Threat Intelligence Sharing Platforms for Autonomous Vehicle Security

By Dr. Magdalena Kwiatkowska

Associate Professor of Computer Science, Warsaw University of Technology, Poland

1. Introduction

As connected, autonomous vehicles advance to market, cyber-physical security assumes profound importance. A system capable of protecting vehicle sensor data from cyber-security risks and physical-layer attacks for Intelligent Transportation Systems and Smart-City applications has been developed. The system is endowed with the capacity to render deep learning sensor data, immunize it in the time domain, recover if necessary, and run safe machine learning decision-making processes using a combination of robust deep neural networks immune to cyber-physical attacks. This cyber-physical reinforcement learning framework is designed to work on multiple connected autonomous vehicles simultaneously. Besides cybersecurity, the challenge of protecting sensor data and providing privacy through cutting-edge privacy-preserving solutions for both hardware and software are considerable factors [1, 10] of complexity in security coordination between autonomous vehicles, smart city infrastructures, IT providers, cyber-insurance companies, and central and local governance levels. These data-protection security layers include IoT data routers, permissioned blockchains, and data transformer agents [1].

The automotive industry has been rapidly evolving due to the increasing demand for autonomous vehicles. As the parts of the mesmerizing mix of inter-networked devices that make up these vehicles, the Internet of Things system has disrupted many elements of the transportation environment: the trip-preparation phase, including navigation, parking, and ride hailing, the trip phase, including infotainment and driver assistance, and the trip-end phase, including connectivity to home systems. With enriched data sources and the communications architectures supporting interconnected applications, mobility IoT systems can make an enormous positive contribution in many domains, while also raising a number

This work is licensed under CC BY-NC-SA 4.0.

of potential issues in various areas, including, and especially, safety and privacy [2]. Cybersecurity and privacy may then impact the adoption of these technologies.

1.1. Background of Autonomous Vehicles

In autonomous vehicles, AI systems are deployed within the vehicle network to facilitate vehicular connectivity and autonomy. Connected and autonomous vehicles feature powerful interconnected wireless systems designed to perform reliable data collection, processing, analytics, decision making, and transmission. However, CAVs that integrate powerful in-vehicle wireless/edge computing networks to enable perceived cognition, decision and control features, soon become vulnerable to all types of data and navigational spoofing or manipulation attacks from external and internal sources. CAVs are particularly vulnerable to driving interface attacks that can potentially disrupt or cause a change in operational parameters of systems that control the safety of the vehicle. As such, connected and autonomous vehicle systems should consider the real-time processing, validation and update of security-significant data products as an essential contribution to security measures for these systems [3].

Enabling unmanned systems with an increased level of autonomy, artificial intelligence (AI) is at the core of the fourth industrial revolution. On one hand, autonomy and AI have the potential to positively transform the society by enabling increased productivity and better, more efficient services [4]. On the other hand, these same systems also introduce new levels of risk and vulnerabilities connected to the potential for remote and local hacking and control interception that can impact system functionality and the safety of the public. As a result, system safety and security is of significant concern in the automotive space because of potential ramifications of system compromise on human life. There is an inherent threat, and risk associated with connected and autonomous vehicle (CAV) systems, therefore it is the responsibility of the entire research community—including academia, industry, and governments—to pursue research on and proactively seek out potential system shortcomings and implementations required to prevent said vulnerabilities [5].

1.2. Importance of Security in Autonomous Vehicles

The Electronic Control Units (ECUs) of autonomous vehicles are essentially computers designed to control the vehicle's components, and are equipped with a wide range of passive and active security measures to provide different levels of defense against hackers.

This work is licensed under CC BY-NC-SA 4.0.

