EPiC Series in Computing

Volume 69, 2020, Pages 48–59

Proceedings of 35th International Conference on Computers and Their Applications

EPiC Computing

Threat and Alert Analytics in Autonomous Vehicles

Aakanksha Rastogi and Kendall E. Nygard
Department of Computer Science
North Dakota State University, Fargo, ND, USA.
{aakanksha.rastogi,kendall.nygard@ndsu.edu}

Abstract

Autonomous vehicles or self-driving cars emerged with a promise to deliver a driving experience that is safe, secure, law-abiding, alleviates traffic congestion and reduces traffic accidents. These self-driving cars predominantly rely on wireless technology, vehicular ad-hoc networks (VANETs) and Vehicle to Vehicle (V2V) networks, Road Side Units (RSUs), Millimeter Wave radars, light detection and ranging (LiDAR), sensors and cameras, etc. Since these vehicles are so dexterous and equipped with such advanced driver assistance technological features, their dexterity invites threats, vulnerabilities and hacking attacks. This paper aims to understand and study the technology behind these self-driving cars and explore, identify and address popular threats, vulnerabilities and hacking attacks to which these cars are prone. This paper also establishes a relationship between these threats, trust and reliability. An analysis of the alert systems in self-driving cars is also presented.

keywords: Self-driving cars, advanced driver assistance systems, trust, reliability, ethics, security, threats, vulnerabilities

1 Introduction

In recent years, human imagination, creativity, artificial intelligence and a relentless quest to expand dexterity of automobiles has led automobile engineers to design and engineer an automobile that is self-reliant, self-sufficient and self-driving. Imagining a future where a self-driving car run errands (such as picking up clothes from dry-cleaning) while you are still at work and reaching office just in time to pick you up when you are done, is not a far-fetched dream. Automobile industries are already on a haul to launch their self-driving cars while still competing amongst themselves towards constantly improving their cars. While attempting to design a self-driving car that is fully autonomous, they perform rigorous testing of their vehicles and prepare them for adverse road conditions, simulate driving conditions and environments. Waymo self-driving cars have claimed to have been driven for over 8 million miles on road, averaging about 25,000 miles per day, and over 5 billion miles in simulation. However, with all the testing techniques these engineers employ in making these self-driving cars to ensure their safety, security and minimally risky, employing ethics into these cars is still a bigger concern. Ethics relates to morality, conscience, self-awareness and responsibility which are an integral part of humans/drivers. These qualities are self-learned and cannot be leveraged to train a self-driving car into taking ethical decisions while encountering adverse situations on the road. Despite the efforts put together in incorporating ethical decision making systems, there are still several examples of countless situations, circumstances and driving conditions where ethical systems of self-driving cars can be challenged. Trappl brought up the concept of utilitarianism and cited several such scenarios which arguably questioned the ethical decision making capabilities of self-driving cars [24]. To which, Borenstein et. al. sought to discuss the ethical responsibilities of hardware and software design engineers throughout the process of design, development and testing of autonomous or self-driving cars and that each designer is ethically obligated towards creating safer technology [4]. Yet another thought-provoking concern is factoring in driver's stress levels while encountering challenging situations on the road. For instance, a situation where a bus driver driving on a slippery road encounters a deer jumping right in front of the bus. In this case, the bus driver could end up slowing the bus just enough to let the deer pass while trying not to skid or ending up killing the deer just for the sake of saving the lives of the passengers. Irrespective of the decision the bus driver takes, he can still be excused in lieu of the stressful situation he/she was in. Self-driving car/bus, on the contrary, would not be excused for any decision it makes since it lacks creativity and ethical decision making capabilities, like human drivers do.

Autonomous vehicles or self-driving cars and semi-autonomous cars are equipped with advanced technology and driver assistance features enabling safe and easier driving experience that abides by the law, rules and regulations and alleviate traffic congestion. However, since these features leverage wireless network, sensors and cameras, it also opens windows to threats, vulnerabilities and hacking attacks. This paper aims to understand and study technology behind self-driving cars and explore, identify and address threats, vulnerabilities and hacking attacks that these vehicles are exposed to. This paper also establishes a relationship between these threats, trust and reliability. An analysis of the alert systems in self-driving cars is also presented.

