CYBR 4360
December 2023

Ensuring Cybersecurity in Connected Autonomous Vehicles

THREAT LANDSCAPE, DEFENSE STRATEGIES, AND VEHICULAR COMMUNICATION SECURITY

MIGUEL ROCHA

Table of Contents

Abstract

Connected autonomous vehicles (CAVs) will improve transportation efficiency and accessibility. CAVs can communicate with other vehicles' infrastructure and operate without user intervention. CAVs have been around since the 1990s, but not until 2010 was there a handful of CAVs on public roads [15]. Since then, the curiosity and popularity of CAVs have increased. Around the world the developers and designers of CAVs have made significant progress in improving the autonomous hardware, software, technology, and security of CAVs. The improvements to the CAVs are allowing the concept of CAV to get closer to the day when we will see CAVs on the roads on a regular basis. However, in the time this happens, many failures will occur including fatalities due to CAV's behaviors that caused accidents. There could be more fatalities if the developers and designers don't focus on CAV's security.

Beyond physical security, CAVs need to be secured from cyberattacks. For the safety of those inside and around CAVs. Cybersecurity of CAVs and IoT around CAVs are complex and have real-world implications. Software controls sensors on CAVs and in a sense, controls the whole CAV and the people inside. The concern is that software can be exploited; thus, CAV's vulnerabilities are potential targets of cyberattacks. Some potential cybersecurity challenges that CAVs face are data privacy, encryption, authentication mechanisms, vehicular networks, ad hoc networks, and the IoT within and around CAVs. CAV's cyberthreats can be minimized by maintaining a robust defense mechanism.

This collection of annotated articles and presentations provides information about CAV's vulnerabilities, cyberattacks against CAVs, and the challenges that CAV's have in cybersecurity. Proactive measures and novel protection tactics are suggested by the authors of the presentations and articles to mitigate cyberthreats against CAVs. The sources are peer-reviewed journals and presentations that were selected from the UNO Criss Library and Google Scholar. These two sources provide links to other reputable publications, such as IEEE and ACM. The sources are focused on the period of 2016 to the present. They cover the CAV's cybersecurity topic in-depth and have relevant information for the annotation bibliography. As CAVs and technology continue to advance, this annotated bibliography has valuable resources for understanding and addressing the complex and dynamic cybersecurity issues that CAVs face in the real world.

Annotated Bibliography

Logic Structures in Connected Autonomous Vehicles

Citation:

DEFCONConference. “Hacking Driverless Vehicles - Zoz - DEF CON China 1.” YouTube, 22 Jan. 2020, www.youtube.com/watch?v=BM2mqrIXY2w.

Summary:

Autonomous is found on road vehicles and in the farming fields. They are also found in/on the ocean and in the air. The constant battle on autonomous vehicles (AVs) is knowing what the vehicle knows and how the AV does with that information to make decisions. Correct state estimation is the key to decision-making [1]. The author outlines the AV logic structure's four priority levels control loops and stability, collision avoidance, navigation/localization, and at the highest-level planners and reasoners. Exploiting AV is through the state estimation process. Each AV on the ocean, on the ground, or in the air will have vulnerabilities somewhere in the AV’s logic structure stack. The safety of the AVs and the people in and around the AVs depends on how well the sensors on the AVs defend against attacks. These attacks range from denial of service (DoS) to spoofing. The presentation outlines many attacks on AV’s sensors that were successful and provides insight into how to attack the AV’s sensors successfully. The emphasized sensors were GPS, LIDAR, camera, millimeter wave radar, international measurement unit and compass, odometry, and ultrasonic sensors. These sensors communicate with vehicle to vehicle (V2V) and vehicle to everything (V2X).

Evaluation:

The credibility of the findings can be considered moderate. The author has an autonomous robotics background and a Ph.D. in robotics. He is a co-host on the TV show “Prototype This!” that pioneered pizza delivery with robotic vehicles, the first autonomous crossing of an active highway bridge in the USA, and airborne delivery of life preservers at sea from an autonomous aircraft. The presentation was at a reputable conference. However, the presentation did not provide in-depth research details or countermeasures. The relevant presentation provides in-depth examples and demonstrations of connected autonomous vehicle sensors and successful attacks against them.

Reflection:

The presenter presented different ways to attack autonomous vehicles (AVs). These attacks are very concerning to the safety of the people in and around the connected autonomous vehicles (CAVs). These attacks can be done with information that is available on the internet and can be cheap. The knowledge that a hacker would need to attack a CAV is minimal due to the accessibility of the resources and hardware. The demonstrations that were presented provide a difficult challenge to have a completely automated CAV on public roads. The infrastructure for vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) is slowly being structured. Wireless standards enable communication between CAVs, exchange information, and perform essential tasks for safe and efficient operation [14]. The concerning issues over other malicious attacks around CAV are unencrypted data, privacy, and tracking.