Furthermore, research focusing on hacking such vehicles intrusively to acquire control has also been pursued for a long time. These studies demonstrated that connected and autonomous vehicles could potentially be vulnerable to cyber attacks due to various ongoing interactions with external resources, and that massive connected autonomous vehicle networks could suffer devastating attacks, potentially causing large-scale accidents or disrupting traffic systems. This paper provides a comprehensive overview of various cyber attacks, along with relevant security methods, and provides insights on the importance of security in connected and autonomous vehicles, along with ways to protect against cyber attacks in the future. [1]

Improvements in automotive technology have led to increased complexity and the use of electronic components, as well as the introduction of wireless technologies, in modern vehicles. In particular, the rise of vehicular networks and connected autonomous vehicles has introduced major security issues and vulnerabilities. [6]

1.3. Role of Threat Intelligence Sharing Platforms

A multi-stakeholder approach including automotive companies, device manufacturers, infrastructure, network operators, security companies, as well as academia and research is necessary. The platform can support actors as well as stakeholders at every level in handling threats and other relevant information such as vulnerability knowledge, generalized threat knowledge, malfunctions, and risks, enabling the provision of actionable knowledge or proximate actions [3]. Intrusions affecting the privacy of a driver or passenger (e.g., in-car location-aware services), intrusions affecting vehicle control, and insecure communication channels from the vehicle to its environment are examples of cases in which automotive-specific knowledge is vital. Providing machine-readable and context-sensitive threat information to automotive companies can help them protect their vehicles and connected infrastructure.

Increasingly sophisticated adversaries and rapidly evolving threats demand the sharing of knowledge and insights to effectively protect an increasingly online population and their infrastructure. Organizations that implement intelligence-driven security are better able to make use of data insights to enhance security operations [7]. By virtually sharing intelligence, output from different techniques can further enhance detection rates and allow more accurate recalibration of security settings to improve robustness and make solving a joint problem

This work is licensed under CC BY-NC-SA 4.0.

more feasible. In general, for connected vehicles and autonomous vehicles, open threat intelligence platform sharing should go beyond the technical boundaries of an automotive company. Cross-collaboration between automotive and network security should be enhanced to facilitate real-time threat intelligence sharing [2].

2. Fundamentals of Autonomous Vehicle Security

Figure 1 presents the interrelations between the main elements of the system responsible for ensuring autonomous vehicle security. For a specific case of an AV, the typical functions of the operating and operations platforms include managing traffic, vehicles, and energy, maintaining user mobility, and vehicle protection. The system discussed presents top-down several layers in which it can be divided in order to facilitate management of AV security in the conditions of its exploitation. It should be emphasised that the described approach uses multilayered building blocks for the heterogeneous AV networks in 5G [8]. In addition to actors such as the manufacturer, edge company and service provider, a dedicated manufacturer-focused top-down approach for managing autonomous vehicle safety systems is proposed [9].

Security plays a crucial role in the development of autonomous vehicle (AV) technology because connected and automated vehicles expose greater concerns of cyber-attacks than conventional vehicles [3]. Cars already store and process large amounts of sensitive personal data, such as locations and driving habits. The emerging trends of shared mobility services and highly personalized in-car experiences, which are largely based on the transmission and processing of customer data in the cloud, only serve to heighten these problems. Moreover, in a future of automated driving, shared mobility, and drones, the vehicle will begin to merge with the transport setting and the city's infrastructure (electric scooters, bicycles, smart signs, buildings, etc.). Secure communication between vehicles and other participants in the smart city, such as a smart infrastructure or drones, will become an important area for verification with regard to ensuring security. Presented in this section is the baseline for the linkage necessary for facilitating lossless autonomous vehicle security management.

2.1. Key Components of Autonomous Vehicle Security

Latency requirements necessitate the transfer of tasks from in-vehicle computation to the cloud. As the practice of cloud services becomes normative for CAV control, the potential for cyber-physical attack grows. An attacker intending to compromise the CAV need not tamper

This work is licensed under CC BY-NC-SA 4.0.

with a vehicle's sensors, actuators or ECUs; they can merely intervene in communication channels between vehicle and command and control servers (Srivivasarao et al., 2021). Moreover, with advances in sensor technology, it is not too far-fetched to imagine a different kind of mischief – re-engineering the physical world to give sensors misinformation.ralel to the budget request, Congress should, "expand the scope of the Data Act and the GPRA Modernization Act of 2010 to require federal agencies to shamelessly divulge designated budget and spending reports, and performance data, about services contracting." This policy would certainly set a standard of transparency in the federal government by increasing the availability of financial data (Kiman et al., 2022).

