Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 238 (2024) 175–183

Procedia Computer Science

www.elsevier.com/locate/procedia

The 15th International Conference on Ambient Systems, Networks and Technologies (ANT)
April 23-25, 2024, Hasselt, Belgium

Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design

Akwasi Adu-Kyere[a,*], Ethiopia Nigussie[a], Jouni Isoaho[a]

[a]*Department of Computing, University of Turku, Vesilinnatie 5, 20500 Turku, Finland*

Abstract

The era of ubiquitously interconnected, intelligent, and self-driving automobiles approaches as contemporary vehicles undergo gradual enhancements in terms of security catalyzed by security analysis in various modules, algorithms, operating systems, and soft and hardware nodes. This work examines the application of a dynamic Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) in real-time using a Renault T520 Heavy-duty truck. It assesses the effectiveness of the security analysis procedure and its execution, focusing on the quality of the analysis concerning data derived from experiment sources. The validation of the security implementation adheres to a unified inbound and outbound.

Keywords: Security; Analysis; in-vehicle; IDS/IPS; Custom; inbound; outbound; Heavy-duty; Freighting; Truck;

1. Introduction

Traditional approaches to present-day security evaluation have technically revealed deficits in terms of dynamism and evolution. Trends in security-related issues in the identification and hunt for vulnerabilities currently are complicated by several facets. These facets rely on dependency, interdependency, and relationality visible in their classification. Nonetheless, security analysis via various techniques is one of the primary avenues for achieving results related to security issues. Security analysis is also a critical component of security evaluation, assessment, and improvement in automotive security [1]. With the advent of machine learning, security analysis, and assessment are boosted further in terms of potential and possibilities[15]. Therefore, the necessity of vehicles appropriated in the security dynamism landscape with Cyber-physical systems qualities [16] has made achieving security complex and challenging. Implying the requirement of self-awareness through context-awareness, hardware, and software sensing to interpret real-time decision-making further heightens the importance of security analysis. However, this form of capabilities expected

* Corresponding author. Tel.: +358 466105858 ; fax: +0-000-000-0000.
E-mail address: akwasi.adu-kyere@utu.fi

1877-0509
10.1016/j.procs.2024.06.013

from vehicles today is far from perfect concerning dynamic security of external resource management, adaptability from embedded security modules and engines, and secure gateways.

Further research is still needed to explore the dynamic nature of security environments in the vehicular context. Intelligent and smart vehicles is evolving today in the use of Mobile Long-term Evolution (LTE) services, which are not immune to vulnerabilities [7]. Data sharing using this form of communication and others via vehicular ad-hoc networks (VANETs) with the intention of cross communication [19] for example, must factor dynamic analysis operations that can compensate for onboard unit (OBU) detection capabilities. Hence, the emphasis is on the significance of real-time intrusion detection systems (IDS) and intrusion prevention systems (IPS) in vehicles.

The research concerning vehicular security is ongoing, with some emphasis relying on machine learning techniques and other methodologies [3, 17, 10]. It is recognizable that the current vehicular security environment and trends towards autonomy have underlined the need for real-time dynamic security intrusion detection, network vulnerabilities, and other in-vehicle network transactions and communications with external resources. Security issues relating to vehicles intertwine with other instances such as Safety and privacy which are directly or indirectly associated. However, they are all consolidators, and as a result, such vehicular security becomes a problem and are affected in a ripple.

1.1. Scope of this research

The scope of this study is to thoroughly investigate the security perimeter and characteristics of vehicles emphasizing IDS/IPS. It also covers the efficacy of communication and transactions between in-vehicle networks and external interacting networks. This investigation relies on a custom computing unit housed in a Heavy-duty truck (HDT) while they traverse urban areas. The experiment followed two security principles to ensure satisfactory security implementation and measures: a unified inbound and a unified outbound for all communications. These communications traverse directly through a firewall, an intrusion detection system (IDS), and an intrusion prevention system (IPS). Furthermore, these equipped systems had supplementary security customizations and enhancements for the operating system (OS). In a nutshell, the results from this specific implementation are not limited to HDTs and FTs but also vehicles employing and transacting with external resources and services.