Challenges of Cybersecurity in Connected Autonomous Vehicles

Citation:

Mudhivarthi, Bhavesh Raju, et al. “Aspects of Cyber Security in Autonomous and Connected Vehicles.” Applied Sciences, vol. 13, no. 5, Feb. 2023, p. 3014. DOI.org (Crossref), https://doi.org/10.3390/app13053014.

Summary:

Connected Autonomous Vehicles, CAVs rely on information and communication technologies (ICT) for safety and communication with CAV's electronic control units (ECUs). The vulnerabilities in vehicle networks, vehicle-to-everything (V2X) communication, and sensors of the CAV can be attacked to take control of the CAV’s controls. These ECUs are responsible for collecting the sensor data to perform a specific task. ECU can do this through communication protocols such as controller area network (CAN) and local interconnect network (LIN). Attackers can attack a CAV through many physical and wireless points that make the CAV vulnerable. The most known attacks are spoofing sensors and GPS and attacking connectivity with Denial of Service (DoS) attacks [2]. Cybersecurity measures are important for CAVs and vehicular networks due to the lack of authentication and encryption capabilities. Some of the defenses that the author mentioned were cryptography, intrusion detection systems (IDS), secure protocols, and firmware updates. In the future, the integration of artificial intelligence (AI) will be part of the defense strategies in CAVs.

Evaluation:

The credibility of the findings can be considered good. The research method that the authors used was by conducting a bibliometric survey. They reviewed the collected data from Scopus database that is the largest citation database of peer-reviewed literature. They also have classified the various attacks in CAVs and researched various defenses for the attacks on the classified regions. The article was peer-reviewed and published in Applied Artificial Intelligence Journal as a Special Issue AI and Security in Cyber Physical System Design collection.

Reflection:

Vehicles are being transformed into information and communication technologies (ICT). This transformation has been occurring for a while. All vehicles that have been produced in the past few years have some type of ICT. They allow the development and operation of CAVs by letting them communicate to each other and to infrastructure. This transformation has to do with human wants and now with human needs. With the growing trend of connected autonomous vehicles (CAVs) a stronger physical and wireless vulnerabilities are present. Cybersecurity is needed to minimize the evolving cyberthreats. CAV’s manufacturers, software developers, and government agencies need to work together to make CAVs and the road secure.

Adversarial Attacks on Connected Autonomous Vehicles

Citation:

Shibly, Kabid Hassan, et al. “Towards Autonomous Driving Model Resistant to Adversarial Attack.” Applied Artificial Intelligence, vol. 37, no. 1, Dec. 2023, p. 2193461. DOI.org (Crossref), https://doi.org/10.1080/08839514.2023.2193461.

Summary:

Connected Autonomous vehicles (CAVs) are thought to bring humans benefits. However currently, the model to control CAVs is the use of end-to-end learning (e2e), but this model uses patterns that can be attacked with adversarial interference. There are two types of adversarial attacks Fast Gradient Sign Method (FGSM) and Generative Model-Based Approaches (AdvGAN) [3]. The authors propose a defense mechanism that uses a generator, a discriminator, and a memory module to capture the input images from the CAV’s cameras and clean the adversarial inputs to receive high-quality output images. This model uses stored data to learn from the data over time. Results show that AdvGAN performs well in the Whitebox environment compared to FGSM. The performance of AdvGAN does decrease when in a Blackbox environment. This suggests that CAVs do have vulnerabilities. However, integrating the memory module improved the defense success rate.

Evaluation:

The credibility of the findings can be considered good. The publisher Applied Artificial Intelligence Journal is a respected resource to find published artificial intelligence articles such as this article. The work that the author’s did was done through their institutions that perform research in information science, technology, and engineering. No potential conflict of interest was reported by the authors. The Udacity dataset was used to gather the data for the model. Udacity database contains real-world road photos taken by CAV’s cameras that were used to train and test their model. Whitebox and Blackbox environments were used to gather results. The authors compared their own proposed model with other current research models or approaches to verify the accuracy of the results.

Reflection:

The model that was proposed by the authors was tested against Hijacking, Vanishing, Fabrication, and Mislabeling attacks. These attacks were carried out using the FGSM and AdvGAN methods against the Nvidia Dave-2 driving model. The success rate of these attacks measures how well the model can withstand adversarial attacks. In the article, figures 5-6 are images of the effects of adversarial attacks on a detection system. These real-world images show how connected autonomous vehicles (CAVs) respond to various attacks on actual roadways. These images provide a good perspective of how attackers exploit vulnerabilities in the CAV’s decision-making process. These cyberattacks can lead to accidents or other undesirable outcomes. Protecting CAVs from such threats is important in ensuring their safety and dependability.

Security & Privacy in Connect Autonomous Vehicles

Citation:

Ghazaleh, Hadeel Ahmad Abu. “An Overview of Security and Privacy Challenges in Connected Autonomous Vehicles.” Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, vol. 5, no. 2, Nov. 2022, pp. 15–26. research.tensorgate.org, https://research.tensorgate.org/index.php/tjstidc/article/view/33.