With all this new technology emerging for CAVs, it is important to consider the accompanying security implications. A CAV's security is intricately linked to its safety. While safety refers to injury prevention and accident avoidance, security is defined as protection from threats (Sparkes et al., 2021). Threats include unauthorized software updates, as well as password and key attacks. The independence and security segmentation of components is paramount in keeping the vehicle secure. Two general approaches to handling these threats are intrusion detection systems and software integrity (Chakrabarti et al., 2021). In addition to confidentiality and integrity, software updates should be authenticated. Out-of-the-box security components for an on-board unit could include a hardware security module to protect cryptographic transactions and a built-in firewall to create network security zones.

[2] [6] [10]

2.2. Challenges and Vulnerabilities

Existing software, communication and hardware security threats and their likely impact in Connected Autonomous Vehicles (CAVs) have been detailed broadly and duties and responsibilities of different stakeholders in terms of CAV security have outlined [2]. Particularly, the authors provide an insight to the security attacks that include unauthorized software updates, password and key attacks and network protocol attacks. It is found that due to lower level of security consciousness in car OEMs, less researches initiated from the manufacturer side, absence of active and fundamental security tools within the vehicle, absence of industry wide framework or legal provisions and also lack of relevant security improvements in many current vehicles, connected vehicles are vulnerable.

This work is licensed under CC BY-NC-SA 4.0.

During the last years, different vulnerabilities were found by the scientific community. The forward collision avoidance system can be deactivated through physical layer attacks in VANET, a vehicle in an autonomous driving mode can be redirected to unauthorized locations controlling the unmanned vehicle using the vehicle-to-infrastructure unit, a collision attack compromised the security of Long term Evolution (LTE) positioning in VANET and discussed device-to-device (D2D) communication of Long term Evolution Academic Research Network sequence number attacks. Apart from that, urea injection attacks based on controller area network, authentication issues in sensor networks and software defined autonomous car attacks in the Internet of Vehicles have been explored recently.

The aim of the reliable communication platform is to establish secure data exchange among connected vehicles or road side units, capable of ensuring effective and efficient traffic management and increases road safety. In doing so, the architecture assumes the presence of vehicles equipped with a long to short-range communication unit. However, beside the advantages of this approach to the increasing urban development, a major drawback is that it is particularly vulnerable to cyber-attacks. It was found that the impact on cyber security in VANETs can be higher compared to non-autonomous cars with only some communication functionality [6]. The origin and the kind of cyber-attack can be different, but the result could always be a risk to safety, privacy or economic interests. A secure data exchange can actually be shielded from cyberattacks ensuring data integrity, confidentiality, authentication, non-repudiation and availability.

3. Threat Intelligence Sharing Platforms

The effectiveness of threat intelligence sharing platform depends on the way the platform receives, processes and gives access to intelligence. In the cyber security domain, organizations are usually focused on receiving the maximum possible intelligence and that in the shortest possible time [4]. The sharing of alongside satellite technology in OTAs to collect co-location data reflecting the spatial correlation of carriers has been integrated into five automotive platforms in use both domestically and abroad. This powerful tool can help verify the performance of the autonomous integrity monitoring service of future autonomous vehicles and in combination with the integrity bounds open doors in order for AVs to delve into maximum benefit scenarios safely, with reliance on GDPR compliance. With a feature-size data set reflecting significant scenarios performance figures across the integrity boundary

This work is licensed under CC BY-NC-SA 4.0.

bounds can be determined. Sharing services form the backbone of connected cars. The trustworthiness and usefulness of these technologies can be researched in publications, research reports, blogs, etc. However, to the best of our knowledge, the concurrent performance and a stronger protocol for co-location confirmation have remained unexplored with respect to traffic safety, and integrity in general.

Continuous valiant security systems must exist to control security breaches and to protect vehicular networks. Threat intelligence sharing platforms (TISPs) play a major role in collecting, analyzing and sharing the information, resulting in effective management and control of cybercrimes [11]. Since the assets and resources of any individual or organization are very limited, it is an absolute necessity to leverage support from outside sources through collaboration like information sharing platforms. TISP organizations interpret raw threat intelligence in such a way that is useful and relevant to enterprises, proactively identifying potential cyber-attacks, identifying trends on emerging threats and sharing it with custodians on time. Numerous types of threats that already have been identified or threats that may emerge in the future, are identified in advance and necessary countermeasures are implemented for the same [12].