The rest of the paper is organized as follows. Section 2 identifies the underlying threats to self-driving cars. Section 3 presents the strategies availed to mitigate and address these threats. Section 4 relates these underlying threats, their mitigation strategies and resolutions to the concepts of overall trust and reliability in autonomous systems. Section 5 provides analytics on the alert-systems in self-driving cars. Section 6 concludes this paper.

2 Identifying threats

Almost every car on the road today comes with advanced semi-autonomous features such as infotainment system (provides vehicle information and entertainment), Traffic Jam Assist in BMW or Traffic Jam pilot in Audi (coordinates live traffic information with satellites and provides alternate routes using car's navigation system), adaptive cruise control (automatically intervenes brakes when needed to maintain safe driving distance with other cars while driving in cruise control mode), self-parking and lane centering steering, Drive Pilot in Mercedes Benz or Autopilot in Tesla (where the driver can keep their hands off the steering wheel and car can lock lane markings and drive itself within the lanes for up to 30 seconds), etc. The basic underlying principle for engineering and managing these semi-autonomous features in these cars is by configuring car's own computers that has car's operating system software which works behind the scenes collaborating with car's electronics, mechanics, power train, wiring, ignition, chassis, etc. Since, these car computers are code behind the scenes, it exposes all semi-autonomous features of the cars to threats and vulnerabilities. It makes these cars prone to hacking attacks. A car's infotainment system can be hacked to gain access to any unit or component inside the car such as ignition, brakes, drive-train, steering wheel, audio/video systems, parking cameras, door locks, wiper blades, etc., allowing hackers to take full control over the car and wreak havoc while the car is still in operation on the road. This can result in highway mayhems, destruction and casualties. Moreover, almost every car has capabilities to sync driver's phone with car's software system via Bluetooth or WiFi which further opens doors to countless attack strategies. Furthermore, Bluetooth, Remote key entry, On-Board Diagnostics (OBD), Dedicated Short Range Communications (DSRC), USB, ABS, sensors [8] and Automobile applications also serve as attack entry points for hackers [9]. Presence of several car hacking demonstration videos and tutorials on the internet second the fact that incorporation of semi-autonomous features aiding car's futuristic appeal is indeed also opening doors to new attack strategies and techniques that can be employed to hack these cars. This can cause destruction to the car itself, the people travelling in it and others sharing the road. Many automobile industries understand and acknowledge these cybersecurity vulnerabilities and threats and even employ white-hat hackers to discover security vulnerabilities in vehicle software. However, with ever increasing technological features being launched in these vehicles, it gets harder to keep up with these security vulnerabilities and address them just in time.

In July 2015, two cybersecurity researchers Charlie Miller and Chris Valasek used their hacking skills to remotely hack into Jeep Cherokee's electrical systems and gained wireless control of the vehicle's computer. They wirelessly accessed the entertainment system which enabled them to send commands to steering wheel, brakes, transmission and other dashboard functions and killed the Jeep on the highway. According to them, Chrysler's vehicles are designed in such a way that their computer networks and electrical systems behave like smartphones being connected to the internet. This opens them to vast variety to vulnerabilities since these car computers can then be wirelessly hacked as they are already connected to the internet via driver's mobile network Wi-Fi hotspot. After successfully hacking the vehicle, they concluded the factors that hackers use to determine the vulnerabilities of vehicles. These included the types and number of radio devices that connect the vehicle's computer systems to the Internet, whether vehicle's critical driving systems were properly isolated from vehicle's on-board computers and, whether the actions of the cyber-physical components could be triggered by digital commands.

The following month, another hacking demonstration was made by the researchers from the University of California at San Diego. The hackers used a small gadget that is placed on the vehicle's dashboard by the insurance firms to monitor location, speed and efficiency of the vehicle. They used this gadget which was connected to Corvette's dashboard to send carefully crafted SMS messages for transmitting commands to the Controller Area Network (CAN) bus of the car and turned on the windshield wipers and even enabled/disabled its brakes. Another hacking threat was reported on Tesla Model X during summer of 2017 where some Chinese researchers managed to remotely hack Model X's brakes while simultaneously opening the doors and the trunk and timed the blinking of lights to the music streaming from vehicle's audio system. This led Tesla to send out security updates to all of it Model X cars.

As these vehicles are gradually progressing from semi-autonomy towards complete autonomy, hacking threats and vulnerabilities become more of a priority than ever. However, it is still a question as to who would be to blame in the even that a self-driving car goes rogue on the road while driving since it was remotely hacked and causes accidents.

