Business Informatics - Winter 2020

Information Security - BINF 711

Security and Privacy of Self-Driving Vehicles

Submitted by:

Zeina Kandil 43-12170

Tutorial Group: "BI T03"

14th of January, 2021

Table of Contents

1. Abstract

Industry experts predict that self-driving cars will be made available to the public population within the next five-to-ten years. However, this sort of heavy reliance on technology presents significant privacy and security issues that should be looked into prior to having these vehicles fully commercialized. This report delves into privacy issues of driverless cars, such as the privacy of owner and passenger information, location tracking, and sensor data about the vehicle's surroundings. It then tackles security issues such as hacking and software bugs. Another security issue is the controversial point of how the car should behave in case of an unavoidable accident.

2. Introduction

Location-based services (LBS) are gaining popularity due to the recent breakthroughs in mobile and wireless network technologies. They provide users with valuable information relevant to their location. However, they do not sufficiently protect the geographical locations of users. Amongst the popular technologies that utilizes LBS is the self-driving car (Asuquo et al., 2018: 1). Thanks to advancements in machine learning and Deep Neural Network (DNN), the promise of mainstream self-driving cars is soon to become a reality. Machine learning can be used by autonomous cars in various ways, such as analyzing road conditions by communicating with other cars, detecting unsafe road conditions, and helping drivers make safer decisions. Additionally, self-driving cars use sensors like cameras, Light Detection And Ranging sensors (LiDAR), and Infrared (IR). The sensors create a stream of data in real-time (Chernikova, Oprea, Nita-Rotaru, & Kim, 2019: 132).

Electronic Control Units (ECUs) of a vehicle are in charge of its mechanical units such as the brakes and engine. They transmit data in an in-vehicle network. Nevertheless, the interconnection is not limited to ECUs within the car itself. Vehicles share data with Road Side Units (RSUs) and other vehicles via Vehicular Ad-hoc Networks (VANets). Their communication with personal devices is through Wireless Personal Area Networks (WPANs) and they connect, via cellular networks, with service center systems. A connected vehicle is one that uses an external network as well as the in-vehicle network (Othmane, Weffers, Mohamad, & Wolf, 2017: 1).

With so many interactions and data collection techniques, the autonomous car is becoming an intimidating sensor platform that gathers information from the environment, other cars, and riders. It then proceeds to feed that information to other vehicles and entities. In spite of its help in achieving safer navigations, pollution control, and traffic management, it has formidable downsides. In essence, the Vehicle Grid has become an Internet of Things (IOT) or more accurately, an Internet of Vehicles (IOV). It has the capacity to make its own decisions on how it will deliver passengers from route to destination. Unfortunately, their ability to communicate with other vehicles threatens the privacy and security of the parties concerned (Joy & Gerla, 2017: 1).

3. Privacy Issues

Connected autonomous vehicles can allow mass surveillance in a comprehensive manner by monitoring the whereabouts of vehicles at all times and receiving data from the car's surroundings. They also have access to information regarding both owners and passengers of said vehicles (Bloom, Tan, Ramjohn, & Bauer, 2017: 358).

3.1. Privacy Violations on Owner and Passenger Information

Owners of self-driving cars, with all intents and purposes, consent to the terms and conditions of autonomous vehicles. This is similar to the way they agree to the terms and conditions of mobile applications like Google Maps. By doing so, owners renounce their legal rights to certain degrees of privacy (Bloom et al., 2017: 358).

Information on passengers is collected in various forms and for a multitude of reasons. One of which is to determine the level of attentiveness of a driver. With the current level of technology, most manufacturers insist on having the driver place their handS on the steering wheel. This ensures that the driver is ready to take over should anything happen. Furthermore, they are developing a system that alerts the driver of any potential dangerous circumstances that necessitate that they take command of the fleet themselves. These circumstances include situations such as pedestrians crossing the road, chaotic traffic jams, and cyclists on the road. In order for manufacturers to determine the efficacy of their alarm system they need to know how much of the results are due to human intervention. On one hand an overly-cautious driver will tend to take over before the alarm sounds off. On the other hand, the alarm might sound off for justified reasons and the driver does not respond quickly enough due to their lack of attention. To ascertain a driver's attentiveness, data is collected every 100 ms, which represents human reaction time. This data tells whether the driver’s hands were on the wheel and eyes were on the road. It also tells whether the driver was eating, reading, or talking (Joy & Gerla, 2017: 1-2).

