Cognitive Threat Analysis Frameworks for Autonomous Vehicle Cybersecurity

By Dr. Jure Žužemič

Professor of Computer Science, University of Ljubljana, Slovenia

1. Introduction to Autonomous Vehicles and Cybersecurity

In the future, CAV systems' architecture will be more complex and will require more attention from the designers in terms of safety and security. How to overcome these challenges and still keep novel features equally available to vehicle users, and how to protect the digital world together with the physical world, are the main government-drawn paths that are good research subjects. In this study [1], authors emphasize the importance of combining cognitive systems' approaches with vehicle network security, paving the way for security development at the vehicle level. Cybersecurity models at the edge of things in the vicinity of the driver and passengers should be as close to "impossible to break" as possible. In this paper, these models' cognitive, vehicle-level cyber security proposals are established considering the potential future features that are built step by step and assist the driver, or replace him controlling the vehicle in the future.

Improvements in the automotive industry, along with advancements in wireless communication technology, have enabled us to move to the era of Internet of Vehicles (IoV). This innovation is expected to considerably improve road safety, traffic efficiency, environmental improvement, and passenger security. In the evolution path of connected, autonomous, and electric vehicles (CAEV), the vehicle components are connected wirelessly, or are controlled through the air. This means that a whole new avenue opened for notorious cyber attacks. For example, a nefarious actor could intrude into a vehicle remotely, tamper with its functions, and gain ownership. One study [2] explains the possible attacks and their countermeasures induced by wireless communication systems in the connected autonomous vehicle (CAV) context. In terms of wireless communication protocols, advancements in low latency communication protocols (5G, Wi-Fi 6, etc.) are contributing to more security breaches. The process of detecting cyber attacks and protecting CAV components are still

challenging with these advanced protocols. Another study [3] describes the details about the vehicle network and the identified attacks on available and proposed communication channels, explains the countermeasures including AI-based data fusion for multi-layered network communication.

1.1. Overview of Autonomous Vehicles

Considerable work has been conducted in this vein to survey both extant vulnerabilities and attack surfaces, highlighting clear trends in the associated hacking risk landscape and historical evolved testing hardware and software exploits. A brief survey conducted in March, 2021 focused on control systems, attacks conducted by third parties and on information broadcast to and received by these vehicles - this survey also included a section on preventative measures that, accompanied by a substantial host of broader surveys on the subject of autonomous vehicles, has used predominantly publicly available sources covering the most up to date and vast white, black and grey literature. Significant vulnerabilities and threats which can be attacked or exploited within connected and autonomous cars have been identified in this research, summarising potential safeguards and measures. Technologies have been researched which can identify and mitigate different threats for autonomous vehicles. An analysis from this research has been used to apprehend the landscape of potential attack vectors as well as proposing up to date dynamic testing solutions.

[4] [3]Autonomous vehicles, or high-automated vehicles, are one of the most anticipated future technologies and have the potential to revolutionise global transport systems. As vehicles are complex systems integrating many sensors, control units (e.g. park assist/table, braking system) and communication modules which are able to conduct movement and spatial awareness based tasks without human intervention, they also face many potential security threats due to these embedded threat vectors. Consequently, the dissemination and implicit reliance in these technologies means that a universal and deep understanding of the extant digital and consequent physical threats is mandatory for the safety of the general public.

2. The Need for Cognitive Threat Analysis Frameworks

Fully connected autonomous vehicles are a new concept with great promise for the future. As every new invention comes with its own challenges, the world of connected autonomous

vehicles brings operational, functional and performance challenges. Securing vehicles from potential cyber attacks according to the stringent requirement of available threat-detection subsystems' implementation cost is one of the identifiable security challenges associated with fully connected autonomous vehicles. In this study, security threats were initially identified and categorized based on their assets, resources and penetration testing histories. The findings of the study can be used to secure the automotive environment from advanced security threats. This work will encourage the automotive industry to pursue non-social (attacker-driven) vehicle security threat analysis for future connected autonomous vehicle developments and tests. [5]

The automotive industry is on the brink of making driverless cars a reality. Security concerns given the advances in vehicle-to-everything and the adoption of software-defined electronics in vehicles mandates that the cybersecurity psychology of a connected autonomous vehicle (CAV) encompasses an aggressive and a defensive security posture. Current efforts to secure CAVs have largely been confined to secure model-based design, limited capability hardware security modules and reactive security mechanisms for critical system components such as the electronic powertrain and the automotive grid communication (Cyber-TAs) systems. Given the rapid rate of change in the connectedness, electronic content and autonomy, attempts to secure CAVs by focusing on individual vehicle components and features that are integrated potentially leave open a lightly less secure attack surface within the CAV. [4]

