A Discussion of the Effects of Autonomous Vehicle Data Security Issues on the Widespread Implementation of this Technology

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Ben Tharakan

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

Introduction

Autonomous vehicles, often hailed as the future of transportation, hold undeniable relevance in today's transportation scene. Advocates believe that they could revolutionize mobility by enhancing safety, reducing traffic congestion, and offering greater accessibility to individuals with disabilities or limited mobility (Sitinjak et al., 2023). Additionally, autonomous vehicles can potentially decrease carbon emissions through optimized driving patterns and efficient use of energy resources, contributing to environmental sustainability. However, these advantages are coupled with notable disadvantages, including limited vehicle data security.

In order to conduct various self-driving operations, autonomous vehicles collect a variety of data using sensors and cameras. Since these vehicles communicate with external sources like other vehicles, the data collected by these devices is vulnerable to being accessed, stolen, or even changed by malicious third parties (Xie et al., 2022). Safeguarding personal data and ensuring passengers' data security in an era of constant connectivity is paramount. Improper data security considerations could lead to personal data leaks, vehicle inoperability, or even fatal accidents through data manipulation. Such pressing issues that compromise the safety of all road users could drastically limit the public's acceptance of this new technology. For my STS project, I will focus on these data security issues caused by the autonomous driving system and how they are affecting support of the adoption of autonomous vehicles. Thus, I have developed the following central research question:

How are data security issues affecting the development of autonomous vehicles?

Background & Context

Today, much of the world lives in car-centric societies. This indicates that the focus of urban planning lies heavily on private car use as the primary mode of transportation. Due to the

emphasis placed on this essential piece of technology, cars have undergone significant transformations over their existence. Some of these improvements aim to protect the occupants of the car, such as the Anti-Lock Braking System or airbags, while others simply improve the comfort of the vehicle, like heated seats and automatic windows. The recent emergence of autonomous vehicles seeks to both increase the safety of everyone on the road and to increase the level of comfort from which a driver can operate the car. Autonomous vehicles use a variety of sensors and cameras to render the car's surrounding environment in order to allow a computer to navigate without human input (Stanchev & Geske, 2016). Once this technology is sufficiently tested, removing the human variability in driving could eliminate a large number of fatalities on the road. Additionally, since drivers will not need to operate their vehicles, they will be able to shift their attention to spending time with their families or taking rest over long distances.

While autonomous vehicles by themselves offer a distinct benefit to society, the Internet of Autonomous Vehicles (IoAV) is a crucial element of this technology that has the potential to either help or significantly derail its development. Similar to the Internet of Things which connects all sensor-based electronics, the IoAV is a platform that allows autonomous vehicles to connect and share information over a network (Nanda et al., 2019). By connecting all autonomous vehicles and allowing them to continuously communicate under one network, several crucial benefits are unlocked including traffic congestion management, incident reporting, and even increased driving efficiency. This system is generally comprised of three layers. The Sensing Layer, located on each individual vehicle, identifies physical objects in the surrounding environment, converts the sensed data into digital signals, then transmits these signals. The Network Layer then receives these signals and distributes them to all other entities on the IoAV. Finally, the Application Layer provides storage and processing power to manage the

vast amount of collected data. Since the entire purpose of the IoAV is to be a widely accessible resource, malicious actors may seek to take advantage of its vulnerabilities. By either using a fake identification or a legitimate access point, hackers possess the ability to access any of the three layers of the IoAV remotely, thus granting them access to all of the data stored and processed in the IoAV. Such a large collection of data is vulnerable to different attacks which may access, insert, delete, or change the data located in this interface (Szűcs & Hézer, 2022). Some examples of such attacks include Denial of Service (DoS) attacks and Sybil attacks. DoS attacks flood the network with irrelevant data packets, thus preventing use of the network by authorized users (Khan et al., 2021). DoS attacks can affect all three layers of the IoAV, making them especially hard to prevent. Similarly, Sybil attacks target all three layers by falsifying the identity of the attacking user to submit incorrect information to the network. This small sample of data security attacks demonstrates the clear lack of safety with the IoAV system and autonomous vehicles as a broader technology. Any of these attacks can be conducted with the intent to sabotage the operation of these vehicles on roadways, jeopardizing the lives and wellbeing of all motorists. As concluded by Ashish Nanda and his colleagues, these security issues must be addressed before both the IoAV and autonomous vehicles can be implemented in our society.