1.2. Motivation and Contributions

The security dynamics of vehicles have been a highlighted subject in research studies, particularly in the passenger vehicle range. Additionally, numerous methodologies have been implemented and are still the subject of ongoing research, particularly concerning the parameters and attributes of in-vehicle IDS/IPS systems that enable adaptive and dynamic compliance with security threats. Therefore, the contributions are as follows:

1. Examine the application of dynamic Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in heavy-duty and freighting vehicles in real-time: To achieve this, a customized compute unit is integrated into the in-vehicle networks to actively monitor, track, and assess the security perimeter.
2. Assess the effectiveness of the security analysis procedure and its execution, focusing on the quality of the analysis concerning the real-time data derived from experiment sources: The evaluation will consider factors such as the quantity of data, filtering techniques employed, data characteristics, and security parameters.
3. Validate the security implementation to adhere to a unified inbound and outbound: This entails establishing a unidirectional flow of traffic for all external connections to and from in-vehicle networks, ensuring that data passes via a single entry and exit point before reaching the in-vehicle secure gateway. Additionally, the system should maintain accountability for all activities within the network.

The rest of this paper entails the following structure. Related works follow the introduction as Section 2. The experiment architecture follows in Section 3 with the subsequent section experiment in Section 4. It covers details on the experiment and its subsections 4.1, 4.2, and 4.3. Implementation and testing are in Section 5, followed by the experiment validation and results in Section 6. A discussion section summarizes the research impact as Section 7 and concludes in Section 8 as the conclusion and future work.

2. Related Works

Over the past few years, our society has become more aware of vulnerabilities associated with security flaws and challenges of vehicles. The benefits of the interconnectivity of vehicular evolution have also widened attack surfaces. Thereby increasing attack actors and vectors addressed using software and hardware security defensive mechanisms. Such mechanisms include white-listing [13], Trusted Execution Environments (TEEs) [4], Access control [18], Tamper-proofing [14], add-on firewalls from third-parties, and others.

In the vehicular realm of dynamic security measures centered on IDS/IPS, there has been a focus on developing and experimenting with intrusion detection systems (IDS) for vehicles. In [12], a survey of in-vehicle intrusion detection systems covers various implementations of deep learning approaches. In addition to research such as [17, 5, 6] and many others, the CAN bus protocol has received much attention for different IDS to detect abnormalities and malicious traffic on CAN frames [11].

In contrast to this work, the theoretical proposals in [1] from the literature practical undertaken in real-life scenarios. The perspective enlightens the security analysis complexities in vehicles centering the IDS/IPS as the primary security gateway. Additionally, in [8], the author the reviews automotive intrusion detections applicable to vehicles similar to the work of [2] is from intra-vehicle perspective.

3. High-Level System Architecture

The experimental configuration in this work uses a base Ubuntu OS, separated into three parts in Figure 1 to illustrate the system implementation architecture. It shows the custom compute unit management implementation, where each block represents a sub-block that visually symbolizes a process or application. It shows code-based hierarchies in color-coded markers: the system integrity checked (SIC), the network, and visualization, leaving the analysis module-based controller a primary focus.

The library block includes proprietary and implementation libraries used throughout the experiment. The proprietary libraries include hardware sensors and drivers. Custom Python libraries, customized third-party libraries, and the experimental configuration's main code are implementation libraries. The implementation libraries for remote and on-road testing sessions are in the Custom development and testing code sub-block.

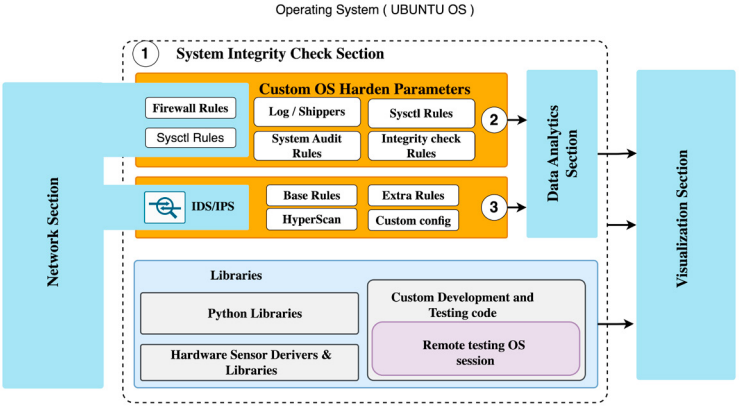


Fig. 1: High-Level System Architecture of experiment

4. Experiment

This section provides a sequential description of the entire experiment. Each stage within this section signifies a subsection and a significant achievement in the experiments. However, it does not inherently correspond to the conducted order.