2.1. Challenges in Autonomous Vehicle Cybersecurity

Another, different kind of attack previews occurring during the entire babysitting time of the lithium buggy, whilst delivering most of the e-mail for the otherwise autonome journey it is allowed to influence the course at will passing the streets present-day crosswalks, kickoff and recommendation overpass—riding over the bumper—to exceed in the excessive and short-running purgatory attempt to keep Slack after the light in its final red phase of a given road, and other daily epiphytic advances and retreats. Exercising the fight of the autonomous adult industry, it is noted that since people as well as animals and connacts are entitled, in contradiction to the pannaking white market of vehicle avatars, act 위아되고 생각, 13(3), <:www:.:acca:.:org:...>. Signal Transduct Target Ther. In addition to its strict substrate ⓒ 2021 College Accounting Ch. Anomaly detection in flying drones based on behavioral

identification techniques. For the first time, the USPTO patents collection published, the extent to be determined by ESI and other indexing citations.

Leszek W. was convicted of a terrorist attack carried out using an autonomous vehicle scheduled by an app. Wilhelm F. was convicted for obstructing the use of an autonomous vehicle ordered and designed in a e-hailing service, as according to the Federal Court (Germany) e-hailing in autonomous transport systems is a branch of the postal service. On April 1, 2016, on Eisenacher Straße, 1–24, Lichtenberg, 10781 Berlin, a well-known search engine and software company presented a car from their electric vehicle fleet to a group of evaluators using an app that was meant to move the car to a different spot and park it, just in a vehicle-parking situation. The software, running on a cloud computer or similar, inside the car accomplished this with or without the car company's GPS satellite navigation system, helped by some sensors check, in doubt, to park itself as narrow as possible. The evaluators surveyed the Kampf der Autonomen Fanclub sternfahrt driverless cab waiting at the destination, mostly likely with the promise to take a random route, and no information at hand about the projected {@link position, route} to think and worry, to believe, trust and feel safe — in case of an alert or simple tenseness feeling unsafe another vehicle-generating internet service can be launched which will "disperse" the handless vehicle, as a human driving skills for handcarts and trailers, driving license, etc. were at all not necessary at all to rent a Petling with app or unlimited KerBKan internet subscription.

3. Fundamentals of Cognitive Threat Analysis

Our multiple sensors detect a group of malicious objects when it comes within the vehicle space. An alert message is conveyed to the driver in case of any danger assessed just as the important information to the driving model. Only when the driving model retrieves the danger and suggests, artificial reasoning or decision-making model reduces the interaction. The response of the autonomous vehicle is executed through the actuation layer. Interconnected sensors employ cognitive learning as a when to behave with which nonfunctional requirements [6]. The proposed framework has been validated for the perception layer to discuss the immune mechanisms in the autonomous vehicle. The performance of the artificial reasoning cognitive model suggests a significant improvement in gap reduction in the decision-making process. The capability of gesture model to apply change on danger warning for decision-making cognitive model reduces interactive activities

of the autonomous vehicle at a faster rate, in comparison to classical nonfunctional requirements with malware attack. In the future, using the modularized features of this comprehensive threat analysis template, we hope to create procedure call graphs to dynamically track how the parallel threads attempt to intercommunicate, and thus use this novel mechanism to catch faulty human or malware related activities and, if necessary, clean the affected areas of the autonomous vehicles.

The cognitive threat analysis framework essentially incorporates threat analysis as a bottom layer and then builds artificial reasoning (AR) and cognitive learning (CL) models [7], which make autonomous vehicles aware of malicious activities and help them make better decisions under uncertain circumstances. In this framework, first the threat model of the autonomous vehicle is designed according to the scenario and strategy chosen to test the vehicle. It thens integrates various types of behavioral nonfunctional requirements (NFRs) and then accurately measures those which are testable with hardware or architectural, and cannot be degraded by cyberattacks termed as security metrics. Safety and security are two main characteristic requirements of the autonomous vehicle, from which safety and security metrics are derived for both the physical and cybersecurity layers. Next, cybersecurity is addressed by improving the perception layer which inherently can distinguish the authentic objects from the malicious one [8]. Anomaly detection is performed in the perception layer to avoid the fatal interaction. In parallel to detecting malicious activities in the vehicle space, cognitive models are developed using sensors, driving models, and proposed cognitive models. The artificial reasoning model using the intelligent search technique, it adopts case base reasoning. The driving model offers real-world scenarios followed by risk assessment and suggestion/alternative for the reduction of risks during the navigation of the autonomous vehicle.

