The Institution of Engineering and Technology

KTN the Knowledge Transfer Network

# **Automotive** Cyber Security:

## An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles







**Transport**

**Information & Communications**

www.**theiet**.org/cyber-security

www.**ktn-uk**.co.uk

# Contents



Images courtesy of iStock. The library images used in this Review appear as generic illustration only, and do not denote or refer to specific types of technology.

Safety first: one compelling reason to connect cars via wireless links is to reduce the risks of collision on the road

# Executive summary

Connected vehicles take us toward a mode of transport that is safer and more efficient, by enabling an interconnected driving experience. One way cars are interconnecting is via the Internet, but there is concern that this could expose connected cars – and the people in them – to potential risks from online threats. This Briefing surveys issues related to this concern, but prescriptions for remedial solutions are not part of its scope.

This Review focuses on the areas of automotive cyber security that, at this stage in their development, are receiving attention. Research undertaken to identify possible automotive cyber security vulnerabilities are highlighted, how automotive OEMs seem to be responding to the claims that cars can be 'hacked', along with examples of media coverage of some of the issues. It looks at some of the motivating factors that might make connected vehicles and their workings attractive to malevolent actors, and where some of the responsibilities and liabilities for countering threats may ultimately be assumed, ranging from automotive OEMs to car users themselves. The document also scopes some Recommendations for further debate.

In brief, these Recommendations encourage consultation between the automotive industry bodies for which cyber security should be an agenda issue and professional bodies in non-automotive sectors already engaged in cyber security awareness-raising; the development of guidelines for issues around professional disciplines with an interest in automotive cyber security and autonomous vehicles; and extended thought leadership into the areas of connected vehicle driver responsibility, and issues around liabilities related to automotive cyber security incidents.

# Background to this Review

This Review is based, in part, on inputs from the Automotive Cyber Security Thought Leadership event (November 2014) attended by more than 50 experts from a range of engineering and technical disciplines. It has been further extended by additional input from the project managers, and by supporting supplementary information and references from external sources. This joint initiative by the Institution of Engineering and Technology (IET) and Knowledge Transfer Network aims to promote cross-industry debate on a topic that has the potential to impact a broad range of professional fields.

It is a topic that stems from the convergence between automotive technology and computer technology: this has increasingly changed the methods by which motor vehicles are developed and are driven. The automotive industry makes extensive use of computers and computerised electronics in the design, production, and operation of vehicles. Within vehicles, sensors, actuators, embedded computers, and audio-visual systems are used to enhance safety, performance, and the driver/passenger travelling experience.

Other industry bodies and interest groups are starting to take an interest in the automotive cyber security issue, as is the media. Professional bodies such as the IET and Knowledge Transfer Network can bring balance to this interest by providing an independent and widely-informed perspective to the topic as events unfold.

# Introduction

It is confidently presumed that new cars travelling future highways will be connected. Powerful communications capabilities will be built-in to automotive systems designed to facilitate a variety of driving functions and other enhanced features. Internal control systems will exchange data via complex internal networks; other applications that interface with drivers through dashboard displays and devices could share information with other connected vehicles; they could also exchange data with connected roadside entities, such as streetlights, that are also linked-in to the Internet of Things (IoT).

The one- and two-way electronic communications systems that road vehicles have increasingly been equipped with over recent decades, such as radio receivers and transmitters, have been augmented by links to cellular voice/data devices and to satellite signals. In-vehicle infotainment networks, and the notion of 'car-as-hot-spot', have been introduced by automotive OEMs (original equipment manufacturers) variously in recent years. These typically co-exist with the automotive control networks that enable the transit and exchange of data relating to the operation of the vehicle itself.

The gaps between the computer technology built-in to vehicles, and computer technology taken into vehicles, is narrowing

Coming generations of connected cars will differ as a result of moves toward greater convergence between automotive communications technology and connections to resources beyond the confines of the car. This prospect of a motor vehicle becoming, in effect, an Internet-linked 'device' is bound to stir debate in a world where awareness of online threats, and the malicious 'hacking' of computer systems, could affect the use of almost any physical entity that qualifies as a 'connected device'.