3 Addressing threats

Autonomous vehicles (self-driving cars) and semi-autonomous vehicles (cars with some self-driving features) rely on external communication systems such as Vehicular Ad hoc Networks (VANETs) to exchange control data and sensitive information with road side units. As previously mentioned, autonomous and semi-autonomous vehicles are prone to wireless hacking attacks since their advanced driving features are connected over the wireless network, making them more vulnerable and prone to remote hacking attacks. To ensure the success of technology based on security of networks of these vehicles, they are equipped with VANETs. However, certain characteristics of VANETs exposes these vehicles to threats and vulnerabilities at all their communication layers and cause security issues such as high dynamic topology, speed of the car, mobility, open medium wireless communication and absence of a fixed security system [1][2]. This leads hackers and intruders to plant their attack strategies and taking control of these cars remotely over wireless network. In a quest to protect the external network of autonomous and semi-autonomous vehicles from attacks such as Denial of Service (DoS), Black hole, Grey hole and Sybil attacks [1][2], Alheeti and McDonald-Maiser proposed an intrusion detection system that is based on Integrated Circuit Metric technology [1][2]. Their detection system called, ICMetric-IDS was based on features generated from bias values of magnetometer sensors and the features extracted from the trace files generated using network simulator [1][2]. Their proposed scheme was able to demonstrate an efficient detection of malicious behavior in external communication of autonomous and semi-autonomous vehicles [1][2].

Apart from being connected to the network, these vehicles also heavily rely on sensors and cameras to support several advanced driver assistance features. This opens doors to another variety of attacks involving sensors and cameras. Sensors and cameras of these cars can be hacked to gain control of the advanced features such as blind spot detection, lane departure assistance, moving object detection, parking sensors and cameras, to name a few. Hence, it is important to carefully consider technical and security aspects of each component that is used during the manufacturing of these cars.

Multiple types of threats, vulnerabilities and attacks have been investigated and described in the literature. Several detection and defense mechanisms have been developed. These attacks, threats and vulnerabilities are categorized in terms of types of attacks and their detection and defense as listed in Table 1.

Table 1: List of threats/vulnerabilities/attacks with their detection /defense

Type of Attack	Attacks/Threats /Vulnerabilities	Detection and Defense
Cyber attack	Sybil attack [1][2]	Social Graph-based Sybil detection (SGSD) (includes Social Network-Based Sybil Defense, Social Community-Based Sybil Detection) [27], SybilGuard [27], SybilLimit [27], SumUp [27], GateKeeper [27], SybilDefender [27], SybilShield [27], VoteTrust [27], Behavior Classification-based Sybil detection (BCSD) [27], Mobile Sybil detection (includes Friend Relationship-Based Sybil Detection, Cryptography-Based Mobile Sybil Detection [27], Feature-Based Mobile Sybil Detection) [27], Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	Black hole attack [1][2]	Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].

Cyber attack	Worm hole attack [1][2]	Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	Grey hole attack [1][2]	Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	Denial of Service (DoS) attack [1][2]	Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], authentication [21],revocation [21], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	Distributed Denial of Service (DDoS) attack [1][2]	Intelligent Intrusion Detection System (IDS) [1][2], IDS using Deep Neural Network [11], IDS using Outlier Detection [10], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	GPS spoofing [21]	Authentication [21], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	GPS jamming [21]	Anti-Jam GPS techniques, high quality inertial measurement units [21], Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Cyber attack	Malware attack [9]	Over-the-Air (OTA) updates [9], Ericsson Connection Vehicle Cloud (CVC) system [9], layer-based solution [9], signature based IDS and anomaly based IDS [20].
Sensor attack	Jamming [26]	Ultrasonic MIMO system [26], attack detection system [26], logic check [26], adding randomness to control parameters [26], confidence priority [26].
Sensor attack	Spoofing [26]	Ultrasonic MIMO system [26], attack detection system [26], logic check [26], adding randomness to control parameters [26], confidence priority [26].
Sensor attack	Acoustic Quieting [26]	Ultrasonic MIMO system [26], attack detection system [26], logic check [26], adding randomness to control parameters [26], confidence priority [26], spectrum analysis [21], other source of data such as radar or lidar [21].
Sensor attack	Relay Attack [26]	Ultrasonic MIMO system [26], attack detection system [26], logic check [26], adding randomness to control parameters [26], confidence priority [26].
Camera attack	Attacking Cameras [26]	Ultrasonic MIMO system [26], attack detection system [26], logic check [26], adding randomness to control parameters [26], confidence priority [26].

