baesystems.com/government

Security Challenges for Connected and Autonomous Vehicles

Understand the technology and security issues associated with autonomous driving

BAE SYSTEMS

Introduction

At the turn of the century, the idea that roads may one day be full of vehicles that drive themselves, and require no human oversight behind the wheel, would still have been considered the stuff of science fiction: part of a future that remained over the horizon, but far enough away not to cause significant public debate.

That was then. In the past decade, the technology behind 'autonomous' vehicles has advanced significantly, and trials of 'driverless cars' have been underway for several years. So much so, that governments across the world are already in discussions with manufacturers and regulators about how and when they may be legally permitted on public roads.

However, as the area receives more focus, more questions arise: although the technology is now significantly advanced, an increasing number of challenges must be more fully understood and addressed before a future for vehicles without drivers can be fully realised. These include solving complex problems in human factors, insurance, regulation, infrastructure, security, and above all others, safety.

With significant expertise in digital transformation, cyber security, transport, and Critical National Infrastructure, BAE Systems Applied Intelligence has a growing focus on helping our government, defence, CNI, and commercial customers understand and overcome these challenges.

This white paper is intended for anyone interested in gaining a high-level understanding of the technology and security issues which may be associated with Connected and Autonomous Vehicles (CAV).

Section 1

An introduction to CAV, including:

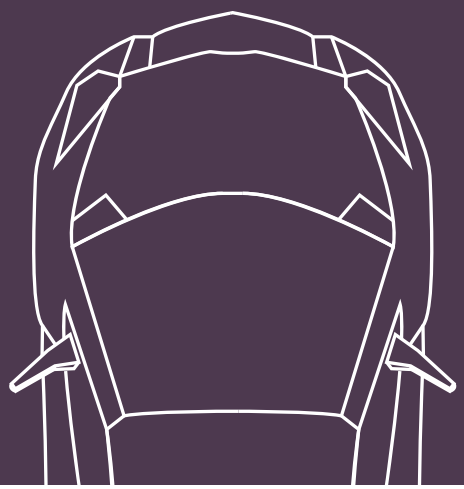
- A high-level overview and discussion on CAV
- An overview of the wider ecosystem that may be necessary to support CAV traffic on public roads
- An overview of the way the automotive industry classifies different levels of automation within driverless cars

Section 2

Security Analysis for CAV threats, including:

- An summary of reasons why threat actors may wish to exploit CAVs
- A view of attack vectors which threat actors could use to compromise CAVs

With significant expertise in digital transformation, cyber security, transport, and Critical National Infrastructure, BAE Systems Applied Intelligence has a growing focus on helping our government, defence, CNI, and commercial customers understand and overcome the challenges and security issues of CAV technology.



Section I

An introduction to Connected and Autonomous Vehicles

Driverless vehicles first appeared in the imagination of science fiction writers purely as an aspect of future technology which readers could only marvel at. Since then, however, the dream is rapidly becoming reality, with several different technologies combining to form what is now frequently referred to as CAV (Connected and Autonomous Vehicles), backed by significant motivators to fully develop this capability and introduce it to society. These include:

Saving lives and preventing injury

According to a recent report by the World Health Organisation[1], it is estimated that in recent years, the annual figure for those who lose their lives in traffic accidents is around 1.3 million, and this figure does not include those injured or hurt. According to statistics - estimated in the UK to be as much as 84%[2] - the vast majority of road accidents result from human error.

Reducing costs incurred in relation to accidents (vehicles, infrastructure, hospital resources, expenses resulting from delayed transport of goods and people) and lost or delayed economic benefits

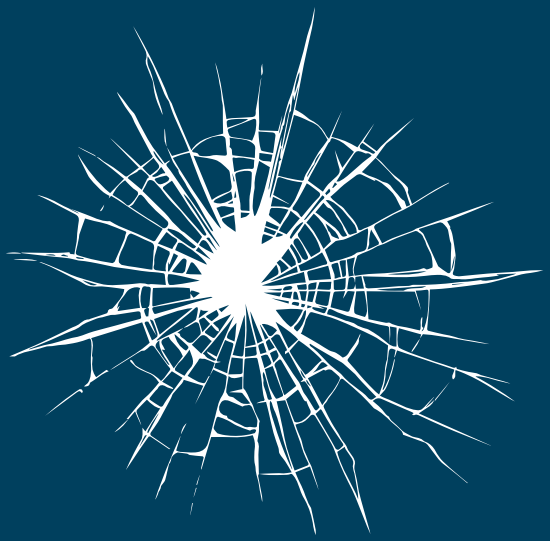
A reduction in road traffic accidents equates to significant savings on expenses and resources utilised as the result of an accident. In the UK it is estimated that a significant reduction in accidents could contribute £2 billion of savings to the economy by 2030[3]. The CAV industry, once established, will itself provide further economic growth and significant opportunities for expansion in employment. Within the UK, it is estimated that the total projected economic benefits resulting from the CAV industry could be in excess of £51 billion[4].

Improving air quality, reducing congestion and freeing up city centres

It is anticipated that the introduction of CAV will result in significant societal change. Fewer people may need to purchase cars, with CAV cars taking users from one destination to another, on demand. Smart connected CAV will coordinate with Smart City infrastructure, resulting in few parking spaces being required within city centres, and less congestion, resulting in improved air-quality. In addition, as governments seek ways to reduce petrol driven car ownership, electric CAV developments may appear on the horizon just as society seeks viable alternatives.

Diversity and Inclusion

For many people, physical or mental disabilities prevent them from driving their own vehicles, and can lead to restrictions in lifestyles and self-reliance. For these groups of people, CAV technology can enable the mobility they have hitherto struggled to achieve.



84%

The amount of road accidents that resulted from human error[4]

CAV technology, however, contrary to what the abbreviation implies, is actually made up of two distinct technology areas **(Connected Vehicles and Autonomous Vehicles)** which have the potential to combine to assist or replace humans in the task of driving a vehicle, resulting in intelligent self-driving vehicles that can communicate with each other and surrounding infrastructure.

According to definitions provided by the UK Charity Brake[5], a **Connected Vehicle** is one that is able to share information (or data) with other sources both inside and outside of the vehicle. This could be with other vehicles, with road infrastructure or with any other connected network or device. Connected vehicles are able to communicate with other vehicles or road traffic infrastructure, giving them the ability, for example, to anticipate oncoming traffic in blind spots, to beware of obstacles in the road around a corner, or to be able to avoid congestion ahead.

Autonomous Vehicles are those which employ automated technology to conduct parts of the task of driving. Ultimately, the goal is to create fully automated cars, where no human driver is required.

