

Cyber Security in the Connected Vehicle Report 2016

Securing the connected car – assessing the shifting landscape of automotive cyber security, threats and solutions in an increasingly connected industry

- **The Attack Surface:** Map out the risk landscape and key attack surfaces and understand the benefits for more up to date cost effective security
- **Real Risks and Real Solutions:** Expert analysis of the real threats posed to the automotive industry and the market solutions and strategies to maximise security
- **Robust Architectures:** Learn the scope and strategy to build strong systems and architectures through connectivity, technology and collaboration
- **Lessons Learned:** Understand the best practices for companies developing robust security strategies to secure against hacks and maintain consumer trust

Industry Overview

The connected car industry is growing fast. In 2013 the research firm GSMA predicted that “the global connected car market will be worth €39 billion in 2018, up from €13 billion in 2012” (GSMA, 2013). They went on to predict that over the same period there will be an “almost sevenfold increase in the number of new cars equipped with factory-fitted mobile connectivity” (GSMA, 2013).

The cyber security of connected vehicles is one of the biggest issues facing manufacturers today. Three significant trends have led to this position:

Complexity. “Complexity is the worst enemy of security”, and yet the past few years have seen a rapid increase in the cyber complexity of vehicles, evidenced by: (i) a massive increase in lines of code in a vehicle – approximately 100 million currently, compared to around 8 million for an F-35 joint strike fighter; (ii) an increase in Electronic Computing Units to something around 100 currently in high-end vehicles, communicating on a multiplicity of networks; and (iii) a rise in heterogeneity of in-vehicle systems – these are now responsible for a massive range of critical and luxury features within vehicles.

Connectivity. This complexity has been exposed to wireless networks through the development of wireless communication interfaces. These interfaces are a double-edged sword – by connecting the vehicle to the Internet of Things, they have led to dramatically extended functionality, but they have opened up the traditionally closed vehicular system, making vehicles a more accessible and more attractive target to adversaries.

Content. Theft of personal information, leading to identity theft, is an attractive goal for cyber-criminals. Personal data is increasingly available in car networks as the cars themselves are more sophisticated, and smartphones and other devices are connected to them.

This report contains five key messages:

1. There are a growing number of connected cars, and their value to the attacker is on the rise. There is a growing attack surface, and a larger number of tools available to the hacker. In short, there is a massive future security problem just around the corner.
2. As barriers between the traditional subsystems are eroded, getting security right across the vehicle will be vital.
3. Security is not something that can be bolted on in the implementation phase: security must be got right in requirements and design phases.
4. The whole ecosystem must be trustworthy: The brand loyalty invested in an original equipment manufacturer can only be as secure as its component suppliers are secure.
5. It is absolutely critical that robust standards are developed. We need to create a future secure environment. Automotive is a massively high-value industrial sector, and collaboration has to become the way of working.

With sincere encouragement,

Jeremy Bryans

Research Fellow, Coventry University

Siraj Shaikh

Research Fellow, Coventry University

Madeline Cheah

Research Fellow, Coventry University

Jack Fowler

Project Director, TU Automotive

Questions Answered

- What does the cyber security landscape look like today?
- How rapidly is this landscape changing and in what ways?
- How are current vehicles at risk and how are vulnerabilities being exploited?
- Why hack a vehicle? What are a hackers motivations?
- What are the real risks and potential consequences? How does this differ from the 'media hype'?
- How do you build holistic security strategies and systems and implement them successfully?
- What are the available market solutions and who are the key players?
- How can these solutions be effectively implemented to guarantee maximum security and ensure consumer trust?