4.1. Experiments Datasets

The experimental data this research utilizes and the acquisition methodology are from Figure 1. The acquisition methodologies encompass custom algorithms to intercept, modify, and analyze data in the clusters labeled from 1 to 3. Third-party log shipping agents were crucial in the visualization process, as they enable smooth analysis, data custom filtering with rules, and collection, discussed in the subsequent sections. In the software and hardware data flow, other parts of the high-level experiment system architecture components are maintained in isolation to enhance data flow efficiency and reduce delay. Other events that extensively rely on data consumption throughput were also segmented.

4.2. Evaluation metrics

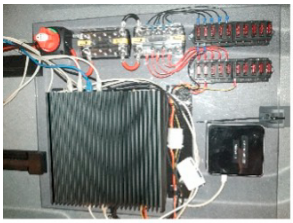
In this work, the research focuses on the examination, precise identification, and differentiation of legitimate and unauthorized traffic transactions, system calls permission, audits, and the effective optimization of algorithm implementation over a broadband connection. The experiment assessment required scaling the security implementations based on the data due to the various streams of data transfers per second and the decision-making restrictions associated with latency, performance, and security parameter overheads. The evaluation of the experiment is via analyzing diverse data acquisition influx in both the hardware and software data pipeline. As indicated in Section 4.1, the assessment algorithms are situated in the data analysis control plane determined by considering the two fundamental factors discussed in Section 1.1 on a unified entry and exit point. This measure extends its application range to include sensor traffic and further security upgrades in the system-space and user-space domains.

4.3. Experiment Details

The experimental setup comprises two phases of implementation utilizing a Renault T520 heavy-duty truck. These phases involve configuring a customized onboard hardware compute processing unit in Figure 2a and implementing software components through the experiment's high-level system architecture. The computing hardware integrated into the system is the DealComp ABOX-5200G4 compute unit. The ABOX-5200G4 has an Intel 6 Cores i7-8700T processor, boasting a 32Gb DDR4-2133 memory configuration. It features a Modem 4G with a SIM7600E-H module with an NVIDIA GeForce GTX graphics processing unit with CUDA Core support. It provides the functionality of Dual Hot Swappable SATA Storage RAID 0, 1, 5, along with a 9-48V DC Input and an operating temperature range spanning from -40 to 60°C. In addition, the device is equipped with ten Gigabit Ethernet (GbE) Local Area Network (LAN) ports, allowing for the possibility of eight Power over Ethernet (PoE) ports. It also offers compatibility with a CAN adapter, PEAK Dual CAN, IPEH-003049, WLE200NX WLAN adapter, and uBlox ZED-F9-P GPS. A further comprehensive inventory of components is also visible in the Table in Figure 2b. This figure provides a detailed overview of the power requirements and other relevant technical parameters.

5. Implementation and Testing

The implementation illustrated in Figure 3 comprises three compute units, each denoted by numerical identifiers. The computing units (CU) specified in this study were utilized extensively throughout the experiment. For example, the first compute unit is the primary element responsible for hosting the Ubuntu operating system and overseeing the allocation of all jobs. The second and third computing unit comprises the onboard computer of the Renault T520 truck's in-vehicle cabin and the Next Unit of Computing (NUC) Mini PC that facilitates external visualization. These compute units are between sensory arrays 1 and 2, indicated with short dash lines. The network traffic input and output in Figure 3 pertains to the ABOX 5200G4 used as fundamental security principles previously stated in section