Summary:

Connected autonomous vehicles (CAVs) have security and privacy challenges. CAVs rely on communication networks and sensors. Communication from and to the sensors can become vulnerable to cyberattacks. Changing the information that is transmitted can put passengers and CAV users at risk. The amount of data that CAVs collect is huge. This raises concern about data privacy, anonymization, and how the information is handled. Figure 1 shows how CAVs can be attacked by cyberattacks.

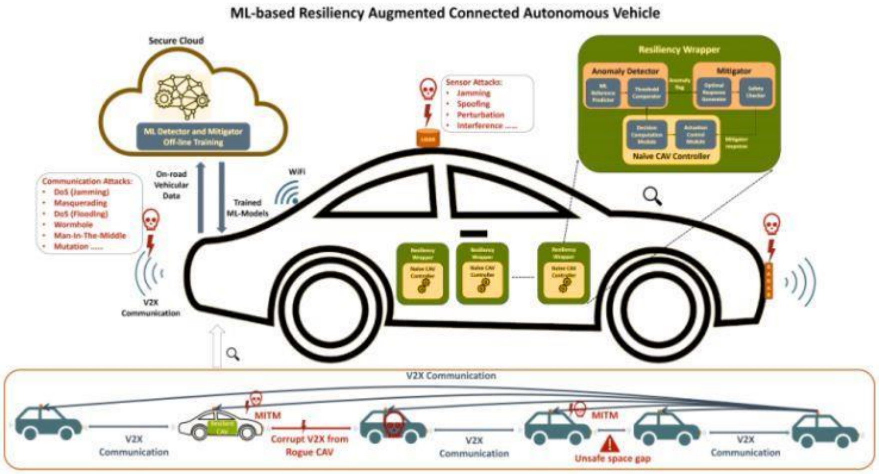


Figure 1- Connected Autonomous Vehicle System [4]

The author puts forth this debatable question, “Is it the car manufacturer, the software developer, or the user?” [4] fault. Does not matter who is at fault there needs to be a framework for handling accidents and developing strategies to prevent them. The CAV’s complex algorithms create challenges in how humans and machines interact, user comprehension, and trust. It is important to have physical security and protection on CAV components throughout the supply chain. There is a need for robust cybersecurity measures.

Evaluation:

The credibility of the findings can be considered good. The security and privacy issues of connected autonomous vehicles (CAVs) that the article discusses is done through secondary sources of literature review. The author has a computer science and engineering background. He does research through the University of Jordan. The research results align with existing knowledge in the field, but some sources may have their own limitations.

Reflection:

Cybersecurity and privacy challenges that surround CAVs have implications for the future of transportation. Cyberthreats can target CAVs in different forms. One of the most concerning ones is vehicle-to-everything (V2X) communication. The context of everything means many vulnerabilities. Secure-by-design methodology and creating a new car assessment program (NCAP) test are suggested to reduce the cybersecurity risks on V2X communication [16]. There has been extensive research into how CAVs need robust cybersecurity, but there has not been extensive research on the interesting question of who is liable, when there is a successful attack. This question brings another aspect to CAVs that needs to be researched and defined in the legal framework for CAVs.

Location Privacy of Connected Autonomous Vehicles

Citation:

Black Hat. “Self-Driving and Connected Cars: Fooling Sensors and Tracking Drivers.” YouTube, 5 Mar. 2016, www.youtube.com/watch?v=C29UGFsIWVI.

Summary:

The presentation focused on exploiting sensors on connected autonomous vehicles (CAVs). The second part focuses on privacy. Each sensor has its vulnerabilities. There are six levels of automation from 0 to 5, this consists of no automation to complete automation [5]. CAVs have many sensors that make up different parts of automation. The presentation focused on the camera and LIDAR. Cameras are the sensors that detect and provide alerts. In CAV’s cameras are part of the 1-5 levels of automation. The camera and LIDAR were exploited easily and cheaply. Even though there are proposed countermeasures, the presenter emphasized, do not trust CAV’s sensors unless there are implemented countermeasures of security by design and validation to mitigate threats.

The privacy that a user has in a CAV is low. GPS, sim cards, 802.11p technology, and others can be used to track CAVs, users, and passengers. The 802.11p technology is used for vehicles to everything (V2X). V2X relies on the location beacon that the CAV provides. This beacon can contain a lot of private information. Vehicle manufacturers are already collecting a lot of data about the user, CAV, and surroundings of the CAV through sensors. This information can be manipulated while it is being transferred or stored. The user privacy location can be compromised when the beacon is broadcasted. The experiment had roads and zone levels with multiple sniffing stations set up at intersections to eavesdrop on the beacon messages. There is a high tracking success rate with just a few sniffing stations. The countermeasure that was proposed was pseudonym change strategies and a privacy metric.

Evaluation:

The credibility of the findings can be considered good. The author presented at a Black Hat conference that is well known among the security professionals. The method that they used was experimental that aligns with the research objective. These results from the research align with other sources that show similar connected automated vehicles' privacy and vulnerability issues. However, the experiment did not provide a comprehensive countermeasures.