4 Relating threats with trust and reliability in autonomous systems

The emergence of self-driving cars started a few years ago with the hopes of achieving full autonomy (level 5 of the levels defined by Society of Automotive Engineers, shown in Table 3). However, in the race to at least get closer full autonomy, manufacturers of popular automobiles, began delivering vehicles with advanced driver assistance systems which brought them closer to level 2 or partial autonomy. These systems were built upon the concepts of artificial intelligence (AI) and machine learning and meant to promise safety of these vehicles on the road. When effectively implemented and thoroughly tested, they hoped to reduce accidents and crashes in turn aiding lesser crash and damage reports to the insurance companies. However, trusting and adopting these autonomous vehicles isn't that easy.

Tussyadiah et. al. conducted a study to investigate how attitude and trust in technology influences the intentions of people to adopt and use self-driving taxi [25]. They conducted a survey with 325 residents and demonstrated that adoption and usage of self-driving taxis is positively influenced by its reliability, functionality and helpfulness and negatively influenced by the perception of technology being dehumanizing [25]. Part of this study with the mention of dehumanizing nature of technology also coincides with the concepts of singularity which is perplexing enough to influence people's trust in self-driving cars. Another study on resistance of users towards radical innovation of self-driving cars showed a psychological barrier of car drivers towards self-driving cars [19]. Several studies have concluded that people are reluctant when it comes to handing over control of their cars to technology because of safety concerns that are caused by fear of system malfunction or potential hacking attacks [12] [13].

Moreover, recently publicized crashes have also questioned the trust and reliability of these self-driving cars. Crash reported in Tempe, Arizona where Uber's self-driving car hit and killed a 49-year-old woman since the system that was supposed to engage emergency stops in dangerous situations was disabled. This led Uber to suspend their self-driving cars. Crashing of Tesla Model S in 2016 also created headlines where the car crashed into an on-coming white truck at the speed of 74 mph killing the car driver. Apart from the actual crash reports and publicity of these self-driving vehicles, other factors such as safety, risk, predictability, trust in engineers that designed the system, technical capabilities of these vehicles and system failures also account for overall user trust and reliance on self-driving vehicles [5].

Even though engineers employ engineering best practices, thoroughly researched and practiced concepts from data mining, machine learning and AI, what they fail to factor in are the social learning skills. Social learning is derived from the terms of responsibility, liability distribution, thresholds of acceptable safety or lines that divide recklessness from negligence that the institutions of society determine [23]. Self-driving cars can only religiously follow the lines of code governing its functionality and operability, but will always fail to apply the knowledge, learning and skills derived from the experiences from complexities and inconsistencies of behaviors of human drivers and pedestrians on the road. Moreover, the lack of standards in the design and implementation of technology behind these self-driving cars, makes it even more difficult for them to operate on the road and survive in the society.

Trust and reliability in self-driving cars also depend on the constantly judging attitude of human drivers in terms of zero-tolerance in the event of mistakes these vehicles are bound to make. Also, the fact that these cars will never be able to predict the behavior of other human drivers on the road, makes it even more difficult to confide in these self-driving cars. Since, there is always so much complex lines of code behind these vehicles that they can accomplish, they are written by a human, and hence are bound to be erroneous and in constant needs of improvement. A possible workaround would be to have designers/developers constantly pushing out software updates to these vehicles wirelessly but determining a set time to push these software updates could be a challenge. Another challenge would be to determine if the updates could be pushed while the vehicle is in motion. Moreover, other than regular software updates to enhance the overall safety of the vehicle, it is also important to consider the security updates which are direly needed to keep up with the hacking attacks, threats and vulnerabilities these vehicles are prone to.

5 Analytics on alert system in self-driving cars

To ensure the safety of drivers, pedestrians and other vehicles sharing the road, most of the automobile manufacturers are designing cars with advanced driver assistance features, safety features and alert systems. These systems are meant to alert the drivers in the event of unfortunate and unfavorable road conditions. To monitor the alertness of the drivers while driving, automobile manufactures use steering wheel monitors, sensors and tiny cameras, to name a few. However, these advanced driver assistance features still exist in most of the cars these days as a semi-autonomous addition.

