View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Huddersfield Repository

University of Huddersfield Repository

Parkinson, Simon, Ward, Paul, Wilson, Kyle M. and Miller, Jonathan

Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges

Original Citation

Parkinson, Simon, Ward, Paul, Wilson, Kyle M. and Miller, Jonathan (2017) Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems. pp. 1-18. ISSN 1524-9050

This version is available at http://eprints.hud.ac.uk/31446/

The University Repository is a digital collection of the research output of the University, available on Open Access. Copyright and Moral Rights for the items on this site are retained by the individual author and/or other copyright owners. Users may access full items free of charge; copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational or not-for-profit purposes without prior permission or charge, provided:

- The authors, title and full bibliographic details is credited in any copy;
- A hyperlink and/or URL is included for the original metadata page; and
- The content is not changed in any way.

For more information, including our policy and submission procedure, please contact the Repository Team at: E.mailbox@hud.ac.uk.

http://eprints.hud.ac.uk/

Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges

Simon Parkinson*, Paul Ward†, Kyle Wilson†, Jonathan Miller*
*Department of Informatics, University of Huddersfield, UK
†Department of Psychology, University of Huddersfield, UK

***Abstract*—Vehicles are currently being developed and sold with increasing levels of connectivity and automation. As with all networked computing devices, increased connectivity often results in a heightened risk of a cyber security attack. Furthermore, increased automation exacerbates any risk by increasing the opportunities for the adversary to implement a successful attack. In this paper, a large volume of publicly accessible literature is reviewed and compartmentalised based on the vulnerabilities identified and mitigation techniques developed. This review highlighted that the majority of research is reactive and vulnerabilities are often discovered by friendly adversaries (white-hat hackers). Many gaps in the knowledge base were identified. Priority should be given to address these knowledge gaps to minimise future cyber security risks in the connected and autonomous vehicle sector.**

I. Introduction

Connected and Autonomous Vehicles (CAVs) incorporate many different technologies to enable driver-less, safe, and efficient transportation. Connection mechanisms support communication between vehicles and infrastructure, sharing of data such as position, and speed of movement, etc [1]. Each of these connectivity functions supports subsequent automation, which transforms the driver's role from actor to monitor by reassigning functions previously performed by humans to technology. Automation is achieved using sensor technology to survey the environment, along with some predetermined knowledge, to plan vehicle activity [2].

The development and commercial release of Connected and Autonomous Vehicles (CAVs) is largely driven by the desire to produce quicker, more reliable and safer vehicles and and more robust and resilient transportation infrastructure. Developing increasingly autonomous and connected vehicles inevitably requires an increase in computing resources. However, as with all connected computing infrastructures, increasing the level of computational functionality and connectivity increases the exposure of potential vulnerabilities, which can increase the likelihood of future attacks.

Considerable research effort is being invested in identifying vulnerabilities, recommending potential mitigation techniques, as well as highlighting the potential impacts of a vehicle and related infrastructure becoming compromised [3], [4], [5], [6], [7]. The extant research has identified vulnerabilities associated with different sensors, controls, and connection mechanisms and detailed vulnerabilities in technology that is currently "on the market", as well as in proposed technology.

Although there is an abundance of detailed and focused technical research, there is an absence of research utilising literature available in the public domain to suggest significant gaps and challenges facing the CAV sector. This paper identified that vulnerabilities are typically being identified and mitigated in a reactive manner and there are many sizeable challenges facing the CAV research community, including manufacturers. The aim of the present research was to review the research on CAV related cyber security vulnerabilities and mitigation techniques, provide an overview of past and current research efforts, and to collate this research in to key areas of activity. The aim of this paper is to identify knowledge gaps that can subsequently be used to motivate a future a roadmap to addressing the cyber security related challenges.

The paper is structured as follows: the following section provides and in-depth analysis of publicly available literature to identify cyber security related knowledge gaps. Following this a summary table is then provided to allow the reader to easily assess the current knowledge gaps and their significance. The paper provides little suggestion of how these knowledge gaps might be resolved, rather it leaves them as open questions for the CAV community.

II. Literature Survey

In this section, we provide a comprehensive review of literature and categorization of the associated cyber threats. Several factors motivated the approach taken in this research and its subsequent organization:

1) The technology on which CAV systems are based is still developing. This technology is yet to be subject to significant, and often financially, motivated adversarial pressures [8]. Rather than to inform specific practice or policy, the primary catalysing factor for identifying vulnerabilities is academic research [4], [3], [7], as well as the desire to improve safety of the technology [9]. A few cases have been reported where adversaries have exploited a relatively low-tech vulnerability [10], [5]. However, there is a lack of evidence that wide-spread attacks are currently taking place with the intent of maximum disruption and damage. As automation and communication technologies become increasingly common in vehicles, an increased interest in discovering vulnerabilities is likely as vehicular cybercrime becomes financially motivated.
2) The nature of the supply chain means that a range of technologies (hardware, software, and infrastructure) are utilised without thoroughly understanding the security implications [11], [12], [13]. For example, an

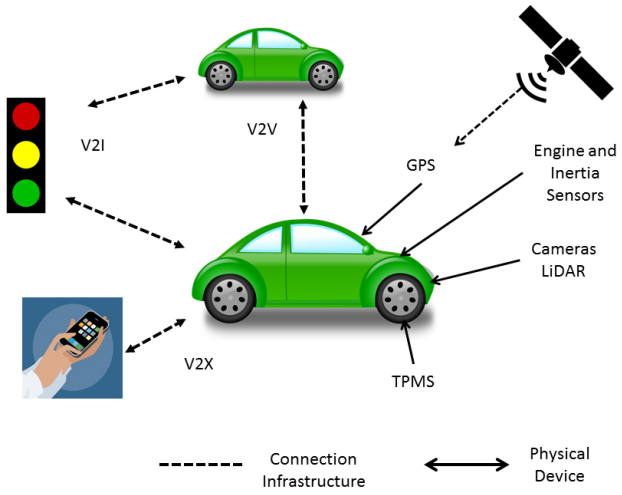

Fig. 1. Overview of the categorised groups of research

electronic chip used in one of the control units may have a vulnerability which is not known by the control unit manufacturer. This may result in the exposure of vulnerabilities that are unknown to the manufacturer but are an 'easy win' for an adversary.

3) In a similar manner to supply chains in the manufacturing sector, vehicle manufacturers outsources much of their activity, including the design and development of components and systems [11], [12]. For example, the development of an electronic control unit used to control another manufacturer's hardware. This leads to a situation where manufacturers are working in isolation and are often only working to contract. It is therefore likely that they will not add additional security measures beyond those specified in the contract. It is also possible that some manufacturers may not have a copy of the source code for a control unit used in their vehicles, thus preventing them from performing additional auditing.

The wealth of literature examined in this paper motivates the categorisation presented in this paper. Figure 1 presents a graphical illustration of the categorisation to aid the reader. In Figure 1, the different infrastructures and technologies reviewed in this paper are summarised. This includes the Vehicle 2 Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to X (V2X), where X is any internet-enabled device. Furthermore, many sensor devices are illustrated, such as Global Position Systems (GPS), Tyre Pressure Monitoring Systems (TPMS), etc. The reader can find an explanation for each term within this paper. It should be noted that due to the large volumes of research in this discipline, it is likely that some research efforts will have been missed. However, due to the cited publication venues, it can be assumed that the majority of significant research has been acknowledged.

A. Vehicle

In this section, a review of cyber security vulnerabilities and mitigation efforts limited to those originating from and affecting the physical vehicle is presented. Those resulting from connection mechanisms and infrastructure are discussed later.

1) Low-level Sensors: CAVs require the use of many sensors to detect information in the surrounding environment, categorise information according to some predetermined or learned criteria, and make predictions about potential vehicle activity. The type, functionality and use of a sensor determines the extent to which it could contribute to scoping out cyber threats, as well as the extent to which it could inform potential implications should it be compromised. The below subsections summarises the most common sensor mechanisms in CAVs [14], [15], and provides information on recent vulnerabilities and mitigation efforts.

Differential Global Positioning Systems (GPS)) provide absolute position data with a one-meter level of accuracy. However, this is a problematic challenge since there are many reported difficulties with the GPS infrastructure and the way in which the technology is affected by obstruction. These limitations are often overcome with the use of an increased number of satellites [16] to provide better coverage. In the public domain GPS is an open standard which is freely-accessible; however, military GPS systems use encrypted signals. The use of GPS is popular, but due to the transparent architecture, rogue signals can easily be generated to mislead or block the GPS device (herein called spoofing and jamming) [17]. GPS spoofing is quite a complex procedure and involves broadcasting incorrect yet realistic and valid GPS signals to mislead GPS receivers. For example, a spoofing attack would begin by broadcasting signals synchronised with genuine signals observed by the target receiver. The power of the counterfeit signals is then increased and the position is gradually modified away from the target. GPS devices are often programmed to utilise the strongest signal as in an ideal world this is likely to be more reliable. In principle this sounds relatively simple; however, the necessary hardware requirements to generate realistic signals make it a challenging procedure.

The generation of simplistic plug-and-play attack devices will become reality as the potential rewards of GPS spoofing are increased. Comprehensive theory of how to perform GPS spoofing attacks is already in the public domain. For example, literature has been published detailing how to perform a successful attack [18]. Currently, however, only examples of "proof-of-concept style attacks can be found in literature. For example, in 2013 students from the University of Texas demonstrated how they could generate counterfeit GPS signals which would gradually overpower authentic GPS signals, resulting in the deviation of a superyacht's course. The superyacht's control then reacted to the changing GPS signals by reporting location discrepancies to the crew who then initiated correction by setting a new course [19]. Figure 2 illustrates that in a GPS spoofing attack, it is only necessary for the attacker to overpower the authentic GPS signals.