3.1. Cognitive Computing and Machine Learning

In order to acquire a cognitive-behavioral image, attackers with different skills start from choosing attack tools or codes compatible with their own operating platforms, network and attacking frequencies, and then conduct PHISHING attacks through email, social networks and SMS. During the tracing process, attackers gradually approach their final targets by means of endpoint traversing and network infiltrating, and finally retrieve the system account, realize privilege penetration and browse files. As the main technology for the

construction of large-scale interactive computing models, malware attacking events that take place mainly between the running instances of autonomous agents, known as agents, are often capable to develop new samples of discrepancy. Operating in harmony with these data emit large-scale security unified research grouping, controlling along-side anecdotally annotated data, identifies autonomous car network traffic of a behavior-based attack. A common vehicle security anomaly datasets, the CAN and LIN bus examples, reaped enrichment and conditional designing while extending the modification of original programs, and might now be performing prediction extensions to enemy attack abundant data by means of detection.

The ability of autonomous vehicles (AVs) to detect cyber-attacks is crucial for onboard cybersecurity [3]. In this regard, a number of research studies developing autonomous cognitive agents (such as the query theory developed by Sven Koenig and Reid Simmons), threat evaluation models, and active learning mechanisms that observe and participate in the learning process have been introduced to provide security from cyber-attacks [9]. Sven Koenig offers a good taxonomy to categorize artificial intelligence-based methods in regard to saturability and learning as well as their necessity of representing and functioning within specific environmental models. Start with the reactive, agent-based, and hybrid concatenations such as Q learning, value learning, and Markov decision processes before delving into the deliberative, belief based, and qualitative models that provide solution to problems through episodic prediction of response. By addressing questions that challenge former cognitive solution, these AI-based methods will move towards "greater computation, more varied experience, more sophisticated models of interaction with the world, and better communication with other agents" It supports for developing and running robust cognitive agents, deep-learned models, and machine-learning plays a role in pondering user input and achieving conclusions by engaging in auxiliary stages of fruition.

4. Existing Threat Analysis Frameworks in Cybersecurity

Apart from the practitioners of the automotive industry, academic interests grew on the pathways to mitigate those threats. Also, practitioners keep track of the recent progress of the automotive security threats and mitigation paths, which can be reached at autonomous driving technology testing efforts, pre-market adoption of the latest cars and post-market prestige of cars [3]. By taking those surveys, about some cyber threats authors constructed threat model frameworks; however, they sparked the objective of and reported about the

constructed framework. However, those efforts mainly focused on the requirements of autonomous driving technology based on driverless capability of next-generation cars.

Many efforts in the literature aimed to construct threat model frameworks to perform detailed threat analysis. Some approaches in evaluating threats like n-tier approach, feed-forward method or object-oriented frameworks, do not match well with some specific cyber threats of multi-level autonomous vehicular systems [2]. However, all these efforts can be considered as threat model frameworks we can take inputs from, to enhance the mapping of micronet-level threats. Also, among the contests of CAVs, it was revealed that not all cyber threats are equally important, that prompts us to merge the threat prevention techniques in efficacy testing efforts of cyber threat modeling. For the V2X security threats, authors in [Challita et al.] comprehensively illustrated the dark side of 5G, 6G, wireless and edge computing technologies for security challenges.

4.1. Overview of Traditional Threat Analysis Frameworks

In the following subsections, we will introduce traditional threat analysis frameworks that have historically been used to identify and characterize cyber threats that could adversely affect autonomous vehicles. These traditional frameworks normally do not target a specific vehicle technology, and are instead applied more generally to automotive systems in order to categorize types of attacks, their likelihood and consequences. This is the fundamental step of the risk evaluation process that is then followed by more in-depth analysis to identify specific vulnerabilities, as well as select and deploy suitable countermeasures to protect vehicle systems. The frameworks we describe in detail in this section are ISO 21434:2019 and J3061:2016 [10].

