Preparing the automotive industry: Investigating the security vulnerabilities and solutions for connected and autonomous vehicle technologies and legislation

William Booth

Technical Report

RHUL–ISG–2022–3

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

2110920

Preparing the Automotive Industry: Investigating the Security Vulnerabilities and Solutions for Connected and Autonomous Vehicle Technologies and Legislation

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

Informaiton Security Group
Royal Holloway, University of London
August 2021

Acknowledgements

I would like to extend my gratitude towards my supervisor for their expertise, guidance and feedback throughout this project. Their engagement and interest has been greatly appreciated, and has contributed towards an enjoyable and insightful MSc. I would also like to express my deepest gratitude towards my partner and mother for their continued support.

Contents

List of Figures

List of Tables

Executive Summary

Connected and autonomous vehicles (CAVs) aim to present solutions for the social, economic and environmental complications caused by traditional vehicles. The way in which vehicles are viewed in society is set to change dramatically, with vehicular mobility being both autonomous and connected. Although the technological development that has brought forward the emergence of CAVs has been significant, the technologies that enable driverless transportation face new and existing cybersecurity threats. Furthermore, the preexisting legislation and principles that apply to traditional vehicles are not suitable for CAVs, with new dangers to security, privacy and personal data being expected. Therefore, a comprehensive assessment of the security vulnerabilities that concerns the underlying technologies, personal data and privacy protection mechanisms, and applicable legislation is required, where recommendations can be made to protect the future of autonomous automotive transportation.

This report will consider the technological developments that have lead to the emergence of connected and autonomous vehicles, looking towards the underlying sensing, perceiving and communication technologies that are used in high level CAVs. With this, applicable security attacks on the technologies and systems will be discussed, with appropriate countermeasures being proposed. Additionally, the implications on personal data and user privacy will be briefly discussed, emphasising the requirement for compatible data protection legislation. Furthermore, relevant and applicable legislation and principles that govern autonomous driving, user data, privacy and cybersecurity will be critically assessed, revealing areas in which governance is failing. Utilising the findings from the aforementioned, recommendations will be made that can be used by the automotive industry to protect the future of CAVs against security threats.

1 Introduction

1.1 Motivation

The automotive and transportation industries are undergoing one of the most revolutionary and disruptive periods since their inception. The development of cheaper chipsets, sensors and software components is enabling the production of connected and autonomous vehicles (CAVs), that proposes a future of transport with minimal human input [1]. CAVs are intriguing and gratifying consumers, industries and governments across varying global economies, with the potential capabilities being heavily invested in; within the last decade alone, we have seen a vast increase in interest and investment from both industry and governments in CAV technologies and infrastructure. The potential benefits CAVs present to the environment, the economy and public safety are not being overlooked. The United Kingdom's Centre for Connected and Autonomous Vehicles (CCAV) estimates the market for CAVs to be worth between £52 billion and £62 billion by 2035, capturing around 6 per cent of the £907 billion global market [2].

The prospect of autonomous vehicles is not simply concerned with making transportation that requires little to no input or cognition. Self-driving technologies aim to mitigate road traffic accidents, reduce greenhouse gases, decrease traffic congestion and improve the logistical use of existing infrastructure. Removing human control from vehicles aims to reduce numerous preventable deaths each year as a result of human error [3]. Furthermore, CAVs will offer cost savings to both individuals and organisations; improvements within navigation, car control and congestion mitigation will help reduce costs associated with vehicle ownership. CAVs also aim to improve mobility accessibility; future applications are set to provide users with access to a large pool of on demand self-driving vehicles for transportation, without the typical constants of public transport [4]. This is referred to as 'mobility as a service (MaaS)', with CAVs presenting opportunities for those who suffer from mobility constraints as a result of disability or age. The aforementioned suggests that there could be a shift away from personally owned vehicles, with private vehicle ownership being drastically reduced [5].

However, in order to realise a future of fully connected and autonomous vehicles, the industry must overcome several challenges that are imperative to its success. Technological development, regulatory requirements, personal privacy safeguards, industry standardisation and consumer trust is required to overcome the challenges CAVs face. Thus, research and development is needed for technologies and legislation in order to see high level CAVs on the road. Additionally, the CAV space has major cybersecurity considerations that must be addressed. Alongside the traditional safety vulnerabilities that concern modern vehicles, CAVs present a vast attack surface for remote attacks on autonomous vehicle hardware, software, user privacy, security and more.

Therefore, the underlying technologies that enable autonomous and connected mobility, as well as the legislation and principles that governs CAV security must be evaluated in order to identify the vulnerabilities. While prior research has identified attack on CAV technologies, and applicable legislation has been discussed, there remains a gap in literature for exploring CAV security as a whole.

1.2 Objectives

The primary aim of this technical report is to identify and assess the security vulnerabilities, shortcomings and implications pertinent to the technologies, data privacy, legislation and principles concerning CAVs. The secondary aim of this report is to utilise the findings presented in the aforementioned to propose recommendations for the automotive industry, legislators and users in order to secure the future of CAVs.

Overall, this report should provide the reader with a comprehensive understanding of the current and future security vulnerabilities CAVs may encounter, and methods to secure the future of connected and autonomous vehicular mobility. This is to be achieved by the following objectives:

1. Discuss the existing landscape of driverless vehicle technologies and the technological development that has lead to their emergence. Furthermore, present a suitable definition that best describes how connected and autonomous vehicles work.

2. Identify the security challenges and security service requirements for CAV technologies. Additionally, discuss the role of legislation and principles in the context of connected and autonomous vehicles.

3. Discuss the sensing and perceiving technologies that facilitates autonomous vehicles and how they work. Additionally, identity the vehicular communication methods and technologies that enables internal and external information sharing.

4. Identify the security attacks and vulnerabilities concerning the technologies and systems incorporated into both connected and autonomous vehicles, and propose suitable countermeasures.

5. Briefly discuss the personal data protection and privacy implications of CAV technologies and their use cases.

6. Critically evaluate the legislation and principles that concerns connected and autonomous vehicular systems and privacy. Identify the areas where legislation and principles fail to support the security of current and future CAV applications and technologies.

7. Utilising the findings from the previous objectives, propose several recommendations that can be used by both the automotive industry and governmental bodies to protect CAVs from security vulnerabilities.

1.3 Report Structure:

The remainder of this report is structures as follows:

Section 2 - Connected and Autonomous Vehicle Background

This section provides an overview of the technological development that has lead to the emergence of CAVs. Definitions will be provided for what it means for a vehicle to be both connected and autonomous, looking towards the Society of Automotive Engineer's 'Levels of Driving Autonomy'. Furthermore, the need for security within the CAV domain will be considered, and the role of legislation shall be discussed. This section addresses the first and second objectives.

Section 3 - Understanding Connected and Autonomous Vehicle Technologies

This section identifies the technologies and systems that facilitates autonomous driving. Following this, the technologies and systems that support information sharing are outlined. Finally, systems such as infotainment, the CAN bus and over-the-air updates will be discussed. This section addresses the third objective.

Section 4 - Security Vulnerabilities: Technologies and Systems

This section evaluates the security vulnerabilities concerning the the aforementioned technologies identified in Section 3. Attacks will be identified, with countermeasures for each being presented. This section addresses the fourth objective.

Section 5 - Personal Data Protection and Privacy Implications

This section briefly discusses the personal data that CAV technologies capture and share, relating to users and non-users. This section provides context for the discussion of legislation and principles relating to CAVs and personal data discussed in Section 6. This section addresses the fifth objective.

Section 6 - Reviewing Existing Legislation and Principles Concerning Connected and Autonomous Vehicles

This section critically evaluates the existing legislation and principles that governs traditional vehicles and CAVs. Relevant law concerning cybersecurity, digital technologies and data protection will be critically evaluated, identifying the strengths and weaknesses of each. This section addresses the sixth objective.

Section 7 - Recommendations: Security and the Future of Connected and Autonomous Vehicles

This section considers the findings presented in Sections 2-6, and proposes several security recommendations that need to be addressed in order to realise a future of secure CAVs. This section addresses the sixth and seventh objectives.

Section 8 - Conclusion

This section provides a summary of the main findings in the report.

2 Connected and Autonomous Vehicle Background

2.1 A Brief History of Vehicle Technologies

Development throughout the first half of the twentieth century brought forward many fundamental advancements in automotive innovation. Improvements in the chassis, engine and drivetrain lead to the introduction of automatic transmissions, power steering and power assisted brakes. Electrical systems became standard by the 1930s [6] and would control the ignition, headlights, signal lamps, windshield wipers etc. The development of these mechanical and electrical systems would provide the foundations for early electronically controlled driver-assisted technologies.

The development of microprocessors lead to the introduction of Electronic control units (ECUs) in vehicles, which has shaped safety technologies since their introduction in the late 1970s. An ECU is an embedded system that is built onto a microcontroller within the vehicle, providing the necessary communication, software and computational power used to control the electrical systems and sub-systems within the vehicle [7]. ECUs allowed for the implementation of many driver safety features such as Anti-lock Braking Systems (ABS) and Electronic Stability Control (ESC) [6]. Such systems would later develop into adaptive cruise control, a low level autonomous feature. Mechanical and ECU development paved the way for further autonomous driving capabilities seen in vehicles today.

However, the development and inclusion of driver assistance technologies brought with it the requirement for multiple ECUs being implemented in to a singular vehicle. Even today, low-end vehicles have from thirty to fifty ECUs, controlling everything from light sensors to adaptive cruise control. In contrast, higher-end car can see upwards of one hundred ECUs, and can execute tens of millions of lines of software code [8]. Vehicles today contain one hundred million lines of code, however research estimates state that autonomous vehicles will require two to three hundred million lines of code in the near future [8].

Electronic driver assistance systems and the introduction of external vehicular communication has provided the foundations for CAVs to emerge, with commercial vehicle manufactures such as Tesla and Mercedes already offering vehicles with partial or full autonomous capabilities. CAV development is expected to be heavily invested in, with high level CAVs being commercial available within the next decade.

2.2 Defining Connected and Autonomous Vehicles

Defining CAVs is best achieved by considering the underlying technologies that qualify a vehicle as being both *'connected'* and '*autonomous'*. CAVs can then be understood as the technologies and capabilities that are inherited from the combined vehicle classifications [4]. The presented definitions have been adapted from Gowling WLG's and Alkheir et al.'s publications [4, 9]:

Autonomous Vehicle (AV): *A vehicle which is capable of fulfilling the operational functions of a tradition vehicle [9] such as the safe and lawful maneuvering of roads without human intervention or a back-end control center [4]. This is to be achieved by utilising a combination of on-board sensors and actuator networks that gathers information on the surrounding environment, including but not limited to infrastructure, road users, pedestrians and potential hazards. Autonomous vehicular decision making is to be supported by computer vision and machine learning capabilities [10].*

Connected Vehicle (CV): *A vehicle which has the technology that enables it to connect to devices within the vehicle, as well as external networks such as the internet, allowing it to "talk" to its surrounding infrastructure and other vehicles [9]. Internally, the communication devices can be connected using a combination of wired or wireless communication technologies, where as externally they are connected using wireless communications such as cellular networks or DSRC [4].*

Both AV and CV features compliment and reinforce one another [11], broadening the capabilities of driverless vehicles. CAVs look to transform the role of the driver in both personal and commercial contexts, by reassigning the functions of vehicular control away from the driver and towards autonomous technologies [2]. CAVs will transform our preexisting vehicular mobility model, ultimately aiming to provide safer and more efficient travel.

2.2.1 SAE Levels of Driving Automation

The SAE is a U.S. based standards organisation for engineering within the automotive and aerospace industry. Their 2018 J3016 publication provides a taxonomy for driverless automation systems for on-road vehicles [12]. The SAE defines six mutually exclusive levels of driving automation, ranging from no driving automation (level 0) to full driving automation (level 5), providing a classification for vehicle driving automation systems that perform part or all of the dynamic driving task (DDT).

The taxonomy describes three primacy actors within autonomous driving: the driver, the driving automation system and other vehicle systems [12]. The levels of driving automation are defined by the specific role played by each of the three primary actors in the DDT [12]. Table 1 summarises SAE's six levels of driving automation.

SAE Level	Description of Driving Automation	Example Features
Level 0 No Driving Automation	The human driver pefroms all aspects of the entire Dynamic Driving Task (DDT), even when enhanced by active safety systems.	Automatic emergency braking, Blind spot monitoring, Lane departure warning
Level 1 Driver Assistance	The driver support features perform either the lateral or longitudinal vehicle motion control subtasks of the DDT, i.e. either steering or acceleration/decelration.	Lane Cenetering, OR, Adaptive cruise control
Level 2 Partial Driving Automation	The driving automation systems can perform sustained lateral and longitudinal vehicle motion control subtasks of the DDT. The driver is responsible for continually supervising the driving automation system and should remain engaged throughout.	Lane Centering, AND, Adaptive cruise control
Level 3 Conditional Driving Automation	The sustained perfoamnce by an automous dirving system of the entire DDT with the expectation that a user is receptive to DDT fallback requests to interviene from the vehicle.	Traffic jam chauffer
Level 4 High Driving Automation	The sustained performance by an autonomous driving system of the entire DDT and fallback without any expectation that a user will need to intervene.	Local driverless taxi, Pedals/steering wheel may or may not be installed
Level 5 Full Driving Automation	The sustained and unconditional performance by an autonomous driving system of the entire DDT and DDT fallback without any expectation that a user will need to intervene.	Same as level 4, but features can drive everywhere in all conditions.

Table 1: SAE's Levels of Driving Automation

2.3 Security Considerations

Although the widespread adoption of connected and autonomous technology is set to be an inevitability, there are several security challenges, attacks and requirements that must be addressed. Security challenges and attacks must be identified, assessed and treated by both automotive manufacturers and the state entities who are developing the supporting infrastructure and controlling legislation. While low level CAVs of today may face minimal real world security threats, there is no guarantee that the future holds the same prospect.

Research [9] suggests that the automotive industry is good at dealing with traditional physical vehicular safety, it however lacks the capability to handle and mitigate cyber risks on security, cyber safety and privacy concerning CAVs. With the increased complexity of vehicles, and the dangers autonomous technologies and external communications present, security risks will consequently increase. It is therefore important to consider the following security challenges, attacks and service requirements:

2.3.1 Security Challenges

The given security challenges have been adapted from Ghosal and Conti's [13] research:

Attack prevention:

The proposed advantages connected vehicular networks and autonomous capabilities offer should not take precedence over the susceptibility of the given technologies. Attackers will find new incentives and surfaces to perform local and remote attacks on networks and vehicles, due to the critical data that is being stored or shared. Networks and technologies must be resilient to attacks, utilising cryptographic mechanisms such as public-key cryptography and digital signatures. Cybersecurity primitives such confidentiality, integrity and authentication should be used to design vehicular networks and technologies.

User's trust and privacy:

Consumers will not purchase connected vehicles if they are vulnerable to attacks, especially when their privacy is at risk. In order to be on the side of the consumer, communication and autonomous technologies must be designed with vehicular safety and user privacy at the forefront. Robust measures to protect user privacy are being explored, utilising cooperative intelligent transport solutions, public-key cryptography and decentralised key distribution [13].

Network scalability:

The widespread adoption of vehicular communication requires scalable control and management for vehicular networks. Security mechanisms such as certificate exchange requires secure, reliable and repeatable performance to ensure vehicles can connect and communicate with the various networks. These tasks are both demanding and critical, a matter which is amplified when considering the sheer number of vehicles worldwide. Therefore, security techniques that require prior information about the vehicle are not appropriate for such networks [13].

Lasting Performance:

The vehicular networks and autonomous technologies of today should be able to meet the demands for future CAV applications. While vehicular networks should be designed so that they are scalable and are able to operate at increased capacities, they should also be designed so that new technologies and architectures can natively integrate into the networks. AV technology should perform as required when faced with the increased demands presented by future urban environments, without imposing performance degradation or loss of security.

Dynamic network topology:

Due to the mobile nature of vehicles, security becomes a challenge. Connections made between networks are short in duration due to the speed in which vehicles are passing through them, therefore the security features of the vehicle requires networks with high-quality connections that are quick to join. Lightweight cryptographic mechanisms and communication technologies that offer low latency transmission should be considered.

Diverse operation:

Connected vehicles will be manufactured worldwide, with varying implementations of the underlying technologies and networks. Consequently, vehicle and network manufacturers will implement the security and privacy requirements that best suit their country' [13]. As a result, vehicular networks and autonomous technologies must be designed so that they can work with vehicles from other nations and manufacturers.

2.3.2 Security Attack Consequences

If the aforementioned security challenges are not addressed, CAVs face a multitude of attacks and security implications that threaten their success. Section 4 delves much deeper into attacks on technologies and systems, however the following highlights the overarching impacts of attacks on CAV users, vehicles and automotive manufacturers:

Failure of Autonomous Driving Functions:

Autonomous driving functions risk becoming either partially or wholly redundant, putting the user, passengers and other vehicles at risk. Manual vehicle driving functions may also become inoperable as a result, further endangering a user's safety.

Vehicular Collisions:

Collisions with other vehicles, pedestrians and infrastructure can directly cause serious user injuries, death, or monetary costs (damage, repair and insurance liability). The liability of collisions can further be debated, as questions will be raises as to whether the user or vehicle should be accountable.

Vehicle Theft:

Attacks on automotive control systems and GPS can result in attacker taking over control and tracking the user's past and present locations. Furthermore, vehicles can be held to ransom, or sold to foreign countries where they are unlikely to be recovered.

Data Theft and Misuse:

Personal and private data remains vulnerable to attackers, with vehicular data also having value. Data can be sold or held to ransom, or can be used to either conduct attacks in the future, or as part of a more substantial attack.

Commercial Loss:

A vehicle manufacture's reputation will incur damage, resulting in consumer confidence being weakened. This can extend to stock prices and revenues falling if attacks are grandiose enough, or serious security flaws have been identified. Hackers may use attacks on vehicles as a bargaining tool for blackmail and ransom.

2.3.3 Security Service Requirements

Security service requirements must be adopted to over the aforementioned security challenges and attacks CAVs face. As CAVs are producing, sharing and storing vast volumes of safety critical data, including personal and private information, there is a requirement for fundamental security services to be enforced throughout the various technologies and networks. Furthermore, autonomous driving systems require security service provisions in order to support and secure high level driverless mobility. The following presents pertinent CAV security service requirements:

Anonymity:

The assurance that legitimate user identities are protected and cannot be viewed by those who do not have the appropriate authorisation and authentication. Vehicles, users and infrastructure should have unique pseudonyms. This further extends to unlinkability , where no clear relation can be found between the real identity of a vehicle or user and their corresponding pseudonym [14].

Availability:

The assurance that vehicular networks and technologies guarantee access to all users and entities who have passed the authentication and authentication requirements, and, the operation of the network and technology is live and performing as expected at all times. Invalid data integrity mechanisms, such as falsified digital signatures should be excluded from the network to avoid malicious transmissions that would cause a Denial-of-Service attacks, as well as excluding time-out requests.