Data security issues not only threaten the wellbeing of autonomous vehicle users, but they also harm the public's perception of this new technology. There are several factors to consider when deciding upon a specific mode of transportation including comfort, cost, safety, reliability, and environmental impact. In a survey conducted by Nóra Krizsik and Tibor Sipos on expectations for self-driving vehicles, it was found that 80.1% of their participants expected safety, the highest of any of their categories (Krizsik & Sipos, 2023). Data security attacks pose a

direct risk to those engaging with autonomous vehicles, indicating that a lack in data security could correspond to a lack of public approval. Additionally, safety is not the only factor to consider when assessing the importance of data security. In a study that analyzed the importance of data privacy to consumers, Anya Skatova and her colleagues determined that individuals would willingly pay to ensure their personal data would remain private (Skatova et al., 2023). By prioritizing privacy ahead of cost, the consumers from Skatova's study demonstrated the distinct importance of data privacy. With the array of sensors and cameras used by autonomous vehicles, including possible iris recognition in some vehicles, data privacy remains all too relevant in this sociotechnical system (Raiyn, 2018). Data security attacks on autonomous vehicles compromise the privacy of its users, suggesting yet another reason why data security poses an obstacle for the development of autonomous vehicles.

In order to conduct an analysis on this research question, a link must be established between the issues with autonomous vehicle data security and the public's opinion on this matter. To do this, the STS concept of Mutual Shaping will be used. This concept suggests that society and technology interact in ways which serve to further the development of both. When applied to this research topic, Mutual Shaping will be used to suggest that the societal factor, the public's perception of autonomous vehicles, and the actual technology, autonomous vehicles, both work together to spur both technological and societal change. Society is shaping autonomous vehicles by necessitating safety, while autonomous vehicles are shaping society by changing the public's opinion on this new technology as its safety continually improves.

Methods

My paper seeks to address how data security issues within the broader technology of autonomous vehicles are preventing the development of this technology. In order to complete

this task, I will perform documentary analyses concerning two principle avenues. First, I will thoroughly explore the extent to which data security attacks can affect the operation and safety of autonomous vehicles. To do this, I will find sources that describe data security attack methods as well as those that document both fabricated and real-world data security attacks on autonomous vehicles. Second, I will locate first-hand opinions on data security issues with autonomous vehicles using primary sources such as blogs, periodicals, and forums. These primary sources will serve to provide insight into society's true opinions on data security with autonomous vehicles. After locating all of the previously stated sources, I will perform documentary analyses on all relevant information. Finally, I will synthesize a conclusive answer to my research question using the STS concept of Mutual Shaping.

Source Collection

In order to gather sources detailing data security attacks on autonomous vehicles, my search began with the reliable scholarly databases such as ProQuest. Within the broader avenue of data security attacks, I first sought out details on the various types of data security attacks on autonomous vehicles that exist. After continuous searching, I arrived at an article titled by Khan et al. that provided a sufficient understanding of several categories of autonomous vehicle data attacks including on-board camera attacks, LiDAR attacks, GPS attacks, and communication system attacks. The next set of sources to find were those detailing actual data security attacks and how they affect autonomous vehicle operation. To do this, I increased the depth of my search by analyzing the references provided by my current sources. This searching led to three relevant sources, one by Petit et al., one by Cao et al., and one by Giannaros et al. Each of these sources details a different data security attack and how that specific attack will be detrimental to autonomous vehicles once integrated into society.

My next goal was to find sources presenting opinions on data security attacks on autonomous vehicles. Initially, I began with a very thorough search of reliable public opinion sources such as the Pew Research Center and research databases with public surveys. Unfortunately, the specificity of my desired research topic proved to be an issue when consulting these databases. Currently, there are no such records of the public's opinion on data security issues with autonomous vehicles in these traditionally reliable sources. Location of the most relevant sources for my research would require a broader search medium. Thus, I decided to explore the contents of Reddit on this topic. One of the best virtual presentations of raw public discourse, I correctly suspected that Reddit could have the exact discussion of public opinion on data security issues with autonomous vehicles that I desired. After perusals of several different subreddits, I located a subreddit page that featured a lengthy conversation on data security issues with autonomous vehicles. Although Reddit is not a typically reliable source of information, in the case of my research, there is no better source of unfiltered public opinion. Additionally, within this subreddit were several other links to primary sources discussing the same topic, including a link to the website for the Human Driving Association. After researching this organization further, I realized their opinions would be valuable as they are dominantly focused on the safety of autonomous vehicles.