(a) Custom Hardware Compute unit ABOX-5200G4

Type	Name	popular in	Explanation
Accessory	combination antenna	2	Antennas for satellite cell network and Wifi
Computing platform	Mobile PC	1	Main computing unit for data fusion and decission making
Computing platform	Mini PC	1	HMI control unit
Communication	Network switch	1	12 port network switch
Communication	Integrated Network switch	1	Integrated Network switch
Communication	Peak	2	Can to USB converter
Communication	Integrated Peak	1	Can to USB converter
Power distribution	DC/DC Converter	1	24 to 12 Vdc - 10A
Power distribution	DC/DC UPS power	1	24 to 12 Vdc - 6A
Power distribution	DC/AC Inverter	1	24 Vdc to 220 Vac inverter

(b) Configuration requirements for the ABOX-5200G4 Compute Unit

Fig. 2: Custom compute unit and technical requirement during physical installation and configuration

1.1 is the primary inbound and outbound interfaces. The existing Controller Area Network (CAN) and Ethernet interface protocols enable the establishment of connections between sensors and devices using their preferred high-speed interfaces. For sensor array 1, the module integrates a continental, brigade, and Mobileye 6 connection via the CAN-Bus protocol. The sensor array (II) also comprises a Basler 6 stereo camera, a Hokuyo sensor, and an Ouster 32-line Li-DAR. These sensors are interconnected using the Ethernet hardware protocol interface.

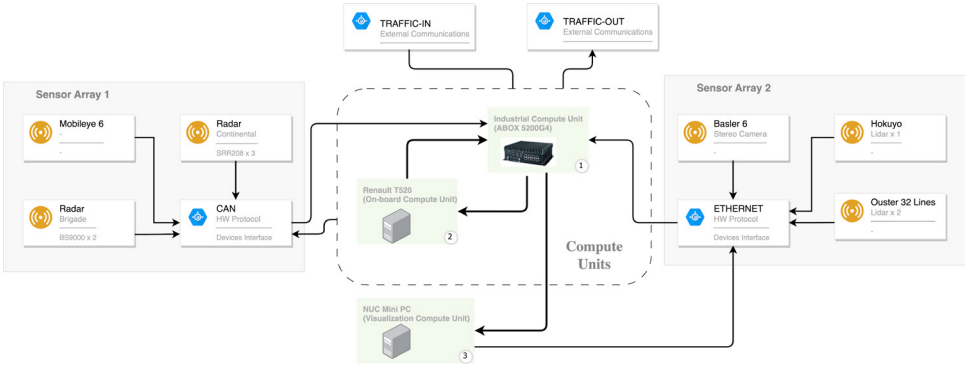


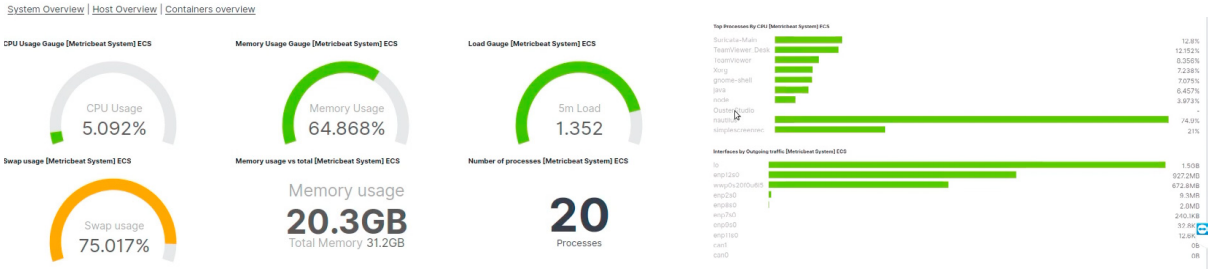
Fig. 3: Scheme for Compute Units deployed in this experiment with all other hardware connectivity

The illustration in Figure 3 demonstrates the management of data stream inputs inside the software and hardware data pipeline. The arrows originating from both hardware protocols, specifically HW Protocol, are a direct connection with the custom compute unit ABOX-5200G4. On the one hand, the bidirectional arrows from CU 1 and 2 also illustrate the dynamic interchange of information and vehicular transmission data between the custom ABOX-5200G4 and the Renault T520 onboard computer unit. The sensor array 1 CAN hardware interface protocol and the Renault computer unit (RCU-T520) communicate via an iterative symbolic link. This link enables the communication between the RCU-T520 and the custom compute unit (CCU) using the CAN protocol, represented by the arrow connecting the T520 CU to the CAN HW protocol. Therefore, ABOX-5200G4 is the tangible security protection employed in the experiment to safeguard in-vehicle nodes.