The hardware involved in the above attack was developed by Humphreys et al., and by their own admission, is the only GPS spoof reported in open literature which is capable of precisely generating counterfeit GPS signals [20]. Using GPS for criminal activity such as being able to redirect vehicles

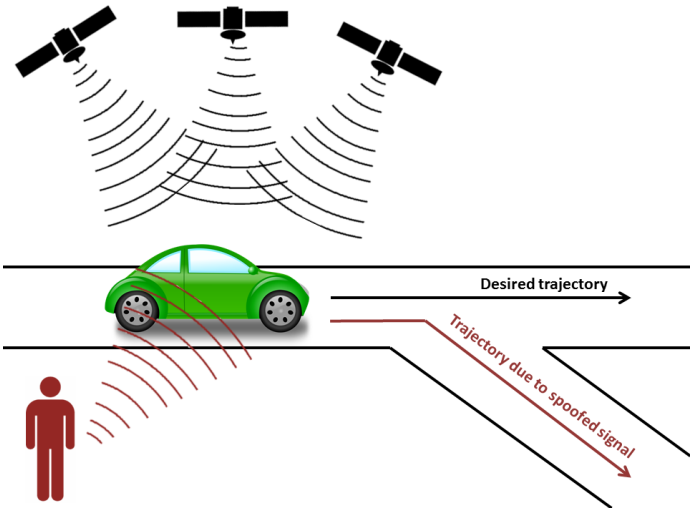

Fig. 2. Illustration of a GPS spoofing attack

of high-value or those transporting goods for theft or wide-scale disruption will be desirable. Research efforts to develop GPS spoofing countermeasures have been taking place since GPS was developed as open-standard technology. There are many simple validation mechanisms that can be put in place to prevent spoofing. For example monitoring identification codes, satellite signals, and the use of time intervals can help detect spoofing attempts. Warner et al. [21] detail how the observed signal strength would be expected to be around –163 decibel watts. A GPS simulator, such as that developed by Humphreys et al. would provide a signal strength many orders of magnitude larger than any possible satellite at the Earth's surface. In addition, GPS signals can be monitored to ensure that their relative change is within a threshold. Warner et al. also discuss the potential of monitoring the GPS signal to check that its strength does vary as expected and is not too perfect. However, if the sophistication of the attack is sufficient to appear genuine, these validation checks will fail and the GPS device will be spoofed. It is widely believed that nothing short of a cryptographic, military-grade implementation will stop spoofing [21]. This view is shared by Humphreys in the context of CAVs [22].

The jamming of GPS is a more primitive and simplistic attack. In comparison with spoofing, jamming only requires that enough radio noise on the GPS frequency (1575.42 MHz) is transmitted to prevent authentic signals from being distinguishable by the GPS receiver. Although illegal to use, GPS jamming devices are readily available. Such devices can be used to ensure that a vehicle's tracking device cannot determine its location through GPS. Executing this attack on CAVs has the potential to disable a vehicle's navigation mechanism, which would be a large inconvenience for the driver and would disable any autonomous navigation capabilities utilising GPS. There is also the possibility of using secondary measurement systems to aid in preventing both spoofing and jamming attacks. However, this does rely on the different positioning system using a different frequency which is not also been attacked. Other measurements are in existence which could be used as a secondary source. For example Russian Federation's GLONASS, China's BeiDou, the European Union's Galileo, and India's NAVIC [23]. However, as their transmission mechanisms are fundamentally the same and just use different frequencies, the use of a secondary satellite navigation system would only prevent against jamming attacks if the attacker did not transmit on the different frequencies. The use of multiple measurement systems for spoofing attacks is much more significant as the attacker would be required to spoof multiple systems which inevitably increases the complexity of the attack.

Knowledge Gap 1: *Although theoretical and controlled experiments have demonstrated the potential to exploit GPS technology to affect a vehicle's autonomous navigation (i.e., see superyacht example), the potential implications of such an attack on CAVs and the ease with which an attack may be executed are not clear.*

Inertial measurement units units are used to provide velocity, acceleration, and orientation data using a combination of accelerometers and gyroscopes. These sensors monitor the dynamics of the environment and provide the vehicle with necessary information. For example, gyroscopes and inclination sensors can determine a change in road gradient and adjust vehicle speed accordingly to maintain safe operation. These systems provide low-level feedback inputs to the control system, which can initiate significant change in the vehicle's behaviour. There is an absence of comprehensive research and literature on the possible exploits of these sensors; however, it is realistic to state that intentionally compromising the sensor to simulate false, yet realistic data will cause the control systems to react. It can be foreseen that compromising a primitive sensor might result in a severe compromise of the vehicle's functionality. For example, simulating that the vehicle is currently on a steep gradient may force the vehicle to travel at very low speeds and make it unusable. This would be classed as a form of Denial of Service (DoS).

Such attacks would most likely require physical access to the sensor to interfere with its readings, or alternatively to intercept communication between the sensor and a control unit. Such communication could be transmitted using a physical cable or through a close proximity wireless connection method. Sensor readings will be validated by a control unit to ensure that it is within tolerance and as expected. However, providing the attacker knows the range of this tolerance, they can ensure that the behaviour of the vehicle is adjusted without causing the Engine Control Unit (ECU) to enter a safe mode. An attack of this nature may have an impact beyond the compromised vehicle. For instance, in the previous example where an inclination sensor is compromised, the resulting slow movement of the compromised vehicle (because the system assumes it is on a steep gradient) will cause delay to other vehicles using the same network.

An attack of this nature will most likely require a thorough understanding of how the sensors are communicating with the ECUs. However, tools such as CarShark can be used to observe traffic on existing networks, such as a Controller Area Network

(CAN) bus system. Research Performed by Karl Koscher et al. demonstrated this utility on a CAN bus network using CarShark. Their work involved performing a detailed packet analysis and modification of packets – simulating a man-in-the middle attack on the CAN network – and observing the effect on the vehicle. Although this research involved testing two modern vehicles with no autonomous functionality, they were able to modify a sensor's value through changing packet data. This resulted in, for example, the ability to falsify speedometer readings while travelling at speed [4].

Certain mitigation mechanisms can be implemented to prevent a low-level attack. The first is through using encrypted communication on the vehicle's communication network. This can ensure that counterfeit signals cannot be easily injected onto the network. The second is through rigorous monitoring of the signals behaviour to ensure that it is within range and is behaving normally. The third is through the use of additional sensors to provide a secondary source of measurement. For example, the use of GPS and mapping data can help determine if the vehicle is currently located on a steep gradient.

Engine control sensors are used to acquire data to regulate engine activity. This includes sensors such as; temperature, air flow, exhaust gas, and engine knock and are all used to acquire performance data which is used to adjust engine conditions. For example, air-flow is used to adjust the amount of fuel required by the engine to achieve the desired output. These sensors have been used on vehicles long before the introduction of levels of automation and connectivity between vehicles. However, as vehicles become connected to a wider networked infrastructure, the sensors become susceptible to outside attacks. Furthermore, data generated by such sensors now have influence beyond the generating vehicle. These sensors are connected to an internal network, such as the CAN [24], [25]. Fortunately, such sensors often require physical access to the vehicle to attack [3]. However, as connectivity increases, care needs to be taken to ensure that these primitive sensors are not vulnerable.

In work presented earlier (inertia measurement section), Koscher et al. [4] demonstrated that packets distributed on an internal network can be modified leading to change in vehicle behaviour. This involves modifying both packets related to Engine Management Module (EMM) inputs and outputs. As discussed in their research, such activity can cause poor vehicle performance and even physical damage. In their research, physical access was required to the vehicle to modify packets on the CAN network. However, research presented in this paper demonstrates how an attacker can inject packets on to a CAN network through remote exploits.

Koscher et al. describe the surprise and ease of generating such unsafe operating conditions with the simple process of modifying and introducing rogue data packets. This raises significant concerns over the security of the critical infrastructure. Mitigation of this vulnerability requires the implementation of a cryptographic solution to ensure data integrity and its authenticity. For example, recent research presents [26] the use of an asymmetric cryptographic using the Advanced Encryption Standard (AES) for ECU authentication and stream authorisation. ECU authentication is performed against a central security module by using stream authentication where every message stream is authorised and the asymmetric keys for stream access are distributed to ECUs. This research makes it computationally infeasible to modify or inject data packets. A challenge of implementing a real-time cryptographic solution is the overhead of extra computation and data transfer time. Although the researcher do not inform of the exact incurred delay, they do report that the "impact of our approach is small". This research demonstrates good potential; however, it is yet to be absorbed and utilised in new vehicles.

Tyre-pressure Monitor Systems (TPMS) are 'direct' small devices that are located on the valve of each tyre and frequently update the vehicle's control system with tyre specific information. This sensor is small and possesses a primitive function relative to the complexity of the entire vehicle; however, recent attention and privacy concerns warrant its discussion in this paper. It is of concern that a sensor with a primitive function can have such consequences on the vehicle and the driver. In the United States it became a legal requirement for all vehicles to be equipped with a TPMS from 2007 [27], and 2012 in Europe [28]. Some manufacturers have also created an algorithm-based 'indirect' monitoring solution to identify a sudden change in tyre pressure. These solutions look for a sudden change in the radius of the wheel by monitoring the circumference, i.e., the distance covered by one revolution of the wheel. There is debate amongst the most reliable and suitable solution as there are many conditions that can create false-positives, such as a rapidly wearing tyre or a significant change in air temperature resulting in an increase or reduction in air pressure and wheel circumference.

Direct TPMS devices operate by transmitting data to one of the vehicle's control units on general purpose (i.e., 315, 443 and 866 MHz) frequencies using either Frequency Shift Keying (FSK) or Amplitude Shift Keying (ASK) to prevent spoofing. However, Ishtiaq Rouf et al. demonstrate that the signals can be identified and modified using packet sniffing techniques at a range of 40m [29]. Literature also informs that security provisions can be reverse engineered, such as the work presented by Checkoway et al. [3], [30], who developed specialist equipment and software to perform this attack. Rouf et al. suggest that asymmetric encryption can be used as a potential mitigation technique [29]. However, researchers have identified that the use of encryption would induce the consumption of more power [31], thus reducing battery life and requiring the device to be replaced more frequently. The researchers considered changing different algorithms on different packet sizes but this always resulted in increased power consumption, suggesting a clear trade-off between security, functionality, and energy efficiency.

The implications of a TPMS-based attack would result in incorrect information being presented to the driver. This could either be to simulate a false change in tyre pressure, or to hide a true reduction in tyre pressure. Either way, the core function of the TPMS is to inform the driver of a flat

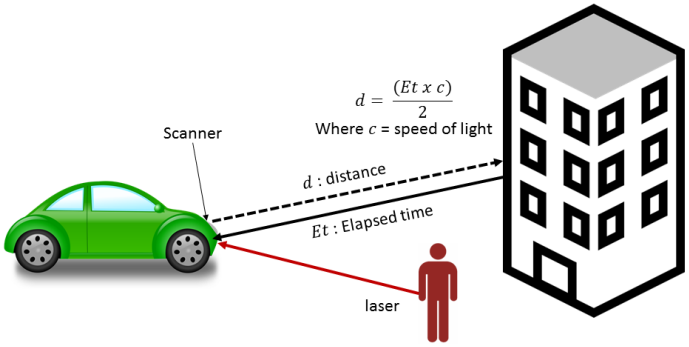

Fig. 3. Illustration of a LiDAR system

tyre. How the user reacts to this information could cause further problems. Based on the research presented by Rouf et al. [29], there is no reason to believe that the tyre pressure is currently used in any vehicle decision system. However, this is still a significant concern to public safety as drivers in receipt of falsified messages may be caused to initiate a dangerous reaction. Hiding a valid tyre pressure warning message may result in the driver missing the opportunity to bring the vehicle to a safe and controlled stop.