Connected and Autonomous technologies both depend upon the generation and analysis of massive volumes of data, much of which must be combined, shared or made accessible to each other, or other systems, for CAV vehicles and infrastructure to be fully developed and made operational.

From a security perspective, this explosion of new technology, connectivity and data results in a significant expansion of the attack surface which presents new opportunities and approaches through which vehicles can be compromised. No longer do attackers need to rod the door or smash a window to get access to a vehicle – in a digital world, the technology can potentially be manipulated to gain access, both locally and remotely.

In the following pages, we will review some of the fundamental aspects of Connected and Autonomous Vehicles, looking into what the terms Connected Vehicle and Autonomous Vehicle really mean.

We will then consider the likely evolution of the threat landscape, with a particular focus on data which is generated and communicated and how that can be exploited.

Connected Vehicles

Connectivity enables the flow of data between systems and networks. The level of connectivity in vehicles is rising exponentially as we demand more data for:

- **Predictive maintenance:** Replacing components and consumables before they wear, to improve safety and reliability, and reduce maintenance and service costs (e.g. AA Car Genie and Otonomo).
- **Insurance:** Assessing risk and dynamically adjusting premiums around driver behaviours and usage, creating new insurance models and more competitive pricing tailored to individual needs.
- **Passenger information:** Real-time traffic information providing updates on journey times and re-routing options; hyperlocal-weather information for destinations or rest-stops; infotainment services to consume audio or video services en route or other applications typically used via smartphones.
- **Fleet management:** Allowing businesses to manage investment, efficiency, productivity, maintenance and asset tracking through real-time tracking and access to in-vehicle sensor data.
- **Convenience and comfort:** Improving user experience through Keyless Entry Systems (KES) (such as Apple CarKey to open new BMWs from smart devices)[6].

Today, modern vehicles roll off production lines with integrated connected systems that deliver most of the above functionality through a combination of: cellular connections; in-vehicle Wi-Fi; Keyless Entry Systems (KES); USB; Bluetooth; Tyre Pressure Monitoring Systems (TPMS); DAB; Electric Vehicle (EV) charging, and so on. Some older and modern but non-connected cars have a degree of connectivity through aftermarket upgrades such as devices that plug into On-Board Diagnostic (OBD) ports (which is what we see with most insurance telematics systems), or by replacing infotainment systems or head units. Once installed, these devices can be accessed remotely and can act as a gateway to connect the outside world to the vehicle's network.

Consumer demand for ever more data and connectivity has accelerated adoption by vehicle manufacturers. This has subsequently led to an uncontrolled increase in a typical vehicle's attack surface. The long history of automobile development has so far been characterised by a steady evolution of mechanical parts. As the integration of connectivity has progressed, these known and trusted components began to be monitored or controlled by electronic systems. Now these electronic systems run embedded operating systems, and drivers interact with them in various ways on a daily basis. This has led to today's modern car - a system of interconnected sub-systems, with over 100 Engine Control Units (ECUs) controlling various vehicle components tied together over one or more Controller Area Networks (CANs) for connectivity.

With this explosion of new connectivity, motivated threat actors no longer need to depend on physical attacks on vehicles. For example, car thieves are now using Software Defined Radios (SDR) to exploit weaknesses in KES, launching man-in-the-middle or replay attacks to remotely unlock vehicles. Many attacks on connected vehicles have been disclosed by researchers, who have demonstrated how simple it can be to recreate attacks on production vehicles. Some notable examples are listed in Appendix A.

Autonomous Vehicles

Key to autonomous vehicles becoming a reality is the enactment of a successful transfer of responsibility and decision making from a human to a machine. This itself is also dependent upon the successful deployment of connectivity to make machine-based decisions without feedback or decisions from humans. It is hoped that if done successfully, eliminating human error from the driving process will deliver significant safety benefits, as well as significant mobility opportunities for disabled and aging populations.

The automation of vehicles generates security concerns for future vehicles. These include:

- **Integrity of Artificial Intelligence (AI) and Machine Learning (ML) algorithms:** integrity is a cornerstone to trustworthiness. Solutions that utilise AI or ML must be able to demonstrate that they continue to operate correctly. Attackers may choose to manipulate these algorithms to gain advantage (e.g. skip a red light, drive faster, drive in a bus lane) or for more sinister means (e.g. to cause a collision).
- **Sensor dependency:** an attacker may compromise one or more of the vehicle's sensory systems to influence its behaviour. An attacker may supress signals (jam or otherwise cause a Denial-of-Service (DoS)) across the wireless medium or manipulate signals into the sensor (e.g. by spoofing an Emergency Vehicle warning signal such that vehicles ahead clear the lane, or by tampering with physical signage such that the sensor will detect an incorrect condition/command). Alternatively an attacker may compromise the object/target e.g. physical road sign, deceiving the vehicle and causing it to misread the sign – as per the attack on the Tesla Mobileye EyeQ 3 camera[7].

CAV Complexity

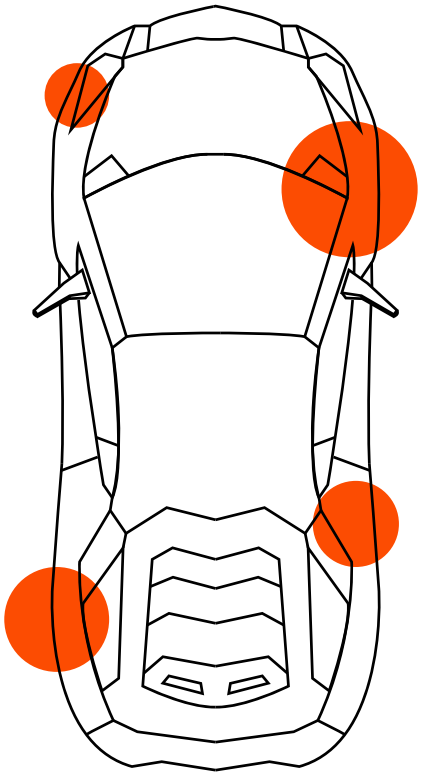
Today's modern car is effectively an IoT ecosystem of its own. It is a system of interconnected sub-systems, with over 100 ECUs and over 150 million Lines of Code (LoC), though NXP[8] predict that by 2025 a modern vehicle is likely to contain over 600 million Lines of Code. Using LoC as a yardstick to measure complexity, this has been suggested as being more code than a Boeing 787 (6.5 million), Facebook (62 million), and a large hadron collider (50 million), but less than the combination of all Google's Internet services (2 billion).[9]

Intel predicts that the first autonomous vehicle will process 4,000GB of data a day[10]:

- Cameras 20-40MB per second
- RADAR 10-100KB per second
- SONAR 10-100KB per second
- GPS 50KB per second
- LIDAR 10-70MB per second

These estimates are just for one vehicle. This could scale to a potential of 300m+ vehicles – the number in circulation today[11].