State-of-the-art automotive systems aim to increase safety and efficiency while reducing the environmental impact of transportation. These systems rely on real-time connections between vehicles and surrounding infrastructure and devices, which are highly susceptible to cyber threats . Autonomous vehicles, in particular, are a combined system of cyber physical systems and Internet of Vehicles that increasingly rely on artificial intelligence models and neural networks [8]. Thus, cybersecurity for autonomous vehicles has evolved from a hypothetical concept to a vital and integral part of the automotive research agenda [4]. Alongside the prospective solutions offered so far, the academic community has shown an interest in

defining traditional methods for threat analysis and has begun to develop frameworks that specialize in cybersecurity for autonomous vehicles.

5. Applicability of Cognitive Threat Analysis to Autonomous Vehicles

Current cybersecurity initiatives concentrate more on signature-based detection approaches, network traffic analysis, and the movement of data through system layers, which are ineffective in providing accurate results at the lowest level of the vehicle's automotive systems in real or near-real time [5]. As a result, there are potential risks to the safety of passengers, pedestrians, and even transITS infrastructure, which can be a potential weapon for terrorists on a large scale. Therefore, an aim of early detection and identifying cyber security threats on automated/autonomous vehicles is becoming important, which can be an important enabler in providing safety on infrastructure and applications that use autonomous vehicles. This study was designed to learn the applicability of cyber security threats classification methods in the literature to autonomous vehicles and the investigation reveals that the cognitive framework stands out as capable of addressing the challenges. Cognitive information processing storage framework approach based algorithms can guide in detection and identification of anomalies and cyber security threats [11]. In never-ending evolving technological landscape, security threats continue to rapidly increase and change almost every single day. These risks are not only within the traditional secure domains, but also the emergent research areas such as securely implementing the Civilian UAVs and autonomous vehicles. Such urgent implementation necessitates the convergence of technologies concerned with human safety, which requires infrastructure components to co-operate with each other for security compliance. To meet this need, it is of prime importance to implement a technical mechanism that is designed considering entire the CPS context. In this study, therefore adaptive network traffic anomaly detection approach having cognitive cybersecurity requirements were proposed with its application to autonomous vehicles. As the technology continues to evolve, connected autonomous and unmanned communication devices are increasing in number with increased interaction between computing systems. This increase naturally results in increased cybersecurity threats, which can potentially be endanger the physical environment and property. As these levels of cybersecurity threats increase, all corporate companies will be indirectly affected by being improved and their production and cost dynamics will also be affected, in short, their digital organizations and all states will face

risks due to the increasing number of corporate companies and their own internal institutions [12].

5.1. Unique Characteristics of Autonomous Vehicles

The presence of numerous devices inside autonomous and connected vehicles and the general insecurity for autonomous vehicle systems put new management in front of serious challenge. Assistance in the task of cybersecurity hardening is provided also in the form of reference, i.e., a proposal of research and research and development activities, which may significantly help to make autonomous vehicles secure against cyberattacks [6]. It is general guidance in designing security architectures for autonomous vehicle and guidelines for cybersecurity analysis. This contribution also presents one of the popular IT security methodologies (particular variants of risk management regarding to autonomous vehicle cybersecurity). Moreover, since usual paper methodology for specification of system for instance in the form of Interface Control Document cannot be directly applied in general to cybersecurity purposes, novel methodology to design autonomous vehicle security architecture management is proposed. The paper finalizes the explanation of customer product support, which has a flexible offer in designing cybersecurity architecture for autonomous vehicles according to customer expectations and requirements.

Automotive electronic systems are complex, and as vehicles become increasingly connected and autonomous, electrical complexity is growing at an extremely rapid pace. In driverless vehicles, automation systems are ultimately making decisions normally performed by human drivers [13]. An autonomous vehicle may be understood as a robotic system operating in a relatively unconstrained environment based on a collection of sensors usable for navigation, mapping, and pedestrian and obstacle detection. These vehicles generally form complex multi-sensor systems controlled by multi-level control algorithms which reflects their safety-critical role in the ecosystem. In this paper, the most crucial sensors are briefly introduced, and vulnerabilities and potential attack vectors from the perspective of cyber attackers are also presented.

