms employed for intrusion detection and prevention for commercial vehicles on a high-end automotive-grade controller, as proposed in [13]. In addition, the author contributed to the research presented in [14], which proposes adversary-resilient architectures for CAN networks. The author assisted in the development of the experimental setup, which consists of an 8 ECU network, one Bus Guardian and several other components. He also implemented and evaluated the proposed algorithms on the S12 microcontrollers. Furthermore, the author supported the work from [15], which studies the influence of wiring on voltage patterns that have been commonly proposed as a source for sender identification in CAN networks.

In summary, the author has contributed to 10 papers discussing various vehicular security applications, out of which the first 5 papers form the main body of the current thesis:

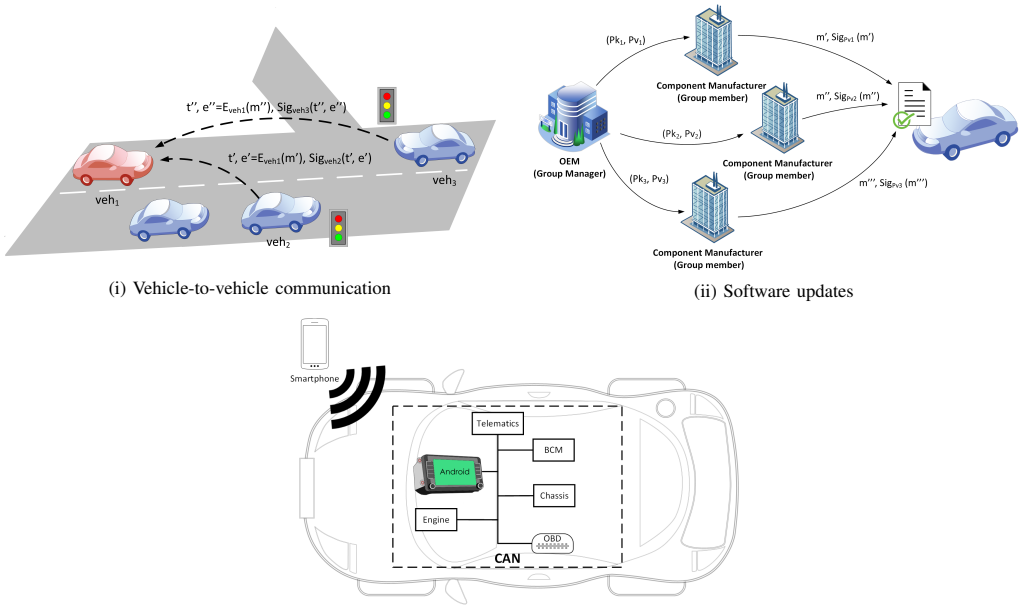
1) Tudor Andreica, Bogdan Groza, and Pal-Stefan Murvay. "Applications of Pairing-Based Cryptography on Automotive-Grade Microcontrollers," In *Computer Safety, Reliability, and Security,* pages 331–343, 2018.
2) Bogdan Groza, Tudor Andreica, Adriana Berdich, Pal-Stefan Murvay, and Eugen Horatiu

Gurban. ”PRESTvO: Privacy Enabled Smartphone Based Access to Vehicle On-Board Units,” *IEEE Access,* 8:119105–119122, 2020.

3) Tudor Andreica and Bogdan Groza. ”Secure V2V Communication with Identity-based Cryptography from License Plate Recognition,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS),* pages 366–373, 2019.
4) Tudor Andreica, Christian-Daniel Curiac, Camil Jichici, and Bogdan Groza. ”Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus,” *IEEE Access,* 10:95161–95178, 2022.
5) Tudor Andreica, Adrian Musuroi, Alfred Anistoroaei, Camil Jichici, and Bogdan Groza. ”Blockchain Integration for in-Vehicle CAN Bus Intrusion Detection Systems with ISO/SAE 21434 Compliant Reporting,” *Scientific Reports*, 14:8169, 2024.
6) Bogdan Groza, Pal-Stefan Murvay, and Tudor Andreica. ”Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers,” in *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications,* page 109–120, 2016.
7) Bogdan Groza, Tudor Andreica, and Pal-Stefan Murvay. ”Designing wireless automotive keys with rights sharing capabilities on the MSP430 microcontroller,” in *International Conference on Vehicle Technology and Intelligent Transport Systems,* 2017.
8) Camil Jichici, Bogdan Groza, Radu Ragobete, Pal-Stefan Murvay, and Tudor Andreica. ”Effective Intrusion Detection and Prevention for the Commercial Vehicle SAE J1939 CAN Bus,” *IEEE Transactions on Intelligent Transportation Systems,* 23(10):17425–17439, 2022.
9) Bogdan Groza, Lucian Popa, Tudor Andreica, Pal-Stefan Murvay, Asaf Shabtai, and Yuval Elovici. ”PanoptiCANs - Adversary-resilient Architectures for Controller Area Networks,” in *Computer Security – ESORICS 2022,* pages 658–679, 2022.
10) Lucian Popa, Camil Jichici, Tudor Andreica, Pal-Stefan Murvay and Bogdan Groza, “Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks”, *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023)*, 2023.