Results and Analysis

Overall, seven sources were gathered for my documentary analysis, four sources pertaining to the data security attacks on autonomous vehicles and three sources detailing the opinions of the public on this topic. Analysis of both groups of sources will be performed in order to determine an accurate response to the research question. This analysis will begin with the data security attack sources followed by the public opinion sources.

In order to analyze the data security attack sources, I will follow the following procedure. First, I will introduce a specific type of data security attack by referencing the article, by Khan et al., which provides a sufficient explanation of several types of attacks, including Camera Attacks, LiDAR Attacks, and Communication System Attacks. Next, I will reference one of the three remaining data security attack sources, which each detail a different occurrence of one of the aforementioned types of attacks. Finally, I will extract the broader implications of that specific attack pertaining to the development of autonomous vehicles. This process will then be repeated for the two remaining types of data security attacks.

Autonomous vehicles are heavily reliant on cameras, which are used to comprehend visual recognition of the vehicle's environment, including traffic signals and signs. This technology's inherent simplicity leaves it particularly susceptible to Camera Attacks. The most common of these attacks, Blinding Attacks, are performed by exposing the camera's lens to a light emitting device such as laser pointers or LED lights (Khan et al., 2021). These attacks can leave autonomous vehicles without camera input for several seconds, a dangerous duration of time for the operation of a motor vehicle. In the paper by Petit et al., a study is performed to determine the effectiveness of Blinding Attacks. Their experiment was performed by directing a Ledsee 650 nm diode point laser at a MobilEye C2-270 camera to analyze the obstruction of a black and white grid (Petit et al., 2015). The pre and post exposure pictures are shown below.

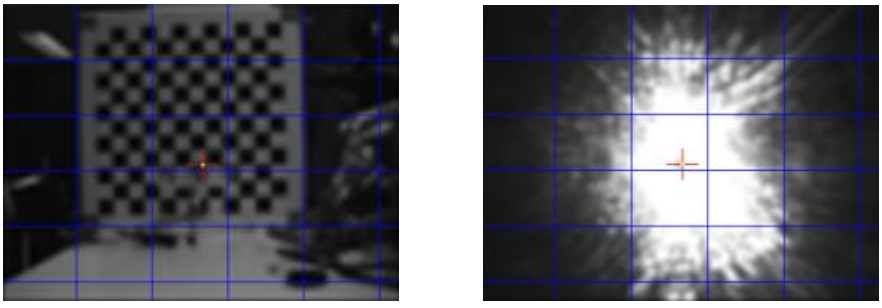

Figure 1: Camera view before (left) and directly after (right) a laser Blinding Attack (Petit et al., 2015)

In the initial picture, the black and white grid is easily distinguishable. However, after the Blinding Attack, the grid is undetectable to the camera. If applied in a real-life scenario, a Blinding Attack could prevent an autonomous vehicle from registering a traffic signal or a stop sign, which could lead to potentially deadly collisions.

Another crucial piece of technology for autonomous vehicles is Light Imaging Detection and Ranging (LiDAR). LiDAR sensors manipulate a rotating laser beam to generate a 3D point cloud of objects surrounding the sensor. Autonomous vehicles use these sensors to determine the locations of obstacles and road features within the vehicle's environment. LiDAR Attacks can be performed by using transceivers to receive a laser point from the sensor and either move, multiply, or block the collected points (Khan et al., 2021). Spoofing Attacks are a common division of LiDAR Attacks where non-existent objects are generated in the LiDAR's 3D point cloud. These attacks can be used to prevent operation of an autonomous vehicle or even to halt traffic on motorways. In the paper by Cao et al., a Spoofing Attack is conducted using a simulation platform. To conduct this attack, an adversarial 3D point cloud was used to spoof an obstacle into the simulated autonomous vehicle's LiDAR sensor data (Cao et al., 2019). A picture of the resulting simulation is shown below.

Figure 2: Simulated Spoofing Attack (Cao et al., 2019)

As shown in the above simulation picture, despite the traffic light being green, the autonomous vehicle will not proceed due to the spoofed obstacle. If applied in a real-life scenario, a major highway could be completely blocked with distributed Spoofing Attacks on multiple autonomous vehicles. An issue like this could cause multiple-vehicle collisions or could prevent emergency vehicles from reaching their destinations.