Confidentiality:

The assurance that transmissions and stored data relating to users, vehicles, infrastructure and external networks cannot be viewed by an unauthorised user. This can be achieved with the use of public-key cryptography, where transmissions can only be decrypted with the use of the legitimate private key.

Data Integrity:

The assurance that received data from vehicular networks has not been altered in an authorised manner, ensuring the accuracy and consistency of communications across the network [15, 16]. Malicious transmissions received along either the in-vehicle network or external network should detected and excluded. This can be achieved with the use of lightweight cryptographic has functions, MACs and digital signatures for transmissions sent over the V2X networks.

Data Origin Authentication:

The assurance that a given entity a network or system was the original source of received data [15]. In the context of vehicular communication, this is the assurance that two or more entities communicating in a vehicular network can be sure that all received data did originally come from those trusted entities. With autonomous technologies, the vehicle must have confidence that incoming sensor data is legitimate and from the correct source. Lightweight symmetric-key cryptography mechanisms such as HMAC can be used for authentication between entities on a network, providing quick generation and verification without a large security overhead [13].

Location Privacy:

The assurance that the location of each node (vehicle) and the location of the network service provider is private and protected [17]. Data regarding timestamps, spatial coordinates and vehicle telemetry is high value to attackers, therefore requiring strict access controls and confidentiality mechanisms to be applied to location data.

Non-Repudiation:

The assurance than an entity cannot deny any previous actions [15]. This requires that any transmissions can be traced back to their original source along, ensuring attempts from external or internal adversaries cannot successfully impersonate others. Digital signatures can be attached to transmissions, providing accountability for vehicular communications.

2.4 The Role of Legislation and Principles

Legislation and Principles from private and state entities are used as instruments for addressing the public concerns and requirements for CAV technologies and applications. Although both are somewhat interrelated and play an important role in the development and realisation of high level CAVs, each has an explicit function, and therefore it is important to know the difference between them. A *principle* simply provides the foundation for the development of legislation and rules [18], whereas *legislation* is declared by a legislator or governing body, and sets out the law, defining the procedure or standard that an organisation or individual must adhere to [19, 20]. Research in the autonomous vehicle field [21] suggests that for policymakers and the public, safe, secure and efficient driverless mobility will be more influenced by the legislation that governs them rather than the technical capabilities of CAVs.

Development in the autonomous vehicle industry has predominantly focused on the hardware and software advancements associated with higher levels of driving autonomy [22]. Coupled with the fact that there is little in the way of a cyber-attack history for CAV vehicle contexts, legislation and principles that governs CAV cybersecurity remains in its infancy. The technology driven development path of CAVs could leave limited space or compatibility between principles and legislation before we see fully autonomous vehicles on the road [23]. Furthermore, the move towards increasingly digitised and inter-connected vehicles leads to an increase in exposure for cybersecurity threats. It has been said [24] that the automotive industry lacks a standardised approach for dealing with cybersecurity concerns, illustrating the need for governance that requires cybersecurity to be at the forefront of CAV development.

Further to cybersecurity, legislation relating to digital technologies, including liability, privacy, data protection and connectivity are becoming increasingly relevant to the driverless automotive industry [25]. For this reason, legislation that is not mutually exclusive to the CAV sector needs to be evaluated. Thus, looking towards general data privacy legislation will be beneficial in identifying key strengths and weaknesses of existing governance. Finally, the need for a collaborative culture between vehicle manufacturers, legislators and other state entities on an international scale is required if high level CAVs are to be fully realised without hindering innovation. This also allows countries that introduce CAVs at a slower pace to get up to speed [23], by looking towards real world applications of policies and legislation elsewhere.

By looking towards existing principles and legislation that concerns CAVs and their underlying technologies, recommendations can be made for the future of automotive legislation. Section 6 will identify and evaluate existing legislation and principles, before providing recommendations for securing CAVs in Section 7.

2.5 Summary

We have seen that technological development within the automotive industry has undergone considerable and rapid development since the mainstream adoption of privately owned vehicles in the early twentieth century. Technological advancements in mechanical and electronic systems has brought forward the emergence of low level driver assistance and autonomous technologies. However, as autonomous technologies develop, the industry required a widely adopted classification for the various autonomous capabilities. Luckily, the SAE's levels of driving autonomy provides a highly applicable and exceedingly regarded taxonomy for the various autonomous driving capabilities, and is used throughout the industry.

However, the security considerations that comes with CAVs cannot be ignored. Security challenges and attacks threaten the success of CAV applications, and the automotive industry must look towards critical security service mechanisms in order to provide safe, reliable and available autonomous transportation. Furthermore, the automotive industry must also consider the role of legislation and principles when designing and maintaining vehicular safety. A 'sit back and wait' approach should not be taken with cybersecurity, especially when the stakes are this high, and therefore, the automotive industry must look towards existing legislation and principles from relevant industries, and must remain proactive.

3 Understanding Connected and Autonomous Vehicle Technologies

3.1 How CAVs Work: Sensing and Perceiving

It is important to have a reasonable understanding of how the technologies in CAVs work in order to begin considering their security vulnerabilities and countermeasures. While humans manually control a vehicle based on cognition, perception and decision making [26], CAVs rely on a variety of sensors and hardware to observe their surrounding, creating a perceptive and locational interpretation of the surrounding environment. This feeds vast amounts of data to the on board artificial intelligence (AI) systems [26, 27], which computes the data in real-time and send instructions to the powertrain, drivetrian and steering assembly.

There are two main types of sensors used within an connected and autonomous vehicles: Exteroceptive sensors, used for sensing and perceiving the surrounding environment, and, proprioceptive sensors, which are used to measure vehicle dynamics, and global positioning. Figure 1 illustrates the exteroceptive sensors used within autonomous vehicles.

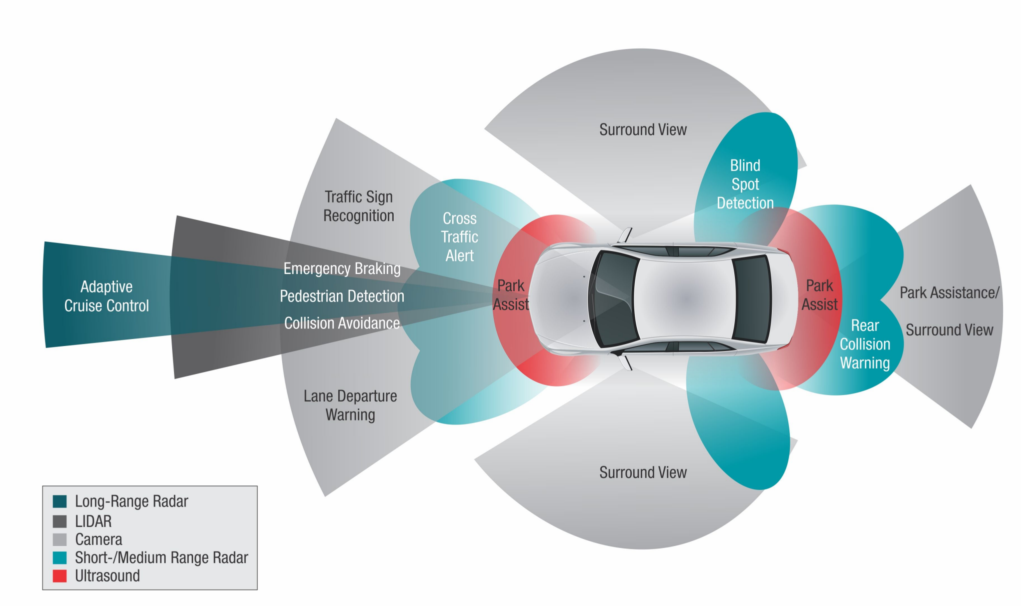


Figure 1: Overview of exteroceptive sensors used on a autonomous vehicle

As with all sensing and perceiving technologies, they are best used in conjunction with one another, as well as localisation and mapping systems. This provides multiple layers of redundancy if one or more system is operating incorrectly, as well as improving the autonomous capabilities of the vehicle.

3.1.1 Exteroceptive Sensing

LiDAR:

Light Detection and Ranging (LiDAR) is a remote sensing technology used to measure distance [27] by processing the time delays (time-of-flight) for emitted optical pulses to be reflected back from an object [28]. It is a popular sensor choice for autonomous vehicles as they are able to generate a detailed three-dimensional view of the surrounding environment, and can provide accuracy of up to one hundred meters range in all directions[29]. However, the technology is not able to differentiate between objects, meaning a stray plastic bag could be interpreted as a road bump for example [30], and its efficacy is affected by adverse weather conditions due to the absorption and scattering of light [28]. These vulnerabilities can be exploited by an attacker, as seen in section 4.1.1. Figure 2 [31] illustrates the LiDAR sensor's view of the surrounding environment.

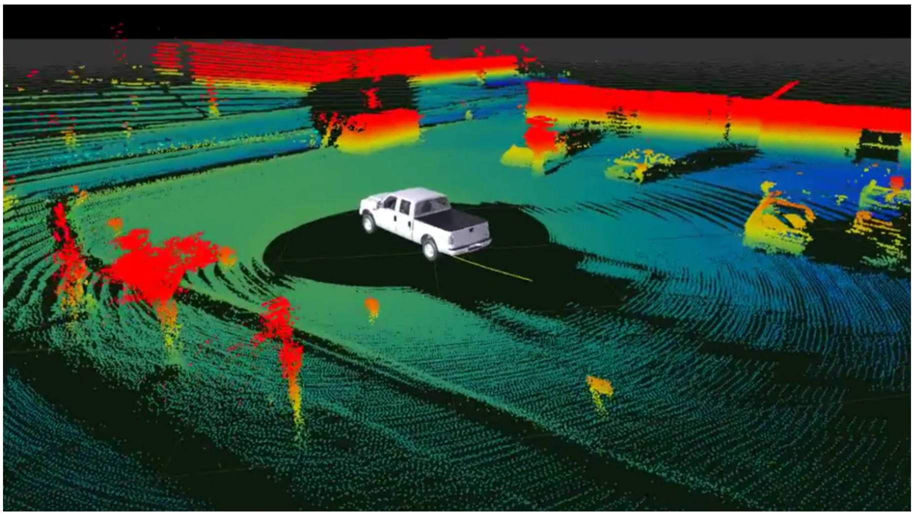


Figure 2: Three-dimensional view of a 360° LiDAR image

Radar:

Radio Detection and Ranging (RADAR), operates in a similar fashion to LiDAR. Millimeter radio wave (mmWave) pulses are emitted from the RADAR transmitter and reflect off objects, and are picked up by the receiving antenna. The system can then measure the properties of the object, including distance, velocity and angle [32]. RADARs have a wide operating spectrum [33], with short-range radars, medium-range radars and long-range radars having ranges of 5 to 250 meters respectively. RADAR systems are robust in challenging environmental conditions, with low visibility not impacting the signal's reliability. Additionally, RADAR technology has been around since the early twentieth century, allowing the technology time to mature, which has resulted in it being a popular choice for automotive manufactures. RADAR offers an improved range over LiDAR [29] and provides more precise velocity measurements, making it ideal for speeds in excess of 50-70km/h.

However, object detection reliability can often be ineffective, with reflections and disturbance producing a false size measurement[32]. This could mean that a drinks can could be misinterpreted as a building due to the noisy response of the material. Furthermore, RADAR radio waves operate at a lessened frequency than LiDAR, resulting in a lower fidelity scan of the environment, making it unsuitable for close proximity sensing and static objects[29].

Camera:

Digital cameras are the most accurate way to create a visual representation of the environment. CAVs incorporate high resolution cameras on each side of the vehicle, producing a three-dimensional view of the surrounding environment. Cameras are often set up so that they overlap, providing depth measuring capabilities in close proximity contexts [34]. Cameras can also distinguish colour, allowing the vehicle to recognise elements in the environment such as traffic lights, road signs, vehicle lights etc [26]. With this, AI systems on the vehicle can identify pedestrians, as illustrated by figure 3[35]. As with RADAR, camera technology has been around for a significant amount of time, meaning that the technology has considerably matured and the cost of implementation is attractive to automotive manufactures.

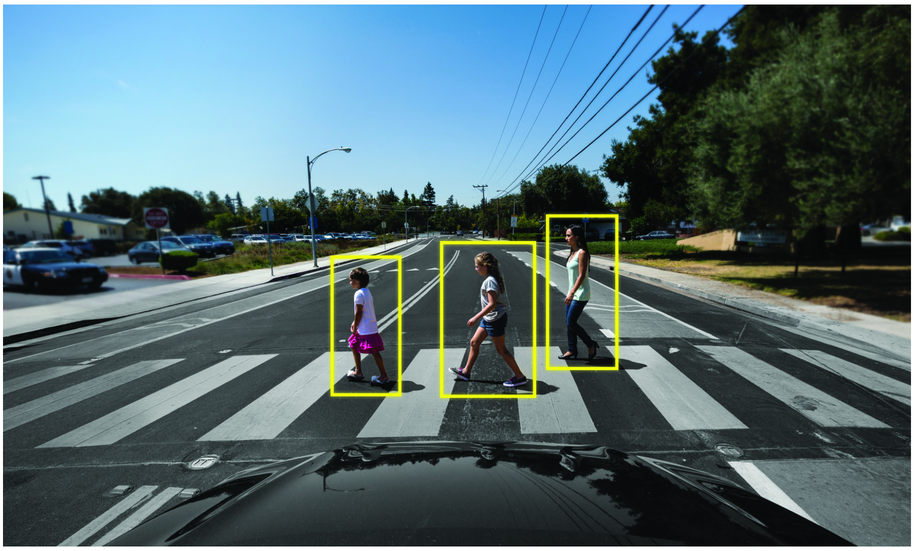


Figure 3: Autonomous vehicle camera using AI to identify pedestrians

Although cameras provide considerable performance relative to their cost, image quality diminishes in low light and extreme weather conditions. Finally, cameras are extremely sensitive to interference from other light sources, leaving room for exploitation from attackers.

Ultrasonics:

Ultrasonic sensors are proximity sensors that detect objects in close proximity of the vehicle (distances under 5 meters [36]). As a result, they are used in low-speed scenarios such as parking assistance or for blind-spot detection. The working principles behind ultrasonics is similar to RADAR, however ultrasonic sensors detect objects by transmitting and receiving ultrasound [37]. As with RADAR, ultrasonic sensors offer strong performance in low light conditions, however they are heavily affected by changes in environmental conditions such as temperature or humidity [26]. Furthermore, they cannot provide a detailed depiction or determination of what an object is, only the relative distance and angle of said object. Due to the maturity of the technology, the cost to implement such sensor is relatively low and therefore makes it a popular choice for automotive manufactures.

3.1.2 Proprioceptive Sensing

Global Positioning System:

Global Positioning Systems (GPS) provide satellite-based radio-navigation that offers longitudinal and latitudinal coordinates relative to the vehicle's position on the Earth's surface [38]. Alongside GPS, the vehicle relies on other positioning sensors to inform the user about their exact position, including direction, altitude and incline [39]. In order for the vehicle and driver to make sense of the received coordinates, the vehicle utilises a detailed map, stored on the vehicle's navigation system, and cross-checks the location on the map with the coordinates. The system can then produce highly accurate route planning algorithms, calculating the most efficient route between two or more points.

GPS systems are highly accurate while remaining relatively inexpensive, and the widespread deployment of GPS and the growing abundance of satellites provides lasting positioning capabilities with integrity. However, radio signals used in GPS do not penetrate buildings, meaning that in built-up urban environments their efficacy is impaired. GPS systems are also vulnerable to signal interference, meaning a hacker could deploy spoofing or jamming attacks to the incoming and outgoing signals.

Inertial Measurement Unit/ Internal Navigation System:

An Inertial Measurement Unit (IMU) is an electronic device embedded within the vehicle that measures the gravitational force, angular rate and the magnetic field of the vehicle [27]. It incorporates accelerometers, gyroscopes and magnetometers. They are implemented into the vehicles Internal Navigation System, or INS, which processes the data produced by the IMU and calculates the vehicle's velocity, altitude and angular positions relative to the global reference frame [27]. This information can therefore be used to calculate the position of a vehicle relative to a reference point.

One of the main advantages to using a IMU system is that there is no need for the vehicle to be connected to an external communication channel, providing reliable information on the vehicle's motion without the need for any additional sensors [26]. Furthermore, IMU and INS measurements can be used to provide a layer of redundancy if the GPS is inoperative.

3.1.3 Artificial Intelligence

Artificial Intelligence (AI) is defined as a collection of methods capable of rational and autonomous reasoning, action and decision making [40]. Autonomous driving is a key application of AI, with CAV systems heavily relying on machine and deep learning to process the data received form the vehicle's sensors. Machine/deep learning systems train, validate and improve the autonomous driving systems [41]. AI can then be used for autonomous driving applications such as object recognition, vehicle localisation, object tracking and identification of roads and infrastructure etc.

However, AI presents security vulnerabilities that can be exploited in order to disrupt and manipulate the operation of autonomous driving systems. The aforementioned exteroceptive and proprioceptive technologies each use a varying degree of AI, and therefore, in many cases, attacks on sensors can also be considered attacks on AI.

3.2 How CAVs Work: Communication and Infotainment

CAVs can communicate and exchange information with other vehicles, infrastructure or external networks. Communication technologies enable the autonomous driving features to be proactive, cooperative, coordinated and well-informed [42], facilitated by the mutual exchange of sensed data. With this, communication that is confidential, retains integrity and is always available is needed in order to support the AV functions.

CVs support Bluetooth and Wi-Fi for in-car applications such as infotainment and smartphone connectivity, as well as external communications including telematics such as Over-the-Air updates. Figure 4[43] illustrates such communication technology applications. As these Bluetooth and Wi-Fi capabilities broaden, they present further security vulnerabilities and areas for exploitation, so their implementation should be governed by strict security measures.

Theoretically, any wireless network technology can be used as a basis for vehicular communication, however the industry has dictated that short range communication technologies such as Dedicated Short-Range Communications (DSRC), or long range cellular technologies such as LTE or 4G/5G are more suitable [44].