6. Proposed Cognitive Threat Analysis Framework for Autonomous Vehicles

While the f & as threat diagnostic predict infrastructure attack threats, they don't act against them. Following the cognitive analyses, asCraes would determine if the attack is indeed a

threat (will it affect at least one of the Vd 's critical functions?), and consequently build an anti-thematic profile. The probative analysis is a separate Vd -specific inter-layer overlapping problem - Is the VdICP oriented expectation relevant true in given new infrastructural conditions? asCraes run k such cognitive follow-up batches (with k called the gesture coarifying level which is determined as the number of orthogonal expressions) and use their stability (echoing coefficient) to give an inference as to whether the diagnostics, prognosis, and entwined branches models are capturing the truth in the current infrastructure-AV setting. [11]

Within the context of AV security, our work has been an unification of three possible pathways of study based on cyber threat analysis: likelihood threat analysis, functional threat analysis, and cognitive threat analysis. We have also presented the progression from a general in-vehicle gateway-based intrusion detection and intrusion prevention system(estrAra) to a vehicular cognitive attack analysis expression system(asCraes). Moreover, asCraes is versatile enough to take in individual data-cognition-needs of each vehicle domain (fuzzily represented as Vd) and the data-cognition-capability of the network it is being exposed to as well as dealing with an evolving situations wherein the status of Vd ’s in-truth cognition changes with every infrastructural attack-event. Taking these three paths into consideration, we have accordingly carves out a previously suggested “layered interference” strategy to attitude diagnostics and unification analysis outlining general entwined methodologies to be used.

6.1. Design Principles

Generally, the study of Autonomy in an unmanned vehicle can be considered synonymous with cognitive self-driving infotainment and telecommunication systems. We look to the exciting space between cyber- and physical security where the autonomous vehicle threat model is expanded from resistance principl es toward those of intruder detection and avoidance. The cognitive safety principles (marketed as various forms of self-defense systems) reviewed reflect both the public and private sectors, targeting technologies in passenger vehicles, captive fleets and syndicated global aggregations. We provided a formal cognitive threat analysis (CTA) methodology to validate the flexibility of our theory-in-use real-time cognitive security assessment skills. We wrap up our review with a candid review of vi acute trust and claims of autonomous vehicle vulnerability. [1]

At the very heart of the design of any autonomous vehicle cybersecurity (AVCS) system is the ability to accurately detect and analyze possible intrusions or adversarial actions [7]. The underlying analysis though, particularly in the domains of cognitive vehicles, can be somewhat involved. It requires a deep understanding of the vehicle and its environment, and it also necessitates a strong appreciation of the possible behaviors that these variables can exhibit across both nominal and abnormal conditions. It is in these cognitive threat analysis (TA) tasks that both the practical feasibility and corresponding effectiveness of AVCS are defined. Recognizing this, and acknowledging the need to drive the AVCS efficacy, optimization, and validation processes, we have designed a modular and formally defined TA language in the scopes of our Cognitive Threat Mitigation (CTM) infrastructure. [13]

7. Case Studies and Applications

In response, these tests compare myriad attack and ADAS case scenario attack impacts with low, medium and high ontological mismatch declarations. With the given partial realism of these case studies and their conclusions, we suggest that employed PDs must be able to systematically reassess the threat defined in every derived attack scenario, detecting changes in system security performance, and choosing between remaining effective, mitigating, new recovery, and new resilience mechanisms based on the achieved CTH analysis [12].

When autonomous vehicles (AVs) are deployed as part of large-scale transportation systems, the total fleet system can be used to detect and respond to cyber-attacks and undetected faults. Nonetheless, in order to create realistic scenarios and data-driven understanding in these situations, few to none procedures currently exist to describe or analyze the details of cyber-attacks. If no such detailed attack description, detection, and resilience analysis method exists for autonomous vehicles, the adaptation of ad-hoc responses cannot react or adapt to threats" [13]. To bridge this gap, this chapter has defined a detailed description of the cognitive threat analysis approach. To demonstrate the possible future application of our proposed cyber-attack scenario library, six case studies have been designed. These case studies evaluate the potential correlation between potential cyber-attack scenarios and adverse impact predictions in the SAE J3016 driving automation level 1–5 cases. Each case primarily looks into what future fleets of fully self-driving vehicles could feasibly control in the context of a sophisticated cyber-attack campaign [3].

