DATA ACQUISITION OF AUTONOMOUS VEHICLES AND IMPLICATIONS ON USER AND PUBLIC PRIVACY AND SECURITY

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

By

Jacob E. Deane

March 28, 2022

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

Catherine D. Baritaud, Department of Engineering and Society

AN EVALUATION OF UPCOMING AUTONOMOUS VEHICULAR TECHNOLOGY AND THE EFFECTS ON ITS USERS AND PUBLIC PRIVACY

Autonomous vehicles (AVs) are the next step in transportation, being the first to transition the common era into the future of artificial intelligence. The rise in popularity of AVs can be attributed to the ease of transportation they would provide compared to current vehicles on the road today. Disabled and elderly would gain immense independence and the roads would become a safer place considering "[a]pproximately 90% of crashes are the result of mistakes by the driver" (Ryan, 2019, p. 1190). Commuters could relax on the way to work and save hours every week by utilizing the autonomous driving capabilities. While the safety of the autonomous software architectures are still being tested, the necessary electrical components of AVs are already on the road today.

Electric vehicles, the first step to self-driving cars, are rising in popularity and it is estimated that "by 2040, 58% of global passenger vehicle sales will come from electric vehicles" (Kopestinsky, 2021, "Electric Car Statistics Worldwide" sect.). In the technical project, the team will be replacing a stand-alone mechanical driving system in a 2008 Ford Escape with an electromechanical drive-by-wire system. The goal is to control the vehicle through a practical external controller, but to do so in a way that would allow for future autonomous driving capabilities to be installed. The team, consisting of fourth-year mechanical engineering students Jacob Deane, Henry Goodman, Logan Montgomery, Alex Pascocello, Vishal Singh, and Matthew Deaton, is led by Professor Tomonari Furukawa, a highly respected and published researcher in the fields of robotics and computational mechanics. A key feature of the project is connecting to and reading the controller area network (CAN) bus of the car, which collects the information on the car's systems.

While current CAN bus systems work remotely in each vehicle, new autonomous vehicles will require a connection to several outside machines to grapple with mass data collection. AVs require these mass amounts of data to operate efficiently in fluctuating environments and use sensors such as LiDar, Radar, and cameras to do so. This opens a dangerous opportunity for hackers to gain control over the systems of the vehicle and the information it holds on the user. While companies are aware of this threat, there have been difficulties in protecting the current designs from malicious hacking.

It must be acknowledged, as well, the impact this immense data collection will have on public privacy. AVs will monitor and record data on parties other than the user who has accepted any terms and conditions. Pedestrians or other cars on the road will be surveilled without clear approval and car companies will have legal access to all the information. Regulations are unclear as to whether companies can sell this data to insurance companies, for example, to monitor clients' motor safety and recalculate interest rates. Police could potentially subpoena collected data for lawsuits or investigations. Hackers could maliciously corrupt or steal this information. The safeguards from thousands of cameras patrolling every street are not currently sophisticated enough to allow AVs to be safely implemented into society.

The intent of this STS research paper, tightly coupled to the technical project, is to identify and analyze potential threats this upcoming technology may cause and compare current solutions being developed. The technology transfer model based on the Social Construction of Technology (SCOT) theory (Pinch & Bijker, 1984, "Social Construction of Technology" sect.) will aim to identify the effects this technology will have once given to the relevant social groups. It is imperative for this research paper that this analysis be thorough in order to accurately assess the risks and threats AVs will have on different groups in society. Autonomous vehicles can create safer roads and give great freedom to those unable to drive, but there must be precautions set forth before their adoption to ensure users' and the public's privacy and control remain safe.