Cyber security is a much-debated aspect of the emerging Internet of Things, especially given malicious agents' tendency to 'follow the market opportunity': as they become more numerous, connected cars would likely represent another addition to the cyber-attackers' expanding hit-list of prospective targets. This may sound conjectural, but some automotive OEMs have acknowledged that they are taking the possibility seriously – and taking steps to defend 'vehicle computer systems' against it.[1]

The importance of identifying potential 'vulnerabilities' – flaws in a connected car's communications and data systems that could be exploited by somebody seeking to 'hack' into that vehicle's control mechanisms or other onboard technology – and protecting such vehicles against interference or attack, has stepped-up in the last five years, as online menaces have become potentially more hazardous – and more penetrative. Some users are becoming accustomed to the practice of protecting their 'endpoint devices'; but nowadays the very communications infrastructures that form the 'backbone' of our hard-wired and wireless networks regularly come under attack. This has created yet another 'field of battle' to be defended, as national Internet exchanges, for instance, and the internetworking equipment they rely on – such as switches and routers – are maliciously probed.[2]

# Terminology

When starting to consider the broad issues necessary for an understanding of cyber security in the automotive sector there can be a tendency to draw comparisons with what might be termed the 'mainstream' cyber security market, where the protection of personal computing devices, enterprise information and communications technology (ICT) systems, and industrial control systems (ICSs), most notably, has escalated into a matter for national concern over the last 15+ years.[3]

A range of cyber security issues are regularly discussed using technical terms whose meanings will not only be unfamiliar to many within the automotive sector, but also hold different meanings to those working within the cyber security market itself. The very words 'cyber' and 'security' may have very different connotations for automotive engineers, for instance, where 'security' is also used in the context of a vehicle's physical security – i.e., its locks and other anti-theft disabling mechanisms.

An example of potential for cross-purpose confusion between audiences, is the falsely-applied, usually pejorative, use of the term 'hack'. In computer programming the term describes an amendment to code intended to fix an error or tweak an effect for a specific purpose. The term is an ethically-neutral, if rather crude, descriptor of a quick fix or tune-up. Perhaps not appreciated in mainstream coverage is that the everyday usefulness of the term has migrated across to any part of life – from re-imagining Lego designs, and adapting Ikea furniture, to getting more power output from an old car model. The issue at hand intersects, however, where hacking is performed remotely and without permission. Both must apply. It can be imagined that such hacking-in to with permission may also be a healthy and productive pastime, but would likely be a minority to pursuit. Exactly what is meant by 'permission' is important. It goes to show that discussions of cyber security and automotive electronics must be mindful of the pitfalls caused by imprecise vocabulary.

However, it is also worth noting that automotive cyber security does present issues that are specific to that industrial sector, and attempts to make comparisons between the mainstream concept of 'cyber security', and the concept as it will affect the road vehicle market, should be drawn with caution.

Many car owners increasing rely on connected technology-based driving aids: they would be lost without them

There could be many possible reasons why somebody would want to 'hack' in to a connected car: owners themselves might want to 'tweak' their vehicle's performance

Another example of this from enterprise information security is the notion of 'insider threat' – individuals working within an information technology system, for instance, who gain unauthorised access to data assets for nefarious or idiosyncratic reasons. Connected cars may also have owners who, for reasons known and unknown, will attempt to reconfigure their car's data systems. (The author of a freely-available online publication called *The Car Hackers Handbook* suggests that owner-access to their vehicle's inner workings is necessary in order for them to personally validate the security of their vehicles.[4])

There is, of course, an established 'after-market' catering to automotive customisation: this has been mainly for physical modifications like spoilers, 'growly' exhausts, and 'nitro-boost' kits; but there are also those who will 'tweak' electronic control units (ECUs) to enhance performance or power output. An increase in the amount of vehicular systems software calls for ever-tighter requirements to prevent (or at least detect) attempts to tamper with it in the event, say, of a warranty or insurance claim. Arguably, this is, in effect, a cyber security issue when viewed in terms of the Parkerian Hexad elements of information security related to authenticity and integrity*; it also has functional safety implications. The general issue of connected vehicle owner responsibilities in the context of cyber security will be returned to later in this Briefing.

Meanwhile, it is reasonable to remind ourselves that, as with 'mainstream cyber security', two facts will crop-up. First, no connected computer system is 100 per cent guaranteed secure in terms of invulnerability or the integrity of the data it holds or processes, and the owners of targeted systems must be ever-vigilant for as-yet unknown threats and undetected vulnerabilities to emerge at some future time. Second, given the history of more conventional cyber security, it is reasonable to hypothesise that some kind of 'arms race' between the automotive OEMs and their cyber foes will establish itself, as each side seeks to outdo the other's efforts to secure/*un*-secure the cars, vans and lorries that use our highways.

* The Parkerian Hexad is a six-element checklist of standard information security attributes – Confidentiality, Possession/Control, Integrity, Autheticity, Availability, and Utility – proposed by Donn B. Parker in 1998.