Key reasons to buy this report

- A vital resources in assessing the global cyber threat in order to develop holistic security approaches
- Analyse the real risks and threats in the auto industry
- Assess the current solutions on offer and the experts providing them
- Develop and implement robust security architectures

Who should buy this report

- OEMs
- Software Companies
- Hardware companies

Purchasers of previous TU-Automotive reports

DAIMLER



MOBIS
driving science

FUJITSU TEN



Contents

Welcome	3
Acknowledgements	4
About TU-Automotive	5
List of figures	8
Key terms	9
Executive summary	10
1 Introduction	12
1.1 Terms and definitions	16
1.2 Summary of report	16
2 Mapping the attack surface within the vehicle	17
2.1 Types of connectivity	17
2.2 The Attack Surface	17
2.2.1 Infotainment	17
2.2.2 DAB radio	18
2.2.3 USB	18
2.2.4 OBD-II	18
2.2.5 Bluetooth	18
2.2.6 WiFi	19
2.2.7 JTAG ports	19
2.2.8 Dedicated smartphone interfaces	19
2.2.9 Tire Pressure Monitoring System (TPMS)	20
2.2.10 Immobilizer	20
2.2.11 Telematics control units	20
2.2.12 Passive keyless entry	21
2.2.13 Remote key entry	21
2.2.14 eCall	21
2.2.15 DSRC (Digital Short-Range Communication)	21
2.2.16 GM's OnStar	21
2.3 The automotive eco-system	22
3 Types of hacks and threats they pose	25
3.1 Introduction	25
3.2 Why hack a vehicle? Hackers and motivations	26
3.2.1 Tuners	27
3.2.2 Academic security researchers	27
3.2.3 White hat hackers	27
3.2.4 Script kiddies	27
3.2.5 Black hat hackers	27
3.2.6 Gray hat hackers	27
3.2.7 Vehicle theft	28
3.2.8 Financial theft and damage	29
3.2.9 The potential for remote hacks	29

3.3	Attack anatomy28
3.3.1	Bridging attacks26
3.3.2	Infotainment26
3.3.3	OBD-II26
3.3.4	Bluetooth27
3.3.5	Wi-Fi27
3.3.6	CAN bus27
3.3.7	Dedicated smartphone interfaces.28
3.3.8	Tire Pressure Monitoring System (TPMS)28
3.3.9	Immobilizer.28
3.3.10	Telematics: manufacturer and after-market telematics29
3.3.11	Passive Keyless Entry and Start.30
3.3.12	eCall30
3.3.13	Advanced Driver Assistance System (ADAS) features.31
3.3.14	Digital Short-Range Communication (DSRC)31
3.3.15	Sensor networks.31
3.4	Attack trees.31
3.5	Hacker heat map32
4	Available market solutions35
4.1	Technical approaches35
4.1.1	Identifying dependencies35
4.1.2	Testing for unanticipated user input35
4.1.3	Techniques that expose vulnerabilities35
4.2	Penetration testing.36
4.3	The holistic approach37
4.4	Plugging the gaps37
4.5	Market initiatives and key players.38
4.5.1	Cyber Security Consortium for Connected Vehicles (CCV).38
4.5.2	UK Department for Transport initiatives38
4.5.3	BT Assure38
4.5.4	NCC Group assurance and testing services39
4.5.5	SBD technical consultancy39
4.5.6	SBD and NCC Group strategic partnership39
4.5.7	Automotive Secure Development Lifecycle (ASDL)40
4.5.8	I Am The Cavalry's Five Star Automotive Cyber Safety Framework40
4.5.9	Plextek40
4.5.10	Intel and the Automotive Security Review Board41
4.5.11	The Markey Report and the SPY Car Act41
4.5.12	The Transport Research Laboratory.41
4.5.13	HORIBA-MIRA42
4.5.14	Scarecrow Consultants.42
4.5.15	Thatcham, UK42
4.5.16	TowerSec automotive cyber security42
4.5.17	Telefónica's M2M connectivity offering42
4.5.18	Elektrobit embedded solutions42