6. Validation and Results

In this session, we present the findings and results from this experiment. The results are in an outline that reflects the contributions of this work. For the first contribution on examining the application of IDS/IPS in heavy-duty and freighting vehicles. With the custom compute unit ABOX-5200G4 in 2a integrated within the HDT via DC/AC converter of 10A, the high-level system architecture in 1 is configured with the Debian Ubuntu operating system with Kernel-5.4.0.81-generic. After implementing the scheme in 3, the IDS/IPS sensors are safely deployed. Hence, ensuring the customized compute unit integration running the IDS/IPS within the in-vehicle network enables active monitoring, tracking, and assessment of the security perimeter. An illustration of feasibility is via Figure 4, which indicates overall system health metrics during a testing instance. For example, the average comparative Suricata process

CPU utilization stayed in the 12 to 15 percent range in Figure 4b while the memory consumption of the data processing contributed approximately 54.9 percent. Processes related to sensors like the OusterStudio and TeamViewer used in remote tests contributed a range approximation from 0.2 percent to 2.337 percent. In assessing the effectiveness of the security analysis procedure and its execution, observing the overall health status of the IDS/IPS became a crucial component. Its background process is also periodically examined to verify that all critical nodes, including the sensing nodes, are operational and that the rules are in effect and functional.



(a) General Health statistics sample

(b) Process specific Health statistics sample

Fig. 4: System operation Health metrics and process resource allocation

On the other hand, validating the security implementation as it adheres to a unified inbound and outbound in 3 considering factors such as the quantity of data, filtering techniques employed, data characteristics, and security parameters. The following sample from the experiment further illustrates the results of the data. The IDS/IPS block depicted in the high-level system architecture for the experiment has four functional sub-blocks responsible for executing rules and custom configurations generated during the initial installation procedure. The sub-blocks inside the network segment, as discussed before in the section on system integrity testing, depend on a GSM network connection for the purpose of external communication. The detection accuracy of the Suricata IDS/IPS was evaluated by testing the data obtained on defaults and additional rules, considering the scope of the evaluation. The reliability of the rules set, rather than the quantity of rules, was the determining factor in assessing detection accuracy. The primary criterion of concern, as determined by the vehicle's architecture, is the accessibility of in-vehicle networks, including Bluetooth, wireless connections, and physical interface ports, which serve as potential access points. Therefore, comprehensive gathered data regarding the distinct parameters and attributes, such as the individuals or devices involved in the connection and the system events linked. The provided sample in Figure 5 depicts a clear illustration from the back-end evaluation of processes matching the network traffic certificate legitimacy and associated the critical parameters such as the TLS validation.

Fig. 5: Visualization of back-end audits on critical system related security metrics

In the span of the experiment duration, the truck's operational routines generated several login attempts recorded in the time frame with their corresponding geographical locations are also in Figure 6 and 7 for root and admin users respectively. Both figures show a timeline for the specific incident with the count on the left. All these results have associating source and destination IP addresses summarized in Figure 8.

The operating system (OS) hardening parameter block comprises two blocks derived from the network section and four fundamental functional blocks at a lower level. This block contains various components, including rules, configu-

Fig. 6: Failed login access in the span of the experiment for ROOT User

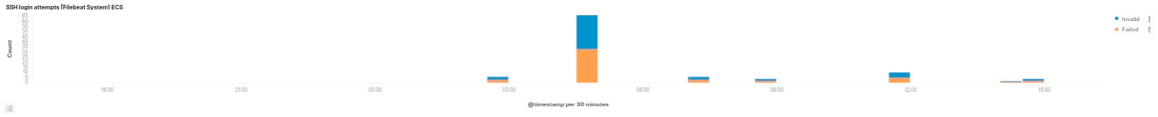


Fig. 7: Failed and invalid login attempts in the span of the experiment for Admin Users