In comparison to traditional ECUs, Android devices have more powerful CPUs and wireless communication capabilities. This thesis highlights and demonstrates how these advanced features can enhance the security of the communication between vehicles and the external environment, particularly in scenarios such as car access control, vehicle-to-vehicle communication and the security of in-vehicle networks. A brief summary of the key findings from each chapter follows.

Chapter 2 explores four automotive scenarios that could greatly benefit from a more modern cryptographic operation, the bilinear pairing. This operation opens road to building advanced cryptographic systems, such as compact signatures, group signatures and identity-based encryptions and signatures. Compact signatures can be used for the authentication of data exchanged on in-vehicle buses, such as the CAN bus, which has a limited frame payload. Over-the-air software updates can be secured using group signatures, as vehicle components are manufactured by dozens of suppliers. In this case, the OEM and component suppliers may become part of a group in which each member can sign and authorize software patches on behalf of the group. However, only the OEM, as the group manager, can disclose the originator of a signature in case of a dispute. The security of vehicle-to-vehicle communication can be enhanced using identity-based cryptography, which removes the need for PKI. The three aforementioned automotive scenarios



(i) Vehicle-to-vehicle communication

(ii) Software updates

(iii) Security of in-vehicle networks

Fig. 2. Applications of Bilinear Pairings in the Automotive Industry

are suggested in Figure 2. Furthermore, identity-based schemes combined with group signatures can be used as a security solution for advanced car access control systems. Chapter 2 also presents experimental results in terms of runtime execution and program flash consumption for two cryptographic software libraries that use bilinear pairings. The evaluations were performed on an Android head unit, an Android smartphone and two automotive-grade controllers. The results of the pairing-based schemes were compared to the regular RSA and DSA schemes, indicating that the pairing-based schemes may require less memory for implementation in some cases, but are generally more computationally intensive. Overall, the results suggest that the pairing-based schemes are feasible to be implemented on automotive devices and can be successfully used in the security of various automotive scenarios, especially due to their additional benefits that cannot be achieved with regular public-key algorithms like DSA and RSA.

Chapter 3 presents a proposal to secure vehicle-to-vehicle communications using identity-based signatures with identities extracted from license plates. Since the Public-Key Infrastructure (PKI) is not yet universally adopted in the context of vehicle-to-vehicle communication and key management poses a significant challenge, identity-based signatures can be a good alternative to regular public-key algorithms as a security solution. The study from this chapter explores the use of identity-based signatures to establish a secure communication channel between two vehicles, using license plates as identities from which the public keys are derived. In this regard, two protocols were proposed for two different scenarios. The first scenario accounts for the situation in which two vehicles are in direct communication range, while the second scenario considers the situation in which the vehicles are in the vicinity but not in direct communication range, and the communication between the two vehicles is mediated by a common neighbor vehicle. To demonstrate the feasibility of the proposal, a proof-of-concept Android application

was developed that uses Wi-Fi Direct to simulate vehicle-to-vehicle communication and reads vehicle license plates using the smartphone's camera. Practical experiments were conducted to explore the distances and angles at which license plates can be recognized. These experiments were performed using two Samsung smartphones running Android and equipped with high-quality cameras. The setup is depicted in Figure 3. Additionally, the cryptographic algorithms