# Connected car trends

Connectivity is set to become a compelling feature of the global car market over the next five years, leading to a market worth €39 billion by 2018, according to forecasts from research firm SBD and mobile industry body the GSMA.[5] In general terms, a connected car is a road vehicle equipped with three sets of communications systems: Internet access, and (usually) also an internal network, usually wireless, which enables the car to route its connection access (sometimes known as vehicle-to-Internet, or V2I) to other devices that are installed inside – and possibly outside – of the vehicle. Alongside these typically there is the CAN bus (or similar) used to interconnect the gamut of ECUs, sensors and actuators that now form part of a vehicle's inner electronic workings. Increasingly, such cars are fitted with specific technologies that link into the Internet access or internal network to provide additional driver benefits: automatic notification of collisions, notification of excessive speeding, and other safety alerts, for example.

There are two additional communications types that could supplement these. The more mature of these is vehicle-to-vehicle (V2V) technology that enables cars to communicate wirelessly and even maintain temporary networks between vehicles that can inform accident prevention, road hazards, and other driving intelligence. A number of automotive OEMs are reported to be developing V2V capabilities. The connected vehicle is also poised to become a bona fide part of the Internet of Things (abbreviated to Vehicle-to-IoT or V2IoT), as a connected entity receiving data from external sources, and sharing data that it captures with remote third-parties for specific applications (traffic flow updates, say). The IoT is an evolving concept, and several aspects of the role of motor vehicles within it are yet to be determined. Connected cars driving in 'smart' built environments – as to be found in 'Smart City' ventures now emerging around the world, and being 'retro-fitted' into many existing metropolitan areas – will be able to take advantage of the infrastructure that is gradually assembling to target and support connected road (and indeed human) traffic. It is important to note that the possibility of cyber-attacks on the wireless communications networks that support connected vehicles should count as another factor in the assessment of automotive cyber security factors. These networks must be secured against signal jamming (devices that do this are cheap and easily obtainable)[6], denial of service attacks, and the transmission of bogus data to connected cars and their drivers.

In considering automotive cyber security going forward, there will be issues concerning the security of intelligent transport systems that communicate with the vehicle. For example, the driverless/autonomous car trials planned in the UK include testing of roadside infrastructure that will communicate with vehicles to inform them of congestion, roadworks, etc., and allow drivers or their vehicles to plan and use alternative routes. Malicious attacks on this infrastructure, or the jamming/interference of satellite navigation signals, could in future severely disrupt traffic in urban areas, and bring large parts of a city to a standstill. It is important, then, that our future vehicles and their supporting smart infrastructure are designed to be resilient under both normal and adverse operating conditions.

# Benefits of automotive connectivity

The connected vehicle concept is not being driven solely by developments in automotive technology, but these developments are key to its progress. It is important to consider the connected car as an integrated system, and as a connected entity, maybe interacting with V2I, V2V, V2IoT, and its own internal automotive systems, becoming a part of a bigger connected 'ecosystem' that may or may not encompass those specific application technologies. Each of these technologies has been conceived with one or more beneficial objectives. Intelligent vehicle re-routing around congested sections of a town or city, for instance, would help alleviate traffic jams, give drivers advance warning of impending delays, or provide the data to enable them to adopt an alternative way of getting to their destination. As they develop, such technologies would also create opportunities to make more efficient use of the existing road transport infrastructure, and find some solutions to road utilisation problems that might otherwise have resulted in costly and contentious new transport infrastructure.

Such technologies would also of course make travelling by car safer – for drivers, passengers, and other road users. As already mentioned, in respect to safety, an important point for connected vehicles is that although a car may be securely designed against a 'direct' cyber-attack; in a connected automotive ecosystem, where many players may be under some obligation to exchange data and share connectivity, vulnerabilities in the system may exist in parts of the system seemingly far removed from car or carriageway.

A range of 'market forces' are influencing the installation of enhanced automotive communications:

- Additional point of transaction for consumer purchases (products and services)
- Consumer preference – embedded communications enhance in-vehicle driver-passenger experience
- Electric vehicle functions (such as mileage/range tracking, plus value-added EV services for optimising range and delivering charging point information)
- Mandated legislation; mandated regulatory communications-based services, such as eCall*
- Non-mandated communications-based services (navigation tools, traffic flow updates, parking apps)
- New unique selling point to sustain car sales – and their contribution to GNP
- Remote diagnostics for servicing/predictive maintenance
- 'Smart' vehicle insurance systems and services that uses vehicle data to adjust premiums
- Stolen vehicle tracking and recovery
- Telemetry – for commercial applications

* eCall is the European Union initiative intended to bring rapid assistance to motorists involved in a collision within the EU. The eCall architecture aims to deploy a device installed in all vehicles that will dial 112 automatically in the event of a serious accident, and wirelessly send airbag deployment and impact sensor information, along with GPS co-ordinates to local emergency agencies.