Ubiquitous sensing capacities can be misused. Countries can use them to identify and locate dissidents. On occasion, an employee of the self-driving car manufacturing company could use the technology and information to stalk a celebrity or an ex-partner. As a matter of fact, Uber employees were exposed doing just that. In addition, sensors can trace the physical movements of all individuals within the scope of the car, which develops a chilling technology that can find anyone anywhere (Bloom et al., 2017: 358).

While this data is collected for sound purposes, its collection poses privacy challenges. If no appropriate measures are taken, auto dealers can have unjustified access to the commuting habits of drivers, which is a grave privacy concern. Therefore, only the data that is deemed strictly necessary to build the model for the optimization of the alarm system should be extracted. Any irrelevant piece of data should be eliminated (Joy & Gerla, 2017: 2).

3.2 Location Tracking

Cars are usually boarded by a certain rider. Therefore, tracking a vehicle is almost equivalent to tracking the driver’s whereabouts. Self-driving vehicles, and on a broader spectrum smart vehicles, are vulnerable to location privacy threats. A location privacy attacker poses a significant threat to location privacy. It reveals the identity of a vehicle and its users with the use of tracking algorithms, rendering users defenseless against social profiling. For example, a rider can be tracked by a malicious vehicle for social profiling using the location information contained in exchanged safety messages. Moreover, malicious vehicles can falsify their location information in an effort to deceive ambulances in emergencies for them to get away with hit-and-run incidents (Asuquo et al., 2018: 1).

The Tire Pressure Monitoring System (TPMS) is an electronic system that monitors the air pressure inside tires using a pressure sensor. It is an in-vehicle network gateway. It reports real-time tire-pressure information to the driver of the vehicle. The pressure sensor sends data to other ECUs located in the intra-vehicular network with the assistance of a radio frequency transmitter. Each tire that uses a TPMS receives a unique ID. Every 6 minutes, the TPMS updates the intra-vehicle network with the pressure in the tires. Since vehicles tend to have the same tires for long periods of time, by tracing TPMS messages, which contain the ID of the tires, the vehicle location can be tracked (Bernardini, Asghar, & Crispo, 2017: 16).

Telematics are also in-vehicle network gateways. They work on long range mobile networks or Global Navigation Satellite Systems (GNSS). Telematics systems are units that are connected to either the Internet or an external network using an integrated modem. Telematics services are often used to protect passengers by contacting emergency services in case of accidents. Consequently, a telematics box within a car monitors the location of the vehicle at any given time. Another helpful functionality of the telematics system is that it aids in finding stolen cars. All the same, this information is subject to privacy concerns (Bernardini et al., 2017: 13).

For instance, some insurance companies base their insurance policy on vehicle information. They are fed such information by the telematics system and analyze it. The insurance companies gather enough information to build a database of location data of the car. As previously mentioned, it is not too difficult to identify the car itself and through it the consumer. A proposed solution for the privacy concerns is a privacy-preserving scheme for the insurance service. It ensures that the insurance company receives only the minimum required data to determine the insurance risk per customer. In fact, the cost is calculated in the black box within the vehicle using encryption proxies. The outcome is sent out to the insurance company. Nonetheless, the insurance company has a right to request evidence. The vehicle would then reveal just the locations requested as evidence and the time (Bernardini et al., 2017: 16-17).