Knowledge Gap 2: *Attacks have been reported that are localised to a primitive and often single function sensor. Such attacks are able to compromise a vehicle's control systems or display false-positive data to the driver which both result in unexpected output. However, the full extent of which sensors might be compromised and their effect on a vehicle's function is not known.*

Light detection and Ranging (LiDAR) sensors are used to generate a map of the vehicles environment for localisation, obstacle avoidance, and navigation. LiDAR is a surveying technology that measures distance through measuring the time of flight of a pulse of light to determine the distance between the sensor and an object. Figure 3 is provided as a visual aid as well to aid the understanding of vulnerabilities with LiDAR. This technology is capable of quickly producing 3D maps of the environment, making it possible to develop a computational model of the 3D environment. This can be used for object recognition, trajectory planning **??**, etc.

This technology has been shown to be a viable aid in autonomous vehicles; however, as there is no guarantee over the validity of the constructed 3D model, it opens the potential for spoofing, deceiving and jamming with low cost hardware. Work conducted by Stottelaart et al. demonstrates the potential for jamming LiDAR by directly emitting light back at the scanner unit which is of the same frequency as the laser reflecting on the target [6]. A similar attack has recently been performed by researchers from the University of Cork [32]. However, what is interesting is that in their research, not only do they manage to compromise a LiDAR laser using low-cost hardware (raspberry Pi and a low-power laser), but they also manage to make the vehicle's control unit assume that there is a large object in front of the vehicle and force it to stop. Furthermore, they also demonstrate the potential to overwhelm the LiDAR sensor preventing the vehicle from moving.

Mitigation techniques exist which involve utilising different wave lengths to try and reduce the potential for jamming and spoofing attacks involving off-the-shelf laser devices and increase the required hardware to perform the attack [6]. Other mechanisms discussed by Stottelaart et al. include the use of vehicle-to-vehicle communication to collaboratively share measurements. However, this has the potential for a compromised measurement to be used beyond the compromised vehicle. Another, and arguably more feasible solution, is to implement random probing. This involves the device frequently changing the interval between scanning speeds to make it difficult for the attacker to synchronise their laser to the correct frequency.

Cameras (stereo- or mono-vision) and infrared systems are used in CAVs to provide static and dynamic obstacle detection, object recognition, and 360 degree information when fused with other sensors. The difference between mono- and stereo-vision systems is the number of cameras which are used. Mono-vision systems need additional support from other sensors to improve accuracy in determining aspects such as depth [33]. Stereo systems use an overlapping region of two cameras to help determine depth. Cameras are often fused with other sensors on CAVs. For example, the Google Driverless Car fuses LiDAR with stereo-vision and Enhanced Maps (Emaps) for road scenery understanding [34]. There are many other applications of cameras in CAVs such as lane detection [35], [36], traffic sign recognition [37], headlight detection [38], etc. The research highlights complex image analysis techniques to identify objects of interest. For example, planning a path through an identified lane requires detailed mathematical modelling, as demonstrated by Yue Wang et al. [36]. Cameras typically contain a Charge-Coupled Device (CCD) or Complementary Metal Oxide Semiconductor (CMOS) sensor which can be partially disabled from a 3-metre distance through using a low-powered laser [39], such as a Class 2 laser found in a CD player [40]. Another potential attack demonstrated by Stottelaart et al. can be taken against auto exposure [6] where sensitivity and exposure is reduced when extra light is introduced. The extra light could be from a high powered torch or a vehicle's headlights. This has the potential to hide information such as traffic signs, road edges and pedestrians.

According to an MIT Technology Review, the Google Driver-less Car is susceptible to this problem where low sunlight is able to blind the vehicle's cameras [41]. The recent tragic events of Tesla clearly illustrates the significance of this problem where neither the car nor the driver identified a white commercial trailer against the brightly lit sky [42]. This raises the concern of whether shining high-powered lights at a CAV may introduce safety concerns. Furthermore, given the uncertainty of the environment, perhaps it is possible for a natural event to occur which creates light conditions suitable to disrupt camera systems.

An adversary could easily perform an attack of this nature by directing a bright light at a vehicle. Compact, high-powered

lights are readily available which have potential to blind a vehicle's cameras. It is also worth noting that an intense light source might be accidentally reflected towards a vehicle. For example, a vehicle or building with a particularly reflective and concave surface might provide sufficient focussing of the sun to disable a vehicle's cameras. An example of this can be found with at 20 Fenchurch St. London which was nicknamed "walkie scorchie" and had been known to melt car paint and parts [43]. The potential implications of an attack of this nature are large. Disabling a vehicle's vision system could result in the vehicle not detecting a physical obstruction. This would be a localised incident; however, natural conditions may cause a wide-spread problem resulting in many localised incidents.

Different mitigation mechanisms have been discussed in literature. For example, the introduction of more cameras, as well as locating them at different strategic points on the vehicle, will make it challenging for an attacker and a natural event to affect them all. For example, the autonomous vehicle developed by Paolo Grisleri at VisLab, Italy [44] integrates 10 cameras located in many different positions alongside the use of 5 lasers. This increased use of sensors allows for a more complete and reliable representation of the perceived environment. Another potential mechanism is through the use of camera filters to remove laser light and to prevent from blinding. Researchers have also discussed the potential for a camera to automatically determine when to try different filters to improve quality [6].

Knowledge Gap 3: *It has been repeatedly reported how technologies used to sense the physical environment can be compromised, and that mitigation techniques often involve utilising a secondary source for redundancy. However, it is not clear what is the best approach to take to reduce the residual risk. For example, should multiple vision systems be used, or should sensors utilising different technology groups be used?*

2) Vehicle Control Modules: All modern vehicles use Engine Control Units (ECU) to control functionality of the vehicle through acquisition, processing, and control of electronic signals. In the previous section, vulnerabilities originating from sensors and their impact upon the system were discussed. In this section, the potential vulnerabilities directly targeting and affecting a vehicle's ECUs are discussed. This is important as CAVs involve a greater number of ECUs (compared to non-CAVs) due to the higher volume of sensors and devices to autonomously control and maintain connected functionality. ECUs are loosely categorised into the following categories (modified from [45]):

- Powertrain – the brain of the ECU. Controls more than 100 factors. Handles charging systems, transmissions, emissions, and control with control modules.
- Safety systems - Collision avoidance, airbag deployment, and active braking.
- Body control - electric windows, mirrors, AC, immobiliser, and locking.
- Data communications data communication between different components, Bluetooth, phone, and Dedicated Short Range Communications (DSRC).

ECUs are typically connected through the following two mechanisms:

1) CAN buses – Controller Area Network [25] is a serial communication protocol which efficiently supports distributed real-time control. The philosophy behind CAN is to achieve compatibility between two CAN implementations.
2) FlexRay [46] is an automotive network communication protocol developed to be faster and more reliable than CAN. However, its high cost has resulted in its implementation in high-end luxury cars only (e.g., BMW X5).

In CAVs there are a number of key ECUs. The below list (not exhaustive) provides a level of importance in descending order [15].

1) Navigation control module (NCM)
2) Engine control module (ECM)
3) Electronic brake control module (EBCM)
4) Transmission control module (TCM)
5) Telematics module with remote commanding
6) Body control module (BCM)
7) Inflatable restraint module (IRM)
8) Vehicle vision system (VVS)
9) Remote door lock receiver
10) Heating, ventilation, and air conditioning (HVAC)
11) Instrument panel module
12) Radio and entertainment centre

Due to the volume of control modules and microprocessors, a CAV can have around 100 million lines of code across 50-70 ECUs [47], [48]. Many researchers have quoted this fact, including those of Carnegie Mellon University, USA [48]. As the number of lines of code grows it becomes infeasible to perform careful code reviews to evaluate the potential security implications. This results in a high probability of unknown vulnerabilities. To put this in to perspective, Microsoft's Windows 7 has around 40 million lines of code [48] and since release there has been the discovery of many significant vulnerabilities. Many vulnerabilities have been identified within the ECU types mentioned above. These vulnerabilities often involve the attacker compromising part of the vehicle's control mechanism. There are many different mechanisms of compromising a control unit. This might result from compromising a vehicle's sensor network or exploiting the control module directly through different levels of connectivity (physical, remote, etc.). Those attacks presented in the previous section (Vehicle sensors) involve falsifying sensor data to cause a desired impact on an ECU. Although there is a large overlap between compromising a sensor and an ECU, this section will focus on the potential impacts on the ECUs.

The navigation control module (NCM) is viewed as important in CAVs [15] as they acquire information from a variety of sensors that are used to detect the environment (GPS, cameras, infrared, etc.) and then select a suitable navigation plan. This module has a high level of control over how the vehicle will navigate to a given location, and if compromised, the vehicle could be commanded to drive to an unintended location. For example, researchers from the University of

Virginia demonstrated that a vehicle's GPS navigation module can be compromised and has initiated a research project to develop inexpensive mitigation solutions [49]. Attacks of this nature have great implications for public safety and it is necessary to implement systems to prevent, detect and mitigate the compromise of navigation control. For example, efforts have been made to develop mechanisms of continuing to navigate without satellite positioning data, for instance, due to temporary loss [50]. Likewise, efforts have been made to counter a Denial of Service (DoS) attack by using a self-contained inertia measurement system. The potential implications of such an attack have already been discussed in earlier sections. Such systems use gyroscopes and accelerometers and are used to track position relative to a known starting location. From a control module's perspective, utilising an increased array of sensors can provide mechanisms to validate and monitor for the exploitation of other sensors.

Many features of CAVs require the complex interaction between multiple ECUs (ECU coupling) [4]. For example, modern vehicles have Electronic Stability Control (ESC) systems that monitor numerous parameters, such as individual wheel speed, throttle position, steering angle, etc. The ESC automatically modulates engine speed and wheel speed through braking and differential control to counteract the effect of dynamic forces on the vehicle's stability. Coupled systems like ESC demonstrate that compromising a single ECU has the potential to exploit large control functionality of the vehicle. In the case of ESC, compromising the ECU responsible for acquiring and processing wheel speed has the potential to impact upon the EBCM module and could cause incorrect braking, as described by researchers at the University of Washington [49]. In their research, CarShark was used to modify data packets transmitted by ECUs to compromise another ECU that caused great impact on the vehicle's functionality. For example, sending falsified packets from the ECM to the EBCM regarding wheel speed can cause the EBCM to apply the brakes. This has the potential to render the vehicle not fit-for-purpose or cause sporadic behaviour, which could be dangerous for the general public.

The potential severity of compromising an ECU is often a driving force for the discovery of vulnerabilities. A recent article published at the 2014 USA Black Hat conference by C. Miller et al. provides a comprehensive guide of vulnerabilities that exist in many popular vehicles in the US [51]. Researchers from National Computing Centre (NCC), Manchester have demonstrated that it is possible to compromise ECUs that control core braking functionality [52] by exploiting the on-board Digital Audio Broadcasting (DAB) radio and injecting packets onto the CAN network. This is a remote exploit utilising the connection infrastructure (discussed later), but it demonstrates the potential for the EBCM module to be compromised. This could have significant implications for public safety and necessary mitigation is required to ensure that critical ECUs cannot be compromised. Researchers at Yokohama National University, Japan, surveyed the use of intrusion detection systems (based on statistical analysis), the use of Message Authentication Codes (MAC), and cryptographies solutions in research literature. The most robust solution is the use of asymmetric encryption; however, considerable development is needed to implement a robust solution.