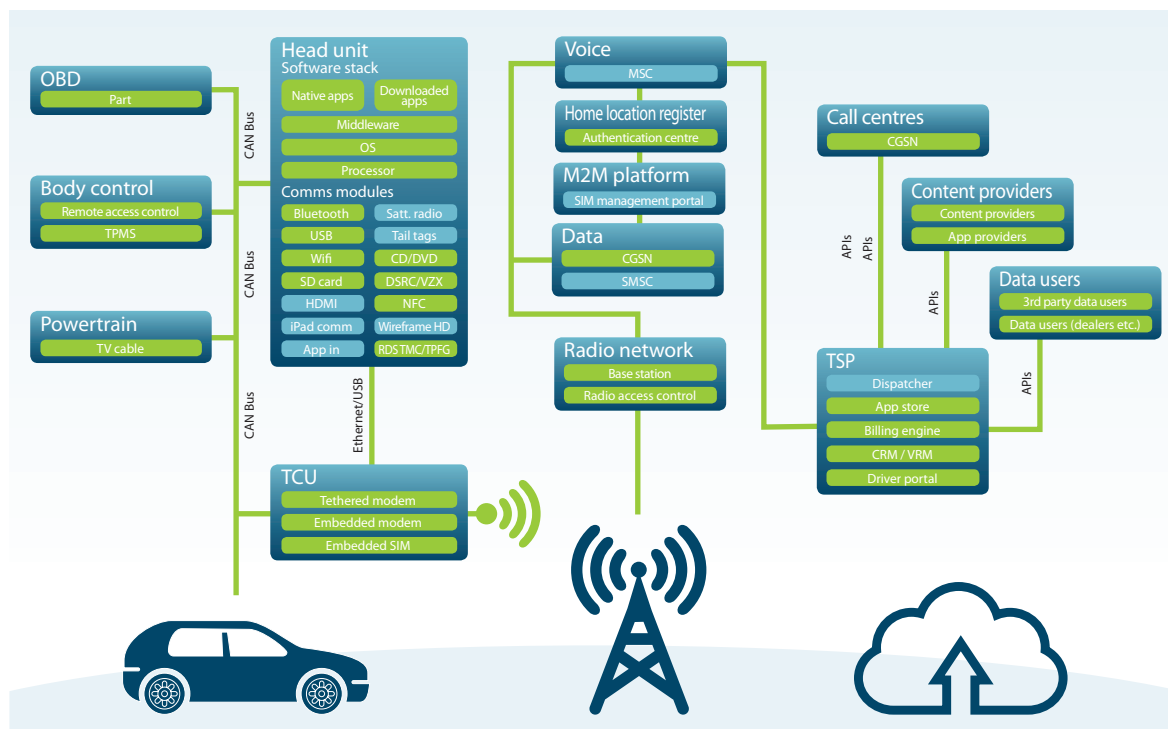
- 4.5.19 Covisint’s secure platform 42
- 4.5.20 HARMAN 43
- 4.5.21 Visteon’s OASIS cockpit 43
- 4.5.22 NXP Semiconductors 43
- 4.5.23 Mocana 43
- 4.5.24 AIRMIKA’s CYBLOK 43
- 4.5.25 Sierra Wireless’s Legato platform 43
- 4.5.26 CAR 2 CAR Communication Consortium (C2C-CC) 43
- 4.5.27 Security Innovation’s high speed communications security 43
- 5 Cyber security-related standards and initiatives 44**
 - 5.1 ISO 26262 44
 - 5.1.1 Limitations and extensions 44
 - 5.2 SAE J2980 44
 - 5.3 SAE J3061 45
 - 5.4 US initiatives 45
 - 5.4.1 SPY Car Act 45
 - 5.4.2 NHTSA work 45
 - 5.4.3 NIST 47
 - 5.5 Threat modeling 47
 - 5.5.1 Checkoway’s threat modeling framework 47
 - 5.5.2 IBM Global’s security model 47
 - 5.6 Other industry initiatives 47
 - 5.6.1 E-safety Vehicle Intrusion Protected Applications (EVITA) 47
 - 5.6.2 Trusted Platform Module (TPM) 47
 - 5.6.3 Secure Hardware Extensions (SHE) 47
- 6 Lessons and conclusions 49**
 - 6.1 Lessons from aviation 49
 - 6.2 Conclusions 50
- Abbreviations 55**
- References 56**

List of figures

- Figure 1 The CIA triangle 10
- Figure 2 How eCall works. An EU Commission infographic 18
- Figure 3 The back infrastructure 24
- Figure 4 Attack tree depicting a safe-cracking 30
- Figure 5: Digital I/O channels appearing on a modern automobile. 32
- Figure 6: Another example map. 33
- Figure 7: An abstract heat map 33
- Figure 8: Composite Threat Model Outline 46

Extract from Chapter 3 – Types of hacks and threats they pose

Figure 3: The back infrastructure.