Reflection:

The author mentioned that the cameras in connected autonomous vehicles (CAVs) are an automated level of 1-2, which is a warning system. At levels 3-5, the camera becomes a decision-making system. The camera can be exploited physically or through cyberattacks. This is concerning due to the safety of people in and around the CAVs.

There is a perception that camera technology has evolved to have better security, detection, and video [13]. The location of the CAV is important for the vehicle-to-everything concept, but at what point is enough information collected to keep people safe and people keep their privacy? It is evident that mobile devices have reduced privacy; now, with CAVs and smart cities, privacy will decrease. The option of opting out of connected technology will not be an option in the future.

Encryption and Authentication Mechanisms in Connected Autonomous Vehicles

Citation:

Han, Jinpeng, et al. “Secure Operations of Connected and Autonomous Vehicles.” IEEE Transactions on Intelligent Vehicles, 2023, pp. 1–15. IEEE Xplore, https://doi.org/10.1109/TIV.2023.3304762.

Summary:

Connected autonomous vehicles (CAVs) are an option for a sustainable and efficient future. However, there are concerns regarding the security of CAVs. With the technology that CAVs use, there are potential cyberattacks with regard to cybersecurity concerns. Cyberattacks can take control of the vehicle operation center (VOC) that controls the lifecycle of the CAV. CAV has different networks and systems within the CAV network that are made up of communication terminals such as vehicles and vehicles (V2V), vehicles and infrastructure (V2I), and vehicle and everything (V2X) [6]. These connections are important to provide reliable communication to the vehicle and everything else. The author proposes a systematic classification of six security threats that affect CAV false data, information theft, privilege escalation, block communication, and time delay. To mitigate these threats the author proposes standardization efforts to regulate manufacturers and service providers. This would increase authentication and verification methods to ensure communication security and operational safety of CAVs. The implement methods can be observer-based, filter-based, and active detection. The vehicle security operations center (VSOC) comprises four integral elements that serve as the centralized hub for safeguarding CAVs against cyberthreats.

Evaluation:

The credibility of the findings can be considered good. The article is peer-reviewed and published in the IEEE. The authors are from a reputable institutions that focus on Systems Engineering. The article presents a systematic top-down classification system for cybersecurity threats for CAVs. Appears that the research method that the authors used is a literature review of various cyberattack methods and cybersecurity countermeasures for CAVs.

Reflection:

An attacker taking control of the vehicle operation center (VOC) is a scary thought. Many people have experienced a ransomware attack where they have lost important information. In the context of a hacker controlling a connected autonomous vehicle (CAV), things can become damaged, users become injured, or worse, die. It is important to understand the entire lifecycle of CAVs and the six classifications of threats that the author emphasizes. Users should be aware of these threats. The authors propose security standards, verification, and validation techniques to mitigate these threats.

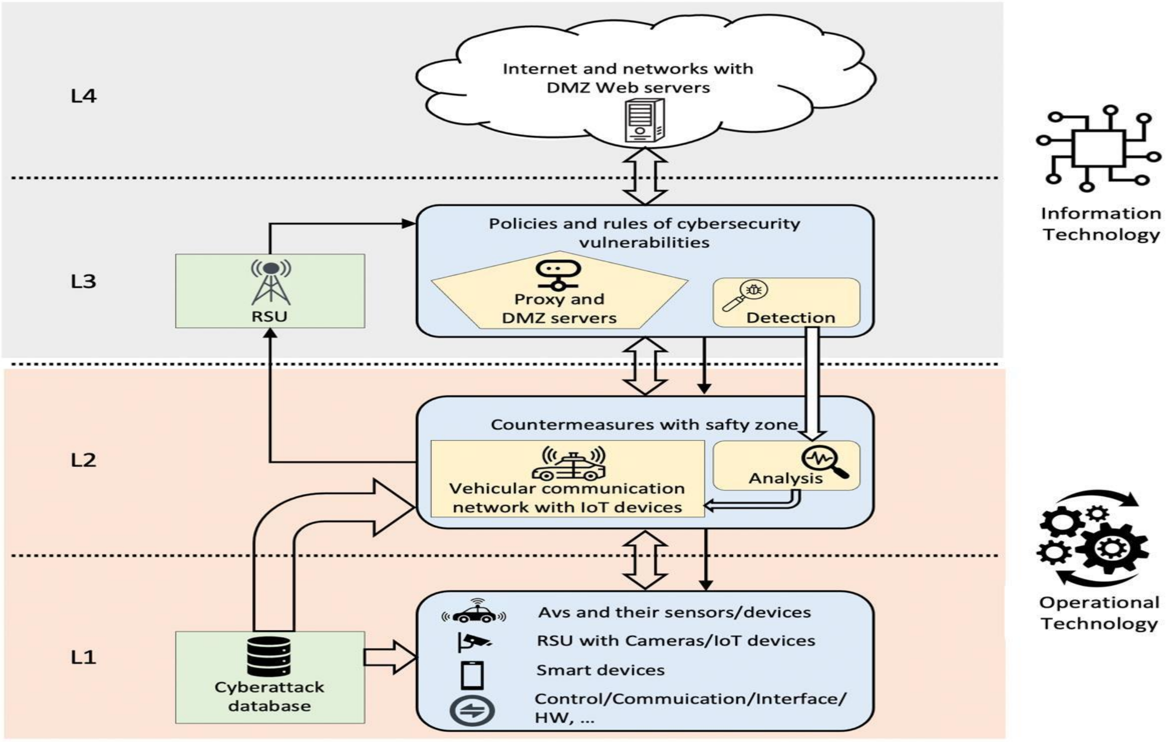
Vehicular Networks in Connected and Autonomous Vehicles