Knowledge Gap 4: *There are many research works demonstrating the potential to compromise ECU functionality through inputs from sensors and other ECUs. The severity of implication is often high as it is possible to cause the ECU to perform dangerous operations (i.e disabling brakes, etc). There is insufficient literature detailing comprehensive vulnerabilities of this nature as well as suggesting reliable mitigation techniques.*

Other exploits have involved targeting control modules to overwrite firmware to change vehicular behaviour. For example, researchers from the University of California have demonstrated how in some cases there are no security provisions from stopping an attacker uploading new firmware [3]. Changing ECU firmware has large implications as it can completely reprogram the vehicle's behaviour, resulting in it becoming a potential threat to public safety. The firmware could be modified or replaced by performing a physical and valid update via the On-Board Diagnostics (OBD) port. In principle this is a relatively easy procedure to perform; however, the use of asymmetric cryptographic (public-private key) architecture to ensure that the firmware came from a genuine source can mitigate this vulnerability, as discussed by NXP, The Netherlands [3].

It is inevitable that frequent updates will be required to the large code basis in order to rectify both functional and security flaws. The current mechanism of performing ECU software updates through physical communication with the control unit is predicted to be unfeasible due to the anticipated high numbers of CAVs. Researchers have proposed the use of remote updates through wireless technology [53], [54], [55]. Such techniques require the use of cryptography to prevent the update mechanism becoming compromised. These systems are recognised as providing a strong solution for distributing the firmware updates [56]. However, the potential for firmware updates being replaced at source with malicious code and allowed to freely propagate through the infrastructure has severe implications for security and safety, and could cause significant damage.

Zhang et al. from Cisco Systems, New Jersey, USA, discuss the potential ways in which attackers could compromise a vehicle's security keys to modify the ECU software, and the significant threat posed by malware to the vehicle's control system [57]. They highlight many potential mechanisms to infect malware, such as through the on-board diagnostic port, embedded web browsers, media players and removable ports. Once the adversary has defeated the security procedure, or discovered a method of exploitation, these authors suggest that the malware can be easily installed and very difficult to identify amongst the high quantities of ECU code. Researchers from Cisco Systems presents the use of cloud-based security architecture for defending against malware. Although this architecture is currently fictional, researchers believe there is credibility in the development of such a system.

Furthermore, it is currently the case that companies are offering aftermarket ECU programming modifications (in particular ECM) to increase driveability, power output, and fuel efficiency. Such aftermarket modification is controversial as the ECU software is proprietary and copyrighted to the manufacturer, making it technically illegal for a third party to make code modifications to an ECU. The caveat is that it often voids any manufacturer's warranty and also runs the risk of reducing life expectancy and reliability of the vehicle. However, this does not stop the hobbyist or car-tuning companies from making modifications. Uploading modified firmware by a trusted organisation also creates the potential for malware to be installed on the ECU.

Knowledge Gap 5: *Although there is a wealth of literature out there focussing on the different components of implementing a secure mechanism to remotely update vehicle software, there is uncertainty and an absence of a consensus regarding how proposed techniques would be implemented and what residual risk would remain.*

B. Human Aspects

Other large networks of connected and autonomous devices (e.g., manufacturing) are facing cyber vulnerabilities of similar significance to CAVs. Due to the number of vehicles on the road, it is likely that the vehicle network will be the largest of autonomous systems in existence. The number of cyber threats resulting from or affecting users in many other domains is often reduced as the users are already operating within, and have specialised expertise in, a controlled environment. For example, manufacturing machines are operated within a manufacturing facility, and although being connected to external networks, they have limited interaction with the physical world outside of their domain. Furthermore, humans interacting with such machines are often technologically competent and understand the implications of their work. This is different in the vehicle sector as vehicles as well as their drivers are operating in an open environment where they may have little expertise with the associated technology, resulting in a heightened cyber risk. This has potential to make them easy prey for attackers as the likelihood of them inadvertently compromising a vehicle through an attack (e.g. phishing) is heightened.

1) Privacy: Many individuals identify themselves psychologically with the vehicle by the way they drive through power choices, control use, etc [47]. The range of different ways in which different individuals will interact with CAVs is still relatively undetermined, and it is unclear what data will be generated from human integration with vehicles. Superficially, assuming the level of automation is not adaptive, there is a zero-sum relationship in the way humans are expected to interact with CAVs. The greater the autonomy of the vehicle, the less autonomy is available for the driver-changing the role of humans from active drivers to monitors. However, this is assuming a binary relationship between the driver and vehicle rather than human-supervised automation [58]. Although it is not clear what personal data will be generated, what value it will have, or what role it will play in future (i.e., adaptive and intelligent) automation systems, it is clear that in a connected environment all possible mechanisms must be taken to preserve privacy.

Data such as a vehicle's location has potential to be of significant value. For example, determining a vehicle's location over a prolonged period provides the opportunity for predetermined theft. More significantly, the vehicle's location is also linked to the driver's location and is of significant privacy concern. For example, the driver could be stalked for theft and advertisement reasons. Determining whether the user has just visited a cash machine and/or has been shopping in an expensive store provides the opportunity for targeted theft. Research undertaken at the Universitat Rovira i Virgili, Spain, details that, in addition, vehicle sensors (video camera, etc.) could be compromised to threaten the driver's privacy [59]. From a non-criminal perspective, tracking a user's location (even anonymously) provides the potential to further track individual behaviour [59] for tasks such as shopping. It may be possible to determine competition and behavioural habits which can further improve suppliers' services. For example, a fast food outlet would no doubt be interested in knowing their customer's location both before and after visiting their premises. A hypothetical example may be determining that at 10AM on Saturday morning 80% of their customers who visit at 11AM are at children football clubs. Such knowledge would have significant value and it is currently unclear who would own such data (i.e., individual vs. infrastructure provider) and have legal rights to sell.

In order to protect individual privacy, data should be robustly anonymised, strongly encrypted, and securely protected to avoid being vulnerable. The exposure of personal data would be extremely damaging for all organisations involved, and therefore the appropriate design of CAVs and the connected infrastructure must be taken to minimise risks. There is a wealth of literature on implementing and suggesting modifications to the Vehicular Ad Hoc Network (VANETs) to ensure privacy preserving techniques are embedded. For example, using the Public Key Infrastructure (PKI) to implement mechanisms of establishing trust and preventing malicious data acquisition [59]. Researchers have recently developed algorithms to implement cryptographic authentication mechanisms to ensure that trust can be maintained when data is broadcasted between vehicles (V2V) and between vehicles and infrastructure (V2I). Furthermore, through the use of encryption, their techniques are able to demonstrate that data transmitted into the public domain is safe if intercepted. Researchers at the Nokia Research Centre are also addressing issues surrounding the release of location information to make it impossible to compute the actual vehicle location should it be intercepted [60]. This research proposes the use of virtual trip lines to determine at what point vehicle's location should be broadcast. The principal idea here is that a vehicle's GPS location is not continually broadcast, rather it will send an updated position once it crosses a line segment in geographic space. There are other vulnerabilities which have detrimental effects on the driver's privacy. For example, the previously discussed exploitation of a vehicle's tyre pressure monitoring system [29] has potential

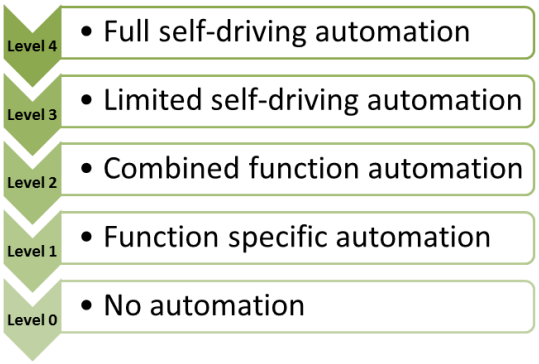

Fig. 4. Automation levels in CAVs

to invade the driver's privacy by invoking fake warning signals, which could cause annoyance and torment.

Knowledge Gap 6: *It is largely unclear what personal data will be generated and stored within a vehicle's software systems. Furthermore, it is also unclear who would own the data, what potential risks there are, how the data can be adequately be protected, and who is responsible for its security.*

2) Behavioural Aspects: It is widely acknowledged that public citizens have reservations over the safety and reliability of CAVs. This coincides with different levels of automation as the public's concern over reliability and safety often increases as the automation level increases. The different levels of automation range from level 0 where the computer offers no assistance to level 4 where the computer does everything ignoring the human [58]. Figure 4 provides a grapical illustration of each level. These reservations are often heightened through negative events and media releases. For example, the recent technical issue with a Tesla vehicle which resulted in the loss of life [28]. To try to understand and improve public perception of CAVs, researchers have performed detailed surveys and research [61], [62]. These works have focussed on understanding acceptance of the core functionality and how humans will interact with CAVs throughout different automation levels. However, one area that is less explored is the extent of human involvement in cyber aspects.

For example, mechanisms can be employed to detect malicious attacks. However, it is less clear how to deal with a non-technical human operator who is being compromised by a malicious user. This raises the following interesting, and largely unanswered questions:

1) Can the vehicle enter a safe mode to ensure operator's safety?
2) How human users should be informed of the situation, and how much control should the operator be given? I.e. what level of automation should be enforced during a detected cyber-attack.
3) Are there mechanisms that can collect sensory and other diagnostic information integrated into a single decision-making process in order to flag a suspicious or potentially harmful situation?

The vehicle's control systems may be able to detect potentially damaging system activity by monitoring on the signal level. Like many other safety-critical systems, vehicles implement runtime monitoring techniques to ensure that internal variables – used to represent sensor data and control parameters – are not allowed to go beyond some predefined safe working range. The use of safety limits in safety-critical ECUs has recently been discussed [63]; however, such safety limits work well in the management of engine functionality, but imposing them on sensors working in a vastly changing dynamic environment can be challenging.

Furthermore, variables often need to be monitored in conjunction because their relationship can often be used as a secondary source of validation. For example, both GPS and wheel speed sensors can be used to determine speed. GPS will be less accurate due to positioning limitations, but it is sufficient to determine if the wheel speed sensors are reliable. The procedure for when a variable goes out-of-range is to enter some kind of safe mode where vehicle speed is significantly reduced, allowing the driver to bring the vehicle to a controlled stop. These techniques work well; however, due to the increased connectivity and presence of cyber threats, it is not clear whether checking mechanisms are sufficient or if they can be easily bypassed.

In 2015, Chris Urmson, the director of the Google Self-Driving Cars project stated that if "software detected an anomaly somewhere in the system that could have possible safety implications; in these cases it immediately handed control of the vehicle to our test driver" [64]. He added that of 69 incidents detected, there would have been no way of knowing the seriousness of incidents if no intervention had been taken. These incidents included those in which a vehicle was unable to plan a safe sequence of moves to navigate in tight spaces. However, there was no evidence that any of these incidents were related to cyber-attacks. This is an area that is relatively unexplored and there is an absence of literature informing on how vehicle safety measures can intervene and prevent cyber-attacks. Due to the volume of literature on attacking and compromising vehicles, it would appear that there is an absence of any cyber-specific control mechanisms and safe-mode.