When it comes to engineering the modern vehicle, manufacturers are effectively system integrators. ECUs are produced by the diverse supply chain and supplied as black boxes to the manufacturer. Detecting normal behaviour, system integrity, malformed data, enforcing access, patching and so on is a complex problem which is only going to become more difficult as more technology is deployed. This complexity introduces a vast attack surface for an attacker to select from, with a high probability of unknown and unpatched vulnerabilities to exploit, or simply out of date software or operating systems in one of the many ECUs.



300

The amount of vulnerabilities found in over 40 ECUs developed by Tier-1 companies and OEMs in 2020[12]

Ecosystems required to support CAVs

At the centre of the connected vehicle ecosystem, we have the vehicle itself. However, supporting the vehicle is a much wider ecosystem, compromising of:

Roadside infrastructure
Devices that will eventually replace fixed gantry signs and signals, delivering in-vehicle information or systems that act as relays/edge processors for assisting with hyperlocal-traffic and safety events. An example here enables the merging of vehicles from slip roads onto motorways, ensuring that vehicles find gaps to maximise road-space utilisation.

Mobile network operators
Cellular service providers of 5G (and beyond) communication to the vehicles. These service providers are likely to play a significant role in the underlying trust model ensuring that safety related data can reach the vehicle (availability) and possibly even for supporting authentication and integrity of messaging. Much of the standardisation for inter-vehicle messaging is still in development, therefore the responsibility for misbehaviour management and management of cryptographic revocation lists and so on is unclear.

Back office systems
The infotainment/in-vehicle market is likely to shift significantly towards a more driverless world, bringing in new services as well as a range of opportunities for improved routing; diagnostics, preventative maintenance and asset management. There will be a number of back office services supporting vehicles, much like the application ecosystems that revolve around smart devices. Increasing dependency on these services could increase the impact of security incidents affecting back office systems, such as the attack on Toll Group, an Australian transportation fleet that was hit with a ransomware attack for the second time in 2020, affecting 1,000 servers and 40,000 employees[13].

We often talk about security being only as strong as the weakest link, which is an important consideration for such a large, diverse and rapidly evolving connected car ecosystem. Successful mitigation will need to span the entire ecosystem and not just the vehicle itself.

Most industry predictions point to 2040 as the peak of Autonomous Vehicles sales, with an estimated 33 million Autonomous Vehicles being sold annually.[14]

As new technology continues to develop, there is significant debate over terminology, and many of the security concerns discussed so far are dependent on the definition of an autonomous system. This is discussed in the next section.

Classification of automation levels

The road to full automation of vehicles is not binary, and will not happen overnight. The Society for Automotive Engineers (SAE) has neatly defined an industry-recognised scale for automotive automation. It is a six-point scale ranging from 0-5, as seen in Figure 2. As technology and regulation advances, the capability of vehicles, and those permitted to operate on public highways, may advance from one level to another, until ultimately, fully autonomous vehicles are achieved and permitted.

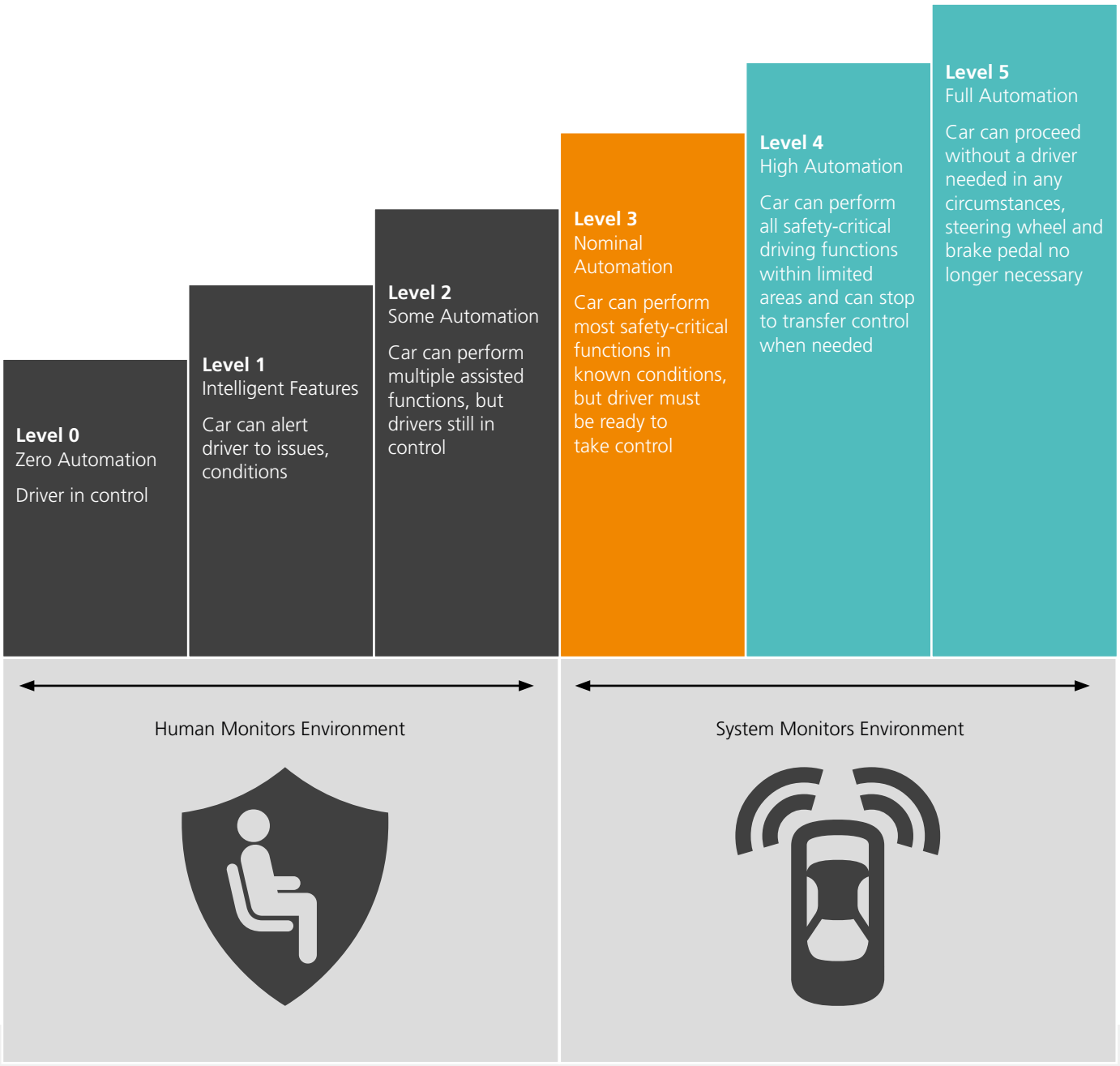


Figure 1
The Society for Automotive Engineers (SAE) scale for automotive automation[15]

The levels in the SAE's automotive automation scale are described below.