Citation:

Algarni, Abdullah, and Vijey Thayananthan. "Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication." Symmetry, vol. 14, no. 12, 2022, pp. 2494. ProQuest, https://login.leo.lib.unomaha.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fautonomous-vehicles-cybersecurity-vulnerabilities%2Fdocview%2F2756784753%2Fse-2%3Faccountid%3D14692, doi: https://doi.org/10.3390/sym14122494.

Summary:

Big data communication provides data to autonomous vehicle's (AVs) components, systems, and communication services that depend on energy efficiency (EE). The large amount of big data has increased the cybersecurity vulnerabilities (CV) and the challenges to mitigate them. The integrity of the AV can be compromised at any point of a data communication failure. The countermeasures for big data communication are to be proactive and secure. There are existing countermeasures, such as artificial intelligence (AI) defense methods, authentication techniques, and intrusion detection systems (IDS). However, there needs to be energy-efficient security solutions, proactive detection, and mitigation strategies [7]. Figure 2 shows the proposed model for mitigating any potential threats in AV and big data communication. The authors show in this model each layer representing specific elements of security systems, tools, and components of an AV. The arrows show the support of countermeasures.



L4
Internet and networks with DMZ Web servers
L3
Policies and rules of cybersecurity vulnerabilities
RSU
Proxy and DMZ servers
Detection
L2
Countermeasures with safty zone
Vehicular communication network with IoT devices
Analysis
L1
Cyberattack database
Avs and their sensors/devices
RSU with Cameras/IoT devices
Smart devices
Control/Commuication/Interface/HW, ...
Information Technology
Operational Technology

Figure 2 - Proposed model for securing autonomous vehicles and big data communication [7]

This theoretical model measures kinetic energy and displacement using Einstein's theory of Brownian motion. Einstein's formulas are used to analyze data transfer and energy levels in CV. The authors propose that using dedicated sensors to measure energy levels before and after cyberattacks, the model can respond to changes in energy levels that occur during attacks. The results show how well the proposed countermeasures detect cyberattacks. It also shows the importance of considering energy measurements in developing low-cost countermeasures that provide detecting and mitigating cybersecurity threats.

Evaluation:

The credibility of the findings can be considered good. This article has made contributions to countermeasures against cyber vulnerabilities (CV) in autonomous vehicles (AV). A section in this article presents and reviews the related and known models on cyber vulnerabilities. The model was developed with protocols and energy efficient algorithms. The model is based on Einstein's theories and mathematical equations. The author declares staying neutral. This research was funded by Deanship of Scientific Research (DSR), King Abdulaziz University.

Reflection:

Big data is everywhere, and it will expand in the future. It is important to secure big data and data communication services to protect the user and the user's private data. Insecure communication between connected autonomous vehicles (CAVs) and everything else can be vulnerable to interception. Implementing secure communication protocols such as encryption and authentication can help protect the data's privacy and security [11]. It is interesting how the authors' proposed model to secure big data communication measures energy variations to validate the countermeasures by using Einstein's theory.

Ad-Hoc Networks (VANETs) for Connected Autonomous Vehicles

Citation:

Hassan, Zohaib, et al. “Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles.” IEEE Access, vol. 8, 2020, pp. 199618–28. IEEE Xplore, https://doi.org/10.1109/ACCESS.2020.3034327.

Summary:

Vehicular ad hoc networks (VANETs) are important to autonomous and connected vehicles (ACVs). VANETs exchange data packets, sensitive messages, and cooperative awareness messages (CAMs) with other vehicles and roadside units (RSUs). The main responsibility of VANETs is to secure the users and their surroundings. The Black Hole Attack attacks the routing of the data packets that the VANETs and ACVs exchange. The Black Hole Attack drops the data packets, causing communication issues and an increase in accidents. Figure 3 shows that a fake route reply (RREP) is sent as a response to a legitimate route request (RREQ) without consulting the routing table [8]. The RREP deceives the Ad hoc on demand distance vector (AODV) to route the packet to the Black Hole, and as a result, the data packet is lost.