In the case of the Google driverless car, the test drivers are all educated to a sufficient standard of the technology and what to do should control be handed back to the driver. However, this might be challenging for drivers with lower technical ability and ignores the safety implications associated with mode errors (I.e., not knowing or not being able to infer the status of the system when control is handed back to the human after a period of automation) that typify this situation [65]. Furthermore, if a cyber-attack was detected and it was established that control should be given to the driver, it would be important for the vehicle to inform the driver of the current situation in a suitable way to mitigate any potential mode error and allow the user to make informed, timely, and safe decisions.

Knowledge Gap 7: *There is a lack of research detailing how the vehicle or driver may react to detecting a potential*

cyber attack. Will the vehicle have a safe mode which the vehicle can enter to ensure that a safe level of control can be maintained? Furthermore, if the vehicle was to detect that it had been compromised, how would it pass control back to the driver with enough information for the driver to quickly make sense of the situation?

C. Connection Infrastructure

In order for vehicles to communicate with the driver, other cars, and the road, they need to utilise many different communication technologies. Three broad classifications of communication mechanisms exist in the literature. These are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and the "Cloud".

V2V communication provides the mechanism for vehicles to communicate with each other in a peer-to-peer mechanism, I.e., no client/server architecture is required. The system uses the unlicensed 5.9GHz band range, known as the IEEE 802.11. This wireless range frequency spectrum has been allocated a harmonised basis in Europe and the United States, although the systems are not yet compatible. The principle is that when two vehicles or ITS stations are in radio communication range, they can connect automatically and establish an ad hoc network where all connected stations can share information such as position, speed, direction, etc.

V2I communication mechanisms provide a means for vehicles to connect to the electronic devices controlling and monitoring the physical environment within which the vehicles are travelling [66]. The infrastructure can then use this information to optimise the traffic control infrastructure to maximise traffic flow, minimizing fuel usage and pollution. A V2I is often described as a centralised control infrastructure, whereas a V2V is decentralised. Example uses of V2I include the control of vehicle acceleration and velocity to optimise travel times, fuel consumption, and congestion levels.

1) Attack Types: Coupling CAVs with an array of different communication mechanisms will inevitably result in them being accessible through a publicly accessible infrastructure (i.e. the internet), or broadcast into public space. This opens the potential for CAVs to experience large-scale, automated and highly damaging attacks. There is great potential for attacks that are damaging to the current information technology to be carried over to CAVs. The list below looks at some of the prominent categories of IT attack types and identifies any relevant literature detailing attacks of this type in CAVs and what mitigation was required.

Password and key attacks are where security restriction mechanisms are continuously tested using different values to see if they can be compromised. Attacks of this nature can generally be classified into the three different categories of a 1) dictionary attack, 2) rainbow table attack, and 3) brute force attack. A dictionary-based attack will use a list of words, which are used individually and in combination, to repeatedly attempt to crack the password. A rainbow table attack is similar in nature; however, it uses a list of pre-computed hashes, constructed from all the possible passwords and a given algorithm. This reduces the time required to crack a password to the time taken to identify the correct hash in the table. A brute force attack is similar to that of a dictionary attack; however, it is also able to identify non-dictionary words by working through all alpha-numeric combinations. This can be a slow process due to the large potential combinations, but it is a complete process meaning that the correct password will eventually be identified. Brute force attacks have been used for compromising VANETs. Research work has discussed the potential of how a brute force attack could be performed to crack the cryptographic keys in VANETs; however, it should be noted that no formal analysis of the complexity of this attack is provided. Therefore, it can only be established that attacks of this nature are possible, but have not yet been performed [67], [68]. Michael Jenkins and Syed Masud Mahmud provide research detailing the ease of which Bluetooth can easily be brute-forced as it usually has a 4-digit pin. In their research they describe how a Pentium IV 3 GHz processor is able to crack the correct pin in 0.06 seconds [69]. An example of a Rainbow table attack is that performed by Flavio Garcia from the University of Birmingham to crack the 96-bit Megamos Crypto algorithm used by many vehicle manufacturers. Building the 1.5 Terabyte rainbow table took less than one week, but exhaustive search only takes seconds [70]. This has potential implications for vehicle owners as it demonstrates that security mechanisms can easily be compromised and the vehicle can easily be stolen. Although this attack is quite complex to perform in that specialist hardware and software is required, there is significant potential for off-the-shelf solutions to become available as attacks of this type will become financially motivated. Attacks of this type can be prevented by implementing stronger mechanisms (i.e. larger keys, more secure algorithms); however there will always be an underlying risk that cannot be eliminated. It is also possible that as technology progresses, and computational power increases, current encryption mechanisms that are deemed secure may become easy to crack.

Knowledge Gap 8: *Mitigation techniques often involve the use of cryptographic techniques. However, due to the long expected life of a vehicle, and the continuing progression of computing power, it is not clear whether the proposed techniques and the vehicle infrastructure will provide a sufficient level of security throughout the vehicle's lifespan.*

Denial of Service (DoS)/Distributed Denial of service (DDoS) attacks are where the normal service of a system is disrupted either by a single or multiple attacking machines. Researchers have demonstrated how DDoS attacks can be performed against VANETs [71] and that it is possible to identify malicious connections for prevention [72], [73]. Different types of DoS attacks can be performed by overwhelming 1) a single network node, 2) vehicle to vehicle (V2V), or 3) vehicle to infrastructure (V2I) [74]. All these attacks are damaging and aim to disrupt the infrastructure. However, V2I DoS attacks are likely to cause widespread disruption to communication mechanisms. Attacks of this

type prevent important communication between vehicles and will ultimately disrupt traffic flow. More significantly, attacks of this type may cause vehicle collisions as potential warning mechanisms may never reach the intended recipient. Furthermore, as with most countermeasures, they can inevitably be broken given enough time and persistence. The implications of compromising VANETs are significant as they are used for functionality such as communicated braking, platooning, traffic information systems, as well as the local infrastructure.

Network protocol attacks are where communication protocols are analysed to identify potential exploitation mechanisms. Once identified, an attack can then be mounted against the acquired knowledge. Researchers have demonstrated that attacks can be mounted and detected against the FlexRay, and CAN protocols [75]. Due to a lack of confidentiality protection, an attacker can read all data sent on the FlexRay bus, as well as send spoofed packets, which can modify vehicular behaviour [76]. It is clear that protocols are carefully analysed by the scientific community to identify exploits, and once identified, suitable mitigation action will be taken. However, such a reactive approach is not feasible as the number of CAVs on the road increases.

Phishing is a form of social engineering where a user masquerades as a trusted entity to gain sensitive information or compromise the system. Phishing attacks are currently the most common form of attacks on PC-based architectures and are often performed through unsolicited email. There is currently an absence of literature detailing significant phishing attacks in CAVs; however, should a user's device that is connected to a CAV be compromised through phishing, the adversary will be able to mount attacks on the vehicle through the connected network via the device. Attacks of this nature are likely to become more wide-spread as the integration between the vehicle and user applications is tightened [77], e.g., as in the recent integration of email systems and the vehicle's entertainment and information system. There are many damaging potential impacts that could happen as a result of a phishing attack, but as detailed in marketing material from FireEye, it is anticipated that ransomware attacks would soon be developed to seize control of the vehicle and render it unusable until the user pays a premium for it to be unlocked [78]. Phishing and ransomware attacks have the potential to be very damaging for the user as the system may become unusable, which can have considerable financial consequences. As the technology of CAVs is currently developing, it is not clear how these attacks may take place and how they may be prevented. However, as this is a financially motivated crime, it is clear that vulnerabilities will be exploited if they are discovered.

Knowledge Gap 9: *The level of connectivity and automation in vehicles is continuously expanding, and hence the dependence on technology integration in the vehicle is increasing. Common examples include vehicles with embedded web browsing, email functionality, and bluetooth connectivity. Although the literature describes the nature of current phishing and ransomware attacks, there is a lack of literature detailing how attacks of this type may occur, and what can be done to mitigate them.*

Rogue updates are where software running on a vehicle's ECUs is updated with software which was not produced by the manufacturer and has hidden vulnerabilities. Many researchers have discussed the requirements for a distribution model where manufacturers can update the firmware on large numbers of vehicles without a large financial overhead. The research community are in agreement that Firmware updates Over The Air (FOTA) is a credible solution. However, they are also in agreement that there are large potential security implications. Furthermore, secure protocols need to be developed that use cryptographic techniques to guarantee with a certain level of confidence that the update is legitimate [54], [79]. These solutions can provide convincing architectures; however, without wide-scale testing there will always be uncertainty over their security.

Knowledge Gap 10: *There is a lack of literature detailing how a manufacturer would respond to cyber incidents. Some manufacturers, such as Fiat-Chrysler, have implemented mechanisms that enable vulnerabilities to be reported. There is no literature detailing how a manufacturer would respond to a significant and wide-spread attack. It is essential to have a robust incident response plan as incorrect management could have huge financial and reputation implications.*

The remainder of this section surveys literature to identify current and likely vulnerabilities and mitigation efforts resulting from the connectivity of vehicles. These are: 1) physical access, 2) close proximity, and 3) remote access.

2) Physical Access: Vulnerabilities arising from exploiting a vehicle's control mechanisms through physical access have been around since the integration of sophisticated ECUs. However, with the increasing use of sensors and control modules in CAVs, the potential implications of compromising a system's sensory, control, and communication mechanisms are heightened.

Physical attacks are often categorised as either 'direct' or 'indirect' attacks. Direct attacks involve targeting specific aspects of the vehicle's electronic control systems through physically accessing the system, whereas indirect attacks involve exploiting or overloading aspects of the system to cause indirect damage. For example, an example of a direct attack is "bus tapping" (I.e., gaining unauthorised access to the underlying network) the CAN protocol and reprogramming ECUs. A recent exposure of a direct vulnerability was the realisation that BMW vehicles can have new keys reprogrammed through on-board diagnostic (OBD) port exploitation [80]. This is a relatively low-cost attack that requires plugging a device into the OBD port to bypass the vehicle's immobilising systems and programme a new key to start the vehicle. As detailed by Clifford UK, prior to this attack, the attacker needs to gain access to the vehicle; however, this is achieved through cracking the 48-bit Hittag system, which is reported to take 3

minutes using standard computer hardware [80].

Physical access vulnerabilities have been evolving since the production of the first motor vehicle and they are not solely a direct consequence of CAVs. However, the number of potential attacks and their significant has evolved considerably with the introduction of more sophisticated electronic sensors and control modules in CAVs. The following sections detail some of the prominent physical access vulnerabilities and mitigation technologies.