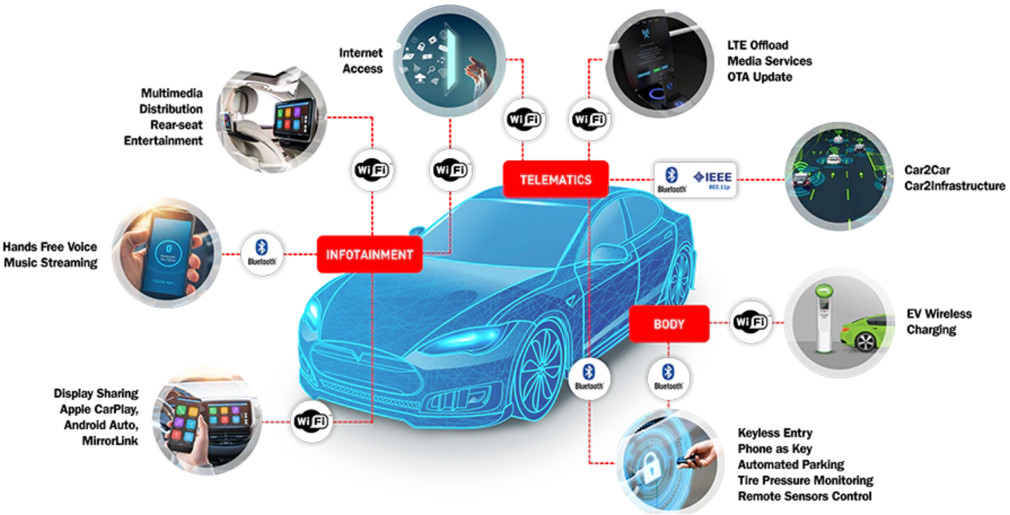


Figure 4: Connectivity applications and technologies connected vehicles offer

3.2.1 V2X Communication Technologies

Vehicle-to-everything communication (V2X) is an umbrella term for the subset of communication systems which a CV posses. These consist of vehicle to vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N) and vehicle-to-pedestrian (V2P) communications. Information collected by the on-board sensors is communicated externally, either to other vehicles, the surrounding infrastructure, pedestrian smartphones, and to data centers [45]. Furthermore, V2X communication informs the vehicle with environmental conditions, traffic dynamics, and road closures etc. Each type of vehicular communication is used simultaneously in order to provide reliable and safe mobility. Figure 5[46] illustrates the communication platforms and their interconnectivity. The various communication systems each carry differing requirements as to how the data is transmitted, balancing efficiency, performance and cost.

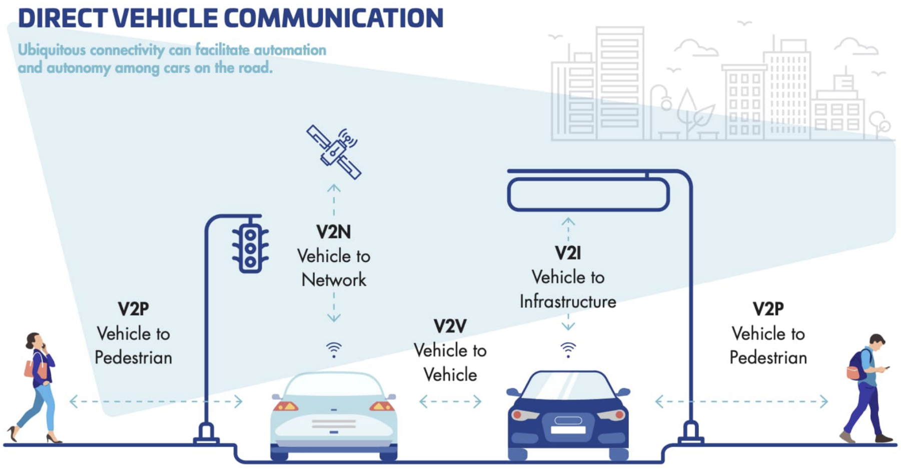

DIRECT VEHICLE COMMUNICATION
Ubiquitous connectivity can facilitate automation and autonomy among cars on the road.
V2N
Vehicle to Network
V2I
Vehicle to Infrastructure
V2P
Vehicle to Pedestrian
V2V
Vehicle to Vehicle
V2P
Vehicle to Pedestrian

Figure 5: The Vehicle-to-Everything (V2X) communication platform

Vehicle-to-Vehicle (V2V):

V2V communication refers to the transmission of data between connected vehicles. Vehicles in relative proximity to one another form a mesh network and exchange information such as traffic dynamics, location, speed and general vehicle attributes [47]. V2V communication allows CVs to broadcast and receive omnidirectional messages, at a rate of up to ten times per second [48], covering a 360° degree field. Communicating vehicles can use this information to determine optimum lane changing procedures, measure the flow of traffic and determine possible road traffic crashes. V2V communication uses DSRC, a wireless protocol similar to Wi-Fi, where vehicles are treated as nodes within the wireless mesh network. DSRC allows vehicles (nodes) to exchange information to other vehicles and infrastructural Roadside Stationary Units (RSU) outside of the vehicle. Message payloads are kept to an economical size in order to aid communication, and the underlying technology ensures the transmission of information has an extremely low latency, a requirement for this context [47]. DSRC communication contributes towards collision prevention and driver assistance tasks [33] for connected and autonomous vehicles, leveraging both information provided by nodes on the network and RSUs. The technology however is vulnerable to several of the same attacks used against Wi-Fi, as well as attacks on user confidentiality. Section 4.2 further discusses the attacks on DSRC.

Vehicle-to-Infrastructure (V2I:)

V2I communication refers to the transmission of data between connected vehicles and roadside infrastructure. Information is transmitted between RSUs or locally available application servers [47]. The RSU acts as a transceiver for incoming communication from a CV, and can transmit information in real-time to vehicles with information about traffic conditions, road-traffic collisions and weather reports etc. The operational principles behind V2I remains similar to V2V communication, and both facilitate the underpinnings for the Vehicular-Ad-hoc-network (VANET) platform. Similarly to V2V, V2I utilises DSRC networking for communication. Again, the message payloads are omnidirectional and can provide multiple CVs with concurrent information on driving conditions. Figure 6[49] illustrates the application of V2I communication.

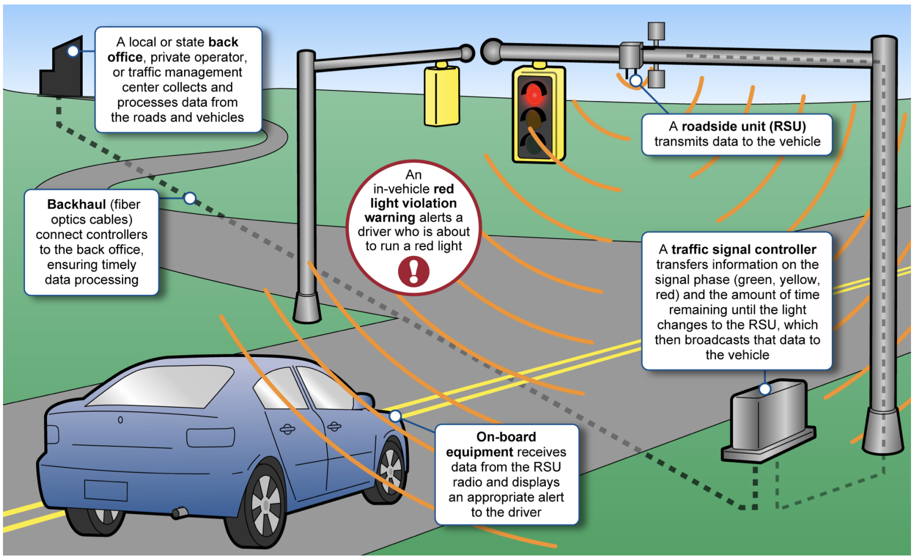

A local or state back office, private operator, or traffic management center collects and processes data from the roads and vehicles
Backhaul (fiber optics cables) connect controllers to the back office, ensuring timely data processing
An in-vehicle red light violation warning alerts a driver who is about to run a red light
A roadside unit (RSU) transmits data to the vehicle
A traffic signal controller transfers information on the signal phase (green, yellow, red) and the amount of time remaining until the light changes to the RSU, which then broadcasts that data to the vehicle
On-board equipment receives data from the RSU radio and displays an appropriate alert to the driver

Figure 6: Vehicle-to-Everything (V2I) communication with a Roadside Stationary Unit (RSU)

Vehicle-to-Network (V2N):

V2N communication refers to the transmission between a vehicle and a V2X application server [47]. V2N systems connect CAVs to existing cellular infrastructure and the cloud (vehicle-to-cloud, V2C), providing in-vehicle services such as traffic updates and and streaming to the infotainment systems. The most common application for V2N communication is for navigation services such as Google Maps or Waze, with the vehicle streaming in live traffic data provided by other connected vehicles and map data from Google servers.

Advanced V2N services enable mobile operators to communicate the functions of the RSU over its network [47]. This helps to reduce the cost and complexity of designing purpose built networks for V2I, as communication between vehicles and the server via 4G or 5G connectivity.

Vehicle-to-Pedestrian (V2P):

V2P communication aims to connect vehicles to pedestrians with connective devices, such as mobile phones, smart wheelchairs or connected bicycles for example. Vehicles and pedestrians will be able send data to one another containing messages and alerts of their position, velocity, location relative to the road and more. Vulnerable Road Users (VRUs) can communicate with multiple vehicles even when they are out of the line of sight and during low visibility conditions, including rain or during the night-time. This greatly improves pedestrian safety and ultimately aims to reduce roadside fatalities.

3.2.2 Infotainment and Smartphone Connectivity

The infotainment systems represent the collection of hardware and software that provides both multimedia and transportation functions to the driver and passengers, including in-car audio system, navigation systems, vehicle telemetry and basic vehicle controls. USB, Bluetooth and Wi-Fi connectivity has brought forward hands free operations, facilitating advanced control over the in-car systems. The adoption of Wi-Fi in modern vehicles allows for hotspot functionality to connect laptops, tablets and smartphones, enabling consumption of rich media content within the car [43]. However, such in-car communication technologies present new security vulnerabilities for CAVs.

Infotainment systems and smartphone applications can allow for advanced vehicle control which connects to the vehicle's various ECUs and CAN bus. This inherently presents opportunities for attackers to remotely seize control of a vehicle, as well as locate the user's current and previous locations.

3.3 How CAVs Work: Automotive Control Systems

3.3.1 Passive Keyless Entry Systems (PKES)

Traditionally, vehicles have utilised physical mechanical keys to unlock the vehicle and operate the ignition. Physical keys were considered relatively secure, however they contained no authorisation mechanisms, and whoever held the key could gain entry into the vehicle. Furthermore, an individual who has access to the physical key or a detailed photograph could create a duplicate key with relative ease. With this, the introduction of electronics within physical vehicle keys has improved convenience and security, and has lead to the implantation of Passive Keyless Entry Systems (PKES) in many modern vehicles and CAVs.

A PKES protocol uses low frequency radio-frequency identification (RFID) tags within the key that communicates with the vehicle from a distance of one to two meters [50]. The low frequency electromagnetic field on the vehicle is used to detect the key when it is close proximity of the vehicle. When the user approaches the vehicle, the PKES key will perform a challenge-response protocol, verifying the key's proximity to the car [51]. The system is passive as it does not require the user physically operate the key, as the locking mechanism will unlock, and the ignition can be operated when the PKES key is within the corresponding regions of the vehicle.

3.3.2 Controller Area Network (CAN) Protocol

Modern vehicles possess numerous ECUs that require complicated and concurrent interactions to support the vehicle's systems and subsystems. These ECUs, or 'nodes', are distributed around the vehicle, with their communication facilitated by the the Controller Area Network (CAN) Bus [52].

The CAN standard allows nodes to communicate to one another without the need for complex dedicated wiring, providing communication that does not overload the controller computer within the vehicle. The CAN bus broadcast network can provide data transmission between ECUs of up to five megabits per second (Mbps), while retaining high levels of immunity to electrical interference [53]. Furthermore, the CAN bus is easy to implement, and has the ability to self-diagnose problems within the network due to the centralised implementation of the CAN system.

However, the CAN bus is primarily designed for reliable communication and not for security [52]. Advancements in driverless mobility require vehicles with even more ECUs, with autonomous systems that communicate through the CAN bus, dramatically increasing the attack surface. This leaves the CAN bus a primary target for attackers.

3.4 Summary

The technologies presented demonstrate a huge technological step forward from more traditional vehicles. Sensing and perceiving technologies scan the surrounding environment, capturing vast volumes to be processed by the vehicle's AI and machine learning systems, where models are generated that can identify pedestrians, vehicles and infrastructure for example. Furthermore, V2X communication technologies support information sharing between other vehicles, pedestrians, infrastructure and external networks, all in aid of more proactive, coordinated and well-informed autonomous driving functionality.

However, such technologies and systems remain vulnerable from a multitude of attacks that threaten CAVs success. Thus, the automotive industry must have a critical understanding of how such technologies work before they can consider the security vulnerabilities they face.

4 Security Vulnerabilities: Technologies and Systems

4.1 Attacks on Autonomous Driving System Components

Hardware sensors present several potential cyber attack surfaces. An attack surface is the set of points on a system where an attacker can try to enter, cause an effect on or tamper with data from that system [54]. Attackers will have additional strategies to accomplish their intentions, with the development and inclusion of sensor technologies further raising the ceiling for potential impacts, and also introducing a new class of vulnerabilities [26]. The following subsections will detail the security vulnerabilities for each of the exteroceptive and proprioceptive sensors mentioned in section 3.1. Additionally, potential countermeasures are be presented that can be used to mitigate such vulnerabilities.

4.1.1 LiDAR

Although LiDAR technology has proven to be a popular sensing aid for autonomous vehicles, with the exception of Tesla [30], there is no guarantee over the validity of the constructed 3D model [55]. LiDAR cannot differentiate between objects, with the system often misinterpreting objects in motion. This poses a great security vulnerability to AVs, as it allows attackers to manipulate LiDAR readings through either spoofing, relaying or jamming.

LiDAR spoofing attacks use the same physical channels as the LiDAR unit to manipulate sensor readings [56]. The goal of a sensor spoofing attack is to deceive the sensor by exposing the LiDAR unit to a counterfeit signal which simulates a falsified circumstance [57]. Such attack exploits the semantic gap between what the sensor interprets, and what in reality the object is. Spoofing attacks can be accomplished without complex or expensive hardware. Research by Jonathan Petit [58, 59], conducted a spoofing attack by manipulating LiDAR sensor data using a Raspberry Pi and a low powered laser. Petit managed to spoof the LiDAR system into perceiving falsely generated cars, pedestrians, and walls, by simply recording pulses from existing LiDAR units and replaying them at a later time.

Relay attacks use the same principles as spoofing attacks, however there is no need to falsely generate an object's signal. A relay attack is where the attacker captures and delays the original signal from the LiDAR unit before relaying the signal back to the sensor, therefore manipulating the position of an object. Research by Bas Stottelaar [60], found that by capturing and using the original LiDAR signal, and using it as a trigger point, one could replay objects and control their position. This can be used to relay the signal received form drivers side of the car, and emit it onto the passengers side. This method can also be used to relay the signal from one vehicle's LiDAR unit to another.

Jamming attacks are comparatively simple. In a jamming attack, the attacker's goal is to disable the sensor by jamming and overwhelming the LiDAR unit, rendering it temporarily redundant, as there is no usable data for the autonomous driving system. Again, Stottelaar [60] demonstrated that, by emitting similar light pulses of the same wavelength and timing as the LiDAR unit, the LiDAR sensor could be jammed. All of the hardware required for this attack can be fitted in a small, battery-powered handheld device [60]. This means that such attack could be made compact and less detectable, and could even be fitted to another vehicle.

Countermeasures:

Utilising different wavelengths can reduce the success of spoofing and jamming attacks involving low-cost hardware components, such as off-the-shelf laser devices [61, 60]. Changing the type of wavelength requires more complicated and expensive hardware, as well as a deeper understanding of the underlying technology, thus reducing the likelihood of a prospective attacker easily breaching LiDAR technology. Although certain LiDAR wavelengths have their disadvantages (range, clarity and accuracy), it is recommenced however that multiple wavelengths are used together to improve the overall sensing capability. Another more feasible method of mitigating spoofing and jamming attacks can be achieved by random probing. This involves periodically and randomly changing the interval between scanning speeds, making it harder for the attack to synchronise to the original wavelength speed [61]. Both of these methods can be implemented in software.

As discussed in section 3.1, sensing technologies should be used in conjunction one another, as well as with CV communication technologies. This is the case for LiDAR, with relay, spoofing and jamming attacks theoretically being mitigated if the vehicle is cross-checking environmental readings with surrounding CAV's LiDAR data[58]. This provides multiple layers of redundancy if a LiDAR sensor is under attack.

4.1.2 Radar

Automotive radar attacks differ from more traditional attacks owing to the fact that AVs are never stationary for an extended period of time. Attacks on radar are comparable to LiDAR, with isolated attacks having a dramatic effect on the autonomous driving capabilities.

Radar remains vulnerable to jamming attacks, with both forward and blind spot jamming attacks effectively disabling the functionality of the radar systems, [33]. Jamming radars can be accomplished with relative ease if an attacker is on the same frequency band. For a simple jamming attack, an attacker would require only a tunable scanner to seek out the operating frequency of the CAV's radar signal. Form here, they can generate a jamming signal of the same frequency [62], filling the vehicle's radar with a saturation of static noise that cannot be computed, subsequently overriding the system. There are a few caveats with jamming an automotive radar signal however. Radars use a considerable amount of directivity - how directional an antenna's radiation pattern is [63] -, providing mmWave radar with improved resilience to jamming attacks. Furthermore, due to the mobile nature of vehicles, successfully jamming mmWave radar in highly mobile environments proves to be challenging, as an attacker may not have enough time to determine the mmWave frequency. Consequently, such attack would be most effective in slow moving traffic, such as inner-city environments [33].

Radar applications are also susceptible to spoofing attacks, where attackers replicate and re-transmit the mmWave signals. The signal structure of automotive radar means that no inherent authentication is performed, allowing attackers to tamper with the vehicle, either by introducing false data, or corrupting received data. Objects in the distance can be entirely fabricated, or their distance relative to the vehicle can be altered [62], greatly effecting the autonomous decision making process and disrupting the collision detection functionalities.

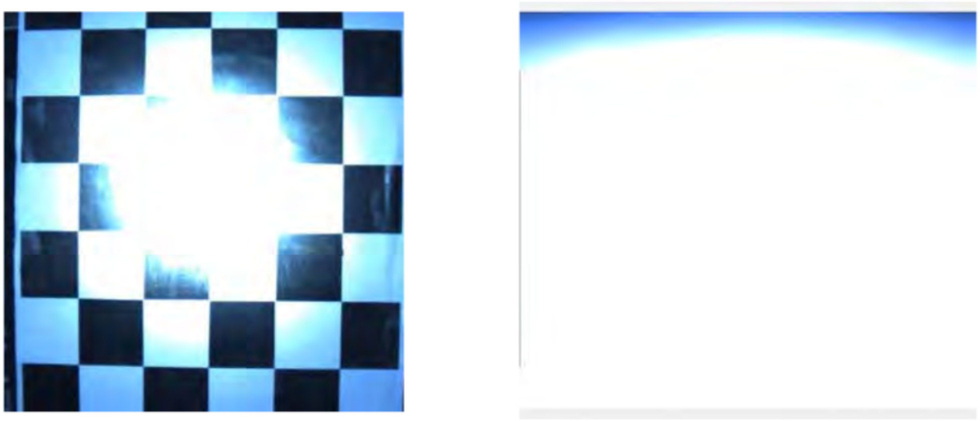
Countermeasures:

Constantly alternating the frequency of the mmWave radar frequency could limit the effectiveness of jamming attempts, as the attacker will not be able to determine and lock onto a single frequency. However, this may only provide finite success, as, in order for mmWave radar to work at each distance, there is a narrow operating window. Coupled with a modern jammer's ability to predict frequency change [64], this may only be a slightly effective method.