Connected carriageways: communications technology built into cars enables them to share data with eachother – and the wider world

# A known problem?

As well as opportunities, the advent of the 'connected' car brings several major challenges to the automotive sector, and will affect the operating models of OEMs, distributors, dealers and mechanics, road infrastructure managers, law-makers, and of course drivers and their passengers. In the public domain verifiable information about automotive cyber security risk levels is scattered, and can tend toward the sensationalist. How far car makers have gone, and still have to go, in terms of treating vehicular cyber security as seriously as passenger safety, for instance, is not easily discoverable. Some manufacturers, however, have acknowledged their awareness of the issues, and say that they are on top of the challenge.[7]

Even without their new connectivity, cars represent much more than powered driving machines. Insurance is a hugely influential governing factor in the automotive market. Questions of liability with respect to driving mishaps of any kind can turn unexpectedly contentious, and could prove a factor in drawing attention to any disquiet over whether more detailed information about the provisions automotive OEMs are making in order to counter any threats. But concern about how this connected technological evolution may play-out is being voiced from within the automotive sector itself, even if not especially stridently from its OEMs.

Interviewed by *The Times* newspaper toward the end of December 2014, Edmund King, President of motoring organisation the AA (and Visiting Professor of Transport at the University of Newcastle), acknowledged the 'hacking threat' to drivers of connected cars: "If cyber-criminals targeted automobiles like they're targeting other things, we'd be in for a hard and fast ride," he said.[8] That a senior industry figure like Mr King has gone on the record to express his forebodings indicates that concerns over whether automotive cyber security is receiving the full measure of attention that it warrants, are both timely and legitimate.

# Media interest in automotive cyber security

Edmund King's remarks at the end of 2014 followed a marked increase in published expressions of concern regarding automotive cyber security risks. These appeared against a media background where computer security in general was a hot topic. Here are some specimen headlines:[9]

- 'Security researchers raise concerns over car cyber safety' (*IT Pro*, 12/8/14)
- 'Hi-tech cars are security risk, warn researchers' (BBC News, 1/9/14)
- 'Is car hacking the Next Big Security Threat?' (*Live Science*, 16/10/14)
- 'Connected cars raise privacy and safety worries' (*Financial Times*, 20/11/14)
- 'Wireless systems expose drivers to cyberattacks' (*The Times*, 27/12/14)

In fact, the media coverage around automotive cyber security was largely based around a very limited number of insider event presentations on the subject that have taken place at cyber security conventions in the United States, and on other automotive cyber security speculation that has appeared in the public domain. The findings of Charlie Miller (a security engineer/researcher at Twitter) and fellow researcher Chris Valasek (Director of Security Intelligence at consultancy IOActive) for instance, have generated much media interest, even though the two highest-profile public declarations of their research into ECUs at two events – Def Con Las Vegas in 2013 and Black Hat USA in 2014 – were based on conditional one-off research projects. They were published as a paper entitled 'Adventures in automotive networks and control units'.[10]

In brief, the researchers reportedly used cables to connect laptops via the on-board diagnostics ports to the electronic control units inside two different makes of car. They wrote software which sent instructions to the cars' network computer and over-rode the commands from the vehicles' actual drivers, enabling them to take control of some steering functions and cause the fuel gauge to show empty – all while the vehicle was in motion under driver control. The underlying issue for automotive cyber security that Miller-Valasek's

demonstrations appeared to confirm, is that the rising number of internally-connected ECUs in the test vehicles seemed to have no screening process for authenticating the messages they received, or for blocking inauthentic transmissions.

"By examining the [controller area network] on which the ECUs communicate, it is possible to send proprietary messages to the ECUs in order to cause them to take some action, or even completely reprogram the ECU," Miller-Valasek have been quoted as stating. "ECUs are essentially embedded devices, networked together on the CAN (controller area network) bus. Each is powered, [with a] number of sensors and actuators attached to them."[11]

The CAN bus operates using an open protocol developed by Bosch in 1983. It is relatively safe under normal operation, but inherently insecure to external influence. According to Roy Isbell, from the Cyber Security Centre in WMG at the University of Warwick, it is essential that any external point of interconnection to the CAN bus is adequately protected. This should include connections to consumer interfaces, such as the vehicle head unit.