rations, applications, and customized scripts such as firewall rules, system control rules in both the firewall domain and the system defaults domain, system audit rules, logs/log shippers, and the integrity checking process. Authentication metrics from the experiment results played a vital role in ensuring the security and integrity of in-vehicle resources, particularly in the context of services accessed through in-vehicle access points and external gateways. Consequently, the focus is on plug-and-play access nodes and interfaces. Customized rules and measures instantiation in the OS hardening parameter block yielded results as demonstrated by the outcomes presented in Figure 8. In-vehicle authentication results assessment was pivotal to the analysis outcome while simultaneously monitoring the resources linked to these procedures. The figure shows unique IP sources and destination counts with a breakdown graph on the right side beneath the destination count.

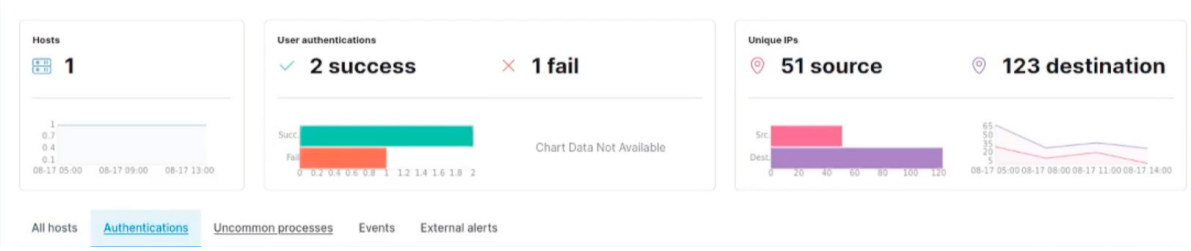


Fig. 8: System and User space Authentication summary for a specific peak in network activity

The analysis block showcases interconnection and utilizes the visualization section for presenting various outputs. The outputs include internal decision-making processes and multi-sensor readings related to security functionalities. They are from hardware and software sources, visual representations of Li-DAR Ethernet traffic scrutiny, and others. The analysis block also receives data streams from the IDS/IPS as inputs. Hence, the examination of connection instances in traffic transactions focuses on elements such as DNS, HTTP, TLS, and others as crucial components that offer significant advantages in identification. The vehicle's network deployment and its transactions, conducted using a designated communication medium (4G connection), are categorized based on their intended purpose and the level of criticality associated with each activity. Services related to the security of in-vehicle on-board infrastructures associated with hardware and software updates and remote data streams had critical attention during the analysis. An illustration showcasing a thorough breakdown of some of the discussed parameters is in Figure 9.

7. Discussion

Recent security events associated with vehicle manufacturers ranging from Toyota to Tesla have shown the significance of dynamic security implementation. Dynamic security implementation can compensate, if not eliminate, certain classes of in-vehicle intrusions and attacks from vehicular theft and malicious agenda. Inferring to the initial Jeep security breach, efforts on in-vehicular centralized IDS/IPS security dynamism have never been relevant. In this evolving and dangling security complexity landscape, the expected life cycle of vehicles is still beyond initial