Sensor fail safe principles can be applied to radar. Utilising the on board AI and machine learning capabilities of the vehicle, as well as cross-referencing the data with other sensors such as LiDAR, the vehicle should perform anomaly detection on scanned objects [62]. This allows for the vehicle to determine if an object has been falsely introduced or its position altered, and can rely on the other sensors to provide more accurate data. This further adds a layer of redundancy, as discussed with LiDAR.

4.1.3 Cameras

Cameras fitted to AVs typically utilise either a Charge-Coupled Device (CCD) or Complementary Metal Oxide Semiconductor (CMOS) sensors [61], which are vulnerable to partial or total blinding, including permanent damage in extreme cases. Such an attack can be achieved through the use of low cost 'interferers', scuh as LED spot lasers, laser pointers and infrared LED spot lasers. The interferer is pointed directly at the vehicle's camera, which can cause total blinding, as illustrated in figure 7(a), or is pointed towards a calibration board and reflected back into the vehicle's camera, which can cause partial blinding, as illustrated in figure 7(b). Both of these figures show the results of blinding through the use of LED spot lasers, however, if an attacker is to use a laser pointer, the degree of partial blinding is increased and permanent damage can be caused.



(a) LED spot laser partial blinding

(b) LED spot laser total blinding

Figure 7: Partial and total camera blinding using a LED spot laser

Automotive cameras are also susceptible to attacks by concealing traffic signs. As discussed in section 3.1.1, one of the primary functions of a CAV camera is to detect road traffic signs, such as speed limit, pedestrian zone and warning signs. Research by Petit and Stottelaar [60, 58] highlighted that it is possible to alter the information and 'hide' traffic signs by surrounding and masking them with other shapes and colours, confusing the AI models. An attacker can further abuse this by placing falsified traffic signs in unsuitable locations. Furthermore, attackers could paint additional lines onto the road, making it difficult for the lane keeping system to work effectively.

Camera object tracking capabilities offered by the vehicle can also be targeted. Due to the resolution of the camera sensor and the limited computational power on the vehicle [58], presenting too many objects to track, i.e. multiple road traffic signs in close proximity, can overwhelm the system. Furthermore, attacks targeting the automatic expose controls and auto-focus of the camera can be conducted by pointing a bright light at the vehicle's camera. When a light is introduced, the camera will reduce its sensitivity and exposure to try and draw out the remaining information from the available image [60], however, this can be easily overwhelmed. Therefore a hacker can abuse this by hiding vital information such as traffic signs or pedestrians by introducing light.

Countermeasures:

Blinding attacks can be mitigated if the vehicle has a secondary reserve camera that can be switched to if the main camera experiences loss of function. This provides a layer of immediate redundancy if a camera experiences partial or total blindness. Furthermore, additional cameras should be implemented at different strategic locations on the vehicle, making it difficult for an attacker to blind every camera. Additionally, lens filters can be used to filter out interference [61]. However, increasing the number of cameras on each vehicle as well as increasing their complexity comes at the expensive of higher implementation cost and increased sizing constraints, presenting an issue for the cost-driven and space-restricted CAV market. [58].

Sensor fail safe principles can be applied to counter both blinding attacks and targeted attacks on camera functionality. The camera's software should have maximum exposure limits, which shuts off the camera unit if a light source causes the exposure to increase to an abnormal level.

This process would allow for the driver to take over controls, or draw from V2V communication and other sensor data to carry out autonomous functionality. V2V communication further allows for anomaly detection, as a targeted vehicle will show dramatically different camera data.

4.1.4 Ultrasonic Sensors

Ultrasonic sensors are vulnerable to the same spoofing and jamming attacks as seen in LiDAR and radar sensors, and therefore this section will not delve into the nuances of the attack. However, there are several noteworthy attacks which can be performed on ultrasonic sensors. Cloaking attacks are performed by concealing the presence of objects by cloaking their ultrasonic signal [65]. In such attack, sound absorbent materials are placed around obstacles such as parking bollards, walls or other vehicles, which absorb the sensor signals and drastically reduce their output, thus removing objects in the eye of the vehicle [36].

Research by Lim et al. [66] highlighted an issue with ultrasonic blind spot detection systems in vehicles, where very thin objects canuld not be perceived by the sensor. This can be exploited by attackers by placing a thin object towards the blind spot of a reversing vehicle. Such attack can be considered malicious but not overtly dangerous as it only has an effect at low speed scenarios.

An advanced attack on ultrasonic involves eliminating legitimate ultrasonic signals. Acoustic cancellation attacks transmit a counterfeit signal with a phase that is opposite to the legitimate signal [65, 66], causing the vehicle's ultrasonic phase to become zero. Such attack can temporarily render the vehicle's ultrasonic sensor redundant, however, acoustic cancellation involves a high degree of knowledge from attackers and resources that are not readily available.

An attacker however can conduct a physical attack on the vehicle's ultrasonic sensor by simply placing certain types of adhesive tape over the vehicle's transmitter and receiver. Lim et al. again tested this by placing scotch tape over the sensor, finding that they were able to completely disable its functionality [66].

Countermeasures:

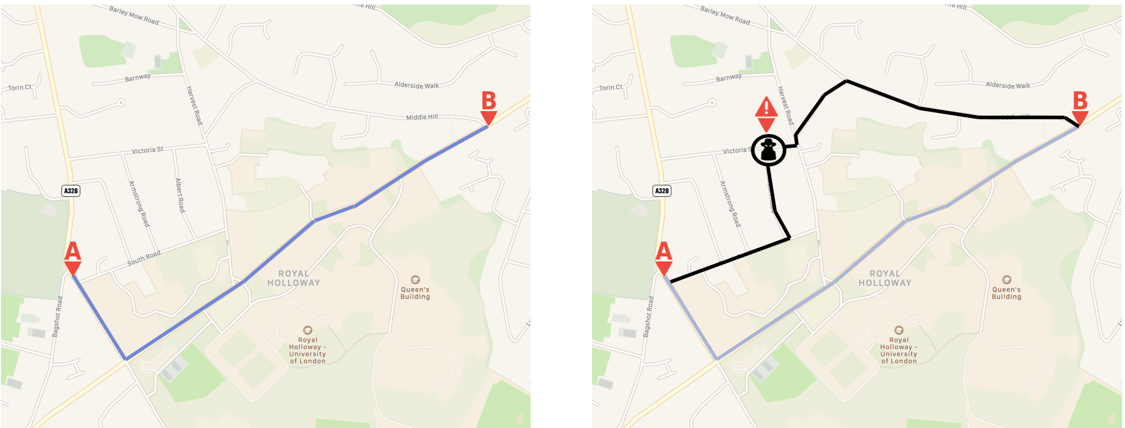
In order to counter blind spot and cloaking attacks, the vehicle should utilise sensor fusion and backup cameras in order to cross-check the object, verifying the legitimacy and accuracy of the ultrasonic sensor readings [65]. This method provides a layer of redundancy as seen with LiDAR and radar countermeasures. A simple, yet effective mitigation strategy against physical attacks would alert the driver to visually inspect their vehicle regularly to see if their sensors have been tampered with.

Mitigating against spoofing and jamming attacks requires the same principles as seen in radar, whereby the waveform of the signal is randomised. The transmitting waveform characteristics should be randomly altered, and should only be accepted by the receiver if they correlate to the given waveform. Furthermore, the frequency at which the waveforms are transmitted should be randomised and continually changed to avoid jamming attacks[66].

4.1.5 Global Positioning System (GPS)

Civilian GPS systems, as used within CAVs, are designed without encrypted and authorised transmission, contrasting military applications which can prevent counterfeit and illegitimate signals [67]. Moreover, traditional civilian GPS systems are not designed for either safety or security critical operations [68]. Although adopting an open standard for GPS within CAVs may well be robust and inexpensive, the accessible and predictable architecture presents the technology with vulnerabilities from counterfeited or spoofed signals.

GPS spoofing is achieved by an attacker broadcasting identical signals to that of the satellite's legitimate signal, then progressively increasing the power of the counterfeit signal and diverging it away from the vehicle's true location [69]. Due to the lack of signal authentication, and the publicly known codes for each satellite [70], the vehicle is unable to verify whether the signal received by the GPS receiver is legitimate or counterfeit. Worryingly, automotive GPS systems do not utilise such authentication procedures, and it has been established that off-the-shelf receivers cannot detect spoofing attacks [68]. Spoofing the GPS signal theoretically allows for the attacker to deviate the vehicle by detouring the victim along a guided route. An extension of this attack is called targeted deviation, as illustrated in figure 8 (b), where the victim is diverted to bypass a predetermined location which could potentially put them at risk [71].



(a) Original route navigation

(b) Targeted deviation on original route

Figure 8: Illustrating targeted deviation of a GPS navigation route

There have been now published real-world spoofing attacks, with the absence possibly be explained by the cost of hardware, and the required skill needed to build a sophisticated GPS spoofer. Dr Todd Humphreys [67] suggests that in order to create a hardware spoofer, the required off-the-shelf components would cost between one and two thousand USD. Furthermore, Humphreys predicts that there are no more than one hundred researchers worldwide in universities that have the expertise in software-defined GPS that could develop a GPS spoofer. For the time being then, spoofer development is likely outside the capability of lone hackers, but remains within the capability of nation-states.

GPS systems remain vulnerable to jamming attacks. During such attacks, GPS sensor signals are jammed to prevent locating the vehicle [65]. GPS signals from satellites are considered weak in nature, with jamming attacks exploiting this by generating strong signals that overwhelm the GPS receiver. Jamming attacks on GPS do not require the advanced levels of competence that spoofing attacks require, and can be carried out with low cost hardware [72]. An attacker can deploy jamming as part of a Denial-of-Service attack. Furthermore, a thief can utilise a jammer to block the vehicle's anti-theft GPS system from knowing and reporting the vehicle's location [72].

Another advanced attack on GPS systems include black hole attacks. In a black hole attack, an attacker can cause the deliberate loss of GPS information across a V2X network. Such attack hinders the reliability and efficacy of V2X communication as attackers falsify their GPS data and advertise themselves as having correct GPS data [65]. Black hole nodes send false information onto other nodes, causing the network to crash.

Countermeasures:

The automotive industry should look towards military applications of GPS and utilise encrypted GPS transmission. However, Humphreys [67] states that this could deny the free and open access which the technology is built on. Therefore, it is important to propose a countermeasure that provides signal authentication without the denial of access. With this, Navigation Message Authentication (NMA) could be implemented. This method embeds public-key digital signatures into the GPS message which can be validated by the vehicle [67]. This allows for only authorised signals to be accepted by the GPS system on the vehicle. An additional spoofing countermeasure looks to utilise multiple GPS receivers deployed in a static, known formation on the vehicle. This method allows the receivers to exchange their individual locations on the vehicle and can each check if their calculated locations preserve their physical formation [68].

To defend against jamming attacks, Petit and Shaldover suggest utilising IMU sensor measurements in the event of an attack [72]. This method however should only be used as a supplementary and/or as a layer of redundancy if the GPS receiver is temporarily unavailable, as CAVs require highly accurate navigation data to provide advanced levels of autonomy.

Defending against black hole attacks requires building multiple routes to the destination (node) in the network [73]. Research by Mahmood and Khan [73] proposed two suitable countermeasures: Firstly, an anomaly-based neighbour-monitoring scheme was evaluated, where each node builds up a profile of it's neighbouring node's behaviour, with traffic features exceeding the predetermined range flagging up an alert. [73, 74] A second anomaly-based approach utilised dynamic training and clustering to identify nodes that deviate from a normal state [73, 75].

4.1.6 Inertial Measurement Unit (IMU)/ Inertial Navigation Systems (INS)

As mentioned in section 3.1.2, INS sensors are embedded within the vehicle and do not possess any external communication capabilities, and therefore are impervious to remote attacks, however, INS sensors remain vulnerable to local spoofing and acoustic attacks.

Spoofing attacks on INS sensors can be conducted with relative ease with the use of off-the-shelf hardware [76]. Spoofing attacks work by either manipulating analog signals and injecting them towards the region of the sensor, influencing the system's digital readings, or, through side-swing attacks. In Side-swing attacks, attackers can manipulate the vehicle's heading value by alternately injecting different waveforms of a varying frequency to achieve phase pacing, which causes the vehicle's heading value to progressively increase [65, 76]. Manipulation and spoofing of INS sensors can cause the vehicle to believe it is travelling faster, is under more lateral gravitational force, or is at a steeper gradient, subsequently changing the autonomous driving dynamics.

Acoustic attacks on INS sensors target spring-mass structures such as gyroscopes and accelerometers (MEMS sensors). An attacker injects falsified acoustic waves where the frequency matches the resonant frequency of the chosen spring-mass sensor, resulting in the sensors vibrating and drastically affecting the behaviour of the sensor [77]. Falsified acoustic waves can be used to obtain full control over an accelerometer or gyroscope, allowing the hacker to manipulate vehicle dynamics, as seen with spoofing attacks.

Countermeasures:

Mitigating both spoofing and acoustic attacks can be accomplished by the use of relatively inexpensive hardware components and lightweight software defence mechanisms. Yazhou Tu et al. [76] suggest implementing microfabric acoustic material and isolating boxes in and around the INS sensors in order to dampen and isolate the unit from acoustic interference. Such materials protect MEMS sensors from attacks without compromising size, weight, cost, or the performance of the system.

Software defence mechanisms can also be applied to counter spoofing and acoustic attacks by utilising low-pass filters and random sampling. Low-pass filters scan be used to eliminate out-of-bands analog signals [76], as well as lowering the cut-off frequency, so that loud acoustic attacks do not remain effective. Random sampling can be used to mitigate against an attacker's falsified signal by eliminating the ability for said attacker to conduct acoustic interference.

4.2 Attacks on V2X Communication

Given the security vulnerabilities presented thus far, one could reasonably argue that closed vehicle systems are easier to secure than connected vehicle systems. Whilst attacks on isolated traditional vehicles can have considerable consequences, security breaches do not compromise or propagate over to other vehicles, connected infrastructure or external networks. Although the communication technologies that enable V2X communication incorporate the security service requirements previously listed, V2X networks are still vulnerable to several attacks on security due to the underlying technologies. This section considers the various attacks on V2X networks, with each attack being applicable to V2V, V2I, V2N and V2P communication.

1. *Blackhole Attacks:* The attacker receives transmissions from the V2X network but denies participation in routing the received data [16]. Information is not relayed to neighbouring nodes, consequently blocking the spread of information across the network.

2. *Bogus Messages:* Compromised nodes spread bogus (falsified) transmissions across the network, either by generating false messages or modifying existing ones. Attackers broadcast bogus messages to misguide other vehicles on the network, i.e. falsifying traffic jams or collision warnings.

3. *Certificate Replication:* Attackers gain access to compromised nodes and exploit replicated certificates to conceal themselves. Certificates that were previously added to a blacklist are recycled by malicious entities on the network [16]

4. *Denial-of-Service:* An attacker injects copious volumes on data into the network, attempting to minimise the packet reception ration (PRR) for nodes on the network [78], jeopardising the availability and performance of V2X.

5. *Eavesdropping:* Attackers collect and 'listen in' to data flowing through a V2X network, aiming to acquire sensitive and confidential information on users, infrastructure and network information. Eavesdropping is considered passive as it has no direct effect on the network [14].

6. *GPS Spoofing:* GPS spoofing attacks have been covered in section 4.1.5.

7. *Impersonation (Masquerading):* The attacker presents himself as a legitimate entity on the V2X network, gaining access to confidential data and abusing authorisation controls. Attackers can then send malicious information to nodes on the network, causing a number of other attacks.

8. *Location Tracking:* An attacker listens over a network and analyses the data collected from neighbouring nodes to identify the current and previous locations of the target. This form of attack is considered passive, however it can be performed regardless whether or not the target changes their pseudonym [79].

9. *Message Modification:* Attacks who have received legitimate messages from nodes on the network modify the message before sending it on. Modifying the original message can achieved by adding to, reorganising or fundamentally changing all or part of the message.

10. *Replay Attacks:* Replay attacks are considered one of the most common attacks in all types of networks [16]. Messages received by adversaries are maliciously replayed repeatedly over the networks, potentially inducing Denial-of-Service across the network.

11. *Sybil:* A sybil attack is any instance where attackers join a network using multiple real or fake identities [14]. Attackers can deploy this attack to generate falsified vehicles on the road, benefiting the attacker.

12. *Unauthorised Access:* Network services are forcefully accessed by attackers who do not originally possess the required access rights or authentication. Confidential data is often targeted as the access controls protecting the given data has been overridden.

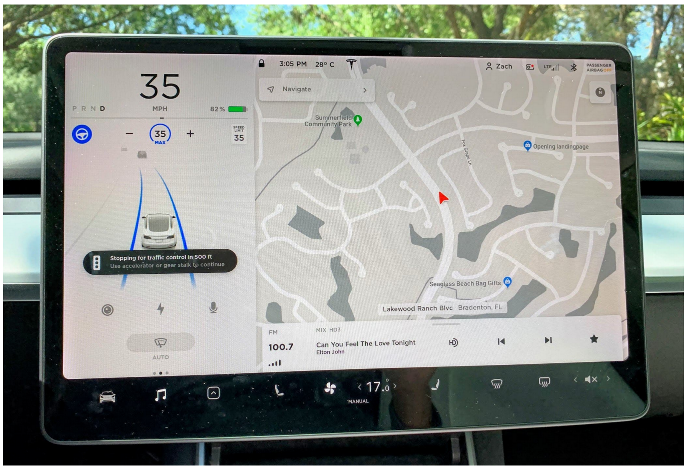
The presented attacks vary in both the complexity and the probability of being detected by the network. While countermeasures are considered outside the scope of this paper, V2X network designers should consider improving the security service mechanisms outlined in Table 2. Table 2 further looks towards both empirical and theoretical research [65, 69, 68, 13, 16, 14, 80, 81] to provide an insight into the difficulty and detection probability for each of the aforementioned attacks on V2X networks.

Attack	Ease of Attack	Detection Propability	Security Service Breaced
Blackhole Attack	Moderate	*Moderate*	Availability, Confidentiality
Bogus Messages	Moderate	*Low*	Data Origin Authentication, Availability, Data Integrity
Certificate Replication	Moderate	*Low*	Data Integrity, Non-Repuidation
Denial-of-Service	High	*High*	Data Origin Authentication, Availability
Eavesdropping	High	*Low*	Data Origin Authentication, Anonymity, Confidentiality
GPS Spoofing	High	*Low*	Data Integrity, Location Privacy, Non-Repuidation
Impersonisation (Masquerading)	Low	*Low*	Data Origin Authentication, Data Integrity, Non-Repudiation
Location Tracking	Moderate	*Low*	Anonymity, Confidentiality, Location Privacy
Message Modification	High	*Moderate*	Data Origin Authentication, Availability, Data Integrity
Replay Attack	High	*Low*	Data Origin Authentication, Data Integrity
Sybil Attack	High	*Low*	Data Origin Authentication, Availability
Unauthorised Access	Moderate	*Moderate*	Confidentiality, Data Integrity
References	[65, 69, 68, 13, 16, 14, 80, 81]		

Table 2: Attack analysis on V2X communication

4.3 Attacks on Infotainment Systems

CAV development suggests a reliance on infotainment systems. One only needs to look to industry leaders such as Tesla and their Model 3 to see the emphasis on driving-related information being almost wholly presented and controlled by the infotainment system, as illustrated by figure 9 [82].