Level 0-2
Hands on, eyes open

Humans monitor the environment and make decisions. As far as consumer-ready, mass-market vehicles are concerned, Level 2 is where we are today. We are supported by a degree of assistance or automation, for example Cooperative-Adaptive Cruise Control working with Lane Departure Warnings to avoid longitudinal and latitudinal collisions. Tesla's Autopilot - a suite of advanced driver-assistance system features[16] - is an example of Level 2 automation, since legally, you need to keep your hand on the steering wheel at all times.

We are likely to see a range of threats emerging here that target the individual driving the vehicle as well as the system. There is an interesting convergence between security, safety and human factors such that an attacker could look to manipulate user behaviour or create a distraction. Some potential examples include: spoofing the current legal road speed limit; manipulating the speedometer to suggest the vehicle is travelling faster/slower than its current moving speed, adjusting audio volume; injecting a new destination into the navigation system; adjusting the volume of the stereo, or spoofing data into other vehicle sensors.

Level 3
Hands off, eyes open

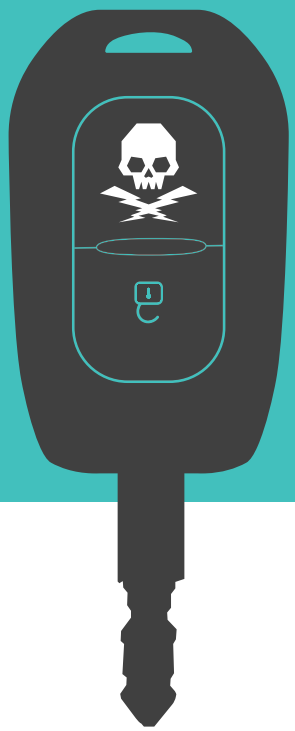
This is generally considered as the level at which 'things get interesting'. At Level 3, the vehicle monitors the environment but when it detects a situation it can't read, such as in severe weather or in response to an abnormal event, it hands back control to the user. The crossover stage between humans and machines is very complex and difficult to do safely, due to cognitive response time and haptic feedback. Responding to an event after being out of the loop for a few minutes has been proven to be very dangerous in a number of studies[17]. For this reason, vehicle manufacturers have generally opted out of investment in this area and the small number that are left have defined clear boundaries/use cases on the condition when to use automation with human fall-back. A recent example of this is Audi's Traffic Jam Pilot, which was due to debut in its flagship A8 this year, but was scrapped due to legal and liability issues that would have seen Audi (not the driver) responsible for an incident when functionality engaged.[18]

Level 4-5
Hands off, eyes off

This is where the vehicle is in total control of all decisions when in operation. Investment is high in this area, with the race on between the main competitors: Tesla, Uber, Waymo and Apple, to see who can achieve full driverless capability first.

Today, this technology is still in the testing phase. There is very little evidence and insight into the maturity and readiness of driverless vehicles available at the moment due in large part to the competition in the marketplace, with limited collaboration between manufacturers and wider industry and regulators.

As we enter Levels 4+, a further shift in security concerns and attacker motivation is likely. We are likely to see more direct attacks on sensory systems to influence the vehicle's behaviour or the collective behaviour of many vehicles driving together, such as platooned vehicles. The Department for Transport recently trialled a platoon of semi-autonomous HGVs on Britain's roads[19], virtually bridging three freight vehicles to behave as one extended entity. In this scenario we may see non-autonomous vehicles preventing or breaking convoys either deliberately to 'bully' the autonomous system, or accidentally as the driver attempts to exit the motorway at a junction. We may also see increased use of autonomous vehicles by criminals, e.g. for the transportation of illicit goods.



Section 2

Security analysis for CAV threats

Attacker objectives and motivations

This section describes some of the attacker motivations and potential consequences in the area of Connected and Autonomous Vehicles.

Remotely control a vehicle

Researchers have successfully demonstrated that it is possible to hack production vehicles from remote locations[2] - allowing the attacker to take control of radio, windows and even brakes, acceleration and steering. There are many variations on this but the attack follows a similar pattern: an attacker exploits a vulnerability in a cellular system and lands on the vehicle's infotainment system. As the infotainment systems in most vehicles provide the driver with information such as service schedules, tyre pressure and oil levels, there is a necessary connection between the infotainment system and the Controller Area Network (CAN) within the main vehicle network that connects all the ECUs together. It is therefore possible in many vehicles to pivot from the infotainment system to the CAN bus and inject commands, spoofing signals that would appear to be coming from, for example, the braking system ECU or the steering system.

As security researchers found in the widely-discussed Jeep Cherokee research[2], a Renesas V850ES/FJ3 chip sits between the CAN bus and the head unit. It is configured to be read-only, receiving vehicle data from the CAN in order to inform the driver of current maintenance status, diagnostics and faults. The researchers studied and reverse engineered the V850 firmware, re-configured it to allow read/write permissions, to learn the CAN message sets and then successfully performed a firmware update. Like with most vulnerabilities, it took a few security researchers several weeks' worth of effort to develop this capability, but once discovered, it could be weaponised and packaged into penetration testing tools.

There is of course variation in implementation and configuration between vehicle manufacturers, but there are three common weaknesses to all designs that are relevant to this attack objective. These are:

- No method for verifying integrity and authenticity of firmware and software
- A lack of boundary control/filtering of data flows
- No device or message authentication[20].

Disable the vehicle

There are several ways an attacker could successfully disable the vehicle. One option would be to exploit smart device/convenience applications that tend to provide functions such as turning on lights, opening and closing windows and turning on Air Conditioning, each of which would allow an attacker to drain the car's battery. Vulnerabilities have been found in a number of these applications, particularly with the authentication process. For example, Nissan launched a convenience app allowing access to the vehicle to access data such as current charge level and range, as well as to enable climate control in advance of the journey and other features. When pairing the smart device to the vehicle, the only authentication details required was the Vehicle Identification Number (VIN). The VIN is generally located at the bottom corner of the windshield, visible from the exterior[21].