3.3. Data From Surroundings

Location information can be abused by malicious vehicles to stalk other road users and expose their personal identity, which is a breach of identity privacy (Asuquo et al., 2018: 1). From the perspective of pedestrians, there is a controversy regarding Street View technology like that of Google Street View. This technology was subject to attack because it does not blur faces sufficiently. Moreover, it detects Wi-Fi signals in the vicinity. In other words, it collects excessive data that is not necessarily relevant or required to perform its functions. Even though Google Street View technology is used in public spaces, the fact that it collects data about random people and their actions and behaviours did not result in a positive response and has prompted significant anxiety (Bloom et al., 2017: 360).

4. Security Issues

Security concerns of self-driving cars are not limited to the traditional security concerns of IT software. Sometimes, approaches that can advance the autonomy of self-driving cars are not adopted due to their perceived riskiness and liability to security attacks (Wagner & Koopman, 2015: 2). Security threats that are purely concerned with the physical safety of the living beings involved include abnormal behaviours of autonomous vehicles and ethical decision-making in algorithms regarding situations with a conflict of interests.

4.1 Security Attacks

A fully autonomous car relies on readings from sensors to form both short-term and long-term driving decisions. This emphasizes the importance of communication between sensors and ECUs. Self-driving cars' control panels are designed to improve the car's autonomous movements. However, the presence of such technology exposes the car to security threats. The car becomes subject to potentially malicious attacks from viruses, bugs, and hackers. This explains why manufacturers arm self-driving vehicles with advanced data encryption and protection to improve their reliability and accuracy. Despite all of that, automatic vehicles are still subject to threats and security attacks can occur on all technology devices built in them (Chowdhury, Karmakar, Kamruzzaman, Jolfaei, & Das, 2020: 207309).

4.1.1 GPS-Based Attacks

Systems that rely on GPS, such as self-driving cars, are susceptible to several types of attacks. Those involve jamming and spoofing among others. The concern here is that they can be successfully executed by relatively unsophisticated attackers (Hubaux, Capkun, & Luo, 2004: 52). GPS jamming and spoofing are further explained in 4.1.1.1 and 4.1.1.2 respectively.

4.1.1.1 GPS Jamming

This form of attack happens at the corporal level. The communication network is interrupted by feeding it noisy signs that elevates the level of intervention. By reducing the signal to noise ratio, the autonomous car is rendered incapable of exchanging messages with other vehicles and the RSUs. In GPS Jamming, the attacker can alter the course of the vehicle, putting the lives of passengers at risk. There are certain techniques that can be applied to detect and moderate such attacks. One potential solution would be to use Frequency Hopping Spread Spectrum (FHSS) tools that depend on intelligent pseudorandom creator algorithms in orthogonal Frequency-Division Multiplexing (OFDM) standards to actualize the rate of recurrence (Chowdhury et al., 2020: 207330-207331).

4.1.1.2 GPS Spoofing

GPS Spoofing is a form of attack that deceives a receiver by using a GPS satellite simulator to broadcast fake GPS signals that are stronger than the legitimate GPS signals (Hubaux et al., 2004: 52). If a GPS signal gets spoofed, the central control system for navigation becomes the first victim to be misled by malicious attackers. When this attack is targeted at vehicles, it has severe consequences because of the criticalness of the locations of vehicles to navigation systems. The severity of the attack is multiplied when the vehicle is self-driving. Autonomous driving depends on sensor data including the position of the vehicle as detected by the GPS (Wang, Lu, Gao, & Qu, 2018: 1).

One straightforward anti-spoofing approach is to employ multiple receivers. By using several receivers to check the incoming signal, slight changes caused by the spoofed source are detected by the external receivers Unfortunately, sophisticated attackers can replicate spoofed signals and send them out to multiple GPS receivers. Sophisticated spoofing attacks are more difficult to detect by multi-receivers due to the way they produce spoofing signals for multiple satellites such that they camouflage in the midst of legitimate signals. Alternative techniques that detect GPS spoofing analyse the signals in terms of arrival time or received strength (Wang et al., 2018: 1).