On-board Diagnostic (OBD) port. The OBD can access the network infrastructure within the vehicle (I.e., all CAN busses). This is an intended level of access as the OBD port is a means of maintenance and upgrading ECU firmware. The OBD port does have a reduced threat level when compared to wireless connection mechanisms as it is located physically within the car; however, once access has been acquired, it is possible to perform significant modification to the ECU's functionality [4]. Examples could include modifying the codebases responsible for engine, lighting, and braking functionality. In addition, it has also been identified that criminal organisations may aim to extract the intellectual property of OEMs, as well as stealing driver sensitive data [5]. The mechanisms of access control within the OBD protocol are relatively weak but allow the attacker to easily extract and modify firmware and parameters, for example, by reducing the mileage count to increase a vehicle's value. This has implications for a potential buyer as they may be sold something which is not genuine. It is also possible that individuals may want to falsify log information on the ECU to hide their involvement in a vehicle accident, or even to commit insurance fraud. Research has demonstrated the possibility of performing a forensic investigation of a vehicle's ECUs through the OBD port is presented [53]. Although this research is in its infancy, it raises the need for manufacturers to consider forensic implications of their devices. Previous research has demonstrated the potential of using cryptographic techniques for message authentication of the CAN network, and has considered backwards compatibility, as a means to mitigate the transfer of unauthorised data on the CAN network. Although the problem of access control mechanisms has been acknowledged and consideration given to how it might be improved (e.g., Escrypt), a solution has yet to be offered. This area of research is largely unaddressed.

Knowledge Gap 11: *If an accident was to occur involving CAVs, or if one was to be involved in financially motivated crime (e.g., clocking, theft, etc.), then it would be necessary to forensically analyse the on-board systems to determine, beyond reasonable doubt, what happened. The literature detailing how software-based systems might be designed with forensic investigations in-mind is virtually non-existent. It is possible to perform forensic investigations to provide a solid legal basis to prosecute criminals participating in criminal activity involve CAVs.*

Media systems. The functionality of a vehicle's media systems is to receive a variety of wireless broadcast signals (AM, FM, etc.), decode them, and play the represented media to the user. A media player will often accept standard compact discs and support decoding many audio formats (MP3, WMA, etc.) on an ISO 9660 file system. In addition, many modern media systems can also play audio from alternative storage mechanisms such as a USB-mounted file system. The media system can also be linked to the CAN network, which has previously resulted in the identification of potential vulnerabilities. For instance, it is possible to inject packets onto the CAN bus network through exploiting a vulnerability of the media player [3]. In this vulnerability, it has been identified that packets can be encoded in WMA audio files. WMA audio files allow embedding pictures and other text-based information which is processed by the media player. In this particular case, it was possible to include executable code which could release CAN packets onto the network. Interestingly, it has also been identified that such executables would have no adverse effects on other media players, even though included in PCs. Researchers also allude to the possibility of a compromised media file being shared through peer-to-peer networks with the attack going unnoticed. This has large implications for the vehicle and the driver as the attack could cause a significant change in vehicle behaviour. It is also worrying that an attack of this nature could potentially rapidly spread by masquerading in a seemingly benign file. Mitigation of vulnerabilities of this type can be performed at both the application (media system) and infrastructure level (CAN protocol). Mitigating such vulnerability in a media system would require patching the system, as well as designing and developing such technology with an increased consideration for cyber security requirements. Mitigation at the CAN level will require robust mechanisms of ensuring authenticity of data packets, as discussed in Section II-A.

3) Close Proximity Vulnerabilities: Close proximity vulnerabilities are those exposed through short-range communication mechanisms. This could involve the exploitation of on-board sensors to attack the system or the network communication mechanism. Such attacks may be primitive and may even happen by coincidence. For example, a situation may arise where a person inadvertently does something in the vehicle's perceived environment (e.g. walking down the pavement with a big box), which causes the system to take reactive measures. On the contrary, attacks may be more sinister and pre-planned to intentionally compromise the system. For instance, a malicious user could just keep sending the vehicle false signals to disorient, hijack, or even restrict it to within a virtual fence, as presented by researchers at the Worcester Polytechnic Institute, Massachusetts [81].

Bluetooth. Many modern cars have built in Bluetooth capabilities for media connectivity purposes. Researchers have identified that the Bluetooth control code contains a potential memory exploit, allowing the execution of code from any paired Bluetooth device [82]. It is possible that a compromised device which is paired to the vehicle could start to attack the vehicle's ECUs without the driver knowing. Researchers have developed and tested a security layer for smartphone-to-vehicle communication over Bluetooth. Previous research discusses the vulnerabilities with Bluetooth-enabled systems, and not just those within the

vehicle domain [83]. Dardenelli's research provides a detailed and lengthy investigation into the vulnerabilities, and it is surprising just how vulnerable Bluetooth-enabled devices are. Furthermore, it is also surprising that although researchers have developed many secure Bluetooth protocols utilising cryptographic techniques, many commercial solutions do not implement such security mechanisms as they can have adverse effects on usability. Furthermore, those techniques that do use cryptography to establish trust do not do anything to prevent the execution of malicious code through memory exploitation. However, it will prevent the attack of using open source tools, such as Bluesniff, for analysing packets distributed in the public domain [84].

Knowledge Gap 12: *Manufacturers are utilising technology (hardware and software) that has inherent security vulnerabilities. This is largely due to a functionality focus in supply chain manufacturing where parts are produced to a functional contract and, due to tight time constraints, no additional effort is taken to ensure rigorous security.*

Keyless entry and ignition systems. It is widely accepted that in primitive systems, remote central locking signals can be captured and replicated to gain access to a vehicle, and more importantly, disable the alarm and immobiliser allowing thieves sufficient time to start and steal the vehicle. Manufacturers have invested heavily in implementing systems that are much harder to circumvent. These often involve using some kind of cryptographic key change protocol. However, vulnerabilities are still being identified allowing adversaries to gain access to luxury vehicles. A news article by The Guardian details that luxury Range Rovers with keyless locking systems are being targeted by thieves. Furthermore, the requirement for new keys to be programmed to a vehicle presents the opportunity to programme a new key and drive the vehicle away. This is something that is being exploited in premium Audi RS4 vehicles [90] (see driving.com) where thieves are able to add a new key into the system once they gain physical access to the vehicle. Although this is a premeditated sophisticated attack to exploit a known vulnerability, Audi have dismissed any liability. Researchers from the University of Birmingham [70] developed techniques of cracking encryption mechanisms used for keyless entry; however were initially prevented from publishing their research by UK government over fears of enabling criminals with knowledge to easily steal luxury vehicles.

Signal jamming for connected devices. As previously discussed in Section II-A1, any sensor that is remotely connected to a vehicle using a form of wireless connectivity can be exploited through a signal jamming attack. Signal jamming attacks aim to deliberately block, jam or interfere with authorised communication. The attacks often work by reducing the signal-to-noise ratio making it challenging to differentiate the desired signals from background noise. Signal jamming is relatively easy to perform and the required signal broadcasting equipment is readily available at low cost. In addition to research detailed earlier in this report, researchers have also demonstrated the potential for wireless inter-vehicle communication to be interrupted through signal jamming, resulting in a DoS attack [85]. In the work undertaken at Pennsylvania State University, researchers demonstrated how the Wireless access in vehicular environments (WAVE) standards (IEEE 1609) can be jammed such that nodes within the network (e.g., vehicles) are no longer able to receive communication. The WAVE standard is an extension of the IEEE 802.11 standard to accommodate communication between vehicles and roadside infrastructure. Their research presents three types of jamming. The first is trivial jamming where an attacker constantly transmits noise, the second is a periodic attack where noise is broadcast for random durations and at random intervals, and the third is a reactive attack where signals are only broadcast when communication signals are detected. A jamming attack on this communication technology has considerable safety implications as vehicles may become unaware of important information coming from both other vehicles and the infrastructure. The required knowledge and hardware depends on the connection mechanism that the attacker wants to jam.

Attacks are also possible on other close proximity networks. For example, the tyre pressure monitoring system (TPMS) uses a 315 MHz or 433 MHz band wireless infrastructure [29]. It has been demonstrated that this network can be exploited by signal jamming and falsification of data [29]. The potential implications of jamming the TPMS are that false tyre pressure warning messages can be generated, which may not only annoy or distract the user but also supress genuine warnings or alerts (e.g., tyre is rapidly deflating) resulting in potential safety concerns should a driver not be able to detect the true status of the system or bring the vehicle to a safe stop.

Signal jamming attacks are often difficult to overcome, but technology and research can be adapted from the military domain. One mechanism to prevent jamming attacks is to develop solutions that still allow the intended signal to be detected in environments with large volumes of noise. This area of research has received significant interest in the Unmanned Aerial Vehicle (UAV) research community. This is not surprising as radio communication is of critical importance for the safe use of a UAV. Scientists at the Beihang University, China, carried out a survey of anti-jamming techniques for UAVs [86] and found that current methods are mainly based on different signal processing, filtering, and identification techniques to help identify the signal amongst large volumes of noise. There may be value in translating this research to CAVs since it is sometimes not feasible (due to safety requirements) to rely on one method of communication given the ramifications of potential failure. For example, in the military domain, especially in weapon guidance systems, multiple systems are fused together to improve reliability. To prevent GPS jamming and spoofing attacks, other types of sensors have been integrated to maintain safe and reliable navigation mechanisms. For instance, an Inertia Measurement System (IMS) was integrated with a GPS system [87] (Naval Surface Warfare Center, USA) to provide navigation mechanisms even when GPS systems are compromised for short periods.

Knowledge Gap 13: *Denial of service attacks are always going to be possible, especially when considering radio-based connection mechanisms. It is currently unclear how CAVs will be able to detect such attacks to prevent any adverse action from autonomously being performed.*

4) Remote Access Vulnerabilities: As CAVs become increasingly connected via different network mechanisms (E.g. Wi-Fi, 3G, GPRS), it is becoming possible to compromise devices – such as the embedded microprocessors connected via a CAN bus – that were not originally intended to be linked to outward-facing networks through remote exploit mechanisms. On the contrary, the connection of CAN-enabled devices can allow for mechanisms that can automatically call for emergency assistance during severe collisions, and pass-on information acquired through vehicle sensors to help emergency services respond more appropriately. For example, passing on information from accelerometers, velocity, and speed sensors can help determine the potential forces involved. In addition, sensory information such as whether an airbag has been deployed can also be used to determine where the forces originated.

Although this connectivity provides much desired functionality, it increases the probability of being remotely attacked. This possibility is becoming increasingly likely as the CAV's infrastructure utilises the internet architecture. The remainder of this section discusses some of the vulnerabilities originating from prominent network connection mechanisms, as well as those attacks which will becoming increasingly likely and have great implications on the security of CAVs.