7.1. Real-World Examples

Preventing design splinters to improve cybersecurity appeared to be a major goal of the research in Wiegard et al.'s (2021) [11]. In the paper they propose a design concept for implementing a cybersecurity system in autonomous devices, where they require a set of generic rules to be respected when adapting the cybersecurity protection to the physical system. Since research on cybersecurity of autonomous systems is still relatively new, the authors consider a literature review as one of the key aspects is to understand the state-of-the-art in autonomous vehicle cybersecurity, that is to say, to assess what is currently known about past attacks against self-driving cars (if any), what kind of countermeasures can be taken to defend from the identified threats, what is already known about possible future attacks and what (if anything) has already been done to defend/identify against/ mitigate the identified threats and to gain an insight into the (state-of-the-art) system representations for AVs on which the cybersecurity analysis must be based. For this reason, although their framework may be considered metatheoretical, its ultimate design is influenced by tactical and practical matters within the cyber-physical domain, making it a hardware and software system synthesis.

Petacheva et al.'s (2021) discusses a salient example of a real-world cyber incident targeting an autonomous vehicle [12]. In this context, the authors did an in-depth review of the approaches to cybersecurity in the context of self-driving cars, and outlined a proposal for a framework for a multi-stage cognitive threat analysis (CTA). The authors showed that cybersecurity problems in autonomous cars have not been well researched and discussed, and considered such systems as environmental IT systems that have to be adequately secured as usually not fail-safe. Furthermore, literature were not specifically aimed at autonomous vehicles; Miehling and Kuhn (2017) did propose a design for a SystemC code generation tool designed to help identify potential cyberattacks against autonomous cars, but a complete development and framework like that introduced by the discussed authors does not exist in the literature. This is a great difficulty, given that autonomous vehicles are machines that interact with the external world in scenarios that are never exactly repeatably self-similar, such as imitations of the real world. Thus their airplanes' cyber-defenses, disallows complete synthesis of cyberattacks during pre-deployment testing as the synthetic stimuli and faked communications have embedded systematic biases that may be very useful for exploiting the information they reveal concerning the autonomous car [6].

8. Evaluating the Effectiveness of Cognitive Threat Analysis Frameworks

The automotive industry is now focusing on cybersecurity to a greater extent due to the evolution of RF exposure and vehicle cyber-physical systems making it easier to launch cyber-attacks. Attack trees (ATs) are used to represent system vulnerabilities and are widely used in various domains to evaluate the security of systems. Based on a team-based approach, different ATA have been designed to develop a sensor-data validation system in which the impact of several plausible attacks has been evaluated on a cyber-physical system [14]. Many standards have been proposed to address the development of automotive cybersecurity, such as ISO/SAE 21434, SAE J3061 standard, and several others from the NHTSA. Because the above-mentioned rulings and standards focus on imposing various actions, they could pose new challenges for researchers who are developing autonomous vehicles.

As new connected and autonomous vehicle (CAV) technologies develop, the threats stemming from various cyberattacks also concurrently develop [2]. Strengthening cybersecurity has become increasingly important due to the increasing susceptibility to potential threats. While traditional rule-based methods are used in autonomous vehicles to deal with various cyber threats or external attacks, the approach of simply assessing the developed system's security is not effective or efficient, creating the need to focus on the safety of the autonomous vehicle system rather than its security. However, addressing only the safety of autonomous vehicles (AV) might not be sufficient without implementing appropriately designed cybersecurity measures, thus necessitating the creation of a security road map focused on AV interfaces [3]. The creation of a cybersecurity road map is crucial to providing a solution for incident prevention by focusing on the performance and security of an automotive control system regarding attacks and intrusions.

8.1. Metrics and Key Performance Indicators

In the COV perspective, this chapter serves two goals. First, as outlined in this chapter's introduction, we aim at providing understandable defense tactics against COVs-final attacks such as those we have exposed in this study, from the view of sensor fusion and control architecture, in contrast to the traditional attacker and intrusion approaches of the field. Secondly, we expose where new COV-network cybersecurity techniques might be created to effectively divert lone-wolf vehicle assaults. We conclude with a brief reflection on Low-hanging fruits that should be a/p targeted by computer-aided real-world cyber evaluations with concrete attacked CAVs.