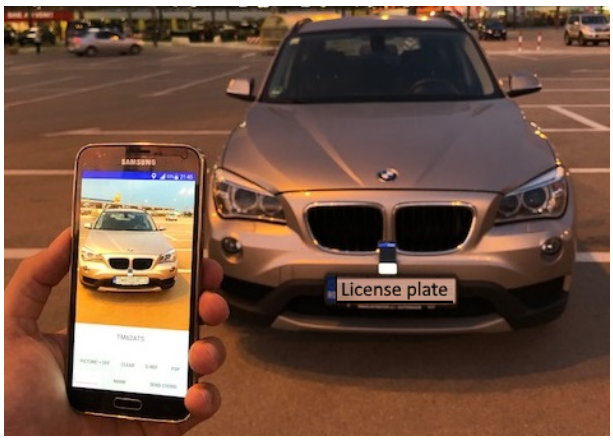


Fig. 3. The smartphones and the car from our experiments from [8]

employed in the proposed handshake protocols were evaluated on the two smartphones in terms of execution speed. The experimental results suggest that license plates can be read at a distance of up to 50 meters and at angles of up to 60 degrees in good weather conditions. The evaluation of the cryptographic functions indicates that modern smartphones can reasonably handle the identity-based primitives. However, due to the tight timing constraints of vehicle-to-vehicle communication, they can only be used to establish secure communication channels based on symmetric primitives that are executed much faster.

Chapter 4 introduces a secure car access control solution implemented on Android smartphones and head units. The proposed system employs a role-based access control policy combined with attributes, enabling users to access different functionalities of the vehicle using their Android smartphones. Access to vehicle functions is facilitated through a rights-based access control policy, similar to a file allocation table found in modern operating systems. This policy permits users to perform read, write or execute operations on various vehicle functions. The system overview is shown in Figure 4. The security and privacy goals of the proposed system are achieved using application-layer protocols that enable the use of various communication technologies such as Bluetooth, Wi-Fi and NFC. The security protocols make use of various cryptographic building blocks, including regular symmetric and asymmetric schemes as well as more advanced algorithms like group signatures and identity-based signatures. Group signatures are used to achieve privacy, as vehicles can only identify the roles accessing them, such as owner, driver, passenger or technician, but not the individual entities behind the roles. The use of identity-based signatures makes public-key management easier and more intuitive. In addition, a proof-of-concept application is presented to demonstrate the feasibility of the proposed car access control system. The procedures that facilitate the sharing of rights and the execution of functionalities were fully implemented using Bluetooth, Wi-Fi and NFC communication technologies and evaluated on various Android smartphones and head units. Furthermore, all

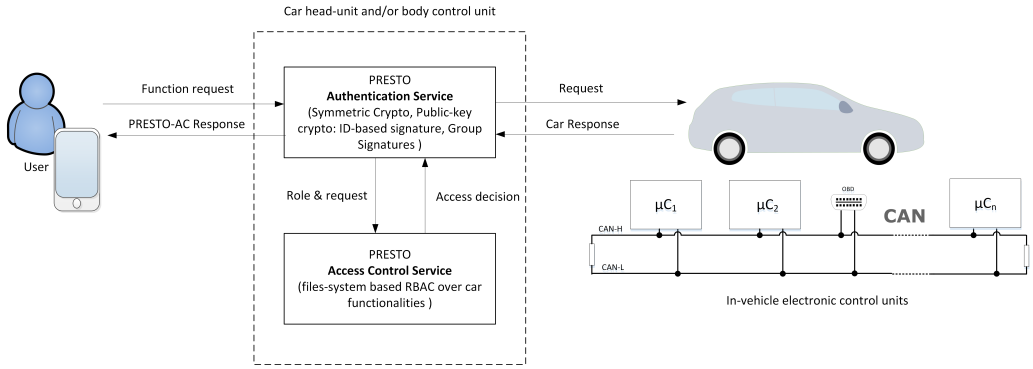
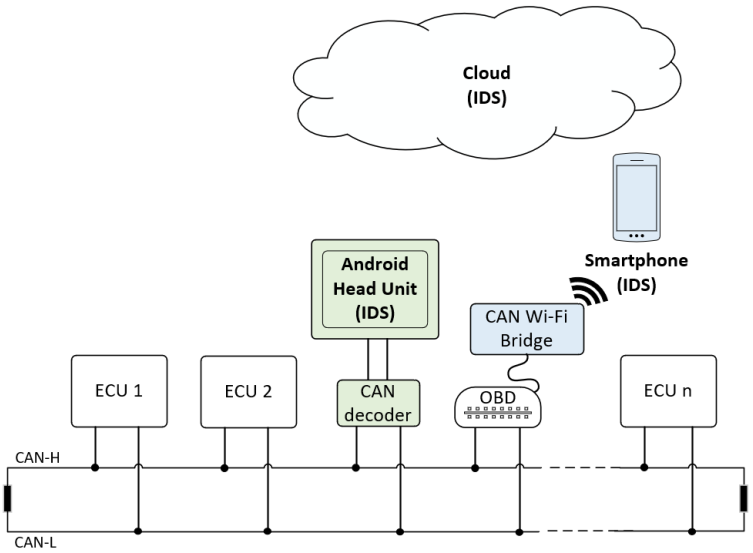


Fig. 4. System design (as illustrated in [7])

the cryptographic schemes included in the security protocols were also evaluated in terms of runtime. The results indicate that the proposed car access control solution can be practically implemented using modern Android smartphones and head units.