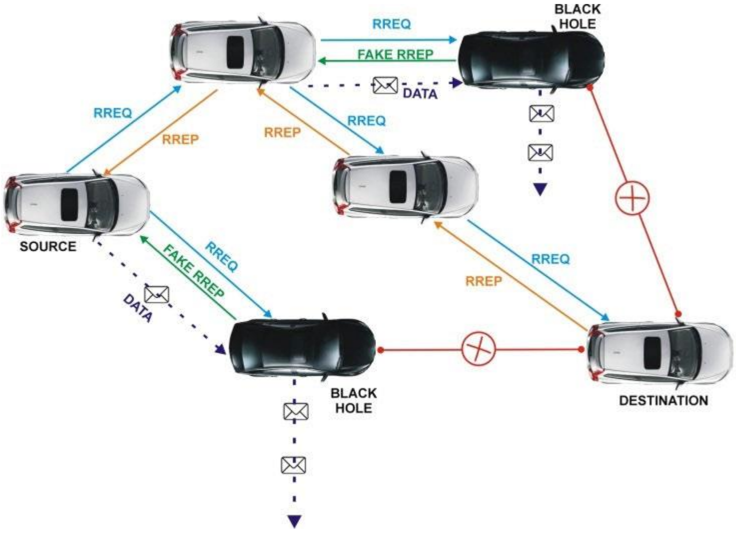


Figure 3 - The black hole attack [8]

There has been research in performing isolation and detection of Black Hole Attacks, but the authors propose an Intelligent Black Hole Attack Detection Algorithm (IDBA) that presents in-depth mathematical models concerning vehicle behavior and connectivity. The model contains four parameters that have never been combined for Black Hole detection Hop Count, Destination Sequence Number, Packet Delivery Ratio, and End-to-End delay [8]. Combining these parameters and pre-calculating the thresholds of the data that was collected from the Sequence Numbers and Hop Count as well as the Packet Delivery Ratio End-to-End (PDR E2E), Figures 6 through figure 10 in the article shows the effectiveness of IDBA in enhancing network reliability, security, and efficiency.

Evaluation:

The credibility of the findings can be considered good. The authors in their research used simulations, mathematical models, and previous models to evaluate their proposed model. The authors are affiliated with reputable institutions. Many grants supported the work. The article is published in IEEE.

Reflection:

Connected autonomous vehicles (CAVs) rely on vehicular ad hoc networks (VANETs) for communication between CAVs and infrastructure. Black Hole Attacks are denial-of-service (DoS) attacks that drop packets instead of delivering them to the correct destination. The Black Hole Attack can cause major issues for CAVs. CAVs rely on real time communication to make decisions and secure people in and around the CAVs. Without Black Hole Attack mitigations people would be at risk. There are few mitigation approaches to Black Hole Attacks. The authors introduce a new model called Intelligent Black Hole Attack Detection Algorithm (IDBA) with four main parameters. Another approach is Detection and Prevention of Black Hole Attacks (DPBHA). This approach detects Black Hole Attacks in the early stage of the route process. This is done by calculating a dynamic threshold value and generating a fake route request (RREQ) packet [17]. DPBHA is a proactive approach compared to IDBA that is a passive approach. This article has shown real-world implementations by showing a model that can directly reduce risk to humans.

Bare Metal Devices on Connected Autonomous Vehicles

Citation:

Black Hat. “Backdooring of Real Time Automotive OS Devices.” YouTube, 23 Sep. 2022, https://www.youtube.com/watch?v=Z2Dgt7XhHGs.

Summary:

A team of security researchers at Algo Cyber Security has successfully hacked into a bare metal device used in the automotive industry. The research started in part to convince their client that his instrument cluster device is vulnerable to cyberthreats. The instrument cluster device that was discussed was the dashboard instruments of a vehicle. The client believed that he had good cybersecurity because they implemented secure boots. A discussion of how modern vehicles are composed of numerous electronic control units (ECUs) that communicate through a controller area network (CAN) that is the bus system of the vehicle. ECUs can run on operating systems such as Linux or monolithic firmware that runs on bare metal. When an ECU is compromised, it typically involves two main steps achieving initial code execution and creating a stable backdoor [9]. The ECU of the client was running on bare metal. The researchers did have some challenges on the way of proving that the ECU did have vulnerabilities. The ECU had very little memory, meaning that the code the researchers had to write had to be efficient. The ECU had a watchdog timer that would reset the ECU if the code didn't run quickly enough. Researchers uploaded code to the ECU to overcome the memory issue by fragmenting it and storing it in a code cave. The code was triggered by using a periodic task mechanism. There was a routine within the firmware of the ECU that allowed researchers to reset the watchdog timer. After overcoming the challenges, the researchers were able to prove to the client that the ECU was vulnerable to attacks. These vulnerabilities would allow an attacker to control the ECU. Researchers are now working with the automotive industry to improve the security of ECU, as they are becoming increasingly vulnerable to cyberattacks.

Evaluation:

The credibility of the findings can be considered good. The researchers analyzed specific Electronic Control Unit (ECU) for vulnerabilities. The research method used in the research is a case study. This research method allows researchers to analyze and perform tests to get results. Algo Cyber Security is a fairly new company founded in 2013. Both Shakir Delarea and the leader of the research, Ariel Kadyshevich, specialize in researching and developing security measures for embedded systems. They have many years of experience in cybersecurity. However, other than that, there is not much information on the researchers. The presentation was presented at Black Hat conference that is well known in the security industry.