Stopping for traffic control in 500 ft
Use accelerator or gear stalk to continue

Figure 9: Tesla Model 3 infotainment system and Autopilot interface

It is therefore conceivable to envisage a future where the majority of a CAVs autonomous systems are exclusively controlled by the infotainment systems. As a result, this leaves the technology, including smartphone connectivity, a target for attackers. The attack surface on infotainment presents vulnerabilities from both local and remote attacks. The following subsections discusses attacks on USB, CD-ROMS and Bluetooth and presents suitable countermeasures for the given vulnerabilities.

4.3.1 USB, CD-ROMS and Infotainment

Vehicle manufactures have increased the security vulnerabilities of infotainment systems by allowing access to both the internet and outside devices such as smartphones [83]. Furthermore, infotainment systems are often connected to the CAN bus on a vehicle which presents attackers with additional incentives and opportunities to exploit autonomous vehicle security and functionality.

There are a several ways one can connect their phone to the infotainment system. Modern vehicles often have one or more Universal Serial Bus (USB) ports that allows for multimedia playback from the user's smartphone or electronic device. Additionally, some vehicles allow firmware and software updates for the infotainment system to be uploaded via the USB or OBD-II ports.

This data communication method leaves the vehicle vulnerable to malware injection attacks. Researchers at Zingbox [84] highlighted that a maliciously crafted USB device could be used to upload malware onto the vehicle's infotainment system. This malware could be deployed to leverage the SMS service of the user's smartphone, allowing the attacker to access personal information, block or accept phone calls, or even keystroke log personal authentication pins [85]. Injected malware can also cause the infotainment system to be in an unusable state by commanded messages through SMS. If this attack is applied to CAVs who have their autonomous controls embedded into their infotainment systems, this could cause potentially hazardous Denial-of-Service attacks.

Attacks can use these various entry points into the infotainment system to tamper with CD, Bluetooth and Wi-Fi in the vehicle, with the use of maliciously designed media files [85]. Adversaries could consequently deliver malicious code into the infotainment system by encoding a Trojan CD or song file with malicious inputs, and use social engineering tactics to persuade the target to unknowingly compromise their infotainment system and vehicle. Research by Checkoway et al. [86] illustrated the threat of malicious CD-ROMs on a vehicle, highlighting the possibility of an adversary gaining access to the CAN bus and tampering with ECU firmware through malicious CD-ROM media. Trojan media attacks can also spread throughout file-sharing networks on the vehicle without being detected.

Countermeasures:

In order to mitigate against USB port attacks, the vehicle should check the format of a USB device and only grant supported file systems the ability to mount to the vehicle's infotainment system [85]. This same principle can be applied to other infotainment connection methods, including CD-ROMs and Bluetooth. Furthermore, automotive manufacturers should consider both adopting read-only permissions for devices, and separating the infotainment system from the autonomous driving system.

Service updates that utilise USB or OBD-II ports do require write permissions however. To protect against illegitimate firmware updates, the cryptographic keys used when establishing a connection to the vehicle and verifying the parties should be securely stored as to avoid an adversary finding and using them. Additionally, update packages should be digitally signed and encrypted, with the vehicle having the ability to refuse malicious updates [85].

4.3.2 Bluetooth

Attacks on Bluetooth risk the adversary gaining control over the Bluetooth system, personal data, and other safety critical systems in the vehicle. Recent research [87] found a mass security vulnerability with Bluetooth in several vehicle brands, dubbed 'CarsBlues'. This security flaw allowed an attacker to steal Personally Identifiable Information (PII) of users who had synced their smartphones to the vehicle's Bluetooth infotainment system. This vulnerability allows an attacker to access stored contacts, call logs, and full messages without the user being aware. The attack was deemed relatively easy to replicate and straightforward to perform against unsuspecting targets, and crucially could be completed without a trace [87]. This raises security and privacy concerns for owners of vehicles, and crucially highlights the vulnerability of rented or shared vehicles.

Bluetooth connection can act as a gateway into the vehicle's systems. Research by the Tencent Keen Security Lab [88] discovered vulnerabilities in certain BMW models that allowed an attacker to gain access into the infotainment systems, the telematics control units and the CAN bus via a Bluetooth connection [83]. Access into the CAN bus via Bluetooth further allows attackers to inject malicious code into targeted ECUs attached to the CAN bus, manipulating vehicle operation. As the Bluetooth connection on vehicle is publicly discoverable, hackers can connect smartphones to target vehicles, take control of the infotainment system and perform Denial-of-Service attacks by flooding the system with data, or jamming systems to cause applications and devices to crash [89].

Countermeasures:

Mitigating against malicious Bluetooth attacks requires the Bluetooth protocols to be properly configured, with unused Bluetooth profiles being disabled [85]. Furthermore, cryptographic user authorisation and authentication mechanisms should be incorporated into the pairing process for new smartphones, including the use of strong passwords and digital signatures to ensure only legitimate connects are made [83].

While many vehicle manufactures separate their infotainment system communication networks from their vehicular operation and safety networks, not all have adopted this. It is recommended that all manufactures separate said networks, especially the operational and safety systems on the CAN from the in-vehicle communication networks. Moreover, reducing the control connected Bluetooth devices have over the vehicle should be beneficial. Limiting control to previously accepted notions, i.e. limited to multimedia playback and basic mobile phone operations as seen in vehicles in the mid 2010s, should reduce the desire for attackers to target vehicular Bluetooth.

4.4 Attacks on Automotive Control Systems

Automotive control systems represent the systems and subsystems that manage and maintain the functionality and operation of the vehicle, including vehicular safety systems, vehicle security, electronic control units (ECUs) and vehicle connection mechanisms. Attacks on automotive control systems frequently target the ECU, CAN bus and the vehicle's key [90]. Similarly to the previous subsections, attacks on such systems will be discussed, and countermeasures will be proposed in order to mitigate against the occurrence and resulting damage of these attacks.

4.4.1 ECUs and CAN Bus

Early implementations of the CAN bus were not designed with an emphasis on secure communication, as vehicles at the time were not transmitting data to external networks [91]. This leaves the CAN bus vulnerable as it does not support the security features required CAVs. CAVs remain vulnerable to active and passive attacks including; eavesdropping, replay attacks, bus injection, denial-of-service attacks, ECU firmware tampering and spoofing. These attacks are largely facilitated in part due to the design of the CAN protocol, as it enables unauthorised access between the various ECUs in the vehicle. Furthermore, there are no authentication mechanisms, and transmission is often unencrypted [92]. Figure 10 [93] illustrates a generic attack on the CAN bus.

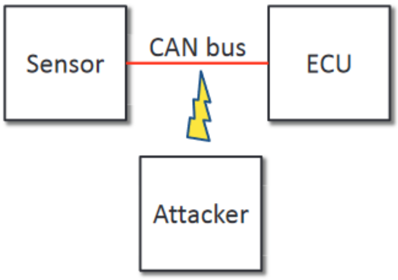


Figure 10: Generic attack on the CAN bus network

The vulnerability for denial-of-service attacks is due to CAN bus' priority-based arbitration mechanism. The design of the protocol grants the node with the highest priority transmission without interruption, if two nodes are transmitting at the same time [94], therefore causing messages with a lower priority to indefinitely hold their transmission. This allows an attacker to inject malicious messages with a high priority into the vehicle's ECU at a high frequency. Thus causing the vehicle to malfunction or freeze, consequently denying communication between nodes and blocking the sensors data. This allows an attacker to disable features of the connected or autonomous systems on the vehicle [95].

The CAN bus is also vulnerable to injection and eavesdropping attacks due to the lack of encryption and authentication mechanisms. Injection attacks allow an attacker to inject data into the CAN bus at an abnormal rate [91, 96]. As the CAN protocol does not offer authentication, the vehicle has no way of verifying whether the injected messages are legitimate or not. Furthermore, the lack of encryption also allows unverified malicious nodes to connect the network and inject data into the bus. Therefore, messages between nodes can be monitored and observed, and further allows an attacker to generate illegitimate and disruptive messages that can be used to simulate incidents, altering the behaviour of the vehicle as required by the attacker [91].

An extension of the aforementioned attacks allows an attacker to analyse the traffic on the bus and learn the behaviours of each ECU embedded in the vehicle. By analysing the CAN bus, an attacker can mimic ECU behaviour [91]. Research by Lehira et al. [97] found that such attacks were often undetected by ECUs. This allows an attacker to target certain ECUs and falsify legitimate messages, raising an error in the ECU controller, forcing the bus to cut transmission between the ECU and network. Again, this attack highlights the vulnerability of negating authorisation mechanisms on a network. The results from their research found that by utilising various spoofing methods, the transmission of legitimate messages was entirely prevented on an actual car, and, 100% of spoofing messages would be received by the target ECU with no error being detected [97].

Access to the CAN bus of a CAV is feasible via a broad range of remote attack surfaces [98]. With the inclusion of external interfaces in CAVs, the CAN bus can be connected to through communication technologies such as Bluetooth, Wi-Fi and cellular. Research conducted by Nie et al. [99] presented the successful implementation of a remote attack on a Tesla Model S, allowing them to inject malicious messages into the CAN bus. This attack targeted the Wi-Fi and cellular capabilities of the vehicle and compromised the physical layer of the CAN bus, meaning the vehicle to be fully controlled by an attacker [99].

Countermeasures:

The attacks on the CAN bus protocol requires strong security countermeasures. As previously mentioned, the CAN protocol does not utilise encryption or authentication mechanisms to control the communication between nodes on the vehicle's CAN network. With this, cryptographic mechanisms should be implemented into the network, providing both dedicated encryption and authentication procedures for traffic on the network. Although this may come at the cost of computational power, lightweight cryptographic mechanisms should be feasible.

Lightweight Message Authentication Codes (MACs) can be used to provide authentication and data integrity for the transmission of messages along the CAN bus. This method however does not provide any means of non-repudiation, meaning it is not possible for the vehicle to know if incoming messages have been tampered with. Additionally, MACs cannot provide confidentiality, meaning an attacker can still perform eavesdropping and reverse engineering attacks on CAN messages [91]. For this, encryption algorithms such as 128 bit Advanced Encryption Standard (AES-128) can be used to provide confidentiality, meaning an attacker cannot perform the aforementioned eavesdropping attacks or learn the behaviour of specific ECUs.

A simple countermeasure against CAN attacks is to separate the CAN network into multiple sub-networks [94]. Network segmentation provides a layer of protection against error propagation, as an attack on an ECU can only cause damage to the specific CAN sub-network in which the ECU is located, and limits the spread of damage to the whole vehicle's CAN network. This means, an attack on less safety critical ECUs does not interfere with higher-priority systems such as ABS or LiDAR units for example. Although network segmentation can reduce the effects of a targeted attack, it does not provide any further protection mechanisms to the nodes on the bus, and further makes system maintenance more complicated.

4.4.2 Keyless Entry Systems

PKES remain vulnerable to relay attacks. Relay attacks target the challenge-response protocol used within the PKES key, allowing the attacker to unlock and start the vehicle's ignition while the key fob is outside the required distance. An attacker needs a key agent and a car agent which has the regular functions of the key and the car, but also the ability to relay communications [51]. The relay channel between the key agent and car agent can transmit the RFID signal significantly further than the vehicle's key fob, and is undetected by the vehicle's PKES system. The challenge signal is relayed from the key to the key agent along the relay channel, and the response from the vehicle is returned through the vehicle agent and back along the relay channel. Figure 11 [51] illustrates the set up of a relay attack. The car is unable to distinguish between the real key and the key agent, and therefore the attacker can conduct this attack without being detected.

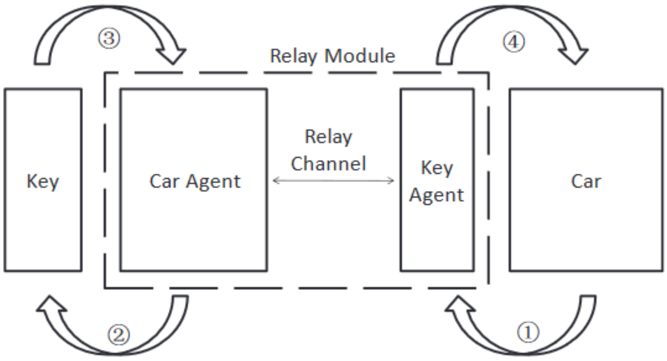


Figure 11: Illustration of a relay attack on a PKES system

Countermeasures:

In order to mitigate against relay attacks on PKES, research [50] suggests that distance bounding is the best method to protect against an attack. Distance bounding protocols denote upper-bounds for the round-trip time (RTT) of messages between the PKES key fob and the vehicle. The verifier (RFID reader on the vehicle) is equipped with a reliable clock that measures the RTT of message exchanges, checking whether the prover (RFID key fob) is no further than the maximum defined limit [100]. In the event of an attack, if the verifier and prover are mutually trusted, the attacker cannot convince the the vehicle that the key is within the required distance, hence blocking the attack. Although the presented distance bounding protocol could be considered as a simple proximity checking mechanisms, distance bounding protocols also provide unilateral authentication utilising cryptographic primitives such as MACs, signature schemes and encryption [100]. This further mitigates against relay attacks in the context of vehicles.

4.5 Summary

The increased complexity of vehicular technologies and systems presents a multitude of security vulnerabilities which can and will be exploited by attackers. The attack surface on modern vehicle is already vast, however CAV applications expands this to unprecedented levels. Attacks on availability, integrity, reliability, efficacy and confidentiality can be conducted in many cases with the use of inexpensive hardware, or a moderate understanding of the technological architecture.

Therefore, the automotive industry must look to existing research, and conduct their own work in order to find the susceptibilities and entry points for hackers into their system. Furthermore, they should consider how an attack on such system will affect other hardware and software on the vehicle, as well as the user's safety and the impact on the autonomous driving features.

Although there are few documented cases of genuine attacks on CAVs in the real-world, researchers have demonstrated multiple susceptibilities for their underlying technologies. In the same vein, attacker's capabilities are expected to improve with technological development in the tools and mechanisms they use, and thus, system designers must ensure the safety and security critical components are secured, and segregated from less safety critical components. Furthermore, CAV provisions should include multiple layers of redundancy in the event of a sensor going offline as the result of an attack.

Thus, the automotive industry should consider adopting core security service principles, cryptographic primitives, software defences and hardware solutions to mitigate against such attacks.

5 Personal Data Protection and Privacy Implications

5.1 Identifying Personal Data

We have seen from section 4 that vehicle sensors and AI systems capture, process and produce vast volumes of data in order to provide the autonomous driving capabilities seen in high level CAVs. In addition to sensor data, CAVs capture and analyse personal and sensitive information relating to users and non-users (pedestrians, infrastructure and passengers who are either associated or connected to the vehicle) [101]. According to the European Data Protection Board (EDPB), the most associated data with CV is considered to be personal data [102]. Personal data can also extend to any information that has been captured and shared that relates to an individual; when a vehicle's sensor and operational information is associated with an identifiable individual, that data becomes personal information [103]. Furthermore, CAV technologies can also capture and share personal information for less obvious insights; for example, vehicles will be able to identify different users based on the differing operations of vehicle controls, i.e. throttle input [104]. Hence, comprehensive data collection on users will become commonplace with jointly owned or shared vehicles, catering to the consumer desire for harmonious integration between CAVs and a user's digitised lives [104].

It is important to understand the full extent of what types of personal data is collected. Table 3 describes the personal data relating to CAVs, its users and external entities, adapted from Krontiris' et al. publication [101]:

Data relating to the vehicle and its users		**Data relating to external entities**	
Related Data	***Example***	***Related Data***	***Example***
User and non-user information	*Name, address, account information, biometric data etc.*	Surrounding vehices information	*License plates, colour, passengers etc.*
Personal devices of users and non-users	*Smartphone ID, MAC addresses, stored contacts etc.*	Camera recordings and images	*Faces of pedestrians, cyclists, house numbers, building names etc.*
Trip information	*Trip history, saved trips, duration and time of journeys etc.*	Sensor data	*Pedestrian identification etc.*
Vehicle location data	*Home parking address, parking history, service centres etc.*	Connected infrastrucure (RSUs)	*Connected vehicles, pedestrians, connection history etc.*
Vehicle identification	*Vehicle make and model, VIN number, chassis code etc.*	V2X communication	*Message information containing vehicle pseudonmys, number of connections, location information etc.*

Table 3: Personal data relating to connected and autonomous vehicles

5.2 Considerations and Implications

While OEMs may utilise personal and sensitive data to improve the autonomous vehicle performance, in many cases, users and non-users are presented with limited consent or opportunities with regards to the collection and handling of their data. These data concerns expose several important privacy implications for CAVs and their information capturing and sharing capabilities, raising questions of who is controlling the data and how is it being managed [105]. Privacy further remain unclear, as many users may object to the reasons as why data is collected, what type of data is required, and the duration that it is stored [103]. This lack of transparency over the handling personal data can damage public perception and acceptance of CAV technologies.

CAVs will also possess information that relates to the user's whereabouts, and general driving habits [106]. This data holds intrinsic value to OEMs and advertisers; Glancy notes that CAV users could be subject to location-based targeted advertising during their commute, for example [103]. While ethical and moral questions will certainly be raised, this could also later lead to personal privacy being abused and breached if users lack control over their information.

In addition to commercial use of personal information, data collected for well-defined purposes risks being later sold or used in unlawful processing contexts. Good sets of personal and private data will fetch high prices online [104], with such data being highly valuable for social engineering schemes or ransom attacks. Furthermore, data collected by CAVs could unknowingly be used by insurance companies or law enforcement authorities. CAVs can detect and share when the user is speeding, or has visited a known location associated with criminal activity. In this case, such information can be passed on to the relevant entities, breaching a user's privacy and confidentiality.

OEMs should also be mindful of excessively collecting personal information on users and non-users. While the AI and machine learning systems on CAVs are fuelled by vast volumes of data, collection should be limited exclusively to what is necessary. Thus, OEMs should consider the the types of personal data and its applicability to their AI systems, referencing table 3.

Therefore, the privacy and protection of user and non-user data is an important safeguard against the mishandling of both personal and vehicular information. Traditionally, there has been little in the way of bespoke CAV data legislation [107]. Although any personal information processed by a CAV should be processed in accordance with existing data protection legislation [108], there is still uncertainty as to the scope and discernment of personal data in the context of CAVs. One of the closest regulations for personal data collection on a vehicle thus far are those of dash cams [109], however, the advanced data collection capabilities of CAV sensors and AI systems extend far beyond the scope of dash cams. Thus, in order to appropriately handle and protect personal data, vehicular and communication systems must be designed with the security service requirements mentioned in section 2.3.3, with an emphasis on integrity and confidentiality, as well as in accordance with existing personal data legislation.