CURRENT PROGRESS OF AUTONOMOUS VEHICLES

HISTORY AND ADVANTAGES TO TRANSPORTATION

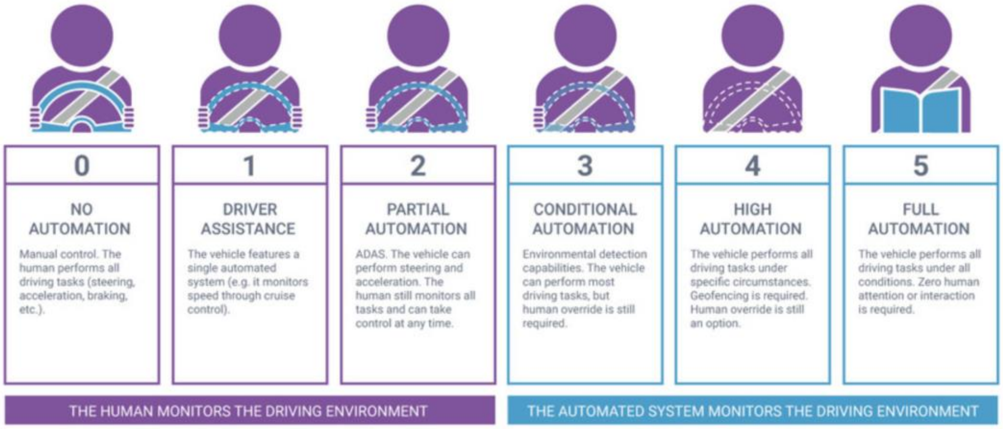
Drive-by-wire vehicles are integral to the progress of autonomous cars in the near future. They provide more freedom of driving to those disabled and can allow for safer roads. Additionally, drive-by-wire techniques can be used by military or medical experts to control machinery from safe distances. Carbon emission decrease is another advantage autonomous vehicles present to society. Reliably, this approach to car manufacturing results in:

> (1) enhanced safety and comfort,
>
> (2) reduced cost associated with manufacturing and maintenance, and
>
> (3) elimination of environmental concerns caused by hydraulic systems. (Xiang, 2008, p.138)

Drive-by-wire was developed following the success of fly-by-wire, a process used by NASA in the 1970s to control the Apollo Lunar Module (National Museum of American History, 2018, para. 1). It is comprised of a series of sensors and actuators connected to the CAN bus matrix. The CAN bus to a car is like "the nervous system in the human body," (Autopi, 2021, "CAN Bus Easily Explained" section) as it enables communication between the sensors within the system. This allows information collected by sensors such as LiDar and Radar to communicate with the system through a central core processing station, simplifying communication across the vehicle.

CURRENT AUTONOMOUS VEHICLES IN PRODUCTION AND USE

When discussing the autonomy of AVs there are several levels of control that the vehicles are classified under. Seen in Figure 1, there are zero to five levels of autonomy, the first three of which are driver controlled with the latter having the autonomous system monitor the driving environment.



Manual control. The human performs all driving tasks (steering, acceleration, braking, etc.).

The vehicle features a single automated system (e.g. it monitors speed through cruise control).

ADAS. The vehicle can perform steering and acceleration. The human still monitors all tasks and can take control at any time.

Environmental detection capabilities. The vehicle can perform most driving tasks, but human override is still required.

The vehicle performs all driving tasks under specific circumstances. Geofencing is required. Human override is still an option.

The vehicle performs all driving tasks under all conditions. Zero human attention or interaction is required.

Figure 1: Classifications of levels of autonomy present in autonomous vehicles. Further classified by the environmental monitor. (Synopsis, n.d.)

The majority of current autonomous controls in cars such as self-parking and certain cruise controls fall under level two autonomy. This is because human monitoring of the environment is required. Currently, there are no truly autonomous vehicles being used on the roads. This is due to arguably the greatest difficulty AVs face: other drivers. The spontaneity of humans creates situations that require instant reaction times.

Tesla, General Motors, and Ford have all begun improvements on their level 2 autonomous vehicles, creating smarter cruise controls to aid in driver functionality (Lewin, 2021, "Where We're At" sect.). Mercedes-Benz in December, 2021 became "the first automotive company in the world to meet the necessary requirements for approval of the Level 3 autonomous driving system." (HT Auto Desk, 2021, para. 1) While this accomplishment is outstanding for the field of AVs, there are still many safeguards to be implemented before further integration can be accepted.

THREATS OF DATA ACQUISITION ON USER AND PUBLIC PRIVACY AND SECURITY

COMPANY REGULATION OVER AUTONOMOUS VEHICLE DATA AND USER CONSENT

As previously stated, AVs will require large amounts of data on the outside environment to successfully understand and adapt to changing road conditions. The use of externally mounted sensors along with wireless connections to roadside sensors will be the eyes and ears of the vehicle, collecting the required information to perform safe driving procedures. Privacy concerns develop regarding the power car companies will have over the data collected on its users. This data includes, but is not limited to, "the speed of the vehicle, its location, and the direction of movement" along with roadside units which record "overall traffic information" (Nanda, 2019, p. 60). With this information someone can know a user's daily route to work, if the user speeds, where the user lives, and that's just with basic data the vehicle collects. If a phone or voice assistant is integrated into the car's software it could record conversations, read texts, or monitor in-vehicle purchases (Karnouskos, 2018, p. 161). While this data can be used to greatly enhance a user's experience, it is also required for general safety to understand what companies can use this data for otherwise.