4.1.2 Impersonation Attack

Impersonation attacks are when owners of vehicles intentionally steal another vehicle’s identity and attribute it to their own vehicle to falsify authentication of vehicular communications (Qin, Wu, Domingo-Ferrer, & Zhang, 2011: 131). This sort of attack can be mitigated by safeguarding the vehicle’s identity in a certified tamper-resistant hardware with the aid of modern authentication protocols. Electronic license plates are better equipped to withstand such attacks than physical ones (Hubaux et al., 2004: 52). Impersonation attacks are also commonly referred to as masquerade attacks (Othmane et al., 2017: 13).

4.1.3 Sybil Attack

When an attacker uses several identities to deceive communicating parties, this is known as a Sybil attack. For instance, a malicious vehicle poses as several different vehicles to report certain data. When the data is received from a large number of vehicles it is deemed credible

(Othmane et al., 2017: 13-14). Sybil attacks can be identified by jammed network systems with some counterfeit nodes hiding in the system. They prevent the self-driving vehicle from transmitting data and detecting attacks. As a consequence, accidents are likely to occur. A well-known Sybil attack took place in 2018 on Google's car. Attackers took advantage of the routing table's flaws, and non-encrypted messages of Google car. They created fake nodes and used them to communicate, to the Google car, false location information and traffic conditions information. The Google car displayed incorrect GPS location which resulted in the vehicle stopping, dangerously, in the middle of the streets (Chowdhury et al., 2020: 207322).

4.1.4 Denial of Service Attack

Malicious attackers flood the communication channel with dummy messages to close off useful communications between a vehicle and external entities in Denial of Service (DoS) Attacks (Othmane et al., 2017: 13). DoS are amongst the most life-threatening attacks that can strike self-driving vehicles. If a self-driving car is denied access to its ECUs or its Onboard Units (OBU) mid driving, the outcome can be fatal. DoS attacks can target cameras, Lidar, and Radar to prevent the vehicle from detecting objects, the road, and safety signs. They can even interfere with the braking system and claim control of it (Chowdhury et al., 2020: 207321).

A proposed solution for DoS attacks is to sign messages, communicated between vehicles, with the Elliptic Curve Digital Signature Algorithm (ECDSA). The downside is that 7ms of computation, on a typical OBU, are needed to verify a single ECDSA signature. Unfortunately, attackers are capable of creating and sending out invalid signatures very quickly. The average time elapsed between the arrival of two messages to the OBU is referred to as the arrival time. Meanwhile, the average time the OBU takes to verify the signature of received messages is known as the processing time. By exploiting the difference between processing and arrival times, a DoS attacker could limit the availability of the OBU by jamming it with useless messages (Othmane et al., 2017: 23).

4.1.5 Wormhole Attack

When an attacker has access to two communicating vehicles, they can tunnel packets of false information broadcasted in one location to another. This is a form of malware attacks called a Wormhole Attack (Chowdhury et al., 2020: 207331). A wormhole attack can deceive the vehicle's traffic management applications by feeding traffic information from a vehicle in a crowded zone to vehicles in another zone (Othmane et al., 2017: 12).

A wormhole attack on VANets steals data from non-neighbouring vehicles. Therefore, an optional solution is to apply Neighbour Verification by Overhearing (NEVO). It is a protocol that verifies the proximity of any vehicle using a sequence of three messages exchanged between neighbour nodes *i* and *j*. In the first exchange, node *i* starts by broadcasting a message probe query (PQ). Upon receiving the PQ from node *i*, node *j* rebroadcasts the message as its probe forward (PF) in the second exchange. The third exchange is when node *j* sends a probe reply (PR) to node *i*. The PR contains the processing delay, *δ*. Node *i* can then verify if node *j* is its neighbor by checking against the equation $toh - txj - \delta \leq 2R / sp$, such that toh is the delay time for node *i* in overhearing node *j*, *txj* represents the propagation range of the radio signal, and the speed of the radio signal propagation is *sp*. (Othmane et al., 2017: 20).