A researcher in the team at University of Warwick has developed CMAP (CAN bus mapper): this is the CAN bus equivalent of the NMAP open-source network mapping tool. This allows researchers and security analysts to enumerate all devices and ECUs connected to the CAN bus, an important capability when addressing functional safety and security issues.

Miller and Valasek's findings made an impression on US Senator Ed Markey. In a series of letters he asked some leading car makers to respond to seven pages of cyber-threat-related questions, including: "How would you be alerted to the possibility that a cyber-attack or inadvertent introduction of malicious code has occurred?", and "Does any of the testing described above include the use of independent third parties who are contracted by your company to attempt to infiltrate your vehicles' wireless entry points?"[12]

Media interest in automotive cyber security was further fuelled in August 2014, when a 'security advocacy group' calling itself I Am The Cavalry proposed an automotive cyber security rating system for car consumers.[13] The 'Five Star Automotive Cyber Safety Program' proposal offers 'a five-point checklist of computer technology best practices for automakers to implement'. The five aspects the program focuses on are: Safety by Design; Third-Party Collaboration; Evidence Capture; Security Updates; critical system segmentation and isolation measures. The move was described as 'an important first step towards a collaborative future between security experts and automakers'.[14]

One automotive OEM who would have been more inclined to respond favourably to Senator Markey and I Am The Cavalry, is electric-powered car manufacturer Tesla. Tesla's product range is highly digitally connected, with the transmission, engine systems, battery, climate control, door locks and entertainment systems all remotely accessible through an Internet connection. The company attracted media attention when it announced that it is hiring penetration testers – tasked with deliberately trying to break-in to Tesla's vehicle security safeguards.[15]

One way to access a vehicle's data systems is via the connect ports intended for use by car mechanics when conducting diagnostic tests

# Academic interest in automotive cyber security

Academic research into automotive cyber security dates back at least five years. In 2010, a team of researchers from the Universities of California-San Diego and Washington set out to see what resilience cars had to an attack on their control systems. Using software called 'CarShark' running on a computer cable-connected to a test car's servicing port, they were able to monitor communications between the electronic control units, and insert their own data to cause attacks.[16]

In 2010 and 2011 two academic research papers published by a team comprising researchers from the University of California San Diego and the University of Washington delved into the areas of ECU exploits in as much – if not greater – detail as Miller-Valasek, yet seem not to have generated the same level of wider interest. The first of these, 'Experimental Security Analysis of a Modern Automobile' (2010)[17] experimentally demonstrated that an informed attacker who is able to infiltrate ECUs can circumvent a broad array of safety-critical systems.

Published the following year, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' (2011)[17] proposed that remote exploitation of connected vehicles is feasible via a broad range of 'attack vectors' (including mechanics tools, compact disc players, Bluetooth links, and cellular radio); and further, that wireless communications channels can allow remote vehicle control, location tracking, in-cabin audio 'exfiltratrion', and vehicle theft.

Over a range of experiments in the laboratory and in road tests, the research teams claim to have demonstrated the ability to take over control of a wide range of automotive functions and 'completely ignore driver input' – including disabling brakes, braking individual wheels selectively on demand, causing the engine to stop, and more. "We find that it is possible to bypass rudimentary network security protections within the car," the researchers noted, "such as maliciously bridging between our car's two internal subnets".

Another academic to raise concerns over automotive cyber security shortcomings is Professor Andry Rakotonirainy of the Queensland University of Technology's Centre for Accident Research & Road Safety. He has claimed that the security protection on [existing fleet, future autonomous and connected cars] is "virtually non-existent... The basic security requirements such as authentication, confidentiality, and integrity are not strong.... This means... that as vehicles become more and more connected and autonomous, with the ability to communicate to other vehicles and infrastructure through wireless networks, the threat of cyber attack increases putting people's safety and security at risk."[18]

# Cyber-threat motives and targets

The question of to what extent the automotive world should be mindful of the cyber security experiences of other targeted vertical sectors, is one that evoked much debate among contributors to this Briefing. For some of these business sectors, cyber security was not a priority agenda issue until relatively recently, as the impact of malicious hacking has scaled-up to include new categories of device. Retail point-of-sale and online gaming are two example business vertical sectors that have had to cope with a recent increase in cyber-crime attacks.[19] One lesson all targeted vertical sectors – including the computer security industry itself – have learned is not to under-estimate the abilities of cyber-criminals to mount formidable challenges to existing information security provision.