Note: Each point represents a possible attack vector
© Mike Parris, SBD.

3.3 Attack anatomy

Automotive security best practice is still emerging, and while it has a lot in common with automotive safety, it is not identical. Safety is probabilistic: individual risks are measured, and the overall risk associated with the vehicle is kept within acceptable bounds. But security is not probabilistic: predicting vulnerabilities is hard, and threats are intentional. The emerging science of automotive security must provide mechanisms and processes for predicting, preventing and containing threats throughout the lifetime of the vehicle.

New vectors could be opened up as new services are introduced to the connected automobile. Services that involve financial transactions will be a prime target, and here the supporting infrastructure is at least as much an attack point as the in-vehicle parts.

Alan Stevens, Chief Scientist and Research Director in Transportation at TRL, identifies that what is really at stake here is public confidence. Responsible for

a project that is investigating the feasibility of a connected corridor from the Dover port and up the A2/M2 highway as far as the Blackwall Tunnel in London, he says: “Unless you have secure systems that people can trust, you cannot protect the data and you cannot protect the safety. There is a need to protect the integrity of the data from mobile device to vehicle to roadside to back office.”

Infrastructure is an increasingly popular target for terrorists, as a 2013 report from the IET points out (The IET, 2013). Mike Parris points out: “There are three areas of risk: Telematics, Airborne Data Automation System (ADAS) and Autonomous and V2X. Each of these areas has its own unique risks; the biggest risk is where they overlap. Who on earth is thinking about the overlaps? We as an industry are still struggling to understand them individually. Hackers will look for weak points. At interfaces between services, the scope for someone making a wrong assumption about some other piece of functionality is huge.”

In Miller & Valasek (2014), the authors look at remote attacks on automobiles. They see safety-critical attacks on automobiles as requiring up to three stages. The first is to remotely gain access to an internal automotive network. The second is to be able to communicate with the network by injecting messages, to allow the attacker to control the targeted ECU. Although one can imagine attacks in which simply exercising this control on the entry point ECU is sufficient, attacks that result in physical control of the vehicle will often require a third stage of interaction with other ECUs. These “cyber-physical” attacks move from the cyber domain to the physical one, and are potentially far more damaging.

It is likely that the first ECU is there to receive and process radio signals, and therefore does not have control of physical parts of the vehicle, and so a cyber-physical attack will usually require “a second step which involves injecting messages onto the internal automotive network in an attempt to communicate with safety critical ECUs, such as those responsible for steering, braking, and acceleration” (Miller & Valasek, 2014). It may well be the case that the two ECUs (the entry point and the target ECU) are on different networks, and this second stage will involve the attacker needing to “bridge” the two networks in order to carry out the attack.

3.3.1 Bridging attacks

A vehicle will usually have multiple networks, each with its own resident ECUs. These could be CAN networks, FlexRay or Local Interconnect Networks (LIN), for example.

There could thus be a network for infotainment and a separate one for engine management functions, for example, and these may be of different types. Communication between these is restricted, and controlled by ECUs which are connected to both networks and act as “bridges” between them.

Bridges implement a set of rules to decide which messages should cross the network boundaries. This rule set can be changed by injecting code to persistently alter

the behavior of one of these bridging ECUs. This could allow an ECU on a less-critical network to communicate directly with an ECU on a safety-critical network, and is an additional complexity in security testing.

In the following subsections, we survey vulnerabilities discussed in open literature.

3.3.2 Infotainment

In Checkoway et al. (2011), an attack is discussed using the CD player as an entry point. Two vulnerabilities were identified the first being “a latent update capability in the media player that will automatically recognize an ISO 9660-formatted CD with a particularly named file, present the user with a cryptic message and, if the user does not press the appropriate button, will then reflash the unit with the data contained therein”. They note that this is not a standard manufacturer method, and therefore speculate that it is a “vestigial capability in the supplier’s code base.” The second followed from the first. Given that the media player can parse complex files, they reverse-engineered a substantial amount of the media player firmware and though an exhaustive examination of this they were able to construct a buffer overflow attack. Finally, they were able to modify a WMA audio file so that, when a CD containing the file was played on the system, it sent carefully chosen CAN packets to the network.