Chapter 5 discusses the deployment of intrusion detection systems for the CAN bus on Android head units and in-vehicle ECUs. This work proposes two setups that can be deployed in modern vehicles: one using Android head units or smartphones, and the other using regular in-vehicle controllers. These setups are illustrated in Figure 5. Specific architectures were presented for each setup, showcasing the integration of Intrusion Detection Systems (IDS) on Android devices and AUTOSAR-compliant in-vehicle ECUs. A two-stage IDS was proposed, where the first stage detects replay and flooding attacks by checking frame arrival time and CAN IDs, while the second stage employs machine learning algorithms to detect frame manipulations caused by fuzzing attacks. To evaluate the proposed IDS, CAN datasets were collected from real vehicles, which were augmented with attacks using a CANoe simulation setup. Twelve traditional machine learning algorithms were evaluated as candidates for the second stage of the proposed IDS. The first evaluation, i.e., the offline evaluation, was performed on the collected datasets using a laptop equipped with a high-performance processor. Subsequently, four algorithms out of the twelve were selected for an online (real-time) evaluation on several Android devices and automotive-grade microcontrollers using an experimental bench setup that simulates the CAN networks of real vehicles. The accuracy of the online evaluation was slightly lower than that of the offline evaluation, highlighting that there are several factors that can influence the detection accuracy of intrusion detection in real-time. This finding is extremely important since many proposals from the literature are only evaluated offline. Furthermore, the experimental results from Chapter 5 showed that the machine learning algorithms are demanding in terms of execution speed and memory requirements, making them difficult to implement on classic ECUs. However, Android devices show great potential to integrate intrusion detection systems for the CAN bus.

Chapter 6 presents an advanced IDS solution that uses Android head units, a cloud-based service, an incident response center and a Blockchain service. Figure 6 provides a high-level representation of the proposed concept. In this IDS approach, vehicles run a locally installed IDS on their head units, which reports CAN intrusion events to a cloud-based IDS operating on CAN data from multiple vehicles. The cloud-based IDS is kept up-to-date with the latest types of attacks, providing classification results that are then further analyzed by a specialized



(i) IDS on Android devices

(ii) IDS on in-vehicle controller

Fig. 5. The two addressed scenarios for intrusion detection (as proposed in [9])

incident response team. In the event of an attack, a TARA analysis is conducted following ISO/SAE 21434 guidelines and the resulting reports are stored on the Blockchain to ensure transparency and traceability of the reported incidents. The proposed IDS was designed with transfer learning capabilities, enabling attacks learned from one vehicle to also be detected on other vehicles. The IDS was evaluated on CAN datasets collected from three identical vehicles, demonstrating good accuracy in detecting intrusions. However, the accuracy was slightly lower when assessed on other vehicles than the one used for training due to deviations in CAN traffic timings between vehicles. The proposed IDS algorithm was also evaluated in terms of runtime on an Android head unit and a cloud-based VM, demonstrating that the proposed IDS algorithm can be effectively implemented on these devices. Finally, this study shows that the computational and communication capabilities of Android in-vehicle head units can be leveraged to implement advanced intrusion detection systems.