Cyber-crime was not a major challenge for the building industry just two years ago – but it has managed to engage with the issue with work on standards within Business Information Modelling (BIM) that are now in development[20]. The same realisation has occurred within the industrial control systems and SCADA (supervisory control and data acquisition) system worlds[3]. Two general similarities with automotive are that (a) these are also mature industries where computer systems have not typically been subjected to offensive attention via the Internet, so have not necessarily been designed with defensive security as a prerequisite; and (b) are both industries which typically have long product development cycles, sometimes stretching over years – this means that even where known security threats are taken into account, emerging threats against which new products are not protected could have appeared by the time those products enter their markets.

One reason why computer systems cannot really be totally secure is because of the demands of maintaining security on all 'attack vectors' at all times. Some of the risk can be balanced by allocating security resources to where it is needed most at any given period. Identifying the motivating factors behind cyber-attacks can prove an effective stratagem in countering cyber-crime and other targeted malevolent Internet-based attacks. Insights gained can help anticipate the nature of future threats. For the automotive sector such motives might include:

## Foreseeable motives:

- Data theft – targeted data types might include:
  1. Access to online automotive apps and services – that contain banking/credit records
  2. Congestion Charge or toll payment information
  3. General personal identification data – e.g., social media users names and passwords
  4. Insurance and tax data – useful for identity theft
  5. International travel permits
  6. Licence plates and other vehicle registration data
  7. Lifestyle information – e.g., fitness club membership
  8. Medical records – a driver suffering from a health issue may have information about their condition either stored on a vehicle or accessible via the vehicle or a mobile device temporarily connected to the vehicle
  9. Vehicle location information – which may be used to identify patterns of use or driver behaviour in anticipation of offensive action against a vehicle
  10. Vehicle physical security data

- Extortion / denial-of-service threat
- Fraud and deception (altering or deleting schedule logs and records)
- Freight and goods theft (activating false alarms that cause goods to be left unattended)
- Automotive 'Hacktivism' – cyber-infiltration of a vehicle's systems that is politically- or ideologically-motivated'
- Immobilisation
- Mischief and malevolence – individual hackers testing defences and their skills; or wanting to inflict damage and/or disruption out of spite
- Premises security and burglary – vehicle data that reveals businesses and homes are unoccupied

## Secondary motives:

- Industrial espionage – illegal access to intellectual property
- Infliction of political or reputational damage
- 'Script kiddies' – adversarial hackers pitting their skills against the automotive software safeguards
- Sabotage or degrading of vehicle and connected system performance
- Terrorism – disabling vehicles as part of an attack, for instance
- Vehicle identification re-assignment (for stolen cars)

# Driver responsibility issues

Such types of dataset listed above as 'Targeted data types' can, of course, also be commonly found in other kinds of online digital storage – storage resources where awareness of cyber security risks may be more overtly highlighted to users. The question arises of how this could or should be carried across to the connected car driver experience. The 'driver-as-consumer' has a part to play in minimising their exposure to any potential threats that would regard their connected car as an 'attack surface'. 'Ordinary' cars may be becoming more technologically complex; but are drivers legally obliged to familiarise themselves with the workings of the new functionality now at their disposal when they are on the road?

The requirement for crews of public transport to demonstrate knowledge of and proficiency with the additional technology appearing in new passenger buses, for example, has been a challenge for transport operators seeking to recruit drivers. Not only do they have to be exemplary drivers, they also have to posses the skills needed to operate the increasingly complex onboard computerised technology.

This, in turn, steers the debate back to another question related to car driver responsibilities: if the connected car is increasingly becoming, in effect, a 'computer on wheels'[21], to what extent does this turn its owners into licensees of the various types of software that their vehicles are running on? And who should take the responsibility for maintaining software updates – driver/owner, manufacturer, or dealer?

It is perhaps appropriate here to add a note about the 'trustworthiness' of the vehicle software in respect to three specific issues. First, the trustworthiness of the software as delivered with the vehicle and maintained through the application of approved updates and patches. In the event of an accident there are going to be questions raised about the quality of the software and potential allegations about malfunctions or unexpected behaviour. Without a vehicle data recorder (like a civil aircraft's black box), how will accident investigators be able to establish whether software malfunction is a cause or contributing factor, and to what extent is the onus thrust back onto the driver to demonstrate that the vehicle was roadworthy? Second, there's the trustworthiness of the software as modified by the downloading of apps or other modifications installed by the owner/operator/user. Most computer users have experienced software or driver incompatibilities at some time: so how do drivers assure themselves that any modifications do not imperil the critical functionality and safety of the vehicle?

The third issue to note in this context is the relationship between functional safety and cyber security – it is difficult to have one without the other, but the integration of the two disciplines is barely at an embryonic stage. The car industry has the Automotive Safety Integrity Level risk classification scheme that relates to safety levels, but it is not altogether clear how this should address both hazards (from a safety perspective) and threats (from a security perspective).