Jim Farley, Chief Executive Officer of Ford, said in a statement in 2014 at the Consumer Electronics Show:

"We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone" (Riontino, 2021, "Addressing Privacy Concerns" section).

Though Farley later retracted the statement, his "quote highlights the privacy implications of data collection and use in vehicles." (Riontino, 2021, "Addressing Privacy Concerns" section). There are few legal regulations on car manufacturers as to the power they have over the data accumulated by their vehicles.

This begins addressing the main struggle maintaining balance between data privacy and the required breach in privacy to collect the data. For example, the General Data Protection Regulation (GDPR) has been hindering the progress of self-driving vehicles precisely due to this dilemma. Countries without the GDPR have been more successful in their advancements of autonomous vehicles because they have not had to "navigate between privacy and data protection on the one side, and the need for vast amounts of processing data for [self driving vehicles] to function, on the other" (Ryan, 2019, p. 1194). In the United States this mass amount of data is privy only to the car manufacturers, which gives them an unprecedented amount of power over traffic, urban planning, home addresses, and private affairs. All of "that information is currently housed in technological and corporate black boxes" (Self-driving cars, 2019, para. 1) which is not transparent even to the user.

A place to begin this conversation would be concerning the "Terms of Use" document required to be signed before purchasing certain data-collecting items. However, due to the absurd length and "knowing that you have little… negotiating power" (Rodriguez, 2019, p. 15) over the terms discourages users from fully understanding the legal ramifications of acceptance. Instead, these Terms of Use should be succinct and clearly inform consumers the rights they are willing to waive for product use. Without these changes there is a lopsided power dynamic between car companies and users, stripping the users of essential privacies.

While users have the choice to opt into an agreement with car companies, the general public is often not given this chance for informed consent. AVs constantly record footage of unknowing pedestrians and drivers all over cities. While this feed can be encrypted, the car companies still have the power to use this footage however they see fit. There are numerous ways this data could be analyzed and used against non-users. Insurance providers could use footage of unsafe driving to raise monthly rates, countries could identify protestors, employees could stalk ex-girlfriends (Bloom, 2017, p. 358). Already, in a murder case in 2019 the GPS of the convicted murderer's Land Rover was used against him in the conviction (Miller, 2020, para. 17). It is very difficult to receive informed consent from random passersby and, since the public domain does not have an expectation of privacy, companies are less likely to attempt to receive it. The dangers of mass surveillance are prevalent in society today and the integration of AVs without proper laws of consent are sure to intrude on the privacy of the public.

INTERNET OF THINGS AND ITS ARCHITECTURE FRAMEWORKS

While electric and drive-by-wire vehicles are the current progression of AVs already implemented today, there are advancements to the software component as well. Before autonomous vehicles can become autonomous, they must first complete the step of looped controls. Several automobiles on the road already use these features such as “cruise control, parking, collision warning, lane-changing warning, pedestrian detection, platooning, and cooperative coordination” (Karnouskos, 2018, p. 160) which are all examples of these beginning decision-making capabilities. However, it may be a while until fully autonomous vehicles can be rolled out onto the streets as Larry Burns, previous head of research and strategy for General Motors said, “it took longer to do the next 9% than the first 90%, and the last 1% is taking longer than the 9%” (Yergin, 2021, para. 22). It’s this problem that the Internet of Things (IoT) platform aims to solve.

The IoT platform is “a network of various devices that connect to form a network and share information (Nanda, 2019, p. 60). These connections could be vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), vehicle-to-pedestrians (V2P), or vehicle-to-device (V2D), and these connections are expanding. The importance of the IoT platform stems from its capability to not only receive data from the vehicle’s mounted sensors, but from roadside sensors and other vehicles as well, drastically increasing data collection to roughly 25GB per hour (Karnouskos, 2018, p. 162). This allows for a broader environment to be mapped and thus improves decision-making capabilities in the vehicle.

A common architecture for IoT platforms resolves into three main layers: the sensing layer, network layer, and application layer. Ashish Nanda, a Ph.D. recipient from the University of Technology Sydney, describes these layers as the following. The sensing layer is responsible for the collection of data through sensors whether that be through the vehicle itself or outside connections. The data is then processed and transmitted through the network layer to the application layer. The application layer is the “resource powerhouse providing both storage and processing for the data (Nanda, 2019, p. 61). It is in this layer that the information can be applied to the vehicle’s decision-making processes. In Figure 2 the classification of layers along with their standard protocols are configured to understand the bottom up flow of data.