The rest of this chapter discusses COV-related cybersecurity strategies and tactics to mitigate the attack abuse, a concept also critical for the autonomous operation paradigm. Only few examples are given spans connected CAVs security, from intrusion detection systems (IDS), cyber–physical systems (CPS) security methods that stress adaptability to general L4 driver assistance methods associated with ADAS, CAVs real-time systems and network security methods. Thus, we omit discussions on IDS and concentrate on the automotive cybersecurity in the following specific scope: intrusion response system (IRS), real-time cyber–physical systems (cps), and our own focus, the vehicle-L4-ADAS-controller layer. ADAS cooperation and especially partial-information cybersecurity related to ADAS technology have rarely been investigated by researchers. and ADAS co-operative works are sparse, emerging mainly from the sensor fusion E2E safety guideline.

[7] [15]As fundamental communication technologies in the automotive field, in-vehicle networks are starting to become increasingly linked to the Internet, where resource-constrained connected autonomous vehicles (CAVs) coordinate E2E. While sparking the security community's attention, most prior work focused on single attacks or static knowledge. With AV architecture research, we argue that, to serve as a decision aid for autonomous security, Lone-Wolf attackers are graduated from to adversary driving tactics, and from static CAV architecture to COVs multi-sensors object tracking and steering vehicular controller for decision-making. This leads to realistic partial-information multiple-step longitudinal attacks. Lone-Wolf attacks are demonstrated to pressure-test practical CAVs within a complex real-world OPT.

9. Challenges and Future Directions

the Cognitive Threat Analysis Technique for Resilience of Critical Systems (CITRICS) aims at analyzing, mitigating and identifying potential intrusions of an Autonomous Vehicle (AV) system. CITRICS mimics the findings of advanced persistent threats (APTs) against the target vehicle's predetermined Attack Surface (AS) and devises an uninterrupted chain of attack paths. Within each identified attack path, CITRICS prioritizes attacks, as per their capability, entry and stealth, for a complete and overwhelming attack. The objective of this chapter is to inform manufacturers and designers of Automated Vehicles (AVs), respective to a novel and unique method for the cybersecurity assessment of AVs [16]. Specifically, the method subsumes formal cognitive models, termed AV Secure Energy (AVSE) Profile Models of

Targeted Adversaries (ABMs). After identifying that the cognitive cyber-security model, CITRICS, lacks association between the skill sets of a threat actor and their respective decision-making in the context of an automobile, we acknowledge, perceive, advise, and implement a de facto cognitive framework for Cognitive Adversary Skill-Graphs (CASP/GTAF) to discover novel and complex reasoning patterns.

Smart mobility is the cornerstone of smart city initiatives. It depends on effective, safe, and secure mobility solutions. Public and private organizations are investing in research and development for integrating connected autonomous vehicles (CAVs) into the road infrastructure. For the successful integration of CAVs with the road infrastructure, cybersecurity is the most concerning aspect. With multiple strategies, they are addressing the computational computing capabilities of CAVs, while the security aspect might remain overlooked [17]. This chapter briefly overviews significant potential cybersecurity attacks on autonomous vehicles (AV) and expands on a methodological framework for […]

9.1. Ethical Considerations in Cognitive Threat Analysis

Researchers should critically address the combined morally and legally approved reinforcement of different agents with respect to the utilitarian distribution of traffic flows where the real challenge in the feeling of responsibility is that it only temporarily rests on both agents, such as making the difference between the human driver and the controller of the service provider. Thirdly, researchers have to simulate the combination and verification of satisfied principles with respect to the final state of the injuredness and agreement among the stakeholders. Researchers should then contrast with other current research in the technical game-theoretical prioritization of power sources for charging electric vehicles, where they contest the multiplicativity of aggregate and supposedly benevolent behavior [18]. Finally, such work in principled plans likely is to expand it with a reconsideration of ethical reflection on the principle of evil like the base of the European Commission for Trustworthy AI. At this point, finding the drive jerk prevailing the others with respect to the normative ought of reacting guide the traffic flow on the one hand, while on the other, all agents are able to follow their respective goal functions in the long term.

To ensure that the decision-making and threat analysis capabilities of connected, autonomous, and intelligent vehicles (CAVs) are appropriate and properly ethically grounded, guidelines are provided [ref: 04d85c13-DB34-45A2-A93E-51C86A2CA12A]. On not just AI principles,

European and global parties agree to guiding values and principles on ethics and legal regulation, such as human autonomy, benevolence, fairness, transparency, explicitness, privacy, and respect for intellectual property rights. Significant work is also needed in prior and refined domain-specific work on policy strategies, such as the Fatima Project and the EU data governance strategy. Moreover, both concrete measures and technologically and morally grounded systems to adapt those principles to situations in traffic must be developed, such as methods to detect failures to respect principles on actual or factual or on the balance of very great harm when failure to respect non-service senior robots.