3.1. Definition and Functionality

Having a pathway to safety and security via route monitoring is a good practice and some proposed security practices that have an appeal toward practical implementation. In contrast, the prebuild security solutions framed by considering the intervehicular communication systems will not the overall long-term security-related issues carry me. Arguably, there are only very limited efforts that consider the comprehensive security of the AVs and those are still not adequate to cover all security-related challenges and frame can block correct intra-V security-based strategies. Therefore, this paper discusses and argues that the intravehicular security-related practices cannot manage the security-related issues those are proposed to execute with its help only. mListener interference, jamming and event-based security threats will be eliminated only by focusing the intravehicular communication architecture by/with an extended and real-time monitoring of the internal components themselves. A comprehensive intravehicular architecture will ultimately be a combination of red-black feeds with shared real-time monitoring from the subsystem's own triggers and actuators thus can efficiently trace the multiphases' integrity map [3].

This work is licensed under CC BY-NC-SA 4.0.

Autonomous vehicles (AVs) are gaining popularity and attracting significant research and development efforts. In the meantime, there has also been extensive exploration of their vulnerability to various security threats due to the interdependence between the physical capabilities and distributed artificial intelligent architecture nature of this technology [1]. The property and causality of these attacks have also been analyzed to a great extent and still continuing as the technology develops. AVs, unlike any other technology in transportation platforms, are indeed immune to a plethora of known cyber and physical attacks, only if the proposed security-enhancement proposals are implemented meticulously. That means we are currently, more concerned about the security of the AVs than any other generalized technology due to their fragility in context to the nature of the human-like-capabilities-based straightway robbery through stealing and thus; controlling such an automated machine [13].

3.2. Types of Threat Intelligence Sharing Platforms

- Unlike Connected Vehicles, Autonomous Vehicles (AVs) are driven by software and decision-making algorithms that interact with dynamic control systems and environment perception systems. Moreover, current AVs are increasingly being designed with data fusion in mind in order to properly treat Partially Observed Markov Decision Processes (POMDPs) that combine vehicle kinematics with perception modules. Communication, Software and Sensor Embedded Resistance, Verification, and Validation (TesV&V) are therefore key in the development of Hi-CAVs. Such requirements provide robustness to security and safety management systems that are frequently being applied in Integrated Safety Management Systems (ISMS). When considering Information Modelling Systems (IMS) and Blockchain, we see a new kind of technology surge where solutions providing Delta-Health status metrics allow for a continuous process within which security and safety can evolve in parallel by inheriting, evaluating, and preserving Security and Privacy metrics at all levels—bridging standards such as ISO 42010, 14001—or even being provided directly in systems—such as ISO 26262 [14].

- Cooperative advanced driver-assistance systems (C-ADAS) is the current key research focus in the field of autonomous vehicles and Intelligent Transport Systems (ITSs) due to their potential to reduce up to 90% of non-alcohol-related traffic accident injuries. Unlike traditional (distributed) ADAS systems, C-ADAS systems typically rely on data aggregators to filter out false data that could lead to misbehaviors in the vehicular environment. However, knowing who should be in charge of distributing filtered messages to which cars—and how to manage

This work is licensed under CC BY-NC-SA 4.0.

and safeguard this process—remains an open issue that we address in this paper from a cybersecurity perspective [1]. Furthermore, Cooperative Intelligent Transportation Systems (C-ITSs) with high levels of Automation (Hi-CAVs) are increasingly being considered in future car-sharing and Mobility-as-a-Service (MaaS) business models, using 5G/6G technologies to connect cars to the Internet.

3.3. Key Features and Capabilities

In the context of V2X communication, security services are required at the transport layer, such as confidentiality, integrity, and authenticity of the information, data origin, and replay protection. Furthermore, availability and non-repudiation services are also necessary. Beyond services, V2X communications also include a variety of heterogeneous technologies. Security solutions have to be designed considering all of these technologies above, covering cellular systems, or intelligent transportation systems, based on vehicular adhoc networks [1]. We envisioned a security dynamic framework that will autonomously grant security services on request via the most suitable security solution available according to the operating environment. The security services will also change through time, according to threats posed to the system. Such a framework could interact with 5G enablers to activate, and tune the security services via the underlying access networks.