Another way to achieve this objective would be to take remote control of the vehicle, as described in the Jeep example above. Alternatively, an attacker could craft and deploy malware such as ransomware to disrupt the vehicle. There is no documented ransomware attack on a vehicle - yet - though as most ECUs are embedded devices running mostly unpatched or outdated operating systems, this is a plausible scenario. Such an infection could in theory come from any of the ports and protocols listed in the above, or from diagnostics equipment used at garages, or aftersales devices such as telematics control units.

Remotely unlock a vehicle/theft

Unlocking the vehicle is one of the simplest and most common attacks on vehicles today, with the Association of British Insurers (ABI) reporting 16,000 claims in the quarter leading up to May 2019, equating to £108 million or £1.2 million a day[22]. Attackers are using cheap and accessible technology such as SDRs to exploit known weaknesses in Keyless Entry Systems. In August 2020, researchers found 19 vulnerabilities in the Mercedes-Benz E-Class which could enable attackers to remotely unlock the car door and start its engine[23]. By January 6th 2020, 4118 thefts were reported in India from cheap electronic devices that enabled the thieves to bypass the engine control module, unlock the vehicle, start the engine, and access the vehicles' computer[24].

It is common for vehicle manufacturers to use symmetric keys between the key fob, entry system and ignition keys. An attacker can compromise the symmetric key either through a brute force or man-in-the-middle attack by sniffing the radio frequency between the key fob and the entry system, and then replaying it against the target vehicle. Equipment affordability (~£200) and open source software, including resources hosted on Github[25], means that it is a relatively simple attack to recreate with limited knowledge or capability.

This problem is likely far greater. Many leading auto manufacturers use the same master cryptographic key for all vehicles within a particular model line - the majority of VW Group vehicles have been secured with only a few master cryptographic keys that have been used worldwide over a period of almost 20 years[26].

Create a safety condition

An attack on a vehicle could deliberately or accidentally create a safety hazard for the occupants of the vehicle. These attacks may be indirect, such as distracting the driver with warning messages and adjusting the volume of the infotainment unit, or direct, such as adjusting throttle position or steering position when the vehicle is in motion. The Lexus OTA update failure discussed in the Connectivity ≠ Automation section is an example of such an attack. More recently a Mobileye 630 PRO and Tesla Model X hack fooled the ADAS and autopilot systems to trigger the brakes and steer into oncoming traffic, when an attacker spoofed phantom objects in the path of the vehicle[27]. As we become dependent on accurate and timely in-vehicle safety messaging for things like traffic jams; emergency stop; roadworks or broken down vehicles, it will impact our driving behaviour and over-dependency could lead to greater consequences from DoS attacks.

Track or monitor the vehicle

The modern vehicle holds and has an increasing potential to hold a great deal of personal data. Already, location, destinations/journeys, travel times, driving style/behaviour, contacts, messages, music preferences and even web-browsing activity is often captured. Increasing use of cameras for monitoring inside and outside the vehicle, as well as microphones for voice control and hands-free, creates opportunities for attackers to spy on the occupants to extract rich pattern-of-life data.

Use the vehicle as a weapon

The most sinister attackers may look to remotely control a vehicle to drive into a crowd of people, in a similar fashion to terrorist attacks already seen in Nice, Berlin, and other cities[28]. Autonomous Vehicles could potentially enable this style of attack to be executed remotely and at scale.

Malware

In addition to a ransomware attack described above, other forms of malware could be used to create botnets for cryptojacking or for launching Distributed Denial-of-Service (DDoS) attacks, leveraging the vast amount of computing power held within the 100+ ECUs. At its peak in September 2016, the IoT botnet 'Mirai' temporarily crippled several high-profile services such as OVH (one of the largest web hosting providers in the world) and Dyn (a popular DNS provider) via a large scale DDoS attack. OVH reported that these attacks exceeded 1 Tbps—the largest on public record. The Dyn attack took down a number of high profile web services including AirBnB, Amazon, Github, HBO, Netflix, Paypal, Reddit, and Twitter. These attacks were carried out via small, innocuous Internet-of-Things (IoT) devices like home routers, air-quality monitors, and personal surveillance cameras. At its peak, Mirai infected over 600,000 vulnerable IoT devices[29].

Distribution of illicit goods

Autonomous vehicles by their nature do not require a driver or any passenger to travel around a road network, so the transportation of illicit goods can be considerably de-risked. This is a similar concept to the use of drones for the transportation of drugs, particularly into secure locations like prisons[30].

Attack vectors

An attack vector is the path that an attacker takes to gain access to its target. In this section we look at the attack vectors which attackers may use to compromise and gain control or influence over a CAV. In previous sections we've discussed the ever increasing level of connectivity within the vehicle. Figure 2 shows the most common communication systems which may be utilised as an attack vector, and these are further analysed in the table on the following page.