10. Conclusion

The defence system of the USA operates its security network on an isolation mechanism of the compartments with no connections, no retrieval rights among them, no messages or states transfer allowed, installed inside the buffer and with this the thoughtful static predictors with trained up of spotted technology to stay silent, away from each other but for short period of time, entrained easy exchange signaling mechanism of neurons-"to introduce with", further exchange of some related synoptic message, and test the compatibility of the functionality ensuring robustness among the family members of the compartment. The Weak Isolation is the Achilles' heel of the defense system of the USA and its allies. Although the incision points are enforcing to build up of strong strength and the politician of the threatening countries as the sovereign one are concentrating to strike likely weaker points of the socio-scenarios of the defense system of the USA in her enemies friendly countries like Nigeria [19].

One of the major benefits of the cognitive threat analysis framework is examining multiple security clearances, each specific to the authority of the individual compartments and their power. Current systems use authority in non-anthropomorphic, non individuating ways. The need for this inadequacy has been brought to attention in multiple security settings ARM peninsula. The main problem stems from the fact that most of the previous generative models do not account for arctan filtering, and systems would want to have hold constant for the estimator value using append dimensions. However, since classifiers are most accurate when they are fitted to the entire dataset, an estimator value with tightly bounded probability is designed which outputs in{0, 1}, but cannot hold a constant value "c" for the corresponding observation x. This causes insecurity and unreliability between the compartments which arises when single public decision is made by switching among all classifiers of the

compartments as whose accuracy is higher rather than employing majority classifier of common viewpont [20].

11. References

1. [1] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019. [PDF]
2. [2] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
3. [3] V. Kumar Kukkala, S. Vignesh Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," 2022. [PDF]
4. [4] C. Oham, R. Jurdak, and S. Jha, "Risk Analysis Study of Fully Autonomous Vehicle," 2019. [PDF]
5. Tatineni, Sumanth. "Cost Optimization Strategies for Navigating the Economics of AWS Cloud Services." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.6 (2019): 827-842.
6. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.
7. Mahammad Shaik, et al. "Envisioning Secure and Scalable Network Access Control: A Framework for Mitigating Device Heterogeneity and Network Complexity in Large-Scale Internet-of-Things (IoT) Deployments". Distributed Learning and Broad Applications in Scientific Research, vol. 3, June 2017, pp. 1-24, https://dlabi.org/index.php/journal/article/view/1.
8. Tatineni, Sumanth. "Deep Learning for Natural Language Processing in Low-Resource Languages." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 11.5 (2020): 1301-1311.
9. [9] M. Basnet and M. Hasan Ali, "A Deep Learning Perspective on Connected Automated Vehicle (CAV) Cybersecurity and Threat Intelligence," 2021. [PDF]
10. [10] C. Abdulrazak, "Cybersecurity Threat Analysis And Attack Simulations For Unmanned Aerial Vehicle Networks," 2024. [PDF]

11. [11] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
12. [12] 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
13. [13] 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]
14. [14] M. Ebrahimi, C. Striessnig, J. Castella Triginer, and C. Schmittner, "Identification and Verification of Attack-Tree Threat Models in Connected Vehicles," 2022. [PDF]
15. [15] R. Spencer Hallyburton, Q. Zhang, Z. Morley Mao, and M. Pajic, "Partial-Information, Longitudinal Cyber Attacks on LiDAR in Autonomous Vehicles," 2023. [PDF]
16. [16] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov
17. [17] L. Liu, S. Lu, R. Zhong, B. Wu et al., "Computing Systems for Autonomous Driving: State-of-the-Art and Challenges," 2020. [PDF]
18. [18] A. Biswas and H. C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," 2023. ncbi.nlm.nih.gov
19. [19] S. N. Saadatmand, "Finding the ground states of symmetric infinite-dimensional Hamiltonians: explicit constrained optimizations of tensor networks," 2019. [PDF]
20. [20] Y. Shao, S. Weerdenburg, J. Seifert, H. Paul Urbach et al., "Wavelength-multiplexed Multi-mode EUV Reflection Ptychography based on Automatic-Differentiation," 2023. [PDF]