Shared threat intelligence can be used to accelerate security planning and advance security capabilities, as well as a source for conducting security research [7]. In this context, a variety of threat intelligence platforms are in use. Such platforms include private information sharing communities and initiatives, such as IACD's ISAO (linked to the STIX/TAXII standards), Auto-ISAC (linked to the MISP information sharing platform), NHTSA's volunteer-based AV-AVP, and the Cybersecurity Threat Intelligence Programs launched by Siemens and Bosh. Public initiatives include services like PoliCTF in Italy, the DARPA Cyber Grand Challenge (a modern capture the flag competition), the Data Science for Good initiative by Comcast, and IARPA's Sirius. Commercial offerings include SentinelOne Ranger, Bosonit, HackerOne, and Slack. Additionally, governments offer threat sharing platforms like the National Institute of Standards and Technology (NIST) NVD, DHS's ICS-CERT, and the National Cyber Awareness System operated by the US Computer Emergency Readiness Team (US-CERT) [12].

This work is licensed under CC BY-NC-SA 4.0.

4. Case Studies

The Autonomous Vehicle (AV) domain is made of a set of autonomous vehicles and a set of communication infrastructure, all built with various protocols from differing Vendors. This diverse ecosystem indeed will result in widespread attacks and compromises on all key components. In particular, because of the vast attack surface, application and service providers potentially fall victim to large-scale attacks that can result in not only data theft, but also identity theft and drone/mobile device hijacking. Architected this way, attacks can be launched not just at the transport layer and the underlying network infrastructure but also at the application layer as well. This design refer to as Context Middleware comprises of numerous enablers that are built to support data-centric services. Enablers themselves expose a vast attack surface right from their security properties such as, secure communication, secure data transformation and encryption to their implementation architecture like secure over-the-air update of new classified service and over-the-air diagnostic monitoring and update of malicious applications that are sandboxed. In this work, present to the best of our knowledge, the first architecture, software component, and analytics platform that encompasses threat intelligence sharing and mechanisms to secure the AVs right from the assembly phase through the deployment phase and finally, in the operational phase.

Self-driving cars are expected to be one of the major means of transportation of the future. The security of autonomous vehicles is a necessary precondition for ensuring passenger safety. The transition of automobiles from user-centric systems towards driverless systems paves the way for services that are accessible via internet. This exposes these systems to a new array of security challenges. We have already witnessed some of the security lapses that have resulted in varying nature of attacks on these systems such as unauthorized software updates, password and keys been stolen. It's not just the CAVs that are vulnerable to attacks, the communication network which connects the vehicles to the backend systems have also been studied of vulnerabilities. It has also been suggested that the attacks can pass on from CAVs to backend sensors and controllers. Since this transition is still underway, it's crucial that security issues need to be addressed as early as possible. These identifies some under studied security challenges for autonomous vehicles and categorize them into their respective attack phases such as software development ('Development' phase), deployment of software onto the CAV ('Deployment' phase), software execution ('Operational' phase). Some of the high-level desiderata for studying this domain are as follows: designing a new autonomous vehicle

This work is licensed under CC BY-NC-SA 4.0.

architecture that's better equipped to offer a secure service model, propose multi-level threat intelligence sharing frameworks whose service model can be horizontally and vertically adaptable across multiple cities, provides design and implementation of the security architecture for Autonomous Vehicles (CAVs) in urban environments.

4.1. Real-world Implementations of Threat Intelligence Sharing Platforms in Autonomous Vehicles

[2] Real-world implementations of threat intelligence sharing platforms in autonomous vehicles. The original IETF definition of Threat Intelligence is "the set of data, information, and knowledge that represents to an organization, the current and historical state of assets from a cyber threat perspective". However, this definition is not enough in the context of connected and autonomous vehicles (CAVs), as it does not take into consideration the cyber-physical effect of the attacks and compromises. In automotive security, we can distinguish between two main categories of threat intelligence streams: passive and active. While the League of Legends and Dota 2 networking tools can effectively mitigate sybil black-hole DDoS attacks in CAVs, and the Google Cloud Provider can be used to combine encrypted and unencrypted data to create and evaluate novel machine learning approaches to identify unauthorised software update attacks. Furthermore, we can apply blockchain technology to secure the automotive IC supply chain.[7] The original IETF definition of Threat Intelligence is "the set of data, information, and knowledge that represents to an organization, the current and historical state of assets from a cyber threat perspective". However, this definition is not enough in the context of CAVs, as it does not take into consideration the cyber-physical effect of the attacks and compromises. As the threat landscape for these ecosystems evolves year-on-year, the same is true for the threat intelligence sharing platforms that support them; although good security practices are common throughout these systems, we propose that it is best to use a variety of strategies to secure these platforms. This includes subverting security protocols with embedded adversarial perturbations, analogous to the way in which an attack can be executed using email. Autophone can be used in the same way to automate threat modelling and exploit crafting. Conclusions on the concrete examples have led to the relevant, ongoing and future work, towards the innovation through prioritization of goal setting.