Reflection:

There is an evolution of nonconnected to connected systems. These systems have hardware, processors, storage, and software. The Internet of Things (IoT) is all around people and connected autonomous vehicles (CAVs). The security impact that developers and designers think of is on the CAV’s system, not on the user. CAV designers and developers cannot rely only on basic cybersecurity tactics. They need to implement software safety systems to protect the CAV, users, passengers, and everything around the CAV. Electronic Control Units (ECU) uses software to send and receive directions. Hackers can exploit and defeat the software safety mechanisms.

While ECUs used to be considered relatively safe, they are now becoming more vulnerable to attacks. This is because they are being used to control more critical systems.

Securing Connected Autonomous Vehicles

Citation:

Parkinson, Simon, et al. “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges.” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, Nov. 2017, pp. 2898–915. IEEE Xplore, https://doi.org/10.1109/TITS.2017.2665968.

Summary:

Connected autonomous vehicles (CAVs) have many cybersecurity challenges. CAV are vulnerable to cyberattacks because they rely on connectivity and automation. Most studies focus on finding and fixing vulnerabilities after they are discovered. White hat hackers need to be involved but have the initiative to be proactive in discovering vulnerabilities and identify significant knowledge gaps. There is a need for proactive measures to address evolving threats and vulnerabilities to reduce cybersecurity risks in CAVs. The potential knowledge gaps and their potential impact include the evolving nature of CAV technology, the complex supply chain of CAVs, safeguarding against GPS spoofing, sensor manipulation risks, and potential attacks on engine control systems [10]. Proactive security needs to be present to mitigate privacy concerns regarding human interactions with CAV, even during cyberattacks. There are knowledge gaps related to vehicle manufacturer responses to cyber incidents and the legal implications of aftermarket electronic control units' modifications. Continuous efforts are necessary to protect CAVs in an increasingly interconnected society.

Evaluation:

The credibility of the findings can be considered good. The article primarily relies on a literature review to categorize vulnerabilities and mitigation techniques related to Connected autonomous vehicles (CAVs). The method that the authors used in the research was suitable as it overviewed previous knowledge and identified knowledge gaps in CAV’s cybersecurity. The article underwent a peer-review process on IEEE.

Reflection:

White hat hackers are important for vulnerability discovery and advocate for proactive research to mitigate cybersecurity risks in the CAVs. It is important for vehicle manufacturers to take cybersecurity seriously and work with white hat hackers to identify and address vulnerabilities. White hat hackers use the same hacking methods as black hat hackers, but the key difference is that they have the permission of the system owner first [12]. The six knowledge gaps related to CAVs have an impact on their safety and need to be addressed. Cybersecurity needs to keep up with the evolving complex supply chain, technology, vulnerabilities, and cyberthreat of CAVs.

Conclusion

Connected autonomous vehicles (CAVs) have become the trend of autonomous vehicles (AVs), which are upcoming technology that allows vehicles and roadside infrastructure to communicate to increase traffic efficiency and safety [5]. People will be increasingly interacting with CAVs in their normal everyday. A vehicle has become a daily need. Information and communication technologies (ICT) are integrated into vehicles that evolve into CAVs. CAVs are integrated into smart systems to evaluate surrounding environments, assist drivers, increase user comfort, and increase safety [2]. The hope is to bring the world together into a place where people live the driverless dream where people can be doing something else while CAV does the driving [1]. While CAVs offer numerous advantages to facilitate people's lives, such as increased safety and efficiency, they also pose risks that must be addressed to realize their full potential [4].

The source pointed out that CAVs have vulnerabilities. CAVs pose significant security and privacy challenges that must be resolved to ensure their widespread adoption, security, and privacy protection. These challenges include cybersecurity, data privacy, liability, human-machine interaction, physical security, and supply chain security [4]. "Aspects of Cyber Security in Autonomous and Connected Vehicles" paper put forth the primary attack areas of the CAVs as classified into three regions safety systems, connectivity, and diagnostics [2]. Tracking CAVs and the people inside the CAVs is feasible by receiving messages that anyone can receive, jeopardizing location privacy [5]. Ensuring data privacy is important for protecting the privacy of CAV users and passengers by preventing the misuse of peoples' personal information [4]. This underscores the importance of cybersecurity in CAVs to protect against evolving cyberthreats.