First, it is useful to discuss the differences between broadcast and addressable channels. Broadcast channels are those that are not specifically directed towards a given vehicle. Rather, they can be received on-demand. Radio transmission, like GPS, is an example of a broadcast channel. The signal is not targeted towards an individual vehicle but perpetrators can tune in to them. Long-range broadcast channels are appealing as a potential attack surface as they are difficult to monitor and control. Furthermore, they can be received by many receivers simultaneously without the need to address a singular vehicle as in other communication mechanisms (E.g., the TCP/IP protocol can be used to address an individual vehicle). An addressable channel of communication is one where part of the vehicle's computerised systems is communicated through being specifically addressed on a network. For example, communicating via Transmission Control Protocol / Internet Protocol (TCP/IP), which requires a known IP address to direct communication. Addressable channels are also advantageous for the attacker as they often communicate over wide-scale data networks (e.g., 3G) and enable exploits to be performed from different geographical locations and jurisdiction.

The below section details the more prominent connection mechanisms for remote-access and provides information into the exploits originating from the different technology used for remote connection mechanisms.

Radio. Communication mechanisms which fall under the umbrella term of radio are those long-range signals which are used by GPS systems, Digital Radio, Radio Data System (RDS), and Traffic Message Channels. The range of signals depends on transmitter power, terrain, and interference [3]. For example, a 5W RDS transmitter can be expected to deliver 1.2kbps over distances up to 10km. The majority of vehicles currently on the road will also have a built-in media player which is capable of receiving mechanisms of radio communication. Furthermore, it is also likely that many of these vehicles will connect to the vehicle's CAN bus. A recent report details that security professionals from NCC, UK have demonstrated that control of vehicles' brakes and other critical systems can be acquired by sending data via Digital Audio Broadcasting (DAB) signals [52]. This attack exploited the fact that many modern entertainment systems process DAB data to display text and pictures on a dashboard screen. Worryingly, it has been highlighted that this attack could be performed using low-cost, off-the-shelf hardware and can be performed on many vehicles at once through a broadcast mechanism. Although the attacker would need to have a detailed understanding of how to construct and transmit DAB data that can exploit a vulnerability, there is the potential for such attacks to be easily compiled into an executable file suitable for an attacker with very limited knowledge.

Cellular and Internet-enabled exploits The cellular (synonymous with mobile) network architecture is used by vehicles as a mechanism for long-range communication. There are many different technologies that use a cellular network infrastructure. In CAVs, connection mechanisms which have a high bitrate are most desirable for performing tasks such as continuous streaming of data. For example, a survey publication discusses the use of 3G as mechanism in inter-vehicle communication [88]. However, in principle, a CAV can be developed to utilise any cellular-based architecture. Addressable cellular data networks are used in CAVs to distribute data such as crash reporting, diagnostics, anti-theft, and convenience (e.g., weather and traffic updates). Cellular enables attackers to conduct remote attacks on a vehicle as it can be performed over a long distance in a largely anonymous fashion [3], [89]. There is an absence of literature detailing attacks that specifically target cellular infrastructure with most of the literature focussing on those targeting to exploit internet-enabled technology regardless of whether it is connected using a cellular network or connected through a WiFi hotspot.

Knowledge Gap 14: *Vulnerabilities are currently identified by white-hat hackers performing research-based penetration testing. However, as CAVs become increasingly connected and common on roads, it is likely that automated attacks will be developed and executed by those without expert knowledge. It is currently unclear how these might be performed and how both infrastructure and vehicle will react.*

The remote connection exploits mentioned thus far would be possible through using an internet-based connection and this creates the potential for wide-scale and automated attacks.

For example, it is likely that attacks will be programmed into a script which can be executed by any attacker with no specialised expertise. Enabling attacks on a large scale raises concerns of the need for strong security mechanisms embedded in CAVs to protect against both known and unknown vulnerabilities. Known vulnerabilities are those which will be common knowledge in the public domain, and will most likely appear in the automated scripts. Unknown attacks are those which have not yet been identified, but may be detectable through closely monitoring CAVs. Another aspect of CAVs that has surfaced in academic literature is how the on-board computer systems and network connection mechanisms can be forensically audited. Previous work has discussed how forensic investigations can be conducted to establish gateway activity [53].

Internet-enabled communication has resulted in car manufacturers developing solutions where a vehicle can be interacted with remotely through application- and web-based communication. However, functionality of this nature is likely to attract the attention of security practitioners. For example, Nissan released an iOS and Android application allowing a driver to remotely interact with their vehicle (e.g., to configure heating controls, etc.). Nissan used the Vehicle Identification Number (VIN) - a unique vehicle ID - to handle the mapping between the driver's application and vehicle without any password based authentication. This was a huge oversight by Nissan as VIN numbers are normally located on the bottom corner of the dashboard and visible from outside. Furthermore, VIN numbers are often allocated in batches meaning that adversaries could simply change the last number and it would be very likely that they would connect to another Nissan Note, regardless of its geographic location [10].

III. Summary of Future Challenges

Table III provides a summary of the knowledge gaps identified in this research survey, as well as highlighting some of the potential impacts that may occur if this knowledge gap was not adequately addressed. Although the identified knowledge gaps are speculative and based on the current research activity, it should be noted that it is not an exhaustive list and some gaps may have been missed. It is also likely that as both research and release of CAVs continues, many new gaps will also be identified that will need to be acknowledged.

The primary aim of this paper was to identify knowledge gaps, but it is particularly noteworthy to state that the identified gaps are sizeable and will most likely require significant research effort to provide holistic solutions. Both research and commercial attention to the cyber security implications of CAVs are becoming increasingly acknowledged and industry is slowly adapting. However, it is crucial that the identified gaps are addressed before more vehicles with increasing levels of connectivity and automation are on the market.

IV. Conclusion

This review was performed through a logical analysis and exploration of literature available in the public domain. The literature has highlighted that there are many focussed areas of research which are identifying potential vulnerabilities as well as proposing potential mitigation techniques. A substantial portion of the identified research details reactive action to the detection of a cyber security vulnerability. There are also publications discussing the potential for a security- and human-centric design process to minimise the likelihood of a vulnerability occurring. However, as far as literature details, such processes are still in their infancy and are not widely adopted.

There are many sizeable gaps in knowledge which require attention from CAV research communities and automotive manufacturers. It is essential that these knowledge gaps are adequately addressed as soon as possible to prevent the need for large-scale reactive action, as well as to standardise the industry and ensure a high-degree of cyber security is maintained across vehicle manufacturers, the travel infrastructure, and the end-users.

References

[1] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE internet of things journal*, vol. 1, no. 4, pp. 289–299, 2014.

[2] M. H. Hebert, C. E. Thorpe, and A. Stentz, *Intelligent unmanned ground vehicles: autonomous navigation research at Carnegie Mellon*. Springer Science & Business Media, 2012, vol. 388.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, 2011.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[5] A. Yadav, G. Bose, R. Bhange, K. Kapoor, N. C. S. Iyengar, and R. D. Caytiles, "Security, vulnerability and protection of vehicular on-board diagnostics," *International Journal of Security and Its Applications*, vol. 10, no. 4, pp. 405–422, 2016.

[6] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," February 2015. [Online]. Available: http://essay.utwente.nl/66766/

[7] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[8] A. R. Ruddle, D. D. Ward, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, "Cyber security riskanalysis for intelligent transport systems and in-vehicle networks," *Intelligent Transport Systems: Technologies and Applications*, p. 83, 2015.

[9] H. Onishi, "Paradigm change of vehicle cyber security," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. IEEE, 2012, pp. 1–11.

[10] "Nissan leaf electric cars hack vulnerability disclosed," http://www.bbc.co.uk/news/technology-35642749l, accessed: 2016-08-16.

[11] McAfee, "Automotive Security Best Practices," McAfee, Tech. Rep., 2015.

[12] CERT-UK, "Cyber-Security risks in the supply chain," Tech. Rep., 2015.

[13] M. Warren and W. Hutchinson, "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management*, vol. 30, no. 7/8, pp. 710–716, 2000.

[14] K. D. Akdemir, D. Karakoyunlu, T. Padir, and B. Sunar, "An emerging threat: eve meets a robot," in *International Conference on Trusted Systems*. Springer, 2010, pp. 271–289.

[15] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, "Security of autonomous systems employing embedded computing and sensors," *IEEE Micro*, vol. 33, no. 1, pp. 80–86, 2013.

[16] Y. Cui and S. S. Ge, "Autonomous vehicle positioning with gps in urban canyon environments," *IEEE transactions on robotics and automation*, vol. 19, no. 1, pp. 15–25, 2003.

[17] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, 2012.

Knowledge Gap	Potential Impact
Unknown implications of exploiting navigation mechanisms	• Gaining remote control over a vehicle's autonomous functionality • Targeted hijacking of valuable vehicles • Large safety concerns for public citizens
Unknown potential to exploit primitive low-level sensors	• Unexpected or unforeseen inputs may result in unpredicted vehicle behaviour • Increases potential for modifying vehicle performance
How many sensors are required to provide sufficient redundancy	• Insufficient use of sensors may allow a cyber attack to create 'blind spots' with large potential consequences • Overuse of sensor devices would inflate manufacturing cost, but may increase end-user confidence
A comprehensive analysis of how and to what effect ECUs can be compromised	• Compromising ECU functionality could significantly change vehicle functionality • Presents danger to citizens as the vehicle could conduct unsafe operations
How ECU software will be updated on a wide-scale whilst maintaining security	• No mechanism to update on a wide-scale will result in many vulnerable systems • Insecure system might be susceptible to rogue updates
What personal data will be generated and stored on a vehicle, and to what extent it can be exploited	• Large volumes of personal data might be generated without the passengers' knowledge • Breaches of privacy might occur should the data be illicitly acquired • Monetisation of CAVs would increase data theft
How will control be passed back to the vehicle if it detects a cyber threat and how will it pass control back to the driver	• Driver might be unable to make sense of the situation and make incorrect decisions • Dangerous to passengers and other vehicles
How the use of cryptographic techniques will withstand the potential increase in computational power	• Infrastructure and vehicles could be vulnerable should any security mechanisms become vulnerable and not fit-for-purpose through the vehicle's anticipated life expectancy
The potential for user targeted attacks (phishing, ransomware) to occur	• User is targeted to increase attack success • Potential for financial damage if the user has to pay for their vehicle to be cleaned of any malware
How would a manufacturer respond to a large scale cyber attack	• The manufacturer might be unable to respond to a cyber attack and the vehicle owners might be left vulnerable
How the added computational resources of a CAV can be utilised in digital forensics	• Inability to prove attacks/theft could impact on the ability to prosecute criminals • Ability to modify historical information (e.g mileometer) would result in a lack of public trust
How manufacturers can adopt a culture of cyber security accountability in the supply chain	• Vulnerabilities will always exist if manufacturers do not operate under a security-centric philosophy
How CAVs can detect and prevent adverse autonomous activity due to Denial of Service attacks	• Simplistic attacks on infrastructure may result in unusable vehicle features • Disabling essential V2V and V2I communication mechanisms could impact upon navigation and collision avoidance systems
Potential implications of large-scale automated attacks which can be executed without expert knowledge	• Automated attacks will allow for vulnerable vehicles to be easily identified • Lack of expert knowledge required will allow non-expert users to execute attacks and potentially cause significant damage

TABLE I
SUMMARY OF GAPS IN KNOWLEDGE AND THEIR POTENTIAL IMPACT

[18] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[19] "Ut austin researchers successfully spoof an $80 million yacht at sea," http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea, accessed: 2016-08-16.