Communication System Attacks pose a significant threat to the safety of autonomous vehicles as well. Within an autonomous vehicle, a central computer is responsible for controlling every vehicular operation. In order to handle this task successfully, the computer must constantly receive and transmit information from every sensor and actuator onboard. This constant flow of information can be maliciously infiltrated in order to alter either alter the processed information or prevent the transmission of information altogether (Khan et al., 2021). Without having access to the proper information, the computer of an autonomous vehicle can make incorrect decisions, which would lead to potential accidents. In the paper by Giannaros et al., a real-life instance of a Communication System Attack on an autonomous vehicle is discussed. In this scenario, a virus was developed to manipulate messages transmitted by the controller are network (CAN) bus, a crucial communication system used to link all vehicle components (Giannaros et al., 2023). This malware was used to remotely lock the doors of a vehicle, preventing external vehicle access. Although this was a relatively local issue, if used on autonomous public transportation, a Communication System Attack such as this one could cause significant widespread issues.

In order to analyze the public opinion sources, I will follow a more straightforward procedure of citing the relevant information from each of the three sources in a cohesive manner. It is worth noting that although they are traditionally viewed as unreliable sources due to their lack of review and biases, forums and blogs can provide unique, unfiltered documentation of

public opinion. Thus, I have opted to feature these primary-sources in order to provide valuable insight into what real people think about my research question.

Located in the subreddit /r/SelfDrivingCars, user Ilovemobility1016 posed the initial question, "What do you think are some of the biggest cyber security concerns related to self-driving cars?" (Ilovemobility1016, 2018). This question sparked a vast discussion of the current data security limitations of autonomous vehicles. More importantly, each reply in this forum featured individual users' opinions on the topic. There were many different perspectives and arguments present in this thread, but the overarching themes emphasized that although there is currently an array of data security issues with autonomous vehicles, the industry is still heading in a direction towards autonomous vehicle domination. This will be an important idea to consider when trying to answer my research question. Another useful trait of this subreddit was the ample supply of external references. One such reference led me to the website for the Human Driving Association (HDA), an organization founded by journalist Alex Roy that seeks to proactively guide the development of autonomous vehicles while still maintaining the freedom choice (Perez, 2018). Perez's explanation of the HDA concludes that despite being members of a group that opposes a complete takeover by autonomous vehicles, they still see the overall value of such a technology and instead are trying to help it develop in a reasonable way. Upon arriving at the HDA's website, I was promptly greeted by the Alex Roy's Human Driving Manifesto, a twelve-pointed list of the HDA's desires for the further development of the autonomous vehicle industry. Point number five of their Manifesto states that they "support defined safety standards & transparency" (Roy, 2018). The pure existence of this organization suggests that there are currently very real safety issues with autonomous vehicles that are threatening enough to generate organized groups who share negative public opinions of autonomous vehicles.

Using the information gathered from an in-depth analysis of these seven sources and the cohesion provided by Mutual Shaping, I can now sufficiently devise an answer to my research question. After analyzing the data security attack sources, it is evident that in their current state, autonomous vehicles are susceptible to a diverse assortment of data security attacks that could threaten the lives of all roadway users. Through the medium of Mutual Shaping, these dangerous data security issues are directly increasing the public's desired level of data safety, as demonstrated by the interactions found in /r/SelfDrivingCars and the Manifesto of the HDA. Conversely, while being opponents of autonomous driving, the HDA is attempting to guide and influence the development of autonomous vehicles to be in agreeance with their values, a clear demonstration of the technological development element of Mutual Shaping. Because of the catalyzation of development between autonomous vehicles and the public's perceptions on data security issues with this technology, Mutual Shaping is evident. ***From this analysis, it is clear that although current data security issues with autonomous vehicles are preventing their immediate, widespread incorporation into society, the Mutual Shaping that exists between the opinions of the public and these data security issues will effectively support the long-term development and adoption of this technology.***

Conclusion:

Just as manually operated cars were once an emerging engineering marvel, now autonomous vehicles have taken their place. However, since autonomous vehicles are still a relatively new technology, there still remain several problems that could threaten their future adoption into society. Data security issues are one such problem that could complicate the integration of autonomous vehicles. In order to determine the extent of this complication, this paper was written to address the research question, how are data security issues affecting the

development of autonomous vehicles? Using a documentary analysis of several papers, journals, and primary sources that all discuss this topic, an answer has been successfully formulated. Based on this evidence and the support from Mutual Shaping, it was concluded that autonomous vehicle data security issues are currently a limiting factor due to safety concerns. However, the repeated iterations of increased public standards and available improvements to autonomous vehicles will ultimately lead to the success of this technology. Additionally, current technological additions to vehicles that increase their data security, such as data encryption and identity authentication, support this conclusion.