The issue of owner 'car hacking' has already been mentioned here earlier – what are the liabilities where even minor adjustments to a car's software configuration result in an accident? And as cyber-enabled features of a vehicle become more intrinsic to its primary safety functions, two subsidiary questions worthy of further discussion are, should awareness of cyber-threats be mentioned more prominently in user guidance? And is there even a case, at some future point, to make 'cyber security for drivers' awareness form part of road proficiency tests and driving license-holder requirements?

# Appendix: Automotive industry initiative examples

## Alliance of Automobile Manufacturers (Auto Alliance)

Advocacy group for the auto industry, claiming to represent 77 per cent of all US car and light truck sales. In July 2014 the Auto-Alliance announced an initiative - later known as Auto-ISAC (see below) – to 'further enhance the industry's ongoing efforts to safeguard vehicle computer systems', adding that to enhance cyber security, 'businesses, government and academia [should] 'work collaboratively to stay ahead of hackers'. Its following statement is worth quoting at length:

*"[We] are undertaking efforts to enhance the industry's cybersecurity posture by working collaboratively to establish a voluntary industry sector information sharing and analysis centre or other comparable program for collecting and sharing information about existing or potential cyber-related threats and vulnerabilities in motor vehicle electronics or associated in-vehicle networks... While researchers have demonstrated how to gain access to various vehicle controls if a vehicle's electronics or in-vehicle network could be compromised by hackers, at this point there has never been an unauthorised accessing of a vehicle in the road today... [Despite this] we are taking action to prepare for possible future threats."*

## The Auto-ISAC (Information Sharing Advisory Centre)

Set-up in October 2014 by the Alliance of Automobile Manufacturers, the Association of Global Automakers, and parts-making giant Delphi to form a voluntary information-sharing and analysis centre for the industry to 'target the threat of hackers as vehicles begin connecting to the Internet and communicating with other cars and trucks sharing the transportation infrastructure'. Auto-ISAC claims it will bring together nearly 25 automotive manufacturer members with other industry and government stakeholders on the issue, beginning with a cyber-policy technical group to lay the groundwork for broader collaboration.

## Automotive Council

The Automotive Council was established in 2009 to enhance dialogue and strengthen co-operation between UK government and the automotive sector. The Council is made up of senior figures from across industry and government. http://www.automotivecouncil.co.uk.

## Automotive Cyber Security Research Partnership

Set-up in December 2014 by global information assurance specialist NCC Group and WMG, at the University of Warwick, this initiative will make use of WMG's expertise in technology innovation, focusing on high-impact research and collaborative security projects with the automotive industry. NCC Group will sponsor a number of PhD students to carry out their studies, focusing on research in the field of automotive cyber security.

# Recommendations from this Briefing

1 Consultation should be encouraged between the automotive industry bodies for which automotive cyber security is, or should be, an agenda issue, and those professional bodies and associations in non-automotive sectors that are already engaged in cyber security awareness building.

2 'A 'working party' or 'consultative committee' should be established to explore the feasibility of initiating briefings between a range of parties with a declared interest in automotive cyber security. Specifically, it could discuss the development of code-of-practice guidelines/reference model that address the systems engineering, security, privacy, legal and ethical issues associated with the increasing autonomy of vehicles.

3 The IET, in consultation with the KTN, other professional industry bodies, associations and employers in the automotive sector, should consider and report on how cyber security issues might affect technical and professional skills in the automotive sector. This should be used to stimulate discussion and planning of the implementation of appropriate initial and continuing professional development, to reduce the threat that cyber security skills gaps in this sector could harm public safety or security.

4 A Thought Leadership Briefing could review how the relationship between the driver, and the connected vehicle (of all kinds) should be reappraised in the context of automotive cyber security developments.

5 The publication is also proposed of a Thought Leadership Briefing that surveys issues surrounding liabilities around automotive cyber security events, and seeks to identify the 'grey areas' that could be clarified in the public interest - the liability, legal and ethical issues of semi-autonomous or autonomous vehicles are a public policy issue where the IET and KTN are ideally placed to take a lead in asking the difficult questions and explaining to the public the implications.

6 A series of events should be proposed to identify common challenges and issues in cybersecurity across all modes of transport. These events would provide an environment for encouraging collaboration and research within industry, in order to accelerate the development of innovative solutions for the challenges that are identified and be in position to exploit business opportunities that arise as a result.

The industry needs to take a lead on most of these recommendations. However, the IET and KTN will look to support and facilitate them wherever possible.