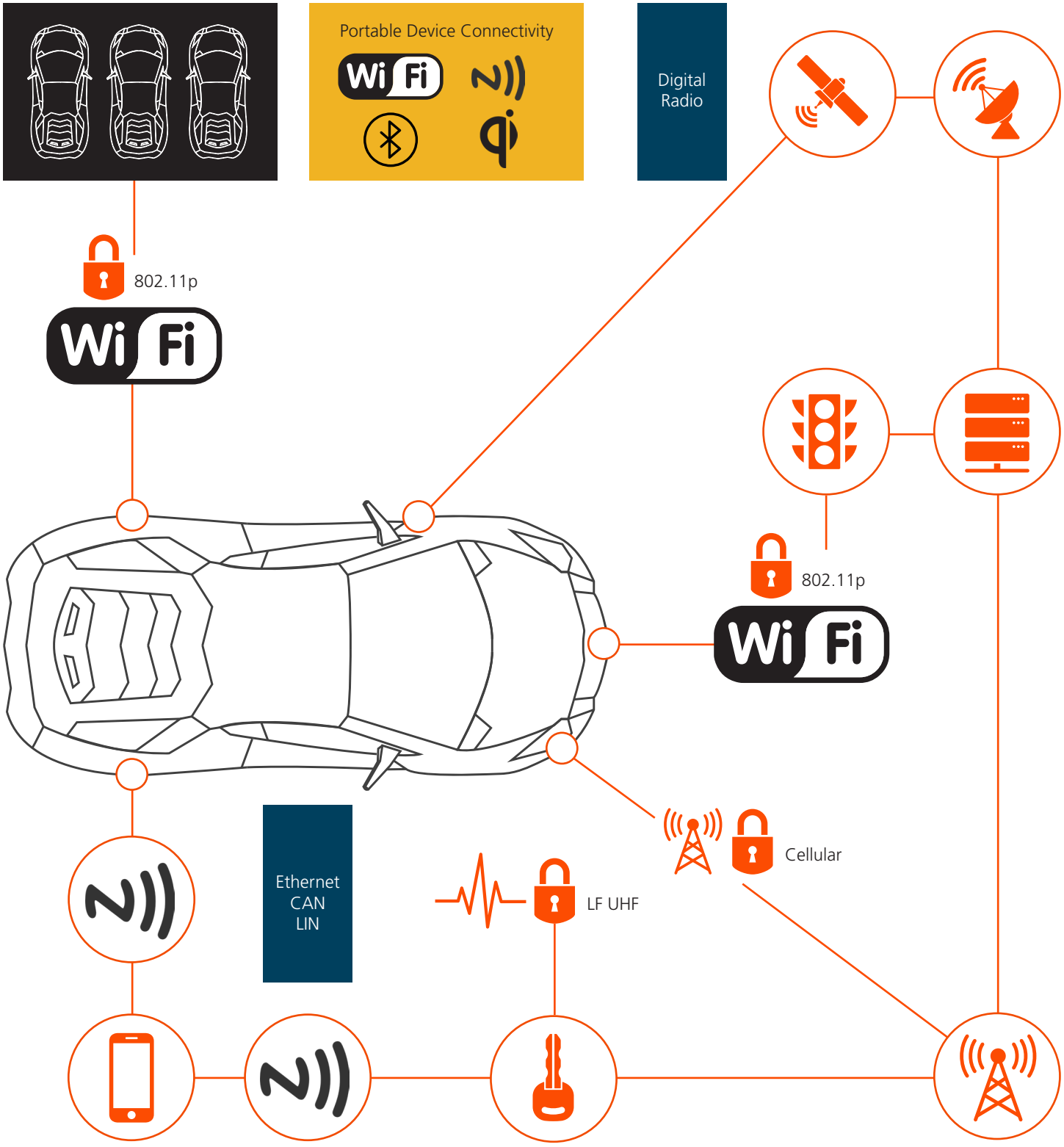


Figure 2
A model connected car and its links – adapted from NXP's vision of the connected car[31]

	CAV Attack Vector	Description
	Cellular	Most vehicles now come with embedded SIMs, supporting European initiatives for eCall services (for rapid assistance to motorists involved in collisions) or for infotainment or fleet management services. Vehicles are now publically addressable from anywhere in the world.
	Personal Area Networks	Some vehicle manufacturers have already deployed local Wi-Fi hotspots in vehicles for passenger use. Wi-Fi is a soft target for many attackers with many authentication weaknesses from poorly implemented cryptographic controls. Bluetooth is used extensively for media and telephone functionality which has also had cryptographic weaknesses in authentication[32]. There is also an emergence of Near Field Communication (NFC), particularly for fleet management for new rental models and car sharing schemes.
	Keyless Entry Systems (KES)	Even the most luxurious cars on the market are notoriously susceptible to cryptographic weaknesses in Keyed and Keyless Entry Systems used for opening, closing and enabling the vehicle. Vehicles can be stolen in minutes using accessible technology that costs less than £100. After-market systems such as Autowatch Ghost 2[33] often invalidate vehicle warranties which discourage owners from installing these devices.
	Vehicle to Anything (V2X)	Most vehicles now come with embedded SIMs, supporting European initiatives for eCall services (for rapid assistance to motorists involved in collisions) or for infotainment or fleet management services. Vehicles are now publically addressable from anywhere in the world.
	Controller Area Network (CAN)	The CAN is a high speed bus that facilitates communication between vehicle ECUs, standardised in the 1990s. Modern vehicles still use one or two CANs (for fault tolerance or for prioritising critical messages). Communication across the CAN is in clear-text with no device or message level authentication. It is internal facing, but largely accessible by pivoting from external systems, with little to no network segregation.
	Tyre Pressure Monitoring System (TPMS)	The TPMS sensor located in the tyre pressure valve or rim of the wheel sends messages to an ECU, which monitors for safety conditions like a sudden loss of pressure. These messages are sent over an UHF radio frequency, in an unlicensed band and are unauthenticated signals. TPMS identifiers are 32 bit unique identifiers. Researchers have successfully managed to demonstrate how vehicles can be tracked from eavesdropping on the communication link from around 40m away – which introduces privacy concerns.[34] More so, as these messages are unauthenticated and unencrypted, an attacker could eavesdrop a TPMS signal, uncover its unique identifier and relay malicious signals pretending to be the TPMS sensor. This attack could cause the vehicle to alert the driver to a safety warning that may disrupt the driver's journey to inspect/replace the tyre.

Conclusions and outlooks

Connectivity has made global access to the vehicle possible through publically addressable cellular systems. The incidents described in this report demonstrate that there is a porous, IP-enabled outer shell that can give way to the soft underbelly of bespoke, proprietary and inherently vulnerable legacy systems that control the mechanical working of the vehicle. Security events are likely to result in safety consequences, driving increased convergence between two previously disparate disciplines. This necessitates and creates a market for new skills, research, standards, and solutions to deal with a disruptive shift in a mature discipline like safety.

Looking to the future, security and safety concerns may at some point lead to threats to CAV being considered a National Defence Issue, where threats and risks arising from 3rd parties becoming capable of managing driverless vehicle and turning it into a weapon, or from being able to take control of whole fleets of CAV connected vehicles, dictate a government-led approach to developing future remediation capability.

+£62bn
economic growth

55%
new automative jobs to be higher skilled

+420,000
new jobs

+20,000
new jobs in automation

+3,900
lives saved (2019-30)

+47,000
serious accidents prevented (2019-30)

Figure 3
Society for Motor Manufacturers and Traders predicted benefits to the UK from CAV technology[35]

It is estimated that 1 in every 5 miles travelled by consumers in the UK could be automated by 2030

In the meantime, as we progress through levels of increased automation, the threat landscape will shift several times as we become more dependent upon machine decision-making and shifting responsibility away from the human driver. This technological revolution is likely to have a disruptive effect on the wider ecosystem that will make the threat landscape difficult to predict at this stage. For example, business models are likely to change from ownership to lease to PAYG services. The market forces around this change are likely to impact the wider ecosystem of garages, maintainers, aftersales and other automotive traders. How this unfolds is difficult to ascertain at present, but what's clear is that security needs to be factored in iteratively through the development of products and services to ensure that security maturity keeps pace with technological advancement.

Much has been done in this space by government, industry and academia:

Government
The development of a code of practice to encourage safety and secure trialling of automated vehicles[36], the development of cyber security principles backed up with a Publically Available Standard (PAS) 1885[37] and a number of security-related projects e.g. to develop Europe New Car Assessment Programme (NCAP) safety ratings for security (5StarS)[38].

Vehicle manufacturers
Introduction of bug bounty programmes to encourage ethical disclosure of vulnerabilities[39], supply chain consideration for security architectures for modern vehicles[40]; improved identity and authentication management solution e.g. biometrics[41].