DAB radios provide another entry point. The data DAB stations send (images and text) must be processed by the software in the radio. Bugs in this software enabled Andy Davis, research director at security firm NCC Group, to compromise the device. He was able to create a DAB radio station using off-the-shelf components. The risk is that a compromised infotainment system of a targeted automobile, once compromised, could be used as a stepping-stone to attack more critical systems. The created station could be used to simultaneously compromise many automobiles.

3.3.3 OBD-II

The OBD connector offers direct access to all CAN buses through a physical port in the cabin of a

vehicle. The fact that the interface and messages are standardized means that there is a plethora of cheap, easily available scan-tools for the OBD port. These scan-tools come in two types: full-featured versions with in-built software, user-interfaces and so on; and dumb tools that must interface with another computing platform such as a phone or conventional PC.

At the 2015 Black Hat Asia security conference in Singapore, a programmable device called the CANtact was shown. When available, it will sell for less than \$100, and form a physical connection between a vehicle's OBD port and a computer's USB port. The device is run on open-source software, and the author has also developed a "Python library designed to make it easy to interact with CAN networks" (Evenchick, 2015). CAN frames can be encoded easily as Python objects and sent, received, logged, and inspected. Among others, the OBD II and Unified Diagnostic Services (UDS) protocols are supported. Supporting UDS gives the ability to read and write arbitrary memory in the vehicle. Although this device promises to make the hacking of automobiles much easier, it requires physical access to the OBD, and is therefore chiefly of interest to the "tuners" discussed above.

Checkoway et al. (2011) notes that: "In 2004 the Environmental Protection Agency mandated that all new automobiles in the US support the SAE J2534 "PassThru" standard – a Windows API that provides a standard, programmatic interface to communicate with a automobile's internal buses." Typically implemented as a Windows DLL, this communicates over a wired or wireless network with a reprogramming or diagnostic tool.

Checkoway and his colleagues refer to a device implementing this standard as a "PassThru device". They chose the most commonly used device and identified two vulnerabilities. First, if the PassThru device is connected to an automobile, an attacker on the same Wi-Fi network can connect to it and obtain control over the automobile's reprogramming.

Secondly, the PassThru device itself can be compromised, and malicious code injected. They were even able to write a worm that automated the attack, spreading itself from device to device.

Perhaps of more immediate concern are Bluetooth interfaces to the CAN port, discussed elsewhere in this report.

3.3.4 Bluetooth

Keijo Haataja (2009) presents a thorough overview of the security architecture and security modes of the Bluetooth protocol before listing the vulnerabilities that Bluetooth networks face. He divides these into three categories, corresponding to the CIA model of security: threat of disclosure of unauthorized information, threat to integrity of information, and threat of denial of service. He also notes that: "Powerful directional antennas can be used to considerably increase the scanning, eavesdropping and attacking range of almost any kind of Bluetooth attack."

Miller & Valasek (2014), meanwhile, consider "Bluetooth to be one of the biggest and most viable attack surfaces on the modern automobile, due to the complexity of the protocol and underlying data. Additionally, Bluetooth has become ubiquitous within the automotive spectrum, giving attackers a very reliable entry point to test."

Checkoway et al. (2011) also investigated the Bluetooth capabilities built in to their test vehicle's telematics unit. They were able (through reverse engineering) to "gain access to the telematics ECU's Unix-like operating system and identified the particular program responsible for handling Bluetooth functionality." They verified that it contained "a copy of a popular embedded implementation of the Bluetooth protocol stack and a sample hands-free application" together with a custom-built interface. The interface contained a vulnerability that allowed a buffer overflow attack to be mounted by any paired Bluetooth device, allowing arbitrary code to be executed on the telematics unit.

Extract from Chapter 4 – Available Market Solutions

What can be done to mitigate the risk of cyber attacks on connected vehicles? In this section, we look at what is available to the automotive industry today. We begin with technical approaches and end with assurance, examining how manufacturers “scale up” to the problem of security, then look at security-specific solutions such as penetration testing, before considering a holistic approach to automobile design. Some specific challenges are addressed in the next short section, before looking at the response of the market.