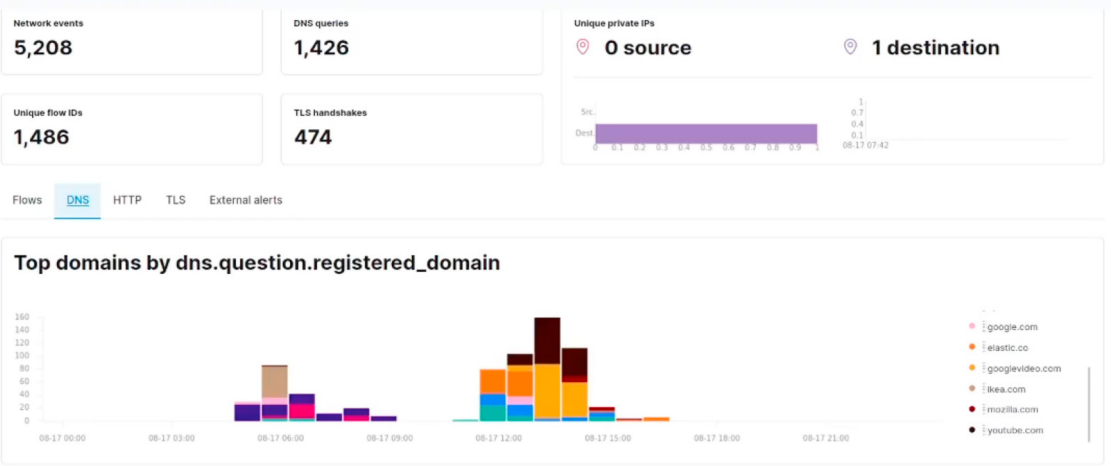


Fig. 9: DNS capture from Suricata with pre-defined rules

warranties and technical support. Hence, the security awareness and adaptiveness fully demonstrated in this experiment extend to accommodate security interconnectivity benefits. Unified inbound and outbound traffic implementation in this work restricts all communications to traverse multi-layered security. The layers include a Firewall, intrusion detection system, and intrusion prevention system for all directional traffic. Implying emphasis on the quality of analysis procedures, algorithms, and the appropriate measures and metrics to track is vital. The impact benefits security challenges such as privacy risks, data thefts, road safety and life threats, sensor manipulations, CIA violations, infotainment system escalations, and more.

In the purview of the life cycle of vehicular security and significance, data and results relating to access, detection signatures, rule optimization and customization, source and destination classifications, TLS, authentications, DNS, certificates, and others are broadly feasible in any vehicle with an external network interaction. Thus, these sample results can be a gateway for updating pre-built white-listings, black-listings, firewalls, and access control mechanisms, among many others, in a dynamic environment. In addition to the principle of quality over quantity, these findings can provide valuable insights for software-defined networks presently undergoing testing in the automotive sector.

The rationale of porting from regular IT infrastructural IDS/IPS directly to the automotive realm is complicated due to constraints and limitations associated with vehicles. However, the significant classes such as CAN, ECU, and central gateways [9] have many approaches elaborated in Section 2. This work considers these approaches from a different perspective and vehicular security on a holistic level. The security IDS/IPD is the first encounter during communications and traffic transactions in both directions. The impact also extends the sub-clusters of isolations and network segments as independent operations or as part of chained operations. Furthermore, the deployments can vary depending on the implementation strategies, but the impact and results discussed in this work are still applicable.

8. Conclusions and Future scope

The era of ubiquitously interconnected, intelligent, and self-driving automobiles gradually enhances the significance of security analysis in various modules, algorithms, operating systems, and soft and hardware nodes within in-vehicle infrastructure and networks. In this work, we thoroughly investigate the security perimeter and characteristics using a custom compute unit housed in a Renault T520 HDT. With the primary focus on examining the real-time application of a dynamic Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), the effectiveness and execution of the security analysis is critical. Hence, the data derived from pre-defined rules, audits, white-listing, access controls, and many others are deemed inadequate without dynamism and self-awareness. As demonstrated throughout this manuscript, a dynamic security inspection is a viable countermeasure to resolve dynamic security challenges.

Acknowledgements

This research was performed within the "Programmable Systems for Intelligence in Auto- mobiles" (PRYSTINE) project. PRYSTINE has received funding within the Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL JU) in collaboration with the European Union's H2020 Framework Programme and National Authorities, under Grant No. 783190.

References

[1] Adu-Kyere, A., Nigussie, E., Isoaho, J., 2023. Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability. Sensors 23, 8817. URL: https://www.mdpi.com/1424-8220/23/21/8817, doi:10.3390/s23218817.

[2] Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D., Mouzakitis, A., 2019. Intrusion detection systems for intra-vehicle networks: A review. IEEE Access 7, 21266–21289. doi:10.1109/ACCESS.2019.2894183.

[3] Desta, A.K., Ohira, S., Arai, I., Fujikawa, K., 2022. Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots. Vehicular Communications 35, 100470. URL: https://doi.org/10.1016/j.vehcom.2022.100470, doi:10.1016/j.vehcom.2022.100470.

[4] Jauernig, P., Sadeghi, A.R., Stapf, E., 2020. Trusted execution environments: Properties, applications, and challenges. IEEE Security and Privacy 18, 56–60. URL: https://ieeexplore.ieee.org/document/9041685/, doi:10.1109/MSEC.2019.2947124.