This work is licensed under CC BY-NC-SA 4.0.

5. Challenges and Future Directions

Aggregated road experimental runs under different environmental conditions were undertaken. Internal and external communication were analysed, and security logs extracted from Raspberry PI Security events generated while road tests of the system were underway. Adversarial activities detected by our AV Honeypots are grouped by using AI-based methods to create security indicators and assign Traffic Light Protocol (TLP) colours and criticality levels. AV_Security_Decision_Maker uses these threat indicators and communicates findings with a random DDOS attack to partners in the vehicle. The collected security events are processed via the embedded MITREpresents ATT&CKTM matrices with techniques. The security response of our Autonomous EV Vehicles is enhanced by combining these security responses with own situational awareness reports and road conditions. Our public technical and business use cases communicate the security decisions with different actors are Carrier (Porsche AG), Supplier (Infineon Technologies AG) and Automobile manufacturer are shown. Such future fully autonomous driving systems must satisfy the request for safe reliable and secure security surrounding. The security of the EV system is undergoing testing and several defence stack are being scored in the cyber security grades of the system.

Security, privacy, and safety of autonomous vehicle (AV) software technologies are evident challenges today [7]. It has been revealed that these system-level security properties are under attack and require immediate threat indicators in Distributed Denial of Service (DDoS) attacks. Consequently, technology providers and automobile manufacturers have shown an interest in innovative solutions that integrate data from different vehicles to detect and report adversarial activities automatically. Motivated by this actual demand, it has recently emerged as a promising direction to aggregate information in one system in vehicle [15]. Our public and open-source solution for AV security extends the Horizon 2020 SecureIoT Project procure autonomous vehicle security techniques from our reservoir of AV-Honeypots and analyse security information in a MISP sandbox. Furthermore, it operates efficiently at the edge with a device like Raspberry PI.

5.1. Current Challenges in Implementing Threat Intelligence Sharing Platforms

[16]Heterogeneous and user-specific threat intelligence, which is often stored by different organizations, tends to be difficult to consolidate and integrate, especially in the field of AV security. The APT, also known as the advanced persistent threat, tends to bypass the known security defense system. The APT threat may be undefined and unknown, and this can weigh

This work is licensed under CC BY-NC-SA 4.0.

heavily on the enterprise infrastructure. With such a vast amount of threat and AV data available, the question may arise where to begin and which data to use.[4]Because the architecture system of self-driving and connected vehicles is complicated, collaboration makes the security of, for example, embedded security systems shallow without the global understanding and involvement of connected vehicles. A number of factors, such as sharing policies, non-functional characteristics and platform performance, will impact the selection of threat data sources. Sharing policies are crucial for the success of any data sharing approach. To adopt threat intelligence, a correct security analysis of the vehicles (i.e. dynamic threat analysis on the part of the vehicle) and the appropriate integration of the collected security and threat data into the threat intelligence frames is needed.

5.2. Future Trends and Innovations

One approach to address this issue includes using digital twins to model alternative input distributions and thus identify when input data is likely to be adversarial. Perhaps as a first draft data, the model might experience the effect of the adversary and readjust the predicted values based on their experience. We identify some key challenges that will need to be addressed in future work creating any such models [6]. First, the adversary may use their own trained ML model to gain insight about countermeasures the adversarial models are producing. This analysis is dangerous because good synthetic data generators can iteratively identify countermeasures by means of neural nets trainers and GANs, improving the good data generator and allowing better and better guesses. Secondly, digital twins require significant computational resources. In future work, we plan to investigate how reasonable performance modeling can be achieved by smarter on-demand sampling in order to minimize the computational costs of mantaining a multi-dimensional digital twin.