An illustration of these advanced driver assistance systems in cars is presented in Figure 1. A comprehensive list of some popular safety, security and advanced driver assistance system (ADAS) features are listed in Table 2.

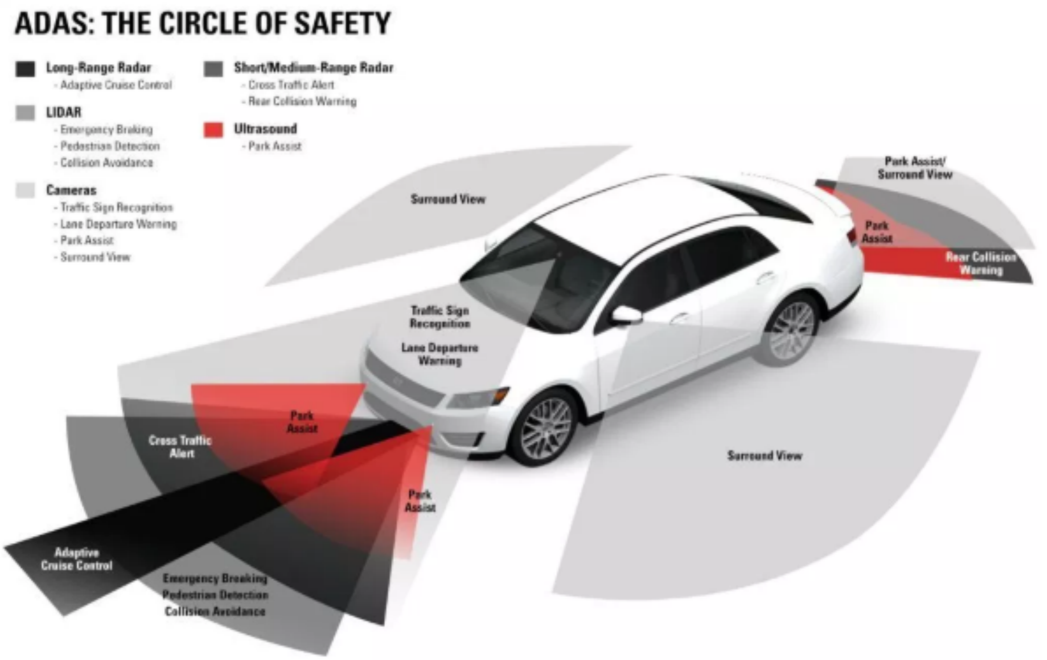


Figure 1: Advanced Driver Assistance Systems (adopted from [6])

Table 2: List of Advanced driver assistance systems (ADAS) (adopted from [14][28][29][6])

ADAS features	Description
Anti-lock braking system	Safety anti-skid braking system
Adaptive Cruise Control	Allows the vehicle to automatically slow down or speed up in response to the speed of the vehicle in front of it
Adaptive Light Control	Controls the headlamps to adjust the lighting in accordance to the natural lighting on the road and illuminate the roads in darkness
Adaptive Lighting	While driving on a darker street, vehicle's headlights are automatically switched to low beam when an oncoming vehicle is passing by and back to high beam when the oncoming vehicle has already passed by