[20] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[21] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time gps spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[22] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[23] S.-S. Jan and A.-L. Tao, "Comprehensive comparisons of satellite data, signals, and measurements between the beidou navigation satellite system and the global positioning system," *Sensors*, vol. 16, no. 5, p. 689, 2016.

[24] M. Farsi, K. Ratcliff, and M. Barbosa, "An overview of controller area network," *Computing & Control Engineering Journal*, vol. 10, no. 3, pp. 113–120, 1999.

[25] R. Bosch, "Can specification version 2.0," *Rober Bousch GmbH, Postfach*, vol. 300240, 1991.

[26] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, "Lightweight authentication for secure automotive networks," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*. EDA Consortium, 2015, pp. 285–288.

[27] S. Singh, K. Kingsley, and C.-L. Chen, "Tire pressure maintenance–a statistical investigation," Tech. Rep., 2009.

[28] "Cars safer from 1 november 2012," http://europa.eu/rapid/press-release_IP-12-1169_en.htm, accessed: 2016-08-16.

[29] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington DC*, 2010, pp. 11–13.

[30] A. Wright, "Hacking cars," *Communications of the ACM*, vol. 54, no. 11, pp. 18–19, 2011.

[31] S. A. Hirani, "Energy consumption of encryption schemes in wireless devices," Ph.D. dissertation, University of Pittsburgh, 2003.

[32] "Researcher hacks self-driving car sensors," http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors, accessed: 2016-08-16.

[33] S. Mahajan, R. Bhosale, and P. Kulkarni, "Obstacle detection using mono vision camera and laser scanner."

[34] J. Du, J. Masters, and M. Barth, "Lane-level positioning for in-vehicle navigation and automated vehicle location (avl) systems," in *Intelligent Transportation Systems, 2004. Proceedings. The 7th International IEEE Conference on*. IEEE, 2004, pp. 35–40.

[35] D. Giveki, G. Bahmanyar, M. A. Soltanshahi, Y. Khademian, and H. Salimi, "Object boundary recognition using b-snake," *Canadian Journal on Image Processing and Computer Vision*, vol. 2, no. 6, 2011.

[36] H.-Y. Cheng, B.-S. Jeng, P.-T. Tseng, and K.-C. Fan, "Lane detection with moving vehicles in the traffic scenes," *IEEE Transactions on intelligent transportation systems*, vol. 7, no. 4, pp. 571–582, 2006.

[37] C. Bahlmann, Y. Zhu, V. Ramesh, M. Pellkofer, and T. Koehler, "A system for traffic sign detection, tracking, and recognition using color, shape, and motion information," in *IEEE Proceedings. Intelligent Vehicles Symposium, 2005.* IEEE, 2005, pp. 255–260.

[38] S. Eum and H. G. Jung, "Enhancing light blob detection for intelligent headlight control using lane detection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 2, pp. 1003–1011, 2013.

[39] K. Boccuzzi, "Investigating the causes of and possible remedies for sensor damage in digital cameras used on the omega laser systems," 2008.

[40] "Mts. analysis of laser light threat to cctv," http://www.mts-iss.com/affects-of-lasers.html, accessed: 2016-08-16.

[41] L. Gomes, "Hidden obstacles for googles self-driving cars: Impressive progress hides major limitations of googles quest for automated driving," 2014.

[42] "Understand the fatal tesla accident on autopilot and the nhtsa problem," http://electrek.co/2016/07/01/understanding-fatal-tesla-accident-autopilot-nhtsa-probe/, accessed: 2016-08-16.

[43] "'walkie-talkie' skyscraper melts jaguar car parts," http://www.bbc.co.uk/news/uk-england-london-23930675, accessed: 2016-09-06.

[44] P. Grisleri and I. Fedriga, "The braive autonomous ground vehicle platform," *IFAC Proceedings Volumes*, vol. 43, no. 16, pp. 497–502, 2010.

[45] "Cyber security and the future of driverless cars," http://www.nesta.org.uk/blog/cyber-security-and-future-driverless-cars, accessed: 2016-08-16.

[46] S. Lorenz, "The flexray electrical physical layer evolution," *SPECIAL EDITION HANSER automotive FLEXRAY*, pp. 14–16, 2010.

[47] D. J. Glancy, "Privacy in autonomous vehicles," *Santa Clara L. Rev.*, vol. 52, p. 1171, 2012.

[48] D. Klinedinst and C. King, "On board diagnostics: Risks and vulnerabilities of the connected vehicle," 2016.

[49] "Researchers hack into driverless car system, take control of vehicle," http://www.nationaldefensemagazine.org/archive/2015/May/Pages/ResearchersHackIntoDriverlessCarSystemTakeControlofVehicle.aspx, accessed: 2016-08-16.

[50] K.-W. Chiang, T. T. Duong, and J.-K. Liao, "The performance analysis of a real-time integrated ins/gps vehicle navigation system with abnormal gps measurement elimination," *Sensors*, vol. 13, no. 8, pp. 10 599–10 622, 2013.

[51] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, 2014.

[52] C. Vallance, "Car hack uses digital-radio broadcasts to seize control," *BBC, July*, 2015.

[53] D. K. Nilsson and U. E. Larson, "Conducting forensic investigations of cyber attacks on automobile in-vehicle networks," in *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 8.

[54] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Creating a secure infrastructure for wireless diagnostics and software updates in vehicles," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2008, pp. 207–220.

[55] D. K. Nilsson and U. E. Larson, "A defense-in-depth approach to securing the wireless vehicle infrastructure," *Journal of Networks*, vol. 4, no. 7, pp. 552–564, 2009.

[56] J. Lindberg, "Security analysis of vehicle diagnostics using doip," 2011.

[57] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 10–21, 2014.

[58] T. B. Sheridan, *Humans and automation: System design and research issues*. John Wiley & Sons, Inc., 2002.

[59] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010.

[60] B. Hoh, T. Iwuchukwu, Q. Jacobson, D. Work, A. M. Bayen, R. Herring, J.-C. Herrera, M. Gruteser, M. Annavaram, and J. Ban, "Enhancing privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines," *IEEE Transactions on Mobile Computing*, vol. 11, no. 5, pp. 849–864, 2012.

[61] J. Wei, J. M. Snider, T. Gu, J. M. Dolan, and B. Litkouhi, "A behavioral planning framework for autonomous driving," in *2014 IEEE Intelligent Vehicles Symposium Proceedings*. IEEE, 2014, pp. 458–464.

[62] V. N. Gadepally, "Estimation of driver behavior for autonomous vehicle applications," Ph.D. dissertation, The Ohio State University, 2013.

[63] A. Kane and P. Koopman, "Ride-through for autonomous vehicles," in *SAFECOMP 2013-Workshop CARS (2nd Workshop on Critical Automotive applications: Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security*, 2013, p. NA.

[64] "Google gives more detail on safety of its autonomous cars," http://www.cnbc.com/2016/01/12/google-gives-more-detail-on-safety-of-its-autonomous-cars.html, accessed: 2016-08-16.

[65] N. B. Sarter and D. D. Woods, "How in the world did we ever get into that mode? mode error and awareness in supervisory control," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 5–19, 1995.

[66] L. Glielmo, "Vehicle-to-vehicle/vehicle-to-infrastructure control," *The Impact of Control Technology*, 2011.

[67] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET communications*, vol. 4, no. 7, pp. 894–903, 2010.

[68] I. A. Sumra, I. Ahmad, H. Hasbullah *et al.*, "Classes of attacks in vanet," in *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International*. IEEE, 2011, pp. 1–5.

[69] M. Jenkins and S. M. Mahmud, "Security needs for the future intelligent vehicles," SAE Technical Paper, Tech. Rep., 2006.

[70] R. Verdult, F. D. Garcia, and B. Ege, "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer," in *Supplement to the 22nd USENIX Security Symposium (USENIX Security 13)*, 2015, pp. 703–718.

[71] A. Pathre, "Identification of malicious vehicle in vanet environment from ddos attack," *Journal of Global Research in Computer Science*, vol. 4, no. 6, pp. 30–34, 2013.

[72] A. Pathre, C. Agrawal, and A. Jain, "A novel defense scheme against ddos attack in vanet," in *2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*. IEEE, 2013, pp. 1–5.

[73] A. Rawat, S. Sharma, and R. Sushil, "Vanet: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[74] H. Hasbullah, I. A. Soomro, and J. Manan, "Denial of service (dos) attack and its possible solutions in vanet," *World Academy of Science, Engineering and Technology*, vol. 65, p. 20, 2010.

[75] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Intelligent Vehicles Symposium, 2008 IEEE*. IEEE, 2008, pp. 220–225.

[76] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol flexray," in *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS08*. Springer, 2009, pp. 84–91.

[77] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, 2012.

[78] "Connected cards the open road for hackers," https://www.fireeye.com/blog/threat-research/2016/06/connected_cars_the.html, accessed: 2016-08-16.

[79] M. S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger, "Secure automotive on-board protocols: a case of over-the-air firmware updates," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2011, pp. 224–238.

[80] "Bmw obd port theft - the solution," http://www.clifford.co.uk/BMW_OBD_Theft.html, accessed: 2016-08-16.

[81] S. Chen, A. M. Wyglinski, S. Pagadarai, R. Vuyyuru, and O. Altintas, "Feasibility analysis of vehicular dynamic spectrum access via queueing theory model," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 156–163, 2011.

[82] K. Haataja, *Security threats and countermeasures in Bluetooth-enabled systems*. University of Kuopio, 2009.

[83] A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, and T. Holz, "A security layer for smartphone-to-vehicle communication over bluetooth," *IEEE embedded systems letters*, vol. 5, no. 3, pp. 34–37, 2013.

[84] D. Spill and A. Bittau, "Bluesniff: Eve meets alice and bluetooth." *WOOT*, vol. 7, pp. 1–10, 2007.

[85] J. J. Blum, A. Neiswender, and A. Eskandarian, "Denial of service attacks on inter-vehicle communication networks," in *2008 11th International IEEE Conference on Intelligent Transportation Systems*. IEEE, 2008, pp. 797–802.

[86] H. Wenzhun, W. Yongsheng, and Y. Xiangyang, "Studies on novel anti-jamming technique of unmanned aerial vehicle data link," *Chinese Journal of Aeronautics*, vol. 21, no. 2, pp. 141–148, 2008.

[87] E. J. Ohlmeyer, "Analysis of an ultra-tightly coupled gps/ins system in jamming," in *2006 IEEE/ION Position, Location, And Navigation Symposium*. IEEE, 2006, pp. 44–53.

[88] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," Tech. Rep., 2004.

[89] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88–105, 2008.