# References


1 Alliance initiates new security forum' – AutoAlliance media alert, July 2014

http://www.autoalliance.org/index.cfm?objectid=ACE2D720-0DD5-11E4-869F000C296BA163

2 'Hacking the Internet: bringing down infrastructure' – *Engineering & Technology*, September 2013

http://eandt.theiet.org/magazine/2013/09/hacking-the-internet.cfm

3 'Industrial control systems and SCADA cyber security' – *Engineering & Technology*, August 2014

http://eandt.theiet.org/magazine/2014/08/cyber-security-new-battlefront.cfm

'Edward Snowden on Cyber Warfare' – PBS Online, January 2015

http://to.pbs.org/145VaH8

4 *Car Hacker's Handbook* by OpenGarages

http://opengarages.org/handbook/

5 'Connected Car Forecast: Global Connected Car Market to Grow Threefold Within Five Years'

http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf

6 'Thousands using GPS jammers on UK roads pose risks, say experts' – *The Guardian*, February 2013

http://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks

'New jamming devices block both GPS and Galileo' – *Engineering & Technology*, February 2014

http://eandt.theiet.org/news/2014/feb/gps-jamming.cfm

7 'GM's New Cybersecurity Chief Aims To Thwart Electronic Car Hackers' – *IB Times*, September 2014

http://www.ibtimes.com/gms-new-cybersecurity-chief-aims-thwart-electronic-car-hackers-1695148

8 'Hacking threat to drivers – wireless networks let cybercriminals seize control of cars' – *The Times*, 27 December 2014

9
- 'Security researchers raise concerns over car cyber safety' – *IT Pro*, 12/8/14

  http://www.itpro.co.uk/security/22878/security-researchers-raise-concerns-over-car-cyber-safety
- 'Hi-tech cars are security risk, warn researchers' – BBC News, 1/9/14

  http://www.bbc.co.uk/news/technology-28886463
- 'Is car hacking the Next Big Security Threat?' – *Live Science*, 16/10/14

  http://www.livescience.com/48310-car-hacking-security-threats.html
- 'Connected cars raise privacy and safety worries' – *Financial Times*, 20/11/14

  http://www.ft.com/cms/s/0/e663c6fa-643b-11e4-bac8-00144feabdc0.html#axzz3PI64yfwE

10 'Adventures in automotive networks and control units'

http://illmatics.com/car_hacking.pdf

11 As quoted in 'Automobiles: A new frontier in hacking and cyber security' – Trend Micro blog, September 2013

http://blog.trendmicro.com/automobiles-new-frontier-hacking-cybersecurity/

12 'As Wireless Technology Becomes Standard, Markey Queries Car Companies about Security, Privacy – Lawmaker sends letter to 20 auto manufacturers after reports of hacking, breaches, privacy concerns' – Markey media statement, December 2013

http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy

13 https://www.iamthecavalry.org/domains/automotive/5star/

14 'Want a safe car? Check its cyber safety rating' - CNET, August 2014

http://www.cnet.com/uk/news/want-a-safe-car-check-its-cyber-safety-rating/

15 'Chinese hackers target Tesla Model S electric car' – *Daily Telegraph*, July 2014

http://www.telegraph.co.uk/technology/internet-security/10980899/Chinese-hackers-target-Tesla-Model-S-electric-car.html

16 'CarShark Software Lets You Hack Into, Control And Kill Any Car' – Jalopnik, May 2010

http://jalopnik.com/5539181/carshark-software-lets-you-hack-into-control-and-kill-any-car

17 'Comprehensive Experimental Analyses of Automotive Attack Surfaces'

www.autosec.org/pubs/cars-usenixsec2011.pdf

'Experimental Security Analysis of a Modern Automobile'

www.autosec.org/pubs/cars-oakland2010.pdf

18 'Car hacking: The security threat facing our vehicles' – *Popular Science*, September 2014

http://www.sciencedaily.com/releases/2014/09/140917120705.htm

19 'Point-of-sale cyber security: hacking the check-out' – *Engineering & Technology*, March 2013

http://eandt.theiet.org/magazine/2013/03/turn-on-log-in-checkout.cfm

20 *Building Information Modelling (BIM): Addressing the cyber security issues* (Institution of Engineering and Technology, 2014)

http://www.theiet.org/sectors/built-environment/design/bim-cyber-security.cfm

21 'Is it a Car or a Computer on Wheels? Door locks and entertainment systems remotely accessible via the Internet' – *Dashboard Insights*, January 2015

http://www.autoindustrylawblog.com/2014/06/09/is-it-a-car-or-a-computer-on-wheels/