Automatic Braking	Allows the vehicle to intervene and engage brakes automatically to reduce the speed to avert high-speed collisions in the event of driver attention lapse
Automatic Parking	Allows the vehicle to parallel park itself without requiring the driver to do so. Some vehicles park themselves completely while others advice drivers on turning the steering wheel and stopping.
Automatic Crash Notification	Notifies the emergency responders of the crash along with its location
Automatic Emergency Braking	Automatically applies brakes when forward collision is about to happen
Backup Camera	Provides image of the area behind the vehicle and helps prevent back-over crashes
Blind Spot Detection	Allows the vehicles to utilize sensors to help drivers with vital information on moving objects around them
Collision Avoidance Systems	Allows vehicles to utilize sensors to determine vehicle's danger of colliding with another object. In the event of potential collision, system accordingly warns the driver or take preventative actions such as pre-charging brakes, applying tension to the seat belts, adjusting the seats just in time for the airbags to deploy for passenger safety
Crosswind stabilization	Sensors are used to compensate for strong crosswinds
Driver Drowsiness Detection	Allows vehicles to utilize sensors or mini-cameras to determine driver's attention while driving
GPS Navigation	GPS navigation with voice instructions, interactive maps and 3D maps
Hands-free steering	Keeps the vehicle in the center of the lane without driver having his/her hands on the steering wheel
Hill Descent Control	Allows vehicle to easily descend steep inclines by automatically activating breaks, the mechanism for which is like anti-lock braking system or traction control system
Intelligent Speed Adaptation	Allows driver to maintain legal speed limit on the road by monitoring the current speed, comparing it to the local speed limit and delivering warnings
Intersection assistant	System monitors cross traffic on an intersection and prompts the driver to apply emergency brakes or automatically engages emergency brakes by activating acoustic and visual warnings
Lane Departure Warning Systems	System uses a variety of sensors to alert the driver while changing lanes.
Lane Keep Assist	If the vehicle is drifting, this system will vibrate the steering wheel or sound an alarm to alert driver to take corrective action to avoid colliding with another vehicle. Some systems even position the car back in its driving lane.
Night Vision	Allows the cars to adjust the brightness of the headlights in several ways including active night vision projecting infrared light or passive night vision relying on the thermal energy from other cars, animals, pedestrians or other objects
Omni-view technology	System turns on the surround and rear cameras allowing the driver to see a 360° view
Parking Sensors	Proximity sensors in the vehicles that alert the driver of the obstacles while parking
Pedestrian Automatic Emergency Braking	System warns the driver of the pedestrian crossing in front of the vehicle or automatically engages brake if the collision is imminent
Rain Sensing	System switches speeds of wiper blades on the windshield depending upon the amount and intensity of rain
Tire Pressure Monitoring	Provides information about inflation level of each tire
Traffic Jam assist	Provides live traffic information during GPS navigation and accordingly suggest alternate routes
Traffic-sign recognition	Recognizes the traffic signs and speed limit signs on the road
Turning assistant	Monitors the oncoming traffic while turning left at low speeds and engages brake in critical situations

Wrong-way driving warning	Emits acoustic and visual warnings in case of signs imposing access restrictions

Figure 2 demonstrates the comparison between number of cars that have key self-driving features over the past 5 years [3][7][15][16][17][18][19][29][22].

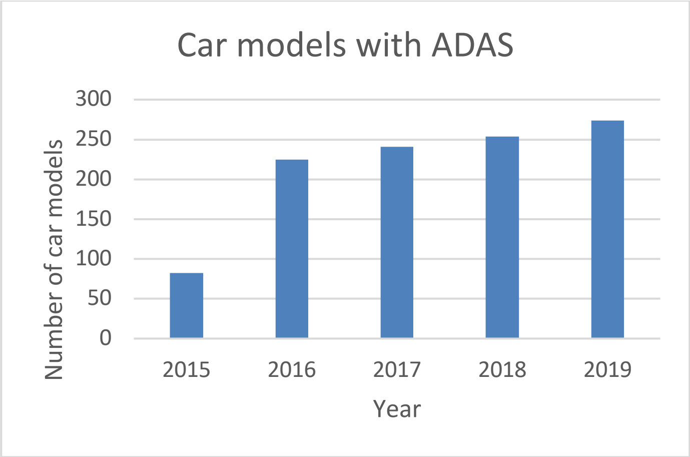
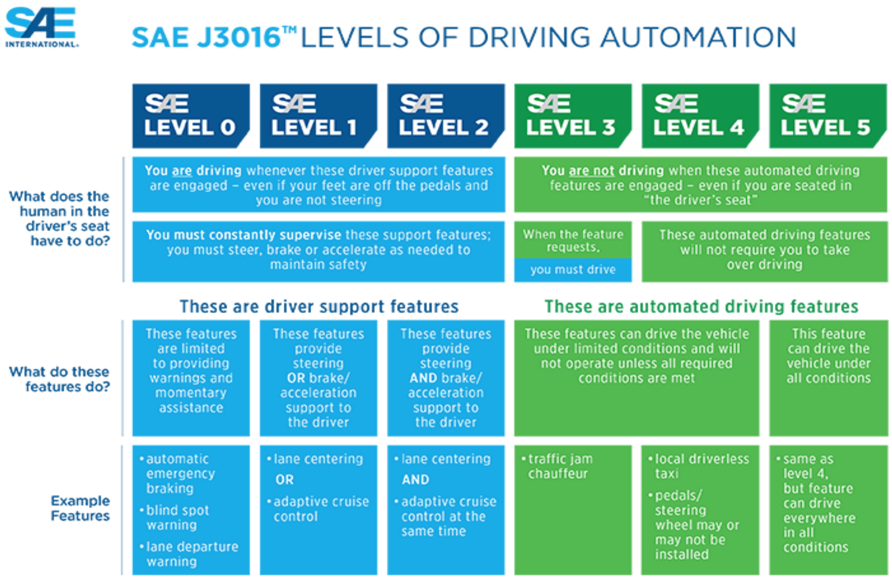