[5] Javed, A.R., Rehman, S.U., Khan, M.U., Alazab, M., Reddy, T.G., 2021. CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU. IEEE Transactions on Network Science and Engineering 8, 1456–1466. doi:10.1109/TNSE.2021.3059881.

[6] Jin, S., Chung, J.G., Xu, Y., 2021. Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network, in: 2021 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE. pp. 1–5. URL: https://ieeexplore.ieee.org/document/9401087/, doi:10.1109/ISCAS51556.2021.9401087.

[7] Kim, H., Lee, J., Lee, E., Kim, Y., 2019. Touching the untouchables: Dynamic security analysis of the lte control plane. Proceedings - IEEE Symposium on Security and Privacy 2019-May, 1153–1168. doi:10.1109/SP.2019.00038.

[8] Lampe, B., Meng, W., 2023a. Intrusion detection in the automotive domain: A comprehensive review. IEEE Communications Surveys & Tutorials 25, 2356–2426. doi:10.1109/COMST.2023.3309864.

[9] Lampe, B., Meng, W., 2023b. A survey of deep learning-based intrusion detection in automotive applications. Expert Systems with Applications 221, 119771. URL: https://www.sciencedirect.com/science/article/pii/S0957417423002725, doi:https://doi.org/10.1016/j.eswa.2023.119771.

[10] Lo, W., Alqahtani, H., Thakur, K., Almadhor, A., Chander, S., Kumar, G., 2022. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Vehicular Communications 35, 100471. URL: https://doi.org/10.1016/j.vehcom.2022.100471, doi:10.1016/j.vehcom.2022.100471.

[11] Lokman, S.F., Othman, A.T., Abu-Bakar, M.H., 2019. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking 2019, 184. URL: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1484-3, doi:10.1186/s13638-019-1484-3.

[12] Luo, F., Wang, J., Zhang, X., Jiang, Y., Li, Z., Luo, C., 2023. In-vehicle network intrusion detection systems: a systematic survey of deep learning-based approaches. PeerJ Computer Science 9, e1648. URL: https://peerj.com/articles/cs-1648, doi:10.7717/peerj-cs.1648.

[13] Pareek, H., 2012. Application Whitelisting: Approaches and Challenges. International Journal of Computer Science, Engineering and Information Technology 2, 13–18. doi:10.5121/ijcseit.2012.2502.

[14] Ramesh, M., Akruthi, S., Nandhini, K., Meena, S., Joseph Gladwin, S., Rajavel, R., 2019. Implementation of Vehicle Security System using GPS,GSM and Biometric, in: 2019 Women Institute of Technology Conference on Electrical and Computer Engineering (WITCON ECE), IEEE. pp. 71–75. URL: https://ieeexplore.ieee.org/document/9092918/, doi:10.1109/WITCONECE48374.2019.9092918.

[15] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. IEEE Access 7, 41525–41550. URL: https://ieeexplore.ieee.org/document/8681044/, doi:10.1109/ACCESS.2019.2895334.

[16] William, A., 2022. Review on security analysis in cyber physical systems. Journal of Machine and Computing 2, 134–144. URL: http://anapub.co.ke/journals/jmc/jmc_abstract/2022/volume_02_issue_03/volume2_issue3_6.html, doi:10.53759/7669/jmc202202018.

[17] Zhang, L., Ma, D., 2022. A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks. IEEE Access 10, 10852–10866. URL: https://ieeexplore.ieee.org/document/9687591/, doi:10.1109/ACCESS.2022.3145007.

[18] Zhang, Q., Zhong, H., Cui, J., Ren, L., Shi, W., 2021. AC4AV: A Flexible and Dynamic Access Control Framework for Connected and Autonomous Vehicles. IEEE Internet of Things Journal 8, 1946–1958. URL: https://ieeexplore.ieee.org/document/9169695/, doi:10.1109/JIOT.2020.3016961.

[19] Zhang, X., Chen, X., 2019. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. IEEE Access 7, 58241–58254. doi:10.1109/ACCESS.2018.2890736.