In the last few years, the V2V and V2I communication paradigms have emerged to help CAVs to respond to safety, environment, and economy requirements through better and lower energy consumption, reduced travel time, and enhanced safety compared to traditional vehicles. These new technologies are primarily motivated to provide CAVs with real-time data about road conditions by enabling vehicles to communicate safety information with the traffic light controllers, road management systems, and other vehicles at a range of 300–500m [7]. This environment will require predicting and detecting data attacks before systems in these CAVs may analyze wrong data as if they are real. In particular, future CAVs will be

This work is licensed under CC BY-NC-SA 4.0.

designed to proactively block false data source or use missing data imputation techniques rather than simply reactively responding to detected attacks on the sensor data.

6. Conclusion

Our survey explains threats to critical functions in AVs. We operationalize the definition of "critical functions" using engine control units (ECUs) from a well-known real-world AV. A layer model of potential threats to critical functions is introduced, to classify abstraction levels. We conclude Active threats against critical functions are rare but possible [17]. Instead, sensors are attacked, especially vision-based systems. This aligns with all survey papers, as the sensors in these threats typically affect critical functions either directly (sensing and perception) or indirectly (control). Given this, we refer to all layer models as cyber-physical (see Table 3). Our classified threats show that, in security terms, the deployed vehicles and their drivers are not ready to handle the adversarial threats to these cyber-physical systems. For attackers, the operational costs are low if quick gains are possible. This suggests that vehicles with larger potential payback may be attacked. Consequently, the privacy issue increases, making intrusions less explicit, as indicated by "weak interceptions" [18].

Autonomous vehicles (AVs) represent the future of the automotive industry. As vehicles become more self-reliant, humans receive more responsibilities, dedicating more time to entertainment. Although current AVs rely on existing technologies and architecture with non-vital operational control, an AV is a complex robot, comparable to an airplane. Airplane architects have decades of experience designing secure systems, where life-critical decisions are made by artificial intelligence, in an electrically hostile environment. Thus, research is needed on how different components can trust each other, from sensing and perception to action planning and command [6].

6.1. Summary of Key Findings

Most of the issues of risks faced by manufacturers during in the stage of system development and verification which cause determination and implementation of security functions tend to be understood mainly from "vehicle-side viewpoint". As an initial step to respond to the arrival of highly autonomous vehicles, it is necessary to induce "seeing and solving problems" through a wide range of viewpoints including threats attributed to the edges of the system. This paper has conducted a risk analysis study of highly autonomous vehicles whose details had not yet been clarified as well as the process of generating feasible solutions [3]. Connected

This work is licensed under CC BY-NC-SA 4.0.

and Autonomous Vehicles (CAVs) need to physically communicate with each other cooperatively and then collaboratively provide operational support services. Many arrays of CAVs bring improvements in reliability, cost, and personal safety, a novel global communication network concerning CAVs needs to be able to provide privacy and security so that the main mission of such an ecosystem in the transportation sector can be effectively and efficiently achieved. Improper design of security and privacy services may lead to unintended consequences, exposing vulnerabilities to adversaries. Without a comprehensive cybersecurity system, it will be difficult to realize a completely secure and safe CAV ecosystem.

The security of Connected and Autonomous Vehicles (CAVs) is crucial - both for passenger and public safety and for the secure digital economy. As CAVs evolve to highly autonomous vehicles, their sensors, hardware, software, and data are accordingly diversified and sophisticated, and the attack surface is increasing as they become more advanced [2]. The impact of incidents getting realized and implemented is constantly expanding - across not only the conventional cyberattack figures, like the confirmation of "Warning display not operation" and stealing signals, but also a plethora of new cyberattack scenarios including "detection of diversion", "theft of images of surrounding environment", and "remote control of CAVs".

6.2. Importance of Threat Intelligence Sharing Platforms in Autonomous Vehicle Security

Unfortunately, those organizations failed to prompt the vehicular anomaly data collectively and confidentially from the surveillance industry due to their lacking high intelligent autonomous vehicles in the city. The autonomous vehicle stealing or damaging incidents have alerted both the manufacturers and the connected vehicles owner also. It is still unclear that what the industrial solution at the availability level will be until artificial intelligent super intelligent level has been reached. It's hard to say that how much efforts would be made to explore the security measures for the secure digital infrastructure. Therefore, it is still important to evaluate the security mechanisms, from the start of the system development cycle up to the disposal level. It is assumed that there are two types of vehicular security risks can be preserved from the malicious intelligent vehicular attacks. On common and high level, two types of system service features are going to be locked. In metric 2, the sharing platform ensures that the security incidents either are unknown, or the sharing is administratively

This work is licensed under CC BY-NC-SA 4.0.

allowed, but the security analyst may be recommended with other solutions. At last, the confidentiality of this vehicle knowledge and deals with new improved measures has been protected.