All sources provided valuable insights into the countermeasures in addressing the cybersecurity challenges of CAV's multiple sensors (LiDAR, radar, camera, etc.) [5]. CAVs use these sensors to operate safely. In this context, sensors must be robust against intentional or unintentional attacks that alter sensor input or data quality [5]. Some proposed defense strategies are cryptography, intrusion detection systems (IDS), secure protocols, and firmware updates [2]. Some other defense mechanisms are to use a generator, a discriminator, and a memory module to capture the input images [3]. A countermeasure that is proposed is a conceptual framework that guides the idea of parallel security and consists of management, detection, orchestration, and response as the basic structure of a centralized control or monitoring center [6]. Another countermeasure that is introduced is an architecture designed for detecting cyberattacks within Autonomous Vehicle Networks (AVNs) [7]. The countermeasure for Black Holes Attacks is an Intelligent Black Hole Attack Detection Algorithm (IDBA) that presents in-depth mathematical models concerning vehicle behavior and connectivity [8].

Ensuring cybersecurity in CAVs is the priority to lower risk. There is an urgent need to continue valuable proactive research, collaboration between stakeholders, and the development of standards and regulations. Knowledge of potential manipulation of hardware, software, supply chain, and network will give cybersecurity an advantage.

References

1. DEFCONConference. “Hacking Driverless Vehicles - Zoz - DEF CON China 1.” YouTube, 22 Jan. 2020, www.youtube.com/watch?v=BM2mqrIXY2w.
2. Mudhivarthi, Bhavesh Raju, et al. “Aspects of Cyber Security in Autonomous and Connected Vehicles.” Applied Sciences, vol. 13, no. 5, Feb. 2023, p. 3014. DOI.org (Crossref), https://doi.org/10.3390/app13053014.
3. Shibly, Kabid Hassan, et al. “Towards Autonomous Driving Model Resistant to Adversarial Attack.” Applied Artificial Intelligence, vol. 37, no. 1, Dec. 2023, p. 2193461. DOI.org (Crossref), https://doi.org/10.1080/08839514.2023.2193461.
4. Ghazaleh, Hadeel Ahmad Abu. “An Overview of Security and Privacy Challenges in Connected Autonomous Vehicles.” Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, vol. 5, no. 2, Nov. 2022, pp. 15–26. research.tensorgate.org, https://research.tensorgate.org/index.php/tjstidc/article/view/33.
5. Black Hat. “Self-Driving and Connected Cars: Fooling Sensors and Tracking Drivers.” YouTube, 5 Mar. 2016, www.youtube.com/watch?v=C29UGFsIWVI.
6. Han, Jinpeng, et al. “Secure Operations of Connected and Autonomous Vehicles.” IEEE Transactions on Intelligent Vehicles, 2023, pp. 1–15. IEEE Xplore, https://doi.org/10.1109/TIV.2023.3304762.
7. Algarni, Abdullah, and Vijey Thayananthan. "Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication." Symmetry, vol. 14, no. 12, 2022, pp. 2494. ProQuest, https://login.leo.lib.unomaha.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fautonomous-vehicles-cybersecurity-vulnerabilities%2Fdocview%2F2756784753%2Fse-2%3Faccountid%3D14692, doi: https://doi.org/10.3390/sym14122494.
8. Hassan, Zohaib, et al. “Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles.” IEEE Access, vol. 8, 2020, pp. 199618–28. IEEE Xplore, https://doi.org/10.1109/ACCESS.2020.3034327.
9. Black Hat. “Backdooring of Real Time Automotive OS Devices.” YouTube, 23 Sep. 2022, https://www.youtube.com/watch?v=Z2Dgt7XhHGs.
10. Parkinson, Simon, et al. “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges.” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, Nov. 2017, pp. 2898–915. IEEE Xplore, https://doi.org/10.1109/TITS.2017.2665968.
11. Algarni, Abdullah, and Vijey Thayananthan. “Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication.” Symmetry, vol. 14, no. 12, Nov. 2022, p. 2494. DOI.org (Crossref), https://doi.org/10.3390/sym14122494.
12. “Black Hat, White Hat, and Gray Hat Hackers – Definition and Explanation.” Usa.Kaspersky.Com, 19 Apr. 2023, https://usa.kaspersky.com/resource-center/definitions/hacker-hat-types.
13. “VIDEO: Roadside Radar and Video Tested to Assist CAV Merging onto Freeways.” Traffic Technology Today, 23 Nov. 2022, https://www.traffictechnologytoday.com/news/autonomous-vehicles/new-research-accelerates-development-of-self-driving-cars.html.

14. “Exploring the Wireless Standards Behind Autonomous Vehicles.” Utilities One, https://utilitiesone.com/exploring-the-wireless-standards-behind-autonomous-vehicles. Accessed 15 Oct. 2023.
15. “A Brief History of Autonomous Vehicles – from Renaissance to Reality | Mobileye Blog.” Mobileye, https://www.mobileye.com/blog/history-autonomous-vehicles-renaissance-to-reality/. Accessed 16 Oct. 2023.
16. V2X Reducing the Cyber-Security Risks – TU Automotive. https://www.tu-auto.com/v2x-reducing-the-cyber-security-risks/. Accessed 18 Oct. 2023.
17. Malik, Abdul, et al. “An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs.” Sensors, vol. 22, no. 5, Jan. 2022, p. 1897. www.mdpi.com, https://doi.org/10.3390/s22051897.