4.1 Technical approaches

To determine that a car is safe, we examine how it behaves in as many circumstances as possible. Testing is well understood and implemented in OEMs, but although ascertaining that an automobile behaves safely is relatively straightforward, identifying the absence of any insecure behaviors (vulnerabilities) is hard. The root of the problem lies in the difference between the intended and the implemented behavior of a system. As Mike Parris says, a hacker “does not care how well architected a system is, he is looking for implementation vulnerabilities.” Nobody really knows what best practice in connected automobile design is, simply because it is a brand new field.

Testing is the prevalent solution to identifying unsafe behavior, but has a fundamental limitation, attributed to Edsger Dijkstra in Randell and Buxton (1970): “Program testing can be used to show the presence of bugs, but never to show their absence.” Nevertheless, some testing techniques do exist. Herbert H. Thompson (2003) surveyed 10,000 security bugs and identified in each case the testing technique that would have exposed the exploited vulnerability. The study resulted in a set of generalized security testing techniques which we briefly summarize below.

4.1.1 Identifying dependencies

Not unlike embedded systems, software exists in an environment where there is a significant level of co-dependence, whether it be the loading of libraries, or interfacing with third party components.

This is analogous to vehicular embedded systems having nodes (ECUs) of various functions which have to work with third party OEM equipment, firmware and possibly high-level software (in the case of infotainment systems) developed by third parties.

In either case, because of these dependencies, there are two issues that may need to be considered: firstly, that the system may inherit weaknesses from one or more components that it depends upon, and secondly that any external security resource might also fail. In an automotive context, where there has yet to be an implementation of integrated security, this should be a primary consideration whilst engineering a solution. Additionally, as a consequence of architectural and implementation heterogeneity and complexity (Salfer et al., 2014), there may be dependencies that are unforeseen or undocumented when components are integrated into the larger system.

4.1.2 Testing for unanticipated user input

With user input, reserved words, escape characters, long strings or boundary values can all cause problems. This is the basis for many of the popular attacks seen against services and software such as cross-site scripting and buffer overruns. The modern vehicle, especially with modern infotainment systems, is not immune to this: for example Checkoway et al. (2011) demonstrate how Bluetooth and cellular wireless technologies can be exploited to gain complete control of the automobile using buffer overflows in order to leverage an authentication weakness.

4.1.3 Techniques that expose vulnerabilities

Herbert H. Thompson (2003) splits these into techniques to expose design vulnerabilities and techniques to expose implementation vulnerabilities. Many vulnerabilities are actually designed into an application. For example, test instrumentation – where program interfaces are added for testing purposes – are sometimes not closed or resolved. Ports could be left open or unsecured, or default configurations could be weak or contradictory. The OBD-II port on a vehicle is a prime example;

it made vehicular diagnostics far simpler, but also opened a gateway to the outside. This could lead to a whole spectrum of problems, ranging from monetary loss (as in theft) to actual physical harm. Similar techniques include side channel attacks such as timing attacks to deduce cryptographic keys as demonstrated by Kocher et al. (2004). Fuzzing is another technique that could be used, as demonstrated by Koscher et al. (2010), who were indeed surprised by the fact that the level of reverse engineering needed was relatively trivial as there is a limited range of CAN packets that can be construed as valid.

These testing techniques, however, essentially only cover very specific types of weaknesses and errors, based on the categories as described above. A password entry field, for example, which is programmed to allow only four characters may be perfectly valid, sanitizes user input, and have no bypass routes available in the software. However, from a security point of view, this still represents a substantial vulnerability, as a four-character password in itself is very weak. Security (essentially a system level concept) requires a careful analysis of relationships, extraneous undocumented capability and requires a more holistic approach: enter penetration testing.

4.2 Penetration testing

In practical terms, the aim of any penetration testing (sometimes referred to as “ethical hacking” or “pentesting”) exercise is to assess the real-world security of a system from the viewpoint of an attacker, by not just discovering vulnerabilities, but actively trying to exploit them.