Figure 2: Car models with ADAS

Researchers at Society of Automotive Engineers (SAE International) introduced levels of self-driving that cars can reach [30]. These levels are described in Table 3. Almost all of the advanced driver assistance systems that present cars or semi-autonomous cars are equipped with fall under Level 2 driving automation.

Table 3: Levels of driving automation (adopted from [30])



SAE J3016™ LEVELS OF DRIVING AUTOMATION

	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You are not driving when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/ acceleration support to the driver	These features provide steering AND brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering OR • adaptive cruise control	• lane centering AND • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

Given the reputation of autonomous vehicles considering crashes and casualties they have caused, rigorous testing is still underway for these autonomous cars before they are rolled out on the roads again with confidence, which is not a possibility for at least next 5 years.

6 Conclusion

There is over hundreds of thousands of lines of code in the car's computer system that accounts for modern semi-autonomous features of the cars and autonomous cars themselves. This opens millions of possibilities to infect the code with bugs and defects and mess with different components of the car simultaneously while the car is being driven on the road. Since self-driving cars leverage wireless technology, Bluetooth, VANETs, V2V communication, Milimeter Wave radar, LiDAR, sensors and cameras, etc., they are exposed to countless threats, vulnerabilities and hacking attacks. Any of these technologies can be twisted with some malicious piece of code to gain remote access to the components of a self-driving car making it a potential hazard on the road and demeaning its concept of safe and secure mode of transportation. This paper presented an understanding and study of these technological features behind these autonomous or self-driving cars. This paper also explored, identified and addressed some popular threats, vulnerabilities and hacking attacks in self-driving cars. A relationship between these threats, trust and reliability was also established. An analysis of alert systems in self-driving cars was also presented.

References

[1] K. Ali Alheeti and K. McDonald-Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles", Systems Science & Control Engineering, vol. 6, no. 1, pp. 48-56, 2018.

[2] K. M. A. Alheeti and K.McDonald-Maier, "An intelligent intrusion detection scheme for self-driving vehicles based on magnetometer sensors", 2016 International Conference for Students on Applied Engineering (ICSAE), pp. 75-78, 2016.

[3] K. Andersson, "Top Rated Used Cars for Safety Features | Instamotor", Instamotor.com. [Online]. Available: https://instamotor.com/buy-used-car/safety-rating/top-rated-used-cars-for-safety-features. [Accessed: 26- Apr- 2019].

[4] J. Borenstein, J. Herkert and K. Miller, "Self-Driving Cars: Ethical Responsibilities of Design Engineers", IEEE Technology and Society Magazine, vol. 36, no. 2, pp. 67-75, 2017

[5] M. S. Carlson, J. L. Drury, M. Desai, H. Kwak, and H. A. Yanco, "Identifying factors that influence trust in automated cars and medical diagnosis systems", 2014 AAAI Spring Symposium Series, 2014.

[6] S. Francis, "ADAS: Features of advanced driver assistance systems", Robotics & Automation News, 2017. [Online]. Available: https://roboticsandautomationnews.com/2017/07/01/adas-features-of-advanced-driver-assistance-systems/13194/. [Accessed: 26- Apr- 2019].

[7] B. Halvorson, "The Safest Vehicles Of 2015", The Washington Post, 2015. [Online]. Available: https://www.washingtonpost.com/cars/the-safest-vehicles-of-2015/2015/01/20/272bb29a-a0c5-11e4-91fc-7dff95a14458_story.html?noredirect=on&utm_term=.fc3971522478. [Accessed: 26- Apr- 2019].

[8] M. Harris, "Researcher hacks self-driving car sensors" IEEE Spectrum 9, 2015.