Furthermore, the privacy of user and non-user information is necessary in ensuring that CAVs are trusted and accepted by consumers. A recent survey *(n=1049)* on the public opinion of CAVs by Gabrhel et al. found that 49.3% of participants were either 'moderately' or 'very' concerned about data privacy [110]. Bloom et al. explored people's perceptions of the sensing and analysis capabilities of CAVs, with their study *(n=302)* finding that 54% of participants would opt out of identifiable data collection [109]. Moreover, their study also found that information collected and processed for recognition, identification and vehicle tracking was associated with overwhelming discomfort, and, privacy concerns also causing participants to express high levels of discomfort[109]. Both studies highlight the need for strict privacy regulation for personal information, owing to the unique challenges of CAV technologies and the ways in which data is managed.

5.3 Summary

Research throughout this report highlighted the unique challenges personal data and the privacy of users and non-users faces. While it might not be evident at first, CAVs produce, share and store vast volumes of personal information that can be used it identify individuals. Such information has an intrinsic value to the automotive industry, advertisers or criminals, where data may not always be used for well-defined purposes.

Thus, the automotive industry should consider adopting tighter security controls over personal data and privacy. However, the lack of bespoke legislation or clarity within existing legislation and guidelines presents challenges for CAVs.

6 Reviewing Existing Legislation and Principles Related to Connected and Autonomous vehicles

6.1 Legislation

6.1.1 GDPR and EDPB

Entered into force on May 25, 2018, the European Union's General Data Protection Regulation (GDPR) applies to all processing of personal data in the EU, including autonomous transport [111]. The GDPR requires that organisations focus on data protection, giving the user control over how their personal data is collected, used and shared. As discussed in section 5, due to the high volume of personal data captured and shared in CAVs, the GDPR is perhaps the most relevant and applicable sets of legislation for personal data and CAVs.

The GDPR sets out several requirements that organisations must adopt to ensure personal data and privacy is protected, including:

1. Lawfulness, fairness and transparency
2. Limitation of purpose, data and storage
3. Data subject rights
4. Privacy by design and by default
5. Data integrity and confidentiality
6. Accountability

In accordance withe the aforementioned, in February 2020, the EDPB - the body responsible for ensuring GDPR data protection laws are applied consistently throughout the EU - published specific guidelines for the processing of GDPR personal data rules in the context of CVs [112]. The EDPB highlighted various privacy and data protection risks associated with CVs. Firstly, they identified a lack of control and information asymmetry, noting that: *"drivers and passengers may not always be adequately informed about the processing of data taking place in or through a CV"* [113]. This alludes to a risk of insufficient options to the user for controlling their data protection and privacy rights, and confusion over data ownership. Secondly, the quality of user's consent was noted, owing to the fact that users may not be aware of the data processing carried out on the vehicle. This is an obvious breach of GDPR rules, as consent must be informed to the user [102]. Therefore, traditional consent mechanisms may need to be updated to be compatible with CAV system. Thirdly, further processing of personal data must be met with additional consent, as initial consent should not constitute further data collection actions. Fourthly, as mentioned in section 5.2, personal data should not be subject to excessive collection, with OEMs often collecting more than is required. This calls for limits on AI processing and machine learning with personal data. Finally, the overall security of personal data was identified as a risk; as previously discussed, the increased functionality of CAVs leads to a broader attack surface, thus opening more attacks on personal data.

The risks identified by the EDPB pose many questions as to whether CAVs are compatible with GDPR, and what directions OEMs should take in ensuring their vehicles are compliant. While recommendations were presented; geolocation data protection, biometric data protection and data revealing criminal offences being carried out under the control of an official authority [113], the ambiguity in GDPR laws still present several personal data concerns with CAVs.

Thus, it is evident that there is a requirement for more applicable sets of legal rules and requirements relating to CAVs, due to the complex nature in which personal data is used. Traditional data protection principles may be incompatible with the ways in which data is collected and processed in autonomous driving contexts. Therefore, there is a a requirement for collaboration between OEMs and GDPR legislators to define commonly agreed data protection rules that strikes a balance between the protection of personal data and allowing CAV technologies to operate as required.

6.1.2 Automated and Electric Vehicle Act 2018

The Automated and Electric Vehicle Act 2018 passed into law on 19 July 2018 [114]. The legislation is part of the UK Government's initiative to promote the development and deployment of autonomous and electric vehicles, with implementation being rolled out via a number of statuary instruments, in order to fulfill the government's goal of fully autonomous vehicles on the road by late 2021 [115]. Sections 1-8 of the act address the insurance issues that arise when the responsibility for a autonomous vehicle is shared between the driver and the vehicle itself [114].

The act acknowledges the position of insurers, considering whether an accident involving an automated vehicle can be considered contributory negligence. The Act states that the insurer is not liable to the person 'in charge of the vehicle' where the accident that it caused was wholly due to the person's negligence in allowing the vehicle to being driving itself when it was not appropriate to do so [114, 115]. This raises questions however of when is it considered appropriate to allow the vehicle to drive itself, suggesting there is a requirement for more clarification.

Section 4 of the Act address unauthorised software alterations and failure to update software, stating that insurers will be able to limit their liability if the vehicle's operating system was tampered with, or the software has not been kept up to date. This looks to shift the responsibility onto the owner or user, as vehicle manufacturers will wish keep CAV software up to date, through emphasis on over-the-air (OTA) updates. It was stated that vehicle manufacturers were more likely to enforce and automatically install updates, helping to improve the safety and reduce the number of insurance claims [116]. Furthermore, although not implemented in the final act, it is recommended that stricture measures should be taken against attackers who tamper with vehicle software, something which other governments may wish to adopt.

It is worth noting that, when the Bill was discussed in parliament, Baroness Sugg *(delegate the Secretary of State for Transport)*, stated that, although the Act is beneficial, the government believes the SAE's 'Levels of Driving Autonomy' lacked precision, and they would be seeking to set their own safety standards by way of a technical committee [115]. Sugg stated:

> *"The categories set out by the SAE are under continual revision. A direct link to the levels creates problems if the definitions move away from what is needed for the proper functioning of the bill." [116]*

Although Sugg later suggests they are not explicitly rejecting the SAE levels, they do not however meet the levels of precision required for approval and regulation. This raises important questions as to which level would be considered safe or lawful when a vehicle is in AV mode, and whether or not the Act need apply. Furthermore, this highlights the need for an internationally accepted definition and classification for CAV capabilities, however, it is recommended that the UK Government does indeed follow the SAE's levels due to their widespread adoption and acceptance in the industry.

While there are many unanswered questions about the future of CAVs on British roads, the Act provides some important provisions for for AVs and the liability of insurers. Thus, legislators should continue to build on this Act, ensuring it remains relevant with the ever-changing landscape of CAVs. However, there is still a distinct lack of specifics in the Act, and the adoption of new legislation is likely to lead to years of uncertainty for victims of an AV accident with regards to liability [115].

6.1.3 United Nations Regulations 155 & 156

The United Nations (UN) World Forum for the Harmonisation of Vehicle Regulations introduced two new regulations on 22 January 2021 [117]. The regulations are applicable to 54 countries that are parties to the 1958 agreement. The regulations require that the authorities responsible for approving vehicle models prior to going on sale in a given country are built with cybersecurity provisions, with manufactures ensuring that their suppliers implement the same measures [118].

The regulations further list examples and specifics for connected vehicle cybersecurity attacks, allowing manufacturers time to prepare and respond to security vulnerabilities. The two regulations are as follows:

UN Regulation No. 155 - Cyber security and cyber security management system:

This regulation applies to connected and autonomous vehicles with automated driving functionalities from level 3 onwards. The regulation governs a vehicle's cybersecurity concerns, introducing audit related provisions [119] that assess the robustness of the cyber security measures implemented by the vehicle manufacturer. These provisions also extend to the manufacturer's suppliers, attempting to mitigate cyber risks along the supply chain. It also requires that manufactures and suppliers monitor, report and share incidents. The regulation further ensures that there is a cybersecurity management system in place, and is available to all vehicles on the road. Mitigation strategies are required and should be in place to reduce the likelihood of a realised attack, with measures in place that can preemptively detect cyber risks . The regulation additionally provides a framework for the automotive industry that can be implemented if necessary, helping manage cybersecurity risks, summarised by [117]:

1. Identify and manage cyber security risks in vehicle design;
2. Verify that the risks are managed, including testing;
3. Ensure risks assessments are kept current;
4. Monitor cyber-attacks and effectively respond to them;
5. Support analysis of successful or attempted attacks;
6. Assess if cybersecurity measures remain effective in light of new threats.

This regulation provides one of the most robust cybersecurity management systems offered by any entity thus far. Although the framework lacks depth, the fact that is has been included helps organisations who may have a weaker understanding of cybersecurity and its relevance to autonomous vehicles.

UN Regulation No. 156 - Software update and software update management system:

The second regulation applies to the approval of vehicles with regards to software update and management. The regulation is the first of its kind to govern OTA software and firmware updates [119]. Prior to selling vehicles on the market, manufacturers must fulfil several requirements pertaining to the software update management system; Software update delivery mechanisms must be protected and ensure integrity and authenticity [117], with software identification numbers being protected and readable from the vehicle. Furthermore, OTA updates should only be executed if the vehicle has sufficient power and the last stable version of vehicle software being used if OTA updates fail. Users should be aware of new updates, and alerts should be created if a mechanic is required. As with the previous regulation, a framework is provided if necessary, and helps manage software update risks, summarised by [117]:

1. Recording the hardware and software versions relevant to the vehicle type;
2. Identifying software relevant for approval;
3. Verifying that the software on a component is what it should be;
4. Identifying interdependencies, especially with regards to software updates;
5. Identifying vehicle targets and verifying their compatibility with an update;
6. Assessing if a software update affects the type approval or legally defined parameters (including adding or removing a function);
7. Assessing if an update affects safety or safe driving;
8. Informing vehicle owners of updates;
9. Documenting all the above.

Again, this regulation is one of the most complete and comprehensive with regards to software updates in vehicles. Although OTA updates provide convenience to the user, and help keep a vehicle's security up to date, there are many considerations and dangers with such update mechanisms. Thus, it is recommended that manufacturers outside of the UN look towards this regulation.

Both regulations take an important step towards considering the growing concerns with CAV cybersecurity and software management. While the regulations may be considered stringent, this is preferable to legislation that lack clarity or depth. OEMs who comply with both regulations will further improve the security of their entire organisation, their supply chain, and their end-products. Furthermore, while the regulations are only applicable to the UN, other countries have the opportunity to build on these. This means that less developed countries outside of the EU, or countries who are behind in the CAV field can quickly catch up with existing international legislation.

6.2 Principles

6.2.1 UK Gov. Key Principles of Vehicle Cyber Security for CAVs

The UK's Centre for Connected and Autonomous Vehicles (CCAV), the Centre for the Protection of National Infrastructure (CPNI) and the Department of Transport published the *'Key principles of vehicle cyber security for connected and automated vehicles'* in August 2017 [120]. The principles are intended for use throughout the automotive industry, CAV systems and their corresponding supply chains, and provides guidance throughout the whole life of the vehicle. While discussing the full extent to the principles is out of the scope of this report, the following outlines the principles, using extracts from [120]:

- *Intelligent Transport Systems (ITS) and CAV System Security Principles:*
  1. Organisational security is owned, governed and promoted at the board level.
  2. Security risks should be assessed and managed appropriately and proportionally including those specific to the supply chain.
  3. Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.
- *ITS/CAV System Design Principles:*
  4. All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.
  5. Systems are designed using a defence-in-depth approach.
  6. The security of all software is managed throughout its lifetime.
  7. The storage and transmission of data is secure and can be controlled.
  8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

Although the principles are not meant to be exhaustive, they provide a solid foundation for OEMs in the UK to improve their resilience to CAV cybersecuirty threats across the organisation and supply chain. However, the principles are offered at a high level only, and may already be evident to larger organisations who have have a strong grasp of cybersecurity responsibilities. Furthermore, the principles are not statutory, possibly alluding to the fact that CAV technologies are somewhat incompatible with strict governance, despite the aforementioned legislations.

6.2.2 ACEA Principles of Data Protection in Relation to CVs and Services

The European Automobile Manufactures Association (ACEA) published the *Principles of Data Protection in Relation to Connected Vehicles and Services* in September 2015 [121]. Their publication outline five high level principles for connected vehicles and services for affiliated companies within the EU. The principles are designed to supplement existing legislation governing data protection, i.e. GDPR. The principles are as follows [121]:

1. Transparency.
2. Give customers choice.
3. Always take data protection into account.
4. Maintain data security.
5. Process data in a proportionate manner.

Importantly, ACEA's principles support the notion that an OEM's control over in-vehicle personal data is fundamental in guaranteeing the safety, security and privacy for both connected vehicles and users [122]. However, while the document provides clear clarification over the different types of CV data and data protection requirements, there is little consideration for future uses of CV data, i.e. AI and machine learning.

6.2.3 SMMT's 2017 Position Paper Guidelines

The Society of Motor Manufacturers and Traders (SMMT) published their *Connected and Autonomous Vehicles Position Paper* in February 2017 [123]. They comment on the state of technical solutions for CAV cybersecurity, and considers the position that guidelines are the most appropriate measures for ensuring CAV cybersecurity without hindering development, as opposed to strict legislation. Thus, the paper supports the following guidelines [123]:

1. The protection of CAVs requires verifiable security measures based on existing security standards.
2. CAVs must be equipped with integrity protection measures.
3. Vehicle manufacturers and their suppliers must have appropriate measures in place to manage used cryptographic keys.
4. The integrity of internal communications between controllers within CAVs must be protected by authentication mechanisms.
5. Online services for remote access into CAVs must have strong mutual authentication and secure communication between involved entities.

The guidelines importantly offers valuable cybersecurity practices that are applicable to both OEMs and entities in the supply chain. Furthermore, SMMT suggests that the aforementioned guidelines should be expanded to include high-level principles on board-level governance [123], reinforcing principle 1 from Section 6.2.1.

Notably, the guidelines are the first to consider relevant existing standards, such as the ISO 2700 series, as being applicable to CAV technologies and systems. Supporting the adoption of applicable standards is an important step in acknowledging the convoluted nature of CAV security, and will further promote a comprehensive CAV cybersecurity management system.

6.3 Summary

While this section has not considered the full scope of CAV governance, the most applicable legislation and principles have been identified. From this, it is clear that the legislative landscape for CAVs is unclear, with a distinct lack of specifics, or comprehensive legislation. While legislators will not want to stifle innovation, we must ensure that the automotive industry does not abuse the lack of governance.

GDPR law and EDPB guidelines are perhaps the most applicable and important in the context of CAVs, and must be adhered to at all costs. However, there remains a lack of specifics and clarity within GDPR laws, and this presents several security and privacy concerns that the legislators and industry must address.

Thus, there is a requirement for the automotive industry and legislators to collaborate and share information in order to produce a new set of bespoke CAV laws that strikes a balance between innovation and security. There is however hope for CAV governance, as new developments and practises within the field being introduced at a steady pace.

7 Recommendations: Security and the Future of Connected and Autonomous Vehicles

7.1 Preamble

The findings presented thus far can now be used to provide high-level security recommendations intended for use by the automotive sector, the supply chain, legislators and users, in order to protect connected and autonomous vehicles from the cyberseucirty implications and vulnerabilities that threaten their future success.

While countermeasures have been provided for each of the attacks identified in Section 4*, and applicable legislation and principles have been critiqued, this section proposes important cybersecurity recommendations that can be used to secure CAV technologies, protect user data and privacy, and enhance existing legislation, both now, and in the future.

**The reader should refer back to the countermeasures identified in Section 4, and should view each as imperative low-level recommendations for vehicle and communication technologies.*

7.2 Recommendations: Vehicle and Communication Technologies

Control Access to Hardware, Firmware and Data:

CAV system designers should consider employing strict access controls on critical system resources such as firmware, hardware or data. Access controls mechanisms are necessary in ensuring that only authorised personnel can have access to the vehicle's systems, provided they have passed the appropriate authorisation and authentication protocols. For instance, access controls on the vehicle's local storage that requires multiple authentication mechanisms dramatically reduces the chances of an attacker gaining entry and modifying such data.

Furthermore, access controls can be used to provide accountability for actions performed on the vehicle's systems. Event logs are an effective mechanisms in ensuring accountability, as the vehicle will retain a detail record of the users who accessed a system, the duration and their actions. Likewise, event logs can provide a certain level of non-repudiation, as insider attacks on a vehicle's systems can be traced back to the malicious insider.

System designers should also consider adopting least privilege access control protocols. According to Saltzer and Schroeder [124], least privilege protocols ensures that every user of the system should operate using the least set of privileges necessary in order to complete their task. This approach limits the damage that can result from an error, and further limits the interactions between critical CAV systems to the absolute minimum while ensuring autonomous operation and security remains intact.

Systematic Security Validation for AI:

Borrowing from Enisa's AI cybersecurity report [26], CAV system designers should adopt systematic security validation mechanisms for AI models and the data which is collected and processed. The large volume of data that CAVs capture and process provide the foundations for the AI models which enables autonomous driving. However, the models are constantly changing, which can present potential security threats, as model updates can add vulnerabilities that can be exploited [26].

Therefore, system designers should ensure that the security of the model updates are systematically assessed and validated in order to keep the vehicle secure and operating as expected. Thus, monitoring and maintenance processes should be introduced that identify security vulnerabilities and rectify them before the AI system can be exploited. Furthermore, risk assessments and incident response procedures should be drafted and regularly carried, so that in the event of an attack, the vehicle or system designers can quickly react and neutralise the threat before the security and safety of the vehicle is compromised.

Network Segmentation:

As previously mentioned in Section 4.4.1, a straightforward methods for protecting in-vehicle networks such as the CAN bus, is to separate the network into multiple sub-networks. Bozdal et al. [94] notes that segmentation provides control over which entities or users can access the particular sub-networks, thus reducing the resulting damage form an attack.

Furthermore, network segmentation ensures that errors or attacks do not propagate onto other networks, as an attack on a node in the network will only spread to the specific sub-network in which it is located. This can be used to help protect safety critical systems, with attacks on Bluetooth not propagating to LiDAR sensors for example. Additionally, the security of the whole vehicle is improved, as it does not rely on a singular point of failure, and the attack surface is consequently segmented.

7.3 Recommendations: Automotive Industry

Cybersecurity Culture:

As discussed in Section 2.3, the automotive industry lacks the capability to handle or manage cybersecurity risks with vehicles. Couple with the fact that there is little in the way of a cyber-attack history, the automotive industry may have not recognised the importance of a strong cybersecurity culture that is originated from the board-level and is shared at the lower levels of the organisation. However, the industry must recognise the need for addressing cyberseucirty issues, and therefore, it is important to identify the elements that can be used in order to provide appropriate resources for a strong cybersecurity culture.