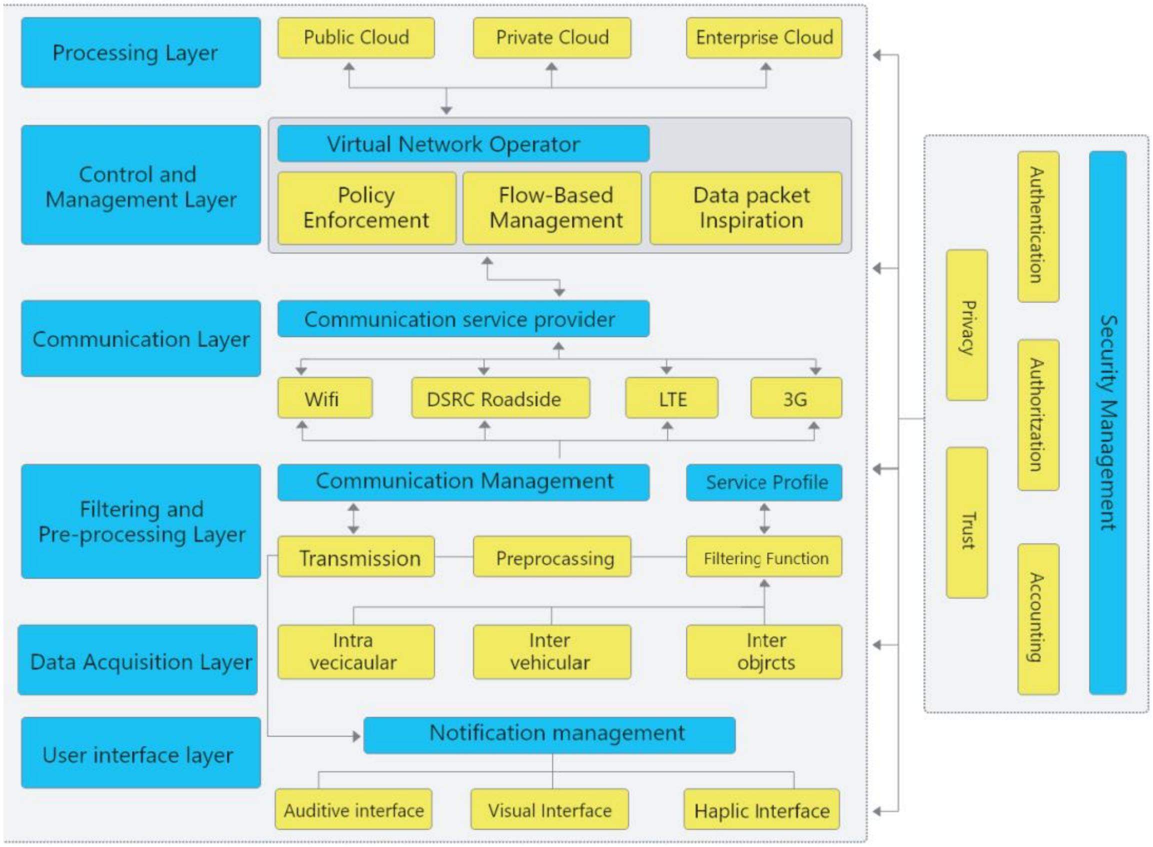


Figure 2: Classification of Internet of Things layered software architecture. The diagram represents the flow of data from the collection to application and how it is securely converted into applicable information. (Nanda, 2019, “Vehicular Communications: Layer Classifications” sect.)

These layers can be further broken down, but for this research paper it is important to know the main layers to understand their vulnerabilities. Also note the security profiles for each layer and the attempted protocols being protected within the architecture.

VULNERABILITY TO HACKING WITHIN INTERNET OF THINGS

While data in the hands of car companies is theoretically safeguarded by legal measures, there is still the real threat of the illegal obtaining of said data through malicious hacking of AVs. Hacking is as old as technology itself, and new technologies create new weaknesses. The IoT platform allows for multiple intrusions due to the abundant connections it creates every second. It would be near impossible to vet and authenticate every one of these connections in real time as decision-making on the road must be virtually instantaneous. These hacking attacks range from less severe instances of controlling the windows and data spoofing to very severe instances of full vehicle control and data theft.

There have already been several attacks on AVs across all companies. Abdullahi Chowdhurry, a Ph.D. recipient from Federation University Australia, along with his co-authors list the different types of attacks in their survey regarding attacks on self driving vehicles (Chowdhurry, 2020, para. V). The following figure showcases several different hacking methods and the part of the AV it attacks.