4.2 Behavioral Anomalies

With the current driving model of humans being behind the wheel, abnormal driving behaviour stems from the susceptibility of human beings to depressants such as fatigue or aggression. Abnormal driving behaviours also encompass weaving, swerving, turning, and sudden braking. Regrettably, autonomous vehicles can also demonstrate driving anomalies due to technology errors. Self-driving vehicles can exhibit erroneous behaviour in situations involving uncertainty, complexity or in unseen environments. There are two main approaches to detect anomalies in autonomous driving: Gaussian Processes (GP) Anomaly Detection and Convolutional Neural Networks (CNN) (Ryan, Murphy, & Mullins, 2020: 1-3).

In GPs Anomaly Detection, the objective is to model driving patterns based on human driving and use them against the driving behaviour of the sample autonomous vehicle, to statistically identify outliers. This is done by modeling normal driving by humans using Gaussians processes to identify statistical anomalies from the probability distribution of observing sensor readings. 95 % of observations of the sample autonomous vehicle exceeded $\mu \pm 1.96\sigma$, for steering angles and velocities. These are referred to as spatial or contextual anomalies and represent unsafe driving events. Anomalies are known as the squared difference between actual observations and mean predictions as extracted from the GPs. One of the advantages of this approach is that it does not mandate the existence of preliminary knowledge of the underlying risk. Instead, it directs its focus on materialized unsafe driving behaviours such as swerving, hard braking, hard cornering, and sudden accelerating. In self-driving cars such behaviours are usually attributed to hardware failures. Regardless of the underlying risk, the GP anomaly detection and risk scoring approach uses the frequency and severity of safety-critical incidents to measure the risk for both self-driving cars and normal cars (Ryan et al., 2020: 5).

This approach is used in a variety of applications. One of them is the vehicle trajectory estimation. The vehicle trajectory can be estimated using lateral and longitudinal velocities, and the coordinates as inputs to the GP. Alternatively, vehicle trajectory models can use GP regression in the identification of normal and anomalous traffic flows (Ryan et al., 2020: 5).

While CNNs are similar to DNNs in the sense that they both consist of a sequence of layers consisting of neurons, they differ in their arrangement; CNNs are 3-dimensional. The weights of CNNs, used to detect anomalies, are trained to minimize the squared error between predicted steering angle and velocity commands and the command output of the human driver. The network observes images generated by human drivers, each of which has a corresponding steering angle and velocity command. Following that, the CNN is trained to mimic the observed behaviour. Different CNNs, with identical network structures, are used in parallel to control the autonomous vehicle, after being trained for steering and velocity predictions. This helps overcome behavioural anomalies in self-driving vehicles (Ryan et al., 2020: 7).

4.3. Ethical Decision Making in Algorithms

Substituting humans with a reliable piece of software, that neither consumes alcoholic beverages, suffers from stress, nor disregards traffic lights and speed limits, is estimated to reduce accident rates by 90%. In addition, it will enable individuals who are currently incapable of driving, like underaged individuals, senior citizens, and those with disabilities, to commute independently. Interconnected vehicles can share important information in real-time such that the safety distances between vehicles on the road can be reduced with no risk. This will permit a more efficient distribution of vehicles within a road network, which should enable a larger number of vehicles to travel together in a faster and safer manner. Not to mention, they will reduce rates of global pollution notably (Coca-Vila, 2018: 60).

Nonetheless, self-driving cars are still subject to traffic accidents. They can be caused by cars driven by humans, reckless pedestrians, wild animals, and unfavourable weather conditions. Autonomous cars can be to blame as well; a car can be poorly programmed; it can have mechanical problems; and its program can be hacked into as mentioned previously in this paper. There are several ethical issues that arise regarding how self-driving cars should be programmed to behave when crashes are inescapable. Ethical decision making in life-or-death decisions made by self-driving cars is a major concern of the public. It has been one of the greatest influences that make people reject autonomous vehicles (Bloom et al., 2017: 358). There are two principles that a self-driving vehicle can be programmed to follow. On one side, the first principle dictates that the vehicle should always take the route that is in favour of the occupants of the vehicle. On the other side, the second principle stipulates that the autonomous car should seek the route that results in the smallest possible social damage for all parties concerned (Coca-Vila, 2018: 59-60).