Testing could take the forms of white box testing (where all necessary information is made available) or black box testing (where only investigation of the system is authorized, but no further information is given). There are several aspects to consider when using either approach. On the one hand, having all the necessary information and data saves time and allows for scrutiny of code or documentation that

might otherwise be left unassessed or unconsidered. Conversely, black box pentesting may allow for a more realistic assessment of the system, as testers would have only the same access as a potential attacker. Nevertheless, it is important to note that either angle will only ever provide points for improvement at that moment in time, and is not in itself, a guarantee of future security.

The formalisms of pentesting and its support mechanisms (such as attack trees and graphs) have already been explored by many in the academic field. However, the modeling of a human attacker and pentesting has so far been imperfect, with challenges in decision-making, the creation of classes, accurate probability distributions, along with difficulties in bringing together model-driven approaches with real-world practicalities.

Although the pentesting process might involve the use of automated scripts, software or hardware tools and frameworks, the test generally hinges on the expertise and experience of the testers themselves. As evidenced by the reports of vehicle hacking, the reason for this lies in the unique nature of the human mind, which is able to think laterally, bypass otherwise sophisticated countermeasures, and work creatively to think within constrained environments (such as is the case with embedded systems).

Considering the need to adopt the mentality of an adversary when using this methodology, system designers may not be the best people for such an effort, as cataloguing all implicit assumptions (especially from a malicious viewpoint) made during system development is extremely difficult; hence the need for an external security testing process.

“In modern cars, the boundaries between the traditional engineering silos have almost completely collapsed”

Jon Holt, Scarecrow Consultants

Methodology

The field of cyber-security is a fast-moving one, and the sub-field of automotive cyber-security moves faster still. This report (Cyber Security in the Connected Vehicle Report 2015-2016) was constructed by drawing on:

Academic or openly available commercial literature. We made substantial use of the academic literature on automotive cyber security as well as commercial literature, and the report contains around 80 references. Confidential information was ruled out.

Interviews with experts. The report would not have been possible without the in-depth interviews that we conducted with automotive cyber-security experts. Their influence and expertise is scattered throughout this report, as well as direct quotes from many of them.

We would like to say a big thank you to all those who contributed to the making of this report.


ORDER YOUR REPORT IN LESS THAN 60 SECONDS

Just fill in this form and access the information and analysis you need to develop your knowledge of how to integrate services into your business model.

- Pages: 60
- Figures: 7
- **Single User License: \$3,195**

Four ways to order:

 www.tu-auto.com/cybersecurity-report/

 Scan and email this form back to:
reports@tu-auto.com

 Or fax: **+44 (0)870 238 7255**

 **Charlotte Wright**
charlotte@tu-auto.com
Marketing Manager on
+44 (0)20 7422 7517

Payment details:

Name (as it appears on card): _____

Card Number: _____

Type of card: _____

Expiry date: _____ Security Code: _____

First name _____

Last name: _____

Company _____

Telephone: _____

Email: _____

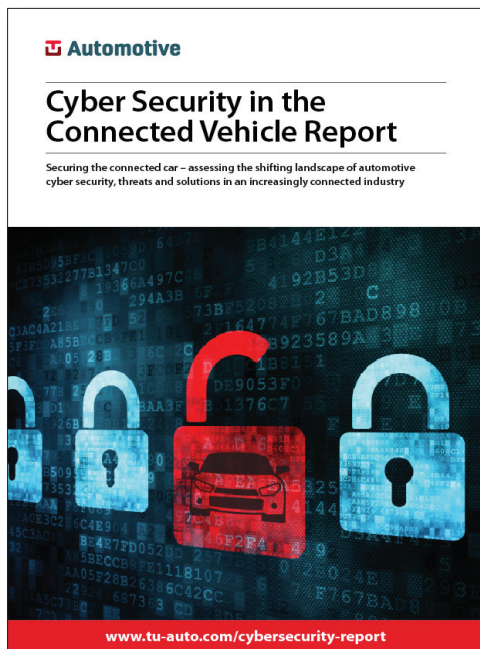
Address: _____

City _____

Zip/Postcode _____

Report Name _____

Quantity _____



Order your copy today at: www.tu-auto.com/cybersecurity-report

About TU-Automotive

TU-Automotive is the reference point and communications hub for the evolving automotive technology segment as it converges with consumer electronics, mobile and IoT to re-define connectivity, mobility and autonomous use-cases.