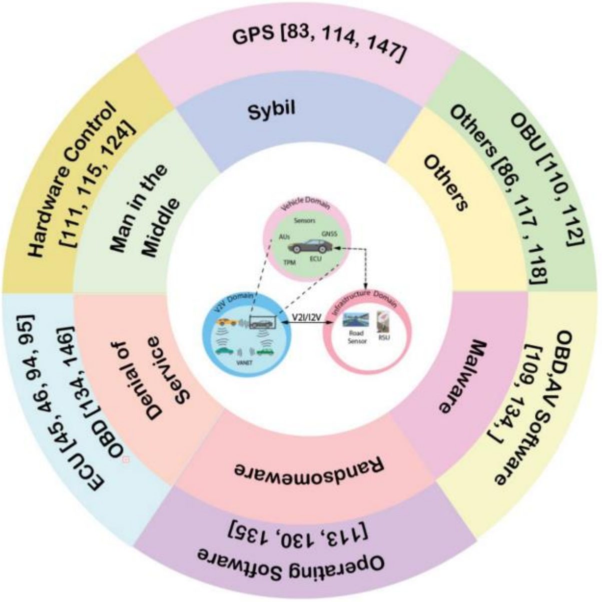


Figure 3: Classification of previously successful malicious hacks on autonomous vehicles by system targeted. The diagram in the center demonstrates V2I/I2V connections and where the connection is disrupted during an attack. (Chowdhurry, 2020, sect. V)

The first attack type is the malware attack where a hacker used bluetooth to insert malware into the On-Board Diagnostics (OBD) and control the brakes of the vehicle. Next there is the man-in-the-middle attack where a hacker can manipulate the communication from connections such as V2V or V2I to spoof the connection and eavesdrop or modify the messages being relayed. There is also a ransomware attack that does not threaten the vehicle itself, but the data it holds. In this attack, hackers encrypt the data commercial AVs hold and hold it ransom so the companies will pay for the decryption. Spoofing attacks focus on spoofing incoming data from onboard sensors to trick the vehicle into making a poor decision based on tampered data. The most common attack is Denial of Service (DoS) where the network is flooded with information and "is no longer responsive to genuine users" and causes poor decision-making (Nanda, 2019, p. 63). Finally, there are sybil attacks which convey false data by faking nodes that the integrated system misinterprets and thus acts inappropriately (Chowdhurry, 2020, para. V). All of these hacking methods have been successfully implemented whether maliciously or to prove a point and present real threats to the security not only to the data these AVs collect, but the safety of public roads.

The most important hacking method which was used by a nineteen year-old German teenager uses smartphones as a backdoor into AVs. David Colombo used a third-party app Tesla drivers used to analyze their vehicle's data to backend his way into 25 Tesla vehicles. He was only able to operate door locks, headlights, and stereo equipment, but it's just one instance of this attack succeeding (McFarland, 2022, para. 1-3). The most common android attack "is the use of an application containing malicious code imported when a specific web page or email is loaded" (Park, 2020, p. 2) to gain access to the vehicle head. The majority of drivers connect their smartphone to their vehicle whether to make hands-free calls or listen to music, and this is the perfect backdoor for hackers to install malware into AVs. Figure 4 explains the process in which a hacker can use a mobile device to gain access to the engine control unit (ECU) of a vehicle.