Firstly, automotive organisations should assign ownership and responsibility for security across the organisation and along the value chain [125], with the security culture being accepted and embodied by each individual, regardless of role. Furthermore, entities along the supply chain should embrace the culture that is emanated at the automotive manufacturer, and should develop practises that are complementary and can integrity with each entity.

Secondly, the organisation's cybersecurity culture should adopt and embrace software-centric approaches to managing cyber risks. While attacks often target the vehicle or the production process, many attacks occur as a result of employee negligence, i.e phishing attacks, impersonation etc, or insider threats. Such attacks have a better chance of being mitigated if employees are aware of the software protection systems in place.

Finally, a dedicated cybersecurity team should be formed that can provide expertise through the organisation. A dedicated team can manage and reinforce the cybersecuirty culture, and can dramatically improve the security awareness of staff. Furthermore, a cybersecurity team and provide regular and up-to-date training programs that reinforce the security culture and keep it relevant, thus improving the overall security of the organisation.

Information Sharing and Transparency:

Information is undoubtedly one of the more important and valuable assets for an automotive manufacturer [126]. Due to the rising threats of cyber attacks discussed, producing effective countermeasures against such attacks relies on high level collaboration and information sharing between a multitude of automotive industry members. Likewise, trust between industry members is needed to ensure such information sharing is effective, with organisations needing to realise the benefits. Thus, an appropriate level of transparency is needed, with organisations sharing their findings with regards to cybersecurity.

When information sharing is transparent, the industry as a whole benefits, with organisation collaboratively producing and developing stronger security mechanisms. For example, if Company A is subject to an previously unseen attack on a CAV's sensor, they can share an incident report with the rest of the industry, where Company B might come up with a strong technical solution and offer it up. While this is not advocating that organisation share all information and give away their competitive expertise, combined knowledge can help manage the cyber related risks the industry faces as a whole.

Therefore, the industry should look towards the National Institute of Standards and Technology's (NIST) *Guide to Cyber Threat Information Sharing* [127], and should adopt the following principles:

1. Establish sharing relationships.
2. Engage in ongoing communication.
3. Organise/store cyber threat information.
4. Produce and publish indicators.

Security Audits:

In addition to the aforementioned, the automotive industry should consider conducting security auditing that includes: risk assessments, penetration testing, and security control reviews. Firstly, the industry should adopt a risk-based approach for assessing vulnerabilities and impacts both within the organisation [128] and along the supply chain. Therefore, a risk assessment should be conducted that covers all aspects of the business and, and details the risks associated with the CAVs, including internal and external vehicle networks, ECU interfacing, sensing technologies and vehicle software.

Secondly, penetration testing on CAV software and organisational systems can determine the risk exposure, and will help to identify the vulnerabilities and attacks both within the vehicle and in the organisation. Both black-box and white-box penetration tests should be conducted, as information shared prior to conducting the tests can influence the results.

Finally, security control reviews can be used to critically assess the effectiveness of the design and mechanisms of the security management process. Typically, this involves an design effectiveness review and operating effectiveness testing [129], and can be used to measure a manufacturers security against another's. Furthermore, automotive manufacturers should strive to attain relevant certification such as the ISO 27000 series.

7.4 Recommendations: Data Protection and Privacy

Bespoke Data Protection and Privacy Laws for CAVs:

When considering the findings discussed in Section 5, it is evident that a lack of bespoke legislation with regards to data protection and privacy in CAVs leads to unique security implications and opportunities for the unethical and unlawful collection and distribution of user data. It was evidenced that personal data holds intrinsic value to both advertisers and criminals, who want to either monetise the data or use it for nefarious proposes. Therefore, there is a requirement from legislators and the automotive industry to collaborate and outline data protection and privacy laws and principles that govern the ways in which data is used, what types of data is collected and the length of which it is stored. Furthermore, legislators can enforce sanctions on excessive personal data collection.

New data protection laws will be instrumental in ensuring the control of personal data is given back to the users. As discussed, users often have limited opportunities for consent with regards to their data, a matter which is exacerbated with CAVs connecting and communicating with other nodes on a network without indication. Therefore, data protection laws based on consent, that also allows users to withdraw it, are imperative to the public acceptance and success of CAVs.

Finally, legislators should look to implement strict security measures and access controls over personal data. The EDPB highlights the importance of access controls on personal data with connected cars, especially when a vehicle is part of a vehicle-sharing scheme, or where multiple associated drivers and passengers have access to the same car [130]. Without appropriate data protection laws that address access controls, users can wrongly access, modify or misuse the personal data of others.

Data Protection by Design and Default:

Borrowing from article 25 of the GDPR, CAV systems must be designed with data protection and privacy by default. Taking into account the privacy considerations and implications of personal data produced and shared by CAVs, technologies should be designed so that the privacy of users and non-users is upheld. Thus, the following obligations of personal data protection from article 25 should be adhered to, and have been adapted for vehicular contexts:

1. *Article 25, section 1* - The data controller is required to implement data protection principles from the initial design and development stage of the vehicle's life cycle. This ensures privacy by design.

2. *Article 25, section 2* - The data controller implements appropriate technical and organisational measures for ensuring that, by default, only personal user data in vehicle which is necessary for each specific purpose is processed [131]. This ensure privacy by default.

While the GDPR only applies to the EU and European Economic Area, legislators and vehicle manufacturers form other political unions and countries should consider data protection by design and default, as data protection built form the ground up is likely to be more effective than adapting existing technologies and legislation to fit CAV data protection and privacy requirements.

Furthermore, this is an important step in ensuring that CAVs are compatible with existing and future personal privacy and data legislation on an international scale.

Local Personal Data Processing:

Where possible, personal data should be processed locally, i.e. using the vehicle's on board computational power, so as to avoid transferring sensitive data outside of the vehicle, and giving the users and non-users control over their data. Although one might question whether this is contradicting CAV functionality due to their reliance on external communication (V2X), it is actually a mechanisms to ensure that sensitive data is appropriately masked locally (pseudonyms, hash functions etc), before it is shared to other entities or nodes on the network.

Local processing limits the risks of impacts on privacy, and prohibits any data processing by entities without the user's knowledge [113]. Furthermore, it enables processing sensitive data such as biometric or data relating to criminal offences, a safeguard against the unlawful data processing mentioned in Section 5.2. In addition to more secure data protection, processing personal data in-vehicle involves a lower latency, making it suited to autonomous driving functions [113].

7.5 Recommendations: Legislation

Collaboration Between Legislators and the Automotive Industry:

As mentioned at various points throughout this report, in order to ensure that legislation supports the future prospects of CAVs without hindering innovation, legislators must work in collaboration with members of the automotive industry. As evidenced, CAV applications can be somewhat incompatible with existing legislation, and Tan and Taeilhag's research additionally demonstrates that "governments alone cannot address all of the intricate issues" [132] that concern such vehicles. Therefore, Legislators need to adopt a collaborative spirit and exercise stewardship to ensure that autonomous mobility succeeded, especially at the early stages of CAV adoption.

While collaboration is not always straightforward, there are examples however where such partnership has been mutually beneficial: the success of Singapore's AV implementation demonstrates the importance of collaboration between governments and the AV industry. KMPG's *'Autonomous Vehicles Readiness Index'* ranked Singapore as the most ready country for AVs in 2020 [133], with the rating reflecting Singapore's policy and legislation development's support and encouragement of AVs. The government demonstrated a collaborative spirit and appropriate stewardship, with going as far as to open one-tenth of its total road network for AV testing, and retraining one hundred bus drivers as safety operators [133].

Thus, international governments should look towards Singapore's experience with AV testing and developments, and should offer up similar schemes where CAV manufacturers can test and develop their vehicles with the same regulatory freedom and support. Furthermore, this collaboration allows for flexibility when implementing CAV legislation and ensures it is compatible with existing vehicular legislation.

Globally Consistent Approach to Legislation:

As demonstrated in Section 6.1, although there are several laws that are applicable to the various applications and technologies of CAVs within the European Union and the United Kingdom, there is an absence of globally consistent legislation. Legislatorial inconsistency could be a barrier to the use of CAVs across Europe and the rest of the world [134], as users may need to disable autonomous systems or communication channels when crossing into different countries. Naturally, along with causing inconvenience for the user, both the autonomous capabilities and the security of the vehicle will be dramatically reduced when in countries that have more restrictive legislation.

While new legislation relating autonomous and connected vehicles and technologies is at different stages of implementation [115, 117, 134], legislators must also work towards a shared timeline that introduces laws within a reasonable period of time to one another. Although this might prove challenging on a global scale, it is reasonable to suggest consistent implementation within political unions, where many laws are already shared. Furthermore, consistent legislation additionally supports innovation in the automotive sector, as vehicle and systems manufactures can better develop technologies and mechanisms when they are aware of the various global requirements on CAVs. Thus, global organisations, political unions, and international governments should attempt to collaborate on agreeable and consistent CAV legislation, and should share their findings with organisations and legislators both inside and outside of their jurisdiction.

Use of Simulation Testing:

Although a vehicle manufacturer obtain their most beneficial data from real-world testing of CAVs, legislators should require vehicles to have completed a considerable amount of hours travel within a simulated environment due to the safety concerns that surrounds autonomous mobility. The commercialisation of AVs slowed in the US after a pedestrian was struck and killed by a test AV form Uber in Arizona [135], and highlighted the importance for simulation testing of collision avoidance systems.

The industry should look towards technological leaders such as Waymo, who have created a 'simulation city' where they can test their AVs and prepare their vehicles for the challenges presented in the real-world. Waymo states that their 'CarCraft' simulation software has driven over five billion miles within their virtual environments [136]. The software can push the virtual car's limits, by introducing complicated scenarios and extreme weather conditions for example, and can measure and report on the vehicle's performance. While conditions like these would put pedestrian safety a risk within real-world testing environments, simulation is wholly safe.

Therefore, legislators can learn from simulator results and use these to better prepare and draft their laws. Furthermore, simulation testing is an important tool in the validation and approval process, as legislators will unearth their own findings on critical areas of public concern, such as vehicle security and pedestrian safety for example.

8 Conclusion

The primary purpose of this technical report was to identify and assess the security vulnerabilities, shortcomings and implications pertinent to the underlying technologies, data privacy, legislation and principles concerning connected and autonomous vehicles. The secondary purpose of this technical report was to utilise the findings and present several recommendations for the automotive sector, supply chain, legislators and users, to protect CAVs both today and in the future.

The motivation behind this report was fuelled by an absence in existing literature that considered CAVs as the product of not only their underlying technologies, but also the legislation that governs their operation, technology and use of data. Consequently, there was little in the way of exploration for the entire scope CAV security, a matter which needed to be addressed.

It was evidenced that there was little in the way of a practical cyber attack history on CAV technologies, however, this is by no means a testament to the security of the vehicle's technologies or systems. Importantly, OEMs should have an awareness of the susceptibilities in their systems.

As autonomous and communication technologies in personal vehicles are in their infancy relative to their lifetime, there has been little time for maturity, with many autonomous applications still within their first few iterations. Although a shift towards advanced vehicle technologies may well provide a multitude of socio-economic benefits, it has also brought forward the emergence of previously unseen cybersecurity threats and vulnerabilities that the automotive industry must address. Although documented that the automotive industry is capable of dealing with traditional security issues, such as car theft, the industry needs to adopt a new outlook on cybersecuirty and should be aware of the cyber threats it faces.

The security vulnerabilities on the sensing, communication and automotive control systems were assessed. The findings unearthed a considerable volume of both theoretical and practical attacks on the underlying technologies, each of which threatening the availability, integrity, confidentiality, and operation of CAVs. Such attacks further threaten the safety and security of vehicular operations. Therefore, OEMs, system designers and legislators should consider the use of core security service principles, cryptographic primitives, software defences and hardware solutions to mitigate against such attacks.

The substantial implications on data protection and privacy appeared to be a recurring theme throughout the research for this report. The automotive industry has much to gain from personal data, however the same rings true for advertisers and criminals, and their intentions are far from pure. Therefore, personal data is highly vulnerable, and is subject to misuse without appropriate safeguards or legislation. Furthermore, the industry should collaborate with legislators to ensure that personal data is strictly managed, with controls on collection, storage, use, and types of data being maintained. Thus, GDPR requirements should be adhered to by OEMs, and legislators should look to draft up new laws and principles that can be used by the industry to protect users and non-users.

In the same vein, the legislative landscape for CAVs must improve and adapt if high level autonomous transportation is to be accepted by consumers. Although no easy feat, legislators must ensure there are comprehensive cybersecurity laws that governs the design and operation of CAVs without hindering the development and innovation within the industry. While many countries are on the uptake with specific legislation, with the UK's Automated and Electric Vehicle Act 2018 being an example, there remains a lack of clarity or depth in such legislation, with the automotive industry left to fill in the gaps. Therefore, the most indisputable solution is for legislators, policy makers and governing bodies to work with players within the industry in order to strike a balance that is beneficial for each.

The next generation of connected and autonomous vehicle technologies will further revolutionise the vehicular transportation, with the ever increasing capabilities of AI and machine learning, and the introduction of even more advanced and complicated technologies. However, attackers will continue to adapt, and advance their ever-impressive competence, and thus, new attack surfaces, vulnerabilities and security implications will leave CAVs and their success in the hands of those who design, manage and govern them.

19,998 words.

Bibliography

[1] Marcello Tamietti and Matthew Kim. Autonomous vehicles: Plotting a route to the driverless future. Technical Report 171969, Accenture, Dublin, Ireland, 2017. Available at https://www.accenture.com/$_{a}cnmedia/pdf - 55/accenture - insight - mobility - iot - autonomous - vehicles.pdf$.

[2] Centre for Connected and Autonomousn Vehicles (CCAV). Innovation is great: Connected and autonomous vehicles. Technical report, UK Government Centre for Connected and Autonomousn Vehicles, 2020. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment$_{d}ata/file/929352/innovation - is - great - connected - and - automated - vehicles - booklet.pdf$.

[3] Dave Maunsell, Praveen Tanguturi, and Jame Hogarth. The new road to the future: Realising the benefits of autonmous vehicles in australia. Technical report, Accenture Digital, 2014.

[4] Ala Abu Alkheir, Moayad Aloqaily, and Hussein T. Mouftah. Connected and autonomous electric vehicles (caevs). *IT Professional*, 20(6):54–61, 2018.

[5] Warwick Goodall, Tiffany Dovey, Justine Bornstein, and Brett Bonthorn. The rise of mobility as a service: Reshaping how urbanites get around. Technical report, Deloitte University Press, September 2017.

[6] George C. Cromer, Orville C. Cromer, Christopher G. Foster, and Ken W. Pudry. History of the automobile, October 2020. Available at https://www.britannica.com/technology/automobile/Other-European-developments.

[7] Embitel Automotive and IoT Blog. Electronic control unit is at the core of all automotive innovations: Know how the story unfolded, July 2017. Available at https://www.embitel.com/blog/embedded-blog/automotive-control-units-development-innovations-mechanical-to-electronics.

[8] Robert N. Charette. This car runs on code, February 2009. Available at https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

[9] Gowling WLG and UKAutodrive. Connected and autonomous vehicles: A hacker's delight - cyber seucirty in the connected and autonomous vehicle industry. Whitepaper 3, Gowling WLG, September 2017. Research was conducted in collaboration with BizWord Ltd.

[10] Thorsten Luettel, Michael Himmelsbach, and Hans-Joachim Wuensche. Autonomous ground vehicles—concepts and a path to the future. *Proceedings of the IEEE*, 100(Special Centennial Issue):1831–1839, 2012.

[11] Juliet Flavell. Connected and autonomous vehicle innovation: Approaches to navigating the hazards. Technical report, RHUL-ISG-2020-1 (Information Security Group Royal Holloway University of London), June 2020. Research was conducted by BizWord Ltd (www.bizword.co.uk), an independent business consultancy.

[12] The Society of Automotive Engineers. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. standard, Society of Automotive Engineers, Warrendale, Pennsylvania, United States, April 2021. Available at "https://www.sae.org/standards/content/j3016$_2$02104/.

[13] Amrita Ghosal and Mauro Conti. Security issues and challenges in v2x: A survey. *Computer Networks*, 169:107093, 2020.

[14] Jiaqi Huang, Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Recent advances and challenges in security and privacy for v2x communications. *IEEE Open Journal of Vehicular Technology*, 1:244–266, 2020.

[15] Keith Martin. *Everyday Cryptography: Fundamental Principles Applications.* Oxford University Press, 2nd edition, June 2017.

[16] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang. Cyber security challenges and solutions for v2x communications: A survey. *Computer Networks*, 151:52–67, 2019.

[17] Chunyong Yin, Jinwen Xi, Ruxia Sun, and Jin Wang. Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3628–3636, 2018.

[18] The Gale Group. West's Encyclopedia of American Law, edition 2. Principle, 2008.

[19] British Ecological Society. An introduction to policy in the uk. *POLICY GUIDE*, 0:1–4, May 2017. Available at: "https://www.britishecologicalsociety.org/wp-content/uploads/2017/05/An-introduction-to-policymaking-in-the-UK.pdf".

[20] Council of European Union. Article 289(3) of the treaty on the functioning of the european union, June 2016.
`https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A12016E289`.

[21] Erik Stayton and Jack Stilgoe. It's time to rethink levels of automation for self-driving vehicles [opinion]. *IEEE Technology and Society Magazine*, 39(3):13–19, 2020.

[22] Rodrigo Gandia, Fabio Antonialli, Bruna Cavazza, Arthur Neto, Danilo Lima, Joel Sugano, Isabelle Nicolaï, and Andre Zambalde. Autonomous vehicles: scientometric and bibliometric review. *Transport Reviews*, 0:1–20, 09 2018.

[23] D. Milakis, N. Thomopoulos, and B. van Wee. *Policy Implications of Autonomous Vehicles.* ISSN. Elsevier Science, 2020.

[24] Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle. The race for cybersecurity: Protecting the connected car in the era of new regulation. *McKinsey Center for Future Mobility*, 0:1–7, October 2019.

[25] European Commission. Connected and automated mobility. *Policies*, June 2021.

[26] Georgia Dede, Rossen Naydenov, Apostolos Malatras, Ronan Hamon, Henrik Junklewitz, and Ignacio Sanchez. Cyberseucirty challenges in the uptake of artificial intelligence in autonomous driving. Technical Report 1, European Union Agency for Cybersecurity (ENISA) and Joint Research centre (JRC), Luxembourg, 2021.

[27] Sean Campbell, Niall O' Mahony, Lenka Krpalkova, Daniel Riordan, Joseph Walsh, Aidan Murphy, and Conor Ryan. Sensor technology in autonomous vehicles : A review. pages 1–4, 06 2018.

[28] Santiago Royo and Maria Ballesta-Garcia. An overview of lidar imaging systems for autonomous vehicles. *Applied Sciences*, 9:4093, 09 2019.