Ethical egoism supports the programming of emergency algorithms to always have the vehicle's passengers' best interests at heart. The argument is that this is how a human driver would behave. As a matter of fact, it is debated that by not doing so they are depriving passengers of their right to self-preservation, which is an instinct accepted socially and ethically. An autonomous car that does not behave in the user's best interests is very dissuading and will not receive much enthusiasm from purchasers; if the car might sacrifice their life to save another then there is no incentive for users to give up driving to rely on it. (Coca-Vila, 2018: 63).

In contrast, a utilitarian self-driving car is the lesser evil for society as a whole. It aims to minimise negative consequences on all parties concerned. This approach is considered consequential as it bases its solution to the conflict on the expected outcome. It is collectivist in the holistic way that it views all living beings involved in the inevitable accident as a single entity by combining the different interests of each individual into one (Coca-Vila, 2018: 63).

5. Conclusion

Self-driving cars are closer than ever to the general population. Their benefits to the human race are undeniable and well-known. However, they come at a price of further invasion of our privacy. They threaten the privacy of passengers and owners in terms of personal information and location tracking. They also get an insight into our surroundings. All of the information they get free access to make security threats more serious. They also enable the vehicle to make inferences regarding users that are not always necessary (Karnouskos & Kerschbaum, 2017 : 5). Moreover, autonomous vehicles are targeted by malicious attackers who use a wide range of attacks, some of which can have fatal consequences. Another concern is how a self-driving vehicle can exhibit anomalies in its driving behaviour. Research has come a long way in brief periods. However, there are still several milestones that research on autonomous vehicles needs to hit before becoming a safe and secure mode of transport that the general public can trust in.

6. References

Asuquo, P., Cruickshank, H., Morley, J., Ogah, C. P. A., Lei, A., Hathal, W., ... & Sun, Z. (2018). Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures. IEEE Internet of Things Journal, 5(6), 4778-4802.

Bernardini, C., Asghar, M. R., & Crispo, B. (2017). Security and privacy in vehicular communications: Challenges and opportunities. Vehicular Communications, 10, 13-28.

Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 357-375).

Chernikova, A., Oprea, A., Nita-Rotaru, C., & Kim, B. (2019, May). Are self-driving cars secure? Evasion attacks against deep neural networks for steering angle prediction. In 2019 IEEE Security and Privacy Workshops (SPW) (pp. 132-137). IEEE.

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.

Coca-Vila, I. (2018). Self-driving cars in dilemmatic situations: An approach based on the theory of justification in criminal law. Criminal Law and Philosophy, 12(1), 59-82.

Hubaux, J. P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. IEEE Security & Privacy, 2(3), 49-55.

Joy, J., & Gerla, M. (2017, July). Internet of vehicles and autonomous connected car-privacy and security issues. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-9). IEEE.

Karnouskos, S., & Kerschbaum, F. (2017). Privacy and integrity considerations in hyperconnected autonomous vehicles. Proceedings of the IEEE, 106(1), 160-170.

Othmane, L. B., Weffers, H., Mohamad, M. M., & Wolf, M. (2015). A survey of security and privacy in connected vehicles. In Wireless sensor and mobile ad-hoc networks (pp. 217-247). Springer, New York, NY.

Qin, B., Wu, Q., Domingo-Ferrer, J., & Zhang, L. (2011, November). Preserving security and privacy in large-scale VANETs. In International Conference on Information and Communications Security (pp. 121-135). Springer, Berlin, Heidelberg.

Ryan, C., Murphy, F., & Mullins, M. (2020). End-to-End Autonomous Driving Risk Analysis: A Behavioural Anomaly Detection Approach. IEEE Transactions on Intelligent Transportation Systems.

Wagner, M., & Koopman, P. (2015). A philosophy for developing trust in self-driving cars. In Road Vehicle Automation 2 (pp. 163-171). Springer, Cham.

Wang, Q., Lu, Z., Gao, M., & Qu, G. (2018, November). Edge computing based gps spoofing detection methods. In 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP) (pp. 1-5). IEEE.