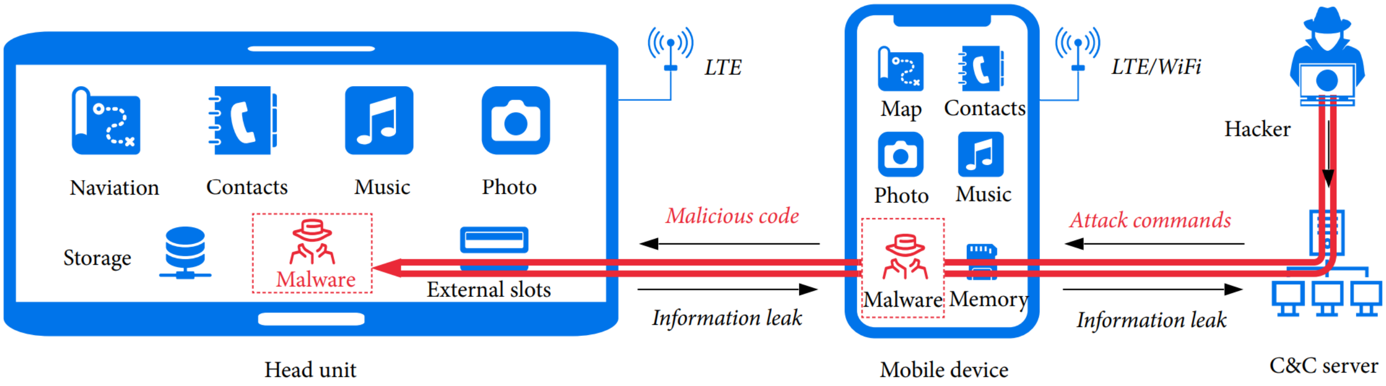
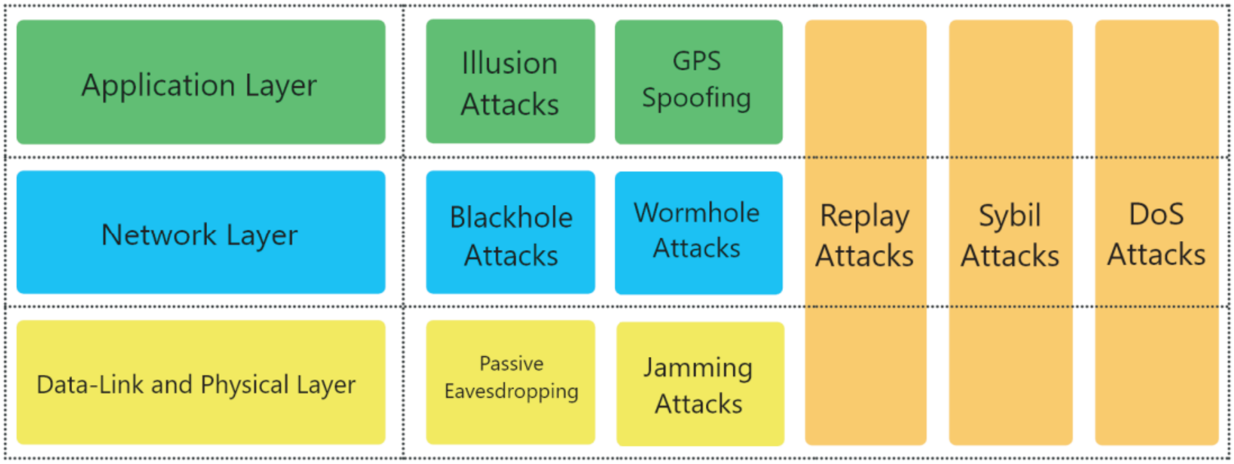


Figure 4: Infographic of malware inserted into autonomous vehicle software through android connection. It shows the hackability of autonomous vehicles through the placement of malware in an android device before connecting to the vehicle. (Park, 2020, sect. 3.1)

These are just some of the hacking vulnerabilities present in current AV software architectures. Figure 5 shows several more and what layer in the architecture they target.



Application Layer	Illusion Attacks	GPS Spoofing	Replay Attacks	Sybil Attacks	DoS Attacks
Network Layer	Blackhole Attacks	Wormhole Attacks			
Data-Link and Physical Layer	Passive Eavesdropping	Jamming Attacks			

Figure 5: Classification of hacking methods characterized by layers of architecture being attacked. (Nanda, 2019, “Taxonomy of Security Threats” sect.)

Blackhole and wormhole attacks convince a vehicle that the attacker is part of the IoT network and once it receives the data from the AV it drops all of it causing "the network to suffer data loss resulting in data retransmission." (Nanda, 2019, p. 63) This major loss in data affects the vehicle's decision-making and can lead to accidents.

As explained, there are a multitude of ways hackers can use the IoT network to deceive or overtake AVs. It is a serious threat to the safety of public roads and the mass data these AVs collect on users and pedestrians. Before the infrastructure can be further developed, solutions and safeguards must be improved to ensure public safety.

CURRENT SOLUTIONS IN DEVELOPMENT TO PREVENT MALICIOUS HACKING OF AUTONOMOUS VEHICLES

There are several ongoing attempts to provide security measures against malicious hackers. While these attempts solve some of the issues pertaining to potential malware threats, there are still weaknesses in the system.

Chowdhurry developed a list of security requirements for any IoT system to ensure safe driving experiences. These requirements include improved authentication between devices, data integrity and confidentiality, privacy and confidentiality of users, availability of exchanged data, traceability of mischievous devices, authorization of devices, non-repudiation of external data, and a robustness against peripheral attacks (Chowdhurry, 2020, para. IV). This is summarized by a spearhead of the autonomous technology and smart city movements, Stamatis Karnouskos's description of "the fundamental categorization of confidentiality, integrity, and availability" which is often used in computer security (Karnouskos, 2018, p. 163). With these security measures in mind, solutions can begin to be tested on IoT platforms.