[29] Michaela Jamelska. Radar vs. lidar sensors in automotive industry, August 2017. Available at https://mse238blog.stanford.edu/2017/08/mj2017/radar-vs-lidar-sensors-in-automotive-industry/.

[30] German Sharabok. Why tesla won't use lidar: And which technology is ideal for self-driving cars, September 2020. Available at https://towardsdatascience.com/why-tesla-wont-use-lidar-57c325ae2ed5.

[31] Gaurav Pandey, James R McBride, and Ryan M Eustice. Ford campus vision and lidar data set. *The International Journal of Robotics Research*, 30(13):1543–1552, 2011.

[32] David Darwall. Lidar vs radar for applied autonomy. Available at https://semcon.com/offerings/applied-autonomy/lidar-vs-radar-for-applied-autonomy/.

[33] Enoch R. Yeh, Junil Choi, Nuria G. Prelcic, Chandra R. Bhat, and Jr. Robert W. Heath. Cybersecurity challenges and pathways in the context of connected vehicle systems. Technical Report D-STOP/2017/134, Data-Supported Transportation Operations Planning Center (D-STOP): The University of Texas at Austin, Austin, Texas, United States, February 2018.

[34] Nicola Bates. Driverless vehicle security: Considering potential attacks and countermeasures for military applications. Technical report, RHUL-ISG-2020-1 (Information Security Group Royal Holloway University of London), Egham, United Kingdom, June 2020.

[35] Katie Burke. How does a self-driving car see? camera, radar and lidar sensors give autonomous vehicles superhuman vision., April 2019. Available at https://blogs.nvidia.com/blog/2019/04/15/how-does-a-self-driving-car-see/.

[36] Chen Yan, Wenyuan Xu, and Jianhao Lie. Can you trust autonomous vehicles: Contactless attacks agasint sensors of self-driving vehicle. Technical report, Zhejian University and University of South Carolina, 2016.

[37] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6):5015–5029, 2018.

[38] Wan Rahiman and Zafariq Zainal. An overview of development gps navigation for autonomous car. In *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)*, pages 1112–1118, 2013.

[39] Automotive Training Center. The science behind car gps systems: What is gps and how does it work in cars, December 2016. Available at https://autotraining.edu/science-behind-car-gps-systems/.

[40] Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach.* Prentice Hall, 3 edition, 2010.

[41] IHS Markit. Artificial intelligence driving autonomous vehicle development. January 2020. Available at: "https://ihsmarkit.com/research-analysis/artificial-intelligence-driving-autonomous-vehicle-development.html".

[42] Na Liu, Alexandros Nikitas, and Simon Parkinson. Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour*, 75:66–86, 2020.

[43] Sivaram Alukuru Trikutam. Driving the connected car revolution, May 2019. available at https://www.cypress.com/blog/corporate/driving-connected-car-revolution.

[44] Christoph Sommer and Falko Dressler. *Vehicular Networking.* Cambridge University Press, 2014.

[45] Charles McLellan. What is v2x communication? creating connectivity for the autonomous car era, November 2019. available at https://www.zdnet.com/article/what-is-v2x-communication-creating-connectivity-for-the-autonomous-car-era/.

[46] Thales Group. V2x: What is vehicle to everything?, June 2021. available at https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/automotive/use-cases/v2x.

[47] Mohammad Kawser, Syed Sajjad, Saymon Fahad, Sakib Ahmed, and Hasib Rafi. The perspective of vehicle-to-everything (v2x) communication towards 5g. 19:146–155, 04 2019.

[48] NHTSA. Vehicle-to-vehicle communication. Technical report, United States Department of Transportation - National Highway Traffic Safety Administration, United States, 2021.

[49] United States Government Accountability Office. Intelligent transportation systems: Vehicle-to- infrastructure technologies expected to offer benefits, but deployment challenges exist. Report to Congressional Requesters GAO-15-775, United States Government Accountability Office, Washington, D.C, United States, September 2015.

[50] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. *IACR Cryptology ePrint Archive*, 2010:332, 01 2010.

[51] Tao Yang, Lingbo Kong, Wei Xin, Jianbin Hu, and Zhong Chen. Resisting relay attacks on vehicular passive keyless entry and start systems. In *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, pages 2232–2236, 2012.

[52] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and I.K. Jennions. Evaluation of can bus security challenges. *Sensors*, 20:16–17, 04 2020.

[53] Mehmet Bozdal, Mohammad Samie, and Ian Jennison. A survery on can bus protocol: Attacks, challenges, and potential solutions. Technical report, IVHM Centre, Cranfield University, Cranfield University, Bedford, United Kindom, August 2018.

[54] National Institute of Standards and Technology. Developing cyber resilient systems: A systems security engineering approach. Technical Report NIST Special Publication 800-160 Volume 2, U.S. Department of Commerce, Washington, D.C., November 2019.

[55] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, 18:1–18, 03 2017.

[56] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 2267–2281, New York, NY, USA, 2019. Association for Computing Machinery.

[57] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, pages 445–467, Cham, 2017. Springer International Publishing.

[58] J. Petit, Bas Stottelaar, and M. Feiri. Remote attacks on automated vehicles sensors : Experiments on camera and lidar. 2015.

[59] Mark Harris. Researcher hacks self-driving car sensors,, September 2015. Available at https://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors.

[60] Bas G.B. Stottelaar. Practical cyber-attacks on autonomous vehicles. Master Thesis Version: 2123ddc, Faculty of Electrical Engineering, Mathematics and Computer Science Services, Cybersecurity and Security Research Group, May 2015. Available at http://essay.utwente.nl/66766/.

[61] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, 18:1–18, 03 2017.

[62] Jianhao Liu, Chen Yan, and Wenyuan Xu. Can you trust autonomous vehicles : Contactless attacks against sensors of self-driving vehicle, 2016. available at https://www.semanticscholar.org/paper/Can-You-Trust-Autonomous-Vehicles-%3A-Contactless-of-Yan/a618dcb13ec42900209e7aa3f88490b587631e13?sort=relevance.

[63] Fabian Roos, Jonathan Bechter, Christina Knill, Benedikt Schweizer, and Christian Waldschmidt. Radar sensors for autonomous driving: Modulation schemes and interference mitigation. *IEEE Microwave Magazine*, 20:58–72, 09 2019.

[64] Gyeong-Hoon Lee, Jeil Jo, and Cheong Park. Jamming prediction for radar signals using machine learning methods. *Security and Communication Networks*, 2020:1–9, 01 2020.

[65] Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity attacks in vehicular sensors. *IEEE Sensors Journal*, 20(22):13752–13767, 2020.

[66] Bing Shun Lim, Sye Loong Keoh, and Vrizlynn L. L. Thing. Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 231–236, 2018.

[67] Todd Humphreys. Statement on the vulnerabilities of civil unmanned aerial vehicles and other systems to civil gps spoofing. Technical Report D-STOP/2017/134, The University of Texas at Austin, Austin, Texas, United States, July 2012. Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security.

[68] Nils Ole Tippenhauer, Christina Pöpper, Kasper Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. pages 75–86, 10 2011.

[69] Minh Pham and Kaiqi Xiong. A survey on security attacks and defense techniques for connected and autonomous vehicles. *ArXiv*, abs/2007.08041, 2020.

[70] Sashank Narain, Aanjhan Ranganathan, and G. Noubir. Security of gps/ins based on-road location tracking systems. *2019 IEEE Symposium on Security and Privacy (SP)*, pages 587–601, 2019.

[71] Kexiong (Curtis) Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang. All your GPS are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1527–1544, Baltimore, MD, August 2018. USENIX Association.

[72] Jonathan Petit and Steven Shladover. Potential cyberattacks on automated vehicles. *Intelligent Transportation Systems, IEEE Transactions on*, PP:1–11, 09 2014.

[73] R.A. Raja Mahmood and A.I. Khan. A survey on detecting black hole attack in aodv-based mobile ad hoc networks. In *2007 International Symposium on High Capacity Optical Networks and Enabling Technologies*, pages 1–6, 2007.

[74] Peyman Kabiri and Aghaei Mehran. Feature analysis for intrusion detection in mobile ad-hoc networks. *International Journal of Network Security*, 12, 01 2011.

[75] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. *Int. J. Netw. Secur.*, 5:338–346, 2007.

[76] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1545–1562, Baltimore, MD, August 2018. USENIX Association.

[77] Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, and Kazuo Sakiyama. Sensor confusion: Defeating kalman filter in signal injection attack. pages 511–524, 05 2018.

[78] Nata˘sa Trkulja, David Starobinski, and Randall A. Berry. Denial-of-service attacks on c-v2x networks. Technical report, ECE Department Boston University and ECE Department Northwestern University, October 2020. Available at: ”https://arxiv.org/pdf/2010.13725.pdf”.

[79] Pandi Vijayakumar, Mohammad S. Obaidat, Maria Azees, SK Hafizul Islam, and Neeraj Kumar. Efficient and secure anonymous authentication with location privacy for iot-based wbans. *IEEE Transactions on Industrial Informatics*, 16(4):2603–2611, 2020.

[80] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 23:100214, 2020.

[81] Jonathan Petit and Steven E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, 2015.

[82] Tesla North Ameirca. Model 3 owner's manual software version: 2021.12.25, July 2021. Available at https://www.tesla.com/sites/default/files/model$_{3o}wners_{m}anual_{n}orth_{a}merica_{e}n.pdf$.

[83] Cabell Hodge, Konrad Hauck, Shivam Gupta, and Jesse Bennet. Vehicle cybersecurity threats and mitigation approaches. Technical report, National Renewable Energy Laboratory, 08 2019. Available at: https://www.nrel.gov/docs/fy19osti/74247.pdf.

[84] Daniel Regalado. Zingbox identifies new cybersecurity threat for cars and drivers at defcon 26. Technical report, National Renewable Enegergy Laboratory, August 2018. Available at: https://www.businesswire.com/news/home/20180809005216/en/Zingbox-Identifies-New-Cybersecurity-Threat-for-Cars-and-Drivers-at-DefCon-26.

[85] Lin Tong and Chen Luhai. Common attacks against car infotainment systems, July 20219. Available at https://events19.linuxfoundation.org/wp-content/uploads/2018/07/ALS19-Common-Attacks-Against-Car-Infotainment-Systems.pdf.

[86] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, H. Shacham, S. Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011.

[87] Cyware and Privacy4Cars. Carblues vehicle flaw found affecting miullions of vehicles worldwide, November 2018. Available at https://cyware.com/news/carsblues-vehicle-flaw-found-affecting-millions-of-vehicles-worldwide-ed357394.

[88] Tencent Keen Security Lab. New vehicle security research by keenlabn: Experimental security assessment of bmw cars. Technical report, Tencent Keen Secueity Lab, May 2018. Available at: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/.

[89] Madeline Cheah, Siraj A. Shaikh, Olivier Haas, and Alastair Ruddle. Towards a systematic security evaluation of the automotive bluetooth interface. *Vehicular Communications*, 9:8–18, 2017.

[90] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers Security*, 103:102150, 2021.

[91] Emad Aliwa, O. Rana, Charith Perera, and P. Burnap. Cyberattacks and countermeasures for in-vehicle networks. *ACM Computing Surveys (CSUR)*, 54:1 – 37, 2021.

[92] Chung-Wei Lin and A. Sangiovanni-Vincentelli. Cyber-security for the controller area network (can) communication protocol. *2012 International Conference on Cyber Security*, pages 1–7, 2012.

[93] Wei Si, David Starobinski, and Moshe Laifenfeld. Protocol-compliant dos attacks on can: Demonstration and mitigation. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pages 1–7, 2016.

[94] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and I.K. Jennions. Evaluation of can bus security challenges. *Sensors*, 20:16–17, 04 2020.

[95] Pallavi Kalyanasundaram, Venkatesh Kareti, Meghana Sambranikar, Narendra Kumar SS, and Priti Ranadive. Practical approaches for detecting dos attacks on can network. In *WCX World Congress Experience*. SAE International, apr 2018.

[96] Mirco Marchetti and Dario Stabili. Anomaly detection of can bus messages through analysis of id sequences. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 1577–1583, 2017.

[97] Kazuki Iehira, Hiroyuki Inoue, and Kenji Ishida. Spoofing attack using bus-off attacks against a specific ecu of the can bus. In *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–4, 2018.

[98] Wufei Wu, Renfa Li, Guoqi Xie, Jiyao An, Yang Bai, Jia Zhou, and Keqin Li. A survey of intrusion detection for in-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(3):919–933, 2020.

[99] Sen Nie, Ling Liu, and Yuefeng Du. Free-fall: Hacking tesla from wireless to can bus, June 2017. Available at https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

[100] Gildas Avoine, Ioana Boureanu, David Gérault, Gerhard P. Hancke, Pascal Lafourcade, and Cristina Onete. *From Relay Attacks to Distance-Bounding Protocols*, pages 113–130. Springer International Publishing, Cham, 2021.

[101] Ioannis Krontiris, Kalliroi Grammenou, Kalliopi Terzidou, Marina Zacharopoulou, Marina Tsikintikou, Foteini Baladima, Chrysi Sakellari, and Konstantinos Kaouras. Autonomous vehicles: Data protection and ethical considerations. In *Computer Science in Cars Symposium*, CSCS '20, New York, NY, USA, 2020. Association for Computing Machinery.

[102] Anne-Gabrielle Haie. Europe: New privacy rules for connected vehicles in europe? *Privacy Matters DLA Piper's Global Privacy and Data Protection Resource*, May 2020.

[103] Dorothy J Glancy. Privacy in autonomous vehicles. *Santa Clara L. Rev.*, 52:1171, 2012.

[104] Leon Nash, Greg Boehmer, Mark Wireman, and Allen Hillaker. Securing the future of mobility : Addressing cyber risk in self-driving cars and beyond. Technical report, Deloitte University Press, 207. Available at https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf.

[105] James M Anderson, Kalra Nidhi, Karlyn D Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A Oluwatola. *Autonomous vehicle technology: A guide for policymakers.* Rand Corporation, 2014.

[106] Lisa Collingwood. Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law*, 26(1):32–45, 2017.

[107] Hazel Si Min Lim and Araz Taeihagh. Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, 11(5), 2018.

[108] Information Commissioner's Office (ICO). The information commissioner's office (ico) response to the joint consultation from the law commission and scottish law commission entitled 'automated vehicles: Consultation paper 3 – a regulatory framework for automated vehicles', March 2021.

[109] Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 357–375, Santa Clara, CA, July 2017. USENIX Association.

[110] Vít Gabrhel, Stanislav Ježek, and Darina Havlíčková. Public opinion on connected and automated vehicles: the czech context. *Transactions on Transport Sciences*, 10:42–52, 01 2020.

[111] Trix Mulder and Nynke E Vellinga. Exploring data protection challenges of automated driving. *Computer Law Security Review*, 40:105530, 2021.

[112] European Commision. What is the European Data Protection Board (EDPB)?, 2018.

[113] European Data Protection Board. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, January 2020.

[114] Louise Butcher and Tim Edmonds. Automated and electric vehicles act 2018. Technical report, House of Commons Library, August 2018. Available at: "https://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf".

[115] Stewarts, Lucie Clinch, and Julian Chamberlayne. The unanswered questions following the automated and electric vehicle act 2018. *Personal Injury*, October 2018. Available at: "https://www.stewartslaw.com/news/unanswered-questions-following-automated-electric-vehicles-act-2018/".

[116] Baroness Sugg. Automated and electric vehicle bill. volume 791: Debated on wednesday 9 may 2018, May 2018. Available at: "https://hansard.parliament.uk/lords/2018-05-09/debates/E1642C10-22AA-4356-995D-7087BB7817DA/AutomatedAndElectricVehiclesBill".

[117] United Nations Economic Commission for Europe. Un regulations on cybersecurity and software updates to pave the way for mass roll out of connected vehicles. June 2020. Available at: "https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll".

[118] The Wall Street Journal. U.n. rules require cybersecurity guarantees for connected cars. July 2020. Available at: "https://www.wsj.com/articles/u-n-rules-require-cybersecurity-guarantees-for-connected-cars-11594287001".

[119] CLEPA European Association of Automotive Suppliers. Three landmark un vehicle regulations enter into force. February 2021. Available at: "https://clepa.eu/mediaroom/three-landmark-un-vehicle-regulations-enter-into-force/".

[120] Centre for Connected and Department for Transport Autonomous Vehicles (CCAV), Centre for the Protection of National Infrastructure (CPNI). The key principles of vehicle cyber security for connected and automated vehicles. August 2017.

[121] European Automobile Manufacturers Association. Acea principles of data protection in relation to connected vehicles and services. September 2015.

[122] Alexandra Campmas, Nadina Iacob, Felice Simonelli, and Hien Vu. Big data and b2b platforms: the next big opportunity for europe. *Annex III. Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector*, pages 1–82, 2018.

[123] Society of Motor Manufacturers and Traders. Connected and autonomous vehicles. *Position Paper*, pages 1–46, February 2017.

[124] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems, 1975.

[125] Automotive World. Automakers must champion cyber security, July 2021. Available at: https://www.automotiveworld.com/articles/automakers-must-champion-cyber-security/.

[126] Konstantinos Rantos, Arnolnt Spyros, Alexandros Papanikolaou, Antonios Kritsas, Christos Ilioudis, and Vasilios Katos. Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*, 9(1), 2020.

[127] National Institute of Standards and Technology. Guide to cyber threat information sharing. *NIST Special Publication 800-150*, 2016.

[128] Naitonal Highway Traffic Safety Administration. Cybersecurity best practices for modern vehicles. *Report No. DOT HS 812 333*, 2016.

[129] Royal Holloway University of London and Chris Mitchell. Iy5501-202021 course material - unit 6: Audit, July 2020. Seucrity Management.

[130] European Data Protection Board. Techdispatch 3: Connected cars, December 2019.

[131] European Parliament and Council of the European Union. art. 25 gdpr data protection by design and by default, 2018. Available at: https://gdpr-info.eu/art-25-gdpr/.

[132] Si Ying Tan and Araz Taeihagh. Adaptive governance of autonomous vehicles: Accelerating the adoption of disruptive technologies in singapore. *Government Information Quarterly*, 38(2):101546, 2021.

[133] KPMG International Limited. 2020 autonomous vehicles readiness index. Technical report, KMPG, 2020. Available at https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehicles-readiness-index.pdf.

[134] Ben Gardner and Dr. Stephan Appt. Driverless cars and mobility: time to shape future regulation, 2020. Available at: https://www.pinsentmasons.com/out-law/analysis/driverless-cars-mobility-future-regulation.

[135] Federation of American Scientists. Issues in autonomous vehicle testing and deployment. Technical Report Updated April 23, 2021, Congressional Research Service, 2021. Available at https://fas.org/sgp/crs/misc/R45985.pdf.

[136] Andrew J. Hawkins. Welcome to simulation city, the virtual world where waymo tests its autonomous vehicles, June 2021. Available at: https://www.theverge.com/2021/7/6/22565448/waymo-simulation-city-autonomous-vehicle-testing-virtual.