Even well-known machine learning algorithms are difficult to distinguish the reliable input data from the corrupted data due to the strong bilateral logical relationship between truly and falsely labelled data. Because of that, a comprehensive security measure should be taken to protect the received vehicular data, guarantee the safety of the driving domain, and enhance the lost services by maximizing the available valid services. Threat intelligence sharing platform should be established for the security and privacy of vehicles in the distributed infrastructure. It is a high-level goal of that that all vehicles have already been protected against known or unknown security and privacy incursion and ensured data security priorities. Most of AV developers are busy in collecting, analysing and storing data sets. Consequently, it has become more difficult for the stakeholders of different levels to share and gain knowledge to secure the urban roads efficiently and safely. After testing the robustness of the machine learning models, there are some associations and domains have been established to promote the security of knowledge and services, including machine learning, autonomous vehicle and CKAN: tools for data accessible by everyone and goal [19].

[1] The security of autonomous vehicle (AV) ecosystem is crucial for the well-being of passengers and other participants of the Intelligent Transportation System (ITS). Recently, researchers have discovered that many types of security vulnerabilities in terms of hardware, software, transportation services and data can directly or indirectly damage the vehicular security services. Consequently, both the physical and cyber layers of the vehicular platform can be impacted. Conventional solutions are generally about the jamming the V2V [vehicle to vehicle] communication links or defeating the internal security measures. However, the interconnected relationship among the internal sensors, data processing units, control systems and communication devices are overlooked. In the validation process, it is important to assess the security attribute of the incoming data. At the same time, it is also important to make sure that the control signal has been successfully sent to the physical actuators [2].

7. References

This work is licensed under CC BY-NC-SA 4.0.

[1] Tatineni, Sumanth. "Exploring the Challenges and Prospects in Data Science and Information Professions." *International Journal of Management (IJM)* 12.2 (2021): 1009-1014.

[2] Vemori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.

[3] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]

[4] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov

[5] J. R. V. Solaas, N. Tuptuk, and E. Mariconti, "Systematic Review: Anomaly Detection in Connected and Autonomous Vehicles," 2024. [PDF]

[6] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]

[7] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]

[8] O. M. Crook, L. Gatto, and P. D. W. Kirk, "Fast approximate inference for variable selection in Dirichlet process mixtures, with an application to pan-cancer proteomics," 2018. [PDF]

[9] A. Chattopadhyay and K. Y. Lam, "Autonomous Vehicle: Security by Design," 2018. [PDF]

[10] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]

[11] P. Malhotra, Y. Singh, P. Anand, D. Kumar Bangotra et al., "Internet of Things: Evolution, Concerns and Security Challenges," 2021. ncbi.nlm.nih.gov

[12] A. Dinesh Kumar, K. Naga Renu Chebrolu, V. R, and S. KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities," 2018. [PDF]

[13] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov

This work is licensed under CC BY-NC-SA 4.0.

[14] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov

[15] M. Dibaei, X. Zheng, K. Jiang, S. Maric et al., "An Overview of Attacks and Defences on Intelligent Connected Vehicles," 2019. [PDF]

[16] L. Liu, S. Lu, R. Zhong, B. Wu et al., "Computing Systems for Autonomous Driving: State-of-the-Art and Challenges," 2020. [PDF]

[17] J. N. Brewer and G. Dimitoglou, "Evaluation of Attack Vectors and Risks in Automobiles and Road Infrastructure," 2020. [PDF]

[18] H. Rivera-Rodriguez and R. Jauregui, "On the electrostatic interactions involving long-range Rydberg molecules," 2021. [PDF]

[19] M. Bakhtina and R. Matulevičius, "Information Security Analysis in the Passenger-Autonomous Vehicle Interaction," 2021. [PDF]

This work is licensed under CC BY-NC-SA 4.0.