Academia
Research into various aspects of CAV including sensors; 5G; AI; ML and IoT[42] through government-funded projects, pilots and trials.

Development in this space will need to become standardised and universally applied across an entire ecosystem such that there is a common baseline of trust between vehicles, related devices and supporting infrastructure. The vehicle is at the centre of this ecosystem, but we also need to secure more than just the vehicle, including:

- **Roadside infrastructure** for edge processing and low-latency communication of safety messaging
- **Humans that interact with the vehicle -** improving cyber hygiene to limit the likelihood of social-engineering attacks such as phishing
- **Aftermarket and third parties -** data services required for vehicle performance, insurance and infotainment management will be new interfaces that create new threat opportunities.

The way that industry, government and academia work together is critical to the success of future CAV adoption. Zenzic, the organisation dedicated to accelerating the self-driving revolution in the UK by bridging this gap, has recently published a roadmap that identifies security as one of the most challenging key enablers[43].

To achieve the perceived safety, environmental and economic benefits of Connected and Autonomous Vehicles, the industry needs to carefully balance the race to market with security assurance. This is a major challenge in a highly competitive market with little consumer demand for security and with a complex and diverse ecosystem. While much of the Level 3+ automation is still in development, attacks against today's connected cars are credible and proven, though fortunately there are few examples of safety-affecting incidents outside of a handful of controlled demonstrations by researchers. However, we have seen time and time again that threat actors are quick to take advantage of new technology for nefarious means: the extant and potential threats described in this report should therefore be taken seriously.

If you would like to learn more about this topic, or have your own challenges within the CAV or wider Transport market that you may like help with, please contact us.

Appendix A

Recent incidents from 2020:

- Extension of the Keyless Entry Vulnerability, extending to wider vehicle manufacturers: Toyota, Tesla, Hyundai and Kia : https://tches.iacr.org/index.php/TCHES/article/view/8546/8111

- Tesla – Mobileye EyeQ 3 camera exploit - Sensor manipulation: by extending the central vertical bar in a number "3" it's possible to trick the Tesla into thinking the number is an "8" and so the speed limit can be manipulated to breach the speed limit e.g. 35MPH becomes 85MPH (American). https://www.forbes.com/sites/daveywinder/2020/02/19/hackers-made-tesla-cars-autonomously-accelerate-up-to-85-in-a-35-zone/?sh=4b5999837245

- Aftermarket modifications / third party services creating backdoors into vehicles – links to the insider threat (customisation of vehicles)
    - Aftermarket remote start capability, allowing the user to turn on heating and auxiliary services so that it would assist a medical condition affected by freezing cold conditions
    - Allows a user to remotely enable a vehicle over the public Internet – now it's reachable worldwide.
    - Could be used to: locate cars, identify them, unlock them, start the car, trigger the alarm.
    - Details on Vulnerability exploited: https://www.kb.cert.org/vuls/id/174715/

- 4,118 vehicles were stolen in India with cheap electronic devices that enabled the thieves to bypass the engine control module, unlock the vehicle, start the engine, and access the vehicles' computer https://timesofindia.indiatimes.com/city/gurgaon/carjackers-go-hi-tech-use-chinese-gadgets-to-steal/articleshow/73113944.cms

- A Mobileye 630 PRO and Tesla Model X hack fooled the ADAS and autopilot systems to trigger the brakes and steer into oncoming traffic. https://securityaffairs.co/wordpress/96966/hacking/phantom-attacks-adas.html

- Vulnerabilities were found in a Mercedes-Benz E-Class car, allowing hackers to control the vehicle remotely, including opening its doors and starting the engine.

https://vulners.com/threatpost/THREATPOST:50210848F5C0B6804DBF8A398FD41F24

- Toll Group, an Australian transportation fleet, was hit with a ransomware attack for the second time in 2020, affecting 1,000 servers and 40,000 employees

https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/

- More than 300 vulnerabilities were found in over 40 ECUs developed by 10 Tier-1 companies and OEMs

https://autosec.se/year-end-lists/

Examples prior to 2020:

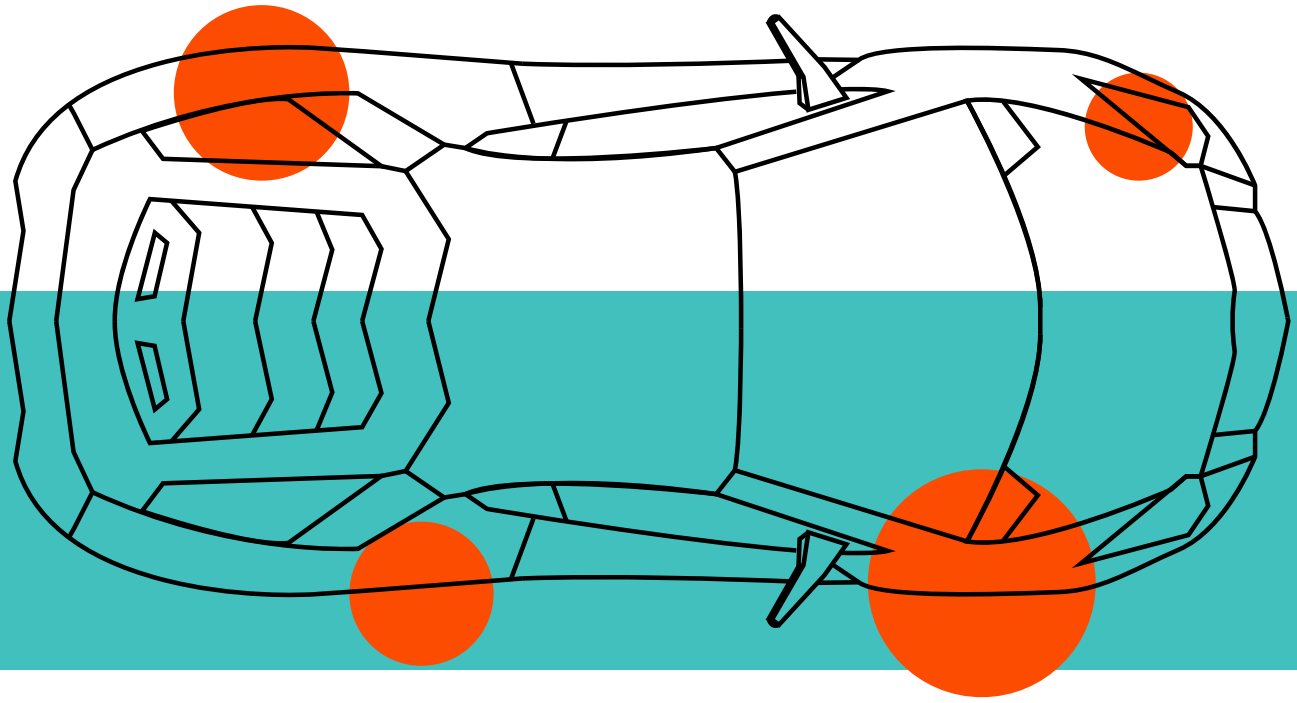
- A group of researchers were able to gain control of a 2014 Jeep Cherokee over a cellular connection, allowing the attacker to adjust air flow through vents; turn on wipers; turn up the radio volume and even cut off the transmission such that the vehicle lost speed and slowed to a crawl. The cellular connection made this vehicle remotely accessible over the Internet, and this attack took place from over 10 miles away.[45]