A main challenge will be to prevent interferences between connected devices. In this area there are two solutions, each with its own drawbacks. First there is the obvious encryption of transmitted data. The drawback of this however, is "this prevents any computation on the data" (Karnouskos, 2018, p. 165) which prohibits the application layer from applying collected data. The other method is data perturbation which creates noise around the data to ensure privacy. The drawback is that "the accuracy of the computation is affected" (Karnouskos, 2018, p. 165) which is dangerous when dealing with AVs which require accurate data to function properly and safely. Recent methods have advanced this technique, but still have progress to be made to ensure complete data accuracy.

The next challenge faced in IoT security is in privacy and data integrity. Sensors must always provide accurate data of surrounding environments which is where hackers can manipulate data to affect negative results. One can attempt to test these connections first is with a zero-knowledge proof system. A proof system is considered to be zero-knowledge if "the verifier can compute while interacting with the prover it can compute by itself without going through the protocol" (Oded, 1994, p. 2). These systems can be performed between connecting devices to ensure trusted sensors. However, the hardware must still be protected as a working fire alarm will still go off if a lighter is held to it. Another possible solution is to maintain scores for devices based on past behaviors and thus developing trust in the system. While this could allow for more trusted connections, there are still ways to take advantage of reputable systems (Karnouskos, 2018, p. 165).

The final and arguably most difficult problem to assess is the spontaneous interactions between AVs. Due to the constant and immediate nature of these connections between autonomous vehicles it is "near impossible… to authenticate the subjects of such interactions"

(Karnouskos, 2018, p. 164). One possible solution being developed is a global ID which “can be used for vehicle identification throughout” (Nanda, 2019, p. 64) the IoT network. This would minimize identification and data spoofing by requiring verification of model RFID tags before communication is accepted, but would also lengthen synchronization periods in V2V connections.

There are some strong advancements in specific hacking attacks, specifically for android-based attacks. Seunghyun Park and Jin Young Choi who work at the Graduate School of Information Security at Korea University studying cybersecurity and computer engineering have developed an algorithm for discovering android-based malware insertion. Their algorithm was tested in comparison to several others and its “overall prediction accuracy was 90% or greater with binary classifications for all algorithms except [gradient boosting classifier]” (GB) which is only because with GB the “learning time costs are too large for general classification” (Park, 2020, p. 7). This algorithm gives hope to malware detection within IoT networks, but still leaves much work to do in overall platform security.

TECHNOLOGY IS A TOOL, AND A DANGEROUS ONE AT THAT

Technology, like a saw, hammer, or ax, is a tool. It is a tool for human use to aid in everyday lives and create a better future for humanity. With the rise of autonomous vehicles, a great tool will be added to society’s toolbox, but, like a saw, hammer, or ax, it could also cause great harm. Autonomous vehicles will require a constant accumulation of data on the outside environment and, because of this, it must be protected. Companies will require regulations over the use of this data and safeguards must be implemented in IoT networks to protect against malicious intervention. By analyzing these threats from the technology transfer framework it is possible to identify and assess the effects AVs will have on certain societal groups and prevent potential safety and privacy risks. If these precautions are adopted by all relevant parties, then there is a bright and exciting future for the world of transportation.

REFERENCES

Anderson, B. D. O. (1993). Controller design: Moving from theory to practice. *IEEE Control Systems*, *13*(4), 16–25. https://doi.org/10.1109/37.229554

Autopi. (2021, March 18). CAN bus explained (2021). *AutoPi.Io.* https://www.autopi.io/blog/can-bus-explained/

Belcarz, K., Białek, T., Komorkiewicz, M., & Żołnierczyk, P. (2018). Developing autonomous vehicle research platform – a case study. *IOP Conference Series.Materials Science and Engineering, 421*(2) http://dx.doi.org/10.1088/1757-899X/421/2/022002

Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). Self-driving cars and data collection: privacy perception of networked autonomous vehicles. *Thirteenth Symposium on Usable Privacy and Security*. Usenix

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. (2020). Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access*, *8*, 207308-207342. http://dx.doi.org/10.1109/ACCESS.2020.3037705

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. (2020). Attacks on self-driving cars and their countermeasures: A survey. [Figure 3]. *IEEE Access.* http://dx.doi.org/10.1109/ACCESS.2020.3037705

HT Auto Desk. (2021, December 11). Mercedes-Benz becomes world’s first to get level 3 autonomous driving approval. *Hindustan Times Auto*. https://auto. hindustantimes.com/auto/news/mercedesbenz-becomes-world-s-first-to-get-level-3-autonomous-driving-approval-41639196499051.html

Karnouskos, S., & Kerschbaum, F. (2018). Privacy and integrity considerations in hyperconnected autonomous vehicles. *IEEE Proceedings*, *106*(1), 160-170. http://dx.doi.org/10.1109/JPROC.2017.2725339

Kopestinsky, A. (2021, August 12). Electric car statistics in the US and abroad. *PolicyAdvice.* https://policyadvice.net/insurance/insights/electric-car-statistics/

Lewin., D. (2021, December 29). The current state of play in autonomous cars. *Hackaday*. https://hackaday.com/2021/12/29/the-current-state-of-play-in-autonomous-cars/

McFarland, M. (2022, February 2). Teen’s Tesla hack shows how vulnerable third-party apps may make cars. *CNN Business.* https://www.cnn.com/2022/02/02/cars/tesla-teen-hack/index.html

Miller, R. W. (2020, February 25). “Barbaric, medieval-style execution”: Man found guilty of killing retired lecturer with crossbow. *USA TODAY*. https://eu.usatoday.com/story/news/world/2020/02/25/gerald-corrigan-terence-whall-guilty-wales-crossbow-killing/4865955002/

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 Connections*, *26*(4), 60-65. https://doi.org/10.1109/MWC.2019.1800503

Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. A. (2019). Internet of autonomous vehicles communications security: Overview, issues, and directions. [Figure 2]. *IEEE Wireless Connections*. https://doi.org/10.1109/MWC.2019.1800503

Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. A. (2019). Internet of autonomous vehicles communications security: Overview, issues, and directions. [Figure 5]. *IEEE Wireless Connections*. https://doi.org/10.1109/MWC.2019.1800503

National Museum of American History. (2018, July 25). Driving by wire. *Smithsonian*. https://americanhistory.si.edu/america-on-the-move/driving-by-wire

Oded, G., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, *7*(1), 1-32. https://doi.org/10.1007/BF00195207

Park, S., & Jin-Young, C. (2020). Malware detection in self-driving vehicles using machine learning algorithms. *Journal of Advanced Transportation, 2020,* 9. http://dx.doi.org/10.1155/2020/3035741

Park, S., & Jin-Young, C. (2020). Malware detection in self-driving vehicles using machine learning algorithms. [Figure 4]. *Journal of Advanced Transportation,* http://dx.doi.org/10.1155/2020/3035741

Pinch, J. T., & Bijker, W. E. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399-441. https://doi.org/10.1177/030631284014003004

Riontino, M. S. (2021, January 15). Who will take care of data privacy on autonomous vehicles?. *Celantur*. https://www.celantur.com/blog/autonomous-vehicle-data-privacy/

Rodriguez, G. (2019). Autonomous vehicles and unmanned aerial systems. *IEEE Technology and Society Magazine*, *38*(3), 14-16. https://doi.org/10.1109/MTS.2019.2930264

Ryan, M. (2020). The future of transportation: Ethical, legal, social and economic impacts of self-driving vehicles in the year 2025. *Science and Engineering Ethics, 26*(3)*,* 1185-1208. http://dx.doi.org/10.1007/s11948-019-00130-2

Self-driving cars and geospatial data: Who holds the keys? (2019). *Ecn,* http://proxy01.its.virginia.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fself-driving-cars-geospatial-data-who-holds-keys%2Fdocview%2F2265708408%2Fse-2%3Faccountid%3D14678

Synopsis. (n.d.). The 6 levels of autonomy explained. [Figure 1]. *Synopsis*. https://www.synopsys.com/automotive/autonomous-driving-levels.html

Vanderwerp, D. (2019, June 11). What is power steering and how does it work? *Car and Driver.* https://www.caranddriver.com/features/a27888229/power-steering/

Xiang, W., Richardson, P. C., Zhao, C., & Mohammad, S. (2008). Automobile brake-by-wire control system design and analysis. *IEEE Transaction on Vehicular Technology, 57*(1), 138-145. https://doi.org/10.1109/TVT.2007.901895

Yergin, D. (2021, April 23). How electric, self-driving cars and ride-hailing will transform the car industry. Wall Street Journal. https://www.wsj.com/articles/how-electric-self-driving-cars-and-ride-hailing-will-transform-the-car-industry-11619189966