Studies such as this one should be repeated for all current issues with autonomous vehicles in order to determine the most relevant issues to address. Some of these problems include vehicle reliability, charging station availability, autonomous decision-making, vehicle affordability, and environmental sustainability. As more research is conducted on this topic, the potential for autonomous vehicles to be publicly accepted will continue to grow until they are ultimately adopted as a reliable mode of transportation.

Works Cited

Banerjee, S. (2021). Autonomous vehicles: a review of the ethical, social and economic implications of the AI revolution. [Autonomous vehicles] *International Journal of Intelligent Unmanned Systems*, 9(4), 302-312. https://doi.org/10.1108/IJIUS-07-2020-a0027

Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q. A., Fu, K., & Mao, Z. M. (2019). Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 10A. https://doi.org/10.1145/3319535.3339815

Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G., & Tsolis, D. (2023). Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy*, 3(3), 493–543. https://doi.org/10.3390/jcp3030025

Ilovemobility1016. (2018, October 16). Cyber Security concerns with Self-Driving Cars? Reddit. https://www.reddit.com/r/SelfDrivingCars/comments/9oohpt/cyber_security_concerns_with_selfdriving_cars/

Khan, F., Lakshmana Kumar, R., Kadry, S., Nam, Y., & Meqdad, M. N. (2021). Autonomous vehicles: A study of implementation and security. *International Journal of Electrical and Computer Engineering*, 11(4), 3013-3021. https://doi.org/10.11591/ijece.v11i4.pp3013-3021

Krizsik, N., & Sipos, T. (2023). Social Perception of Autonomous Vehicles. *Periodica Polytechnica Transportation Engineering*, 51(2). https://doi.org/10.3311/pptr.20228

Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. A. (2019). Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. *IEEE Wireless Communications*, 26(4), 60–65. https://doi.org/10.1109/mwc.2019.1800503

Perez, S. (2018, March 27). The Human Driving Association. Turo. https://turo.com/blog/gearheads/the-human-driving-association/

Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015, November). Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Black Hat Europe.

Raiyn, J. (2018). Data and Cyber Security in Autonomous Vehicle Networks. *Transport and Telecommunication Journal*, 19(4), 325–334. https://doi.org/10.2478/ttj-2018-0027

Roy, A. (2018). Human Driving Association. Human Driving Association. https://humandriving.org/

Sitinjak, C., Tahir, Z., Toriman, M. E., Lyndon, N., Simic, V., Musselwhite, C., Simanullang, W. F., & Hamzah, F. M. (2023). Assessing Public Acceptance of Autonomous Vehicles for Smart and Sustainable Public Transportation in Urban Areas: A Case Study of Jakarta, Indonesia. Sustainability, 15(9), 7445. https://doi.org/10.3390/su15097445

Skatova, A., McDonald, R., Ma, S., & Maple, C. (2023). Unpacking privacy: Valuation of personal data protection. PLOS ONE, 18(5), 1–21. https://doi.org/10.1371/journal.pone.0284581

Stanchev, P., & Geske, J. (2016). Autonomous Cars. History. State of Art. Research Problems. Communications in Computer and Information Science, 601, 1–10. https://doi.org/10.1007/978-3-319-30843-2_1

Szűcs, H., & Hézer, J. (2022). Road Safety Analysis of Autonomous Vehicles An Overview. *Periodica Polytechnica Transportation Engineering*, 50(4), 426-434. https://doi.org/10.3311/PPtr.19605

Xie, C., Cao, Z., Long, Y., Yang, D., Zhao, D., & Li, B. (2022). Privacy of Autonomous Vehicles: Risks, Protection Methods, and Future Directions. *ArXiv.org*. https://doi.org/10.48550/arXiv.2209.04022