Chapter 7 serves as the conclusion of this thesis. In summary, the thesis highlights the advantages of using Android head units in vehicular security applications. The practical experiments demonstrated that these devices have powerful computational capabilities that can handle complex cryptographic schemes like group signatures and identity-based signatures, as well as demanding machine learning algorithms for intrusion detection systems. Additionally, their

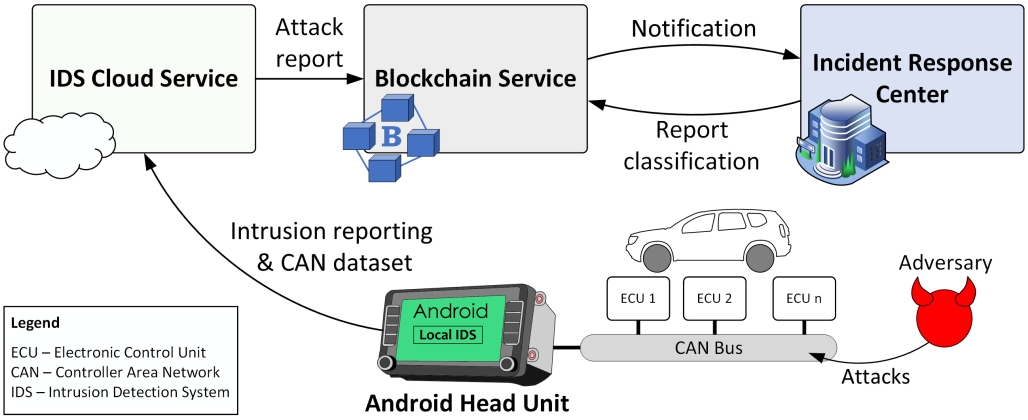


Fig. 6. Overview of the proposed intrusion reporting system (as illustrated in [10])

wireless communication capabilities make them suitable for a variety of functions, including V2V communication, car access control systems and cloud-based intrusion detection systems. Overall, the findings of this thesis suggest that Android head units could play an essential role in enhancing the security of modern vehicles.

REFERENCES

[1] A. Greenberg, "Hackers remotely kill a jeep on the highway - with me in it. www.wired.com," 2015, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[2] ——, "After jeep hack, chrysler recalls 1.4m vehicles for bug fix. www.wired.com," 2015, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[3] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," *Black Hat USA*, vol. 25, pp. 1–16, 2017.

[4] S. Nie, L. Liu, and W. Zhang, "Over-the-air: How we remotely compromised the gateway, bcm, and autopilot ecus of tesla cars," *Black Hat USA*, 2018.

[5] A. Greenberg, "Radio attack lets hackers steal 24 different car models. www.wired.com," 2016, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[6] T. Andreica, B. Groza, and P.-S. Murvay, "Applications of pairing-based cryptography on automotive-grade microcontrollers," in *Computer Safety, Reliability, and Security*, B. Gallina, A. Skavhaug, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2018, pp. 331–343.

[7] B. Groza, T. Andreica, A. Berdich, P.-S. Murvay, and E. H. Gurban, "Prestvo: Privacy enabled smartphone based access to vehicle on-board units," *IEEE Access*, vol. 8, pp. 119 105–119 122, 2020.

[8] T. Andreica and B. Groza, "Secure v2v communication with identity-based cryptography from license plate recognition," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 366–373.

[9] T. Andreica, C.-D. Curiac, C. Jichici, and B. Groza, "Android head units vs. in-vehicle ecus: Performance assessment for deploying in-vehicle intrusion detection systems for the can bus," *IEEE Access*, vol. 10, pp. 95 161–95 178, 2022.

[10] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "Blockchain integration for in-vehicle can bus intrusion detection systems with iso/sae 21434 compliant reporting," *Scientific Reports*, vol. 14, p. 8169, 2024.

[11] B. Groza, P.-S. Murvay, and T. Andreica, "Evaluating sram as source for fingerprints and randomness on automotive grade controllers," in *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications*, ser. ICETE 2016. Setubal, PRT: SCITEPRESS - Science and Technology Publications, Lda, 2016, p. 109–120. [Online]. Available: https://doi.org/10.5220/0005966401090120

[12] B. Groza, T. Andreica, and P.-S. Murvay, "Designing wireless automotive keys with rights sharing capabilities on the msp430 microcontroller," in *International Conference on Vehicle Technology and Intelligent Transport Systems*, 2017.

[13] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, "Effective intrusion detection and prevention for the commercial vehicle sae j1939 can bus," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 17 425–17 439, 2022.

[14] B. Groza, L. Popa, T. Andreica, P.-S. Murvay, A. Shabtai, and Y. Elovici, "Panopticans - adversary-resilient architectures for controller area networks," in *Computer Security – ESORICS 2022*, V. Atluri, R. Di Pietro, C. D. Jensen, and W. Meng, Eds. Cham: Springer Nature Switzerland, 2022, pp. 658–679.

[15] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, "Impact of wiring characteristics on voltage-based fingerprinting in controller area networks," in *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2023, pp. 000 231–000 236.