[9] M. Hashem Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity", IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 45-51, 2017.

[10] J. Jabez and B. Muthukumar, "Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach", Procedia Computer Science, vol. 48, pp. 338-346, 2015.

[11] M. Kang and J. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security", PLOS ONE, vol. 11, no. 6, p. e0155781, 2016.

[12] M. König and L. Neumayr, "Users' resistance towards radical innovations: The case of the self-driving car", Transportation Research Part F: Traffic Psychology and Behaviour, vol. 44, pp. 42-52, 2017.

[13] M. Kyriakidis, R. Happee and J. de Winter, "Public Opinion on Automated Driving: Results of an International Questionnaire Among 5,000 Respondents", Transportation Research Part F, vol. 32, pp. 127-140, 2015.

[14] J. Laukkonen, "Advanced Driver Assistance Systems", Lifewire, 2018. [Online]. Available: https://www.lifewire.com/advanced-driver-assistance-systems-534859. [Accessed: 26- Apr- 2019].

[15] A. Lott, "Least Expensive Cars With Active Safety Systems - MotorTrend", MotorTrend, 2015. [Online]. Available: https://www.motortrend.com/news/least-expensive-cars-with-active-safety-systems/. [Accessed: 26- Apr-2019].

[16] K. Mays, "Which Cars Have Self-Driving Features for 2016? | News from Cars.com", Cars.com, 2016. [Online]. Available: https://www.cars.com/articles/self-driving-cars-the-big-list-of-which-automakers-do-what-1420684684889/. [Accessed: 26- April- 2019].

[17] K. Mays, "Which Cars Have Self-Driving Features for 2017? | News from Cars.com", Cars.com, 2017. [Online]. Available: https://www.cars.com/articles/which-cars-have-self-driving-features-for-2017-1420694547867/. [Accessed: 26- Apr- 2019].

[18] K. Mays, "Which Cars Have Self-Driving Features for 2018? | News from Cars.com", Cars.com, 2018. [Online]. Available: https://www.cars.com/articles/which-cars-have-self-driving-features-for-2018-1420699785509/. [Accessed: 26- Apr- 2019].

[19] P. Nobile, "Newsday | Long Island's & NYC's News Source | Newsday", Newsday.com, 2015. [Online]. Available: https://www.newsday.com/classifieds/cars/the-safest-cars-crossovers-and-suvs-in-2015-include-subaru-toyota-and-acura-1.9807785. [Accessed: 26- Apr- 2019].

[20] J. Pacheco, S.Satam, S. Hariri, C. Grijalva and H. Berkenbrock, "IoT Security Development Framework for building trustworthy Smart car services", 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 237-242, 2016.

[21] J. Petit and S. Shladover, "Potential Cyberattacks on Automated Vehicles", IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546-556, 2015.

[22] S. Salomon, "The cars with most advanced safety features | Boston.com", Boston.com, 2015. [Online]. Available: https://www.boston.com/cars/news-and-reviews/2015/09/01/the-cars-with-most-advanced-safety-features. [Accessed: 26- Apr- 2019].

[23] J. Stilgoe, "Machine learning, social learning and the governance of self-driving cars." Social studies of science, 48(1): 25-56, 2018.

[24] R. Trappl, “Ethical Systems for Self-Driving Cars: An Introduction”, Applied Artificial Intelligence, 30(8):745-747, 2016.

[25] I.P. Tussyadiah, F. J. Zach, and J. Wang, "Attitudes toward autonomous on demand mobility system: The case of self-driving taxi", Information and Communication Technologies in Tourism, pp. 755-766, 2017.

[26] C. Yan, W. Xu and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle." DEF CON 24, 2016.

[27] K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things", IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372-383, 2014.

[28] "Driver Assistance Technologies", NHTSA, 2019. [Online]. Available: https://www.nhtsa.gov/equipment/driver-assistance-technologies. [Accessed: 26- Apr- 2019].

[29] C. Reports, "Cars With Advanced Safety Systems", Consumer Reports, 2019. [Online]. Available: https://www.consumerreports.org/car-safety/cars-with-advanced-safety-systems/. [Accessed: 26- Apr- 2019].

[30] "SAE International Releases Updated Visual Chart for Its “Levels of Driving Automation” Standard for Self-Driving Vehicles", Sae.org, 2018. [Online]. Available: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles. [Accessed: 02- May- 2019].