- In 2015, another group of researchers successfully hacked a vehicle's infotainment system through DAB radio signals - using nothing but off-the-shelf technology. This attack required no prior knowledge or crafted messaging towards a particular vehicle and scaled easily - by sending one stream of data, the attack could reach many cars simultaneously under the disguise of a common radio station.[46]

- The Nissan Leaf application that was launched in 2016 required only the Vehicle Identification Number for authentication. This number - visible through the windscreen of most vehicles - allowed attackers access to app functionality for sounding the horn, flashing lights and accessing other vehicle information.

- In 2018, multiple vulnerabilities were found in the infotainment system of Volkswagen and Audi vehicles that allowed remote access to microphone, navigation systems and speakers.

- Applications and system updates for new or improved functionality to geographically distributed systems has resulted in adoption of Over-The-Air updates. As well as this being another attack vector,[47] it also introduces non-malicious threats. Lexus fell victim to this threat back in 2016 after a software update caused the navigation and infotainment system to enter a constant reboot cycle[48] which, if occurring mid-journey, would have introduced a safety hazard through driver distraction.



References

[1] https://www.who.int/publications/i/item/9789241565684

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643799/self-driving_cars.pdf

[3] https://www.smmt.co.uk/wp-content/uploads/sites/2/CRT036586F-Connected-and-Autonomous-Vehicles-%E2%80%93-The-UK-Economic-Opportu...1.pdf

[4] https://www.smmt.co.uk/wp-content/uploads/sites/2/CRT036586F-Connected-and-Autonomous-Vehicles-%E2%80%93-The-UK-Economic-Opportu...1.pdf

[5] https://www.brake.org.uk/get-involved/take-action/mybrake/knowledge-centre/vehicles/connected-and-autonomous-vehicles#:~:text=Connected%20and%20autonomous%20vehicles%20%28or%20CAVs%29%20combine%20connectivity,and%20remote%20processing%20capabilities%3B%20GPS%20and%20telecommunications%20systems

[6] https://www.bmw.com/en/innovation/bmw-digital-key-iphone-as-secure-bmw-car-key.html

[7] https://www.forbes.com/sites/daveywinder/2020/02/19/hackers-made-tesla-cars-autonomously-accelerate-up-to-85-in-a-35-zone/?sh=4b5999837245

[8] https://www.nxp.com/company/blog/cars-are-made-of-code:BL-CARS-MADE-CODE

[9] https://www.visualcapitalist.com/millions-lines-of-code/

[10] https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/#gs.hcx5x6

[11] https://www.acea.be/statistics/tag/category/vehicles-in-use

[12] https://autosec.se/year-end-lists/

[13] https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/

[14] https://ihsmarkit.com/research-analysis/autonomous-vehicle-sales-to-surpass-33-million-annually-in-2040-enabling-new-autonomous-mobility-in-more-than-26-percent-of-new-car-sales.html

[15] https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles

[16] https://www.tesla.com/support/autopilot

[17] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812043_hf-evaluationlevel2andlevel3automateddrivingconceptsv2.pdf

[18] https://europe.autonews.com/automakers/audi-quits-bid-give-a8-level-3-autonomy

[19] https://www.environmentalengineering.org.uk/news/truck-platooning-trials-begin-uk-5753/

[20] https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

[21] https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[22] https://www.abi.org.uk/news/news-articles/2019/05/gone-in-20-seconds-payouts-every-8-minutes--car-crime-continues-to-rise-in-2019/

[23] https://vulners.com/threatpost/THREATPOST:50210848F5C0B6804DBF8A398FD41F24

[24] https://timesofindia.indiatimes.com/city/gurgaon/carjackers-go-hi-tech-use-chinese-gadgets-to-steal/articleshow/73113944.cms

[25] https://github.com/trishmapow/rf-jam-replay/blob/master/README.md

[26] https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

[27] https://securityaffairs.co/wordpress/96966/hacking/phantom-attacks-adas.html

[28] https://www.telegraph.co.uk/news/2017/10/31/terror-attacks-using-vehicles-feel-like-new-normal-incredibly/

[29] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[30] https://www.bbc.co.uk/news/uk-england-45358876

[31] https://www.electronicspecifier.com/products/design-automation/what-autonomous-driving-technology-is-now-available

[32] See TI_20114_TF_Threats_to_Wireless_Networks

[33] https://autowatch.co.uk/veh-sec/ghost-2-menu

[34] https://www.schneier.com/blog/archives/2016/09/hacking_wireles.html

[35] https://www.smmt.co.uk/reports/connected-and-autonomous-vehicles-the-global-race-to-market/

[36] https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CONNECTED-REPORT-2019.pdf

[37] https://www.gov.uk/government/consultations/automated-vehicle-trialling-code-of-practice-invitation-to-comment

[38] https://shop.bsigroup.com/ProductDetail?pid=000000000030365446

[39] https://gtr.ukri.org/projects?ref=103284

[40] https://www.bugcrowd.com/solutions/automotive-security/

[41] https://www.nxp.com/applications/automotive/functional-safety-and-automotive-security/secure-vehicle-architecture:AUTOMOTIVE-SECURITY

[42] https://www.biometricupdate.com/201911/new-vehicles-with-biometrics-features-coming-as-auto-access-control-market-grows

[43] https://www.theengineer.co.uk/uk-cav-security-driverless/

[44] https://zenzic.io/news/uk-connected-and-automated-mobility-roadmap-to-2030-shows-cyber-security-is-critical-for-self-driving-vehicles-to-be-on-uk-roads/

[45] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[46] https://www.bbc.co.uk/news/technology-33622298

[47] See TI_19120_TF_Firmware_Over-The-Air_Updates

[48] https://www.theguardian.com/technology/2016/jun/08/lexus-navigation-entertainment-software-update-bug

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 87,800 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra
ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/government

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai