nccgroup
freedom from doubt

RESEARCH INSIGHTS

Sector Focus: Automotive

Author: David Clare

CONTENTS

AUTHOR

DAVID CLARE

David is a security consultant at NCC Group and currently holds the position of technical lead for automotive testing and research. Specialising in testing embedded systems with a focus towards automotive and ICS, David has more than ten years' experience in the IT sector, having held numerous technical roles spanning many different industries. With a passion for electronics, security, and mechanics, David pursues these interests both professionally and as a hobbyist.

INTRODUCTION

Driven by demands for cleaner emissions and increased vehicle safety for both drivers and pedestrians, the modern vehicle has become increasingly computerised, and now has more in common with an industrial control system than with a simple mechanically-controlled car from 30 years ago.

Modern vehicles consist of a multitude of different inter-connected process control systems which each govern or modulate a specific mechanical or environmental process. Control is gradually being taken away from the driver and placed under the supervision of embedded computerised control systems. These systems work together to automate the driving process in the pursuit of increased safety both for drivers and for other road users.

This automation is being achieved by integrating advanced driver assistance systems (ADAS) with the mechanical powertrain, to provide the vehicle with an increasing degree of awareness about its operational environment. The ADAS systems comprise individual components such as light detection and ranging (LIDAR) systems, laser range finders, forward-looking infra-red (FLIR) cameras, ultrasonic sensors, and stereoscopic vision systems, all of which are interconnected and communicate with other vehicle systems via the heart of the vehicle network, the controller area network bus (CAN-BUS).

We are now able to do more in our vehicles while on the move; modern in-vehicle infotainment (IVI) systems provide occupants with the ability to listen to audio and watch video from a variety of local and remote sources, and to make and receive phone calls, use satellite navigation, receive live traffic information, and even access the Internet. Due to the prevalence of these features and an industry push for standardisation, modern vehicle systems are becoming increasingly integrated with consumer mobile devices, and with publicly-accessible communications networks such as the Internet.

The use of telematics services to track vehicle movements and to collect performance and diagnostic data is now a widespread practice. These services are used both by vehicle manufacturers, in order to support warranty claims and regular vehicle maintenance, and by insurance companies, who are able to offer consumers lower insurance premiums in return for safe and responsible driving.

Vehicle owners can also use telematics services to interact with the vehicle remotely, for example using a phone app to activate climate control prior to starting a journey, activate the horn, or even unlock the doors. The prevalence of telematics in modern vehicles has enabled the European Commission to promote an initiative known as eCall (emergency call), which is intended to bring rapid assistance to motorists involved in a collision anywhere in the European Union. eCall will be standard feature of all new vehicles from 2018, with a follow-up system named Breakdown Call (bCall) following shortly after.

The integration of these technologies, services, and systems, together with the convergence of the vehicle environment with consumer mobile devices and the Internet, means that the attack surface of the modern vehicle is one of the largest for any single piece of transport infrastructure. In addition to this large attack surface, a vast quantity of data and metadata is generated, collected, and stored by manufacturers, telematics service providers (TSPs), emergency services, and various third-party companies on Internet-facing systems and back-end databases.

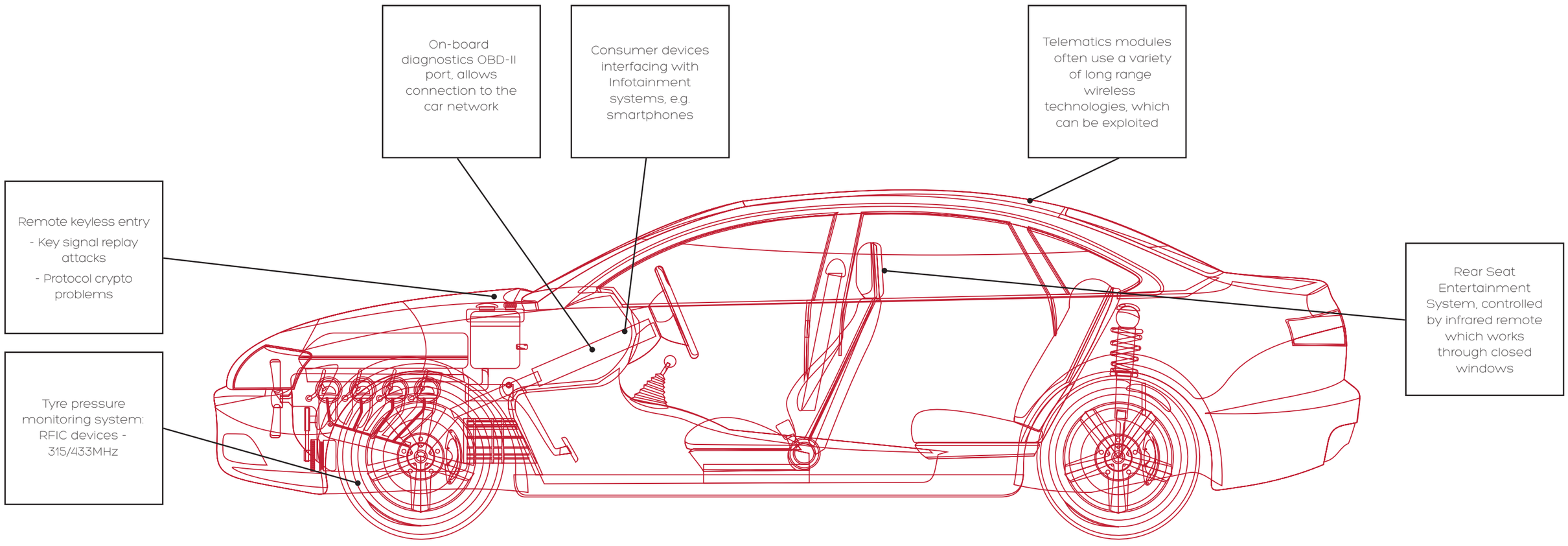
The interconnected nature of these different systems, services, and networks brings with it not only the concern that attacks upon automotive systems can have severe consequences from a public safety perspective, but also concerns surrounding big data such as consumer privacy, data ownership, and data retention. The obligation to protect consumer data from unauthorised access, both when stored and during transmission, has never been higher; but the demand for increased data sharing between organisations is also increasing, as is the ability for the security services to tap that data source to support operational intelligence,.

These facts, together with the sheer number of vehicles in use, mean that automotive systems are increasingly viewed as an attractive target by those with malicious intent. Because of this, the potential both for cyber-security weaknesses to exist and for those weaknesses to be exploited by threat actors is incredibly high.

Some of the security issues that specifically affect automotive systems include:

- In-vehicle infotainment systems – IVI systems expose a large attack surface and connect directly to the heart of the vehicle network, meaning any vulnerability present may allow manipulation of critical vehicle functions if successfully exploited.
- Telematics – Telematics services connect vehicles to Internet-facing systems, allowing operational data to be collected and limited remote control of vehicle functions, which can be exploited to compromise the security or safety of the vehicle.
- Vehicle diagnostics and software – Software is easily obtainable and in some cases poorly developed. Software can be reverse engineered to uncover sensitive information, allowing legitimate diagnostic services to be exploited to compromise the security or safety of the vehicle.
- Internal vehicle networks – Internal communications protocols used on-board the vehicle for communications between control modules are not secure and can easily be manipulated and used to control almost all critical vehicle functions.
- Automotive secure development lifecycle – The automotive industry is largely unfamiliar with the principles of a secure development lifecycle, leading to vulnerabilities being introduced into automotive systems during the design and development phases.
- Physical vehicle security – External access to internal vehicle network wiring allows attacks that compromise the security of the vehicle from outside.
- Intelligent transportation systems – Future plans for a fully integrated intelligent transportation network allowing vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) communications need to be carefully considered and developed with the help of the cyber-security industry.
- Advanced driver assistance systems – The increased attack surface and interconnected nature of these systems means that deploying these new systems within modern vehicles can have unforeseen consequences, introducing new attack vectors into the vehicle network.

AUTOMOTIVE SECURITY



AUTOMOTIVE SECURITY

While it has been known for some time in the vehicle modification and security industries that electronic vehicle systems contain exploitable vulnerabilities, it is only recently that academics [1], government [2], vehicle manufacturers, and the cyber security research community [3] have begun to focus on automotive security from a cyber perspective, as opposed to the traditional viewpoint of vehicle theft.

With the cost of advanced electronic components decreasing, the equipment required to interface with both wired and wireless vehicle networks is no longer cost-prohibitive for the hobbyist or casual hacker, security professional, or small criminal organisation. As a result the automotive industry is facing increased interest in the security of their systems from threat actors different to those to which they are accustomed.

In-Vehicle Infotainment

The IVI system typically represents the component with the largest attack surface within the vehicle network. The IVI system provides occupants with the ability to access telephony, audio, video, satellite navigation, live traffic information, and sometimes even provides Internet access. As a result of the IVI system being multi-functional there exist numerous wired and wireless interfaces to the system, some of which can be accessed by the occupants of the vehicle. These include the human-machine interface (HMI), USB ports, disk drives, auxiliary audio connectors, and Bluetooth or Wi-Fi wireless communications channels (which can also be targeted from outside the vehicle).

An IVI system is typically based around a system-on-chip or field-programmable gate array (FPGA) that features an ARM or x86 microprocessor supported by numerous smaller systems, which each contain specialised microcontrollers and firmware required to support their primary function. The software component of the IVI system is usually an operating system (OS) designed specifically for an automotive application, but could be based on either an open source OS such as Linux or a proprietary OS such as Microsoft Windows or QNX. In either case the OS and supporting systems will contain large amounts of code required to process data in many different forms, such as media parsing libraries, wired and wireless communication stacks, and user interface frameworks. Use of unmanaged languages such as C is common; these languages require skilled developers familiar with writing secure code, and subsequent thorough review, in order to ensure vulnerabilities are not introduced through the use of unsafe memory management functions [4].

Individual IVI system components may be designed and manufactured by different third-party companies, each of which may have different standards of quality when it comes to developing and testing secure code. As a result, the probability of security vulnerabilities being present in the software or firmware of any part of the IVI system is high. This represents a significant risk to the security profile of the vehicle, since there exists a logical network path, starting wirelessly from outside the vehicle, to the internal CAN-BUS network. Any vulnerability which could be exploited to gain control of the IVI system and send frames onto the internal CAN-BUS network could have catastrophic consequences for the safety or security of the vehicle.

It is also possible for malicious code to be deployed to the IVI system without the user's consent, if the user browses unsafe websites that attempt to exploit connecting systems. Such websites could inject malicious code into the web page which is in turn rendered by the browser. Malicious applications masquerading as an official application could also be unwittingly installed on a user's smartphone or onto the IVI itself.

Telematics

While in the past they were deployed only on large commercial fleets and heavy goods vehicles, wireless telematics services are now widely used throughout the private vehicle market. Telematics services allow the vehicle to collect and transmit operational data to the manufacturer's head-end telematics systems, and to receive data from manufacturer systems or other third-party service providers.

The bulk of the information collected and transmitted by the vehicle under normal operations consists of location information, timestamps, and data describing the status and condition of critical vehicle components; this data is used to support ongoing service schedules and warranty claims, and to provide real-world performance data for subsequent analysis. Data sent to the vehicle includes live traffic and navigational data, service alerts, and even over-the-air software upgrades. Some manufacturers' telematics services provide the vehicle owner with the ability to interact with the vehicle remotely via a phone app, allowing the owner to remotely activate climate control prior to beginning a journey, upload maps and navigational information to the IVI system, locate the vehicle using GPS, activate vehicle horn and lights, or even remotely unlock the doors to the vehicle.

The on-board telematics system is connected to multiple critical vehicle subsystems via the CAN-BUS network and consists of numerous smaller electronic systems. Wireless communication takes place over 2G, 3G, and even 4G networks (depending upon availability), and is provided by both a cellular modem and SIM card, or by a custom machine-to-machine module with the modem and SIM card electronics integrated into a single device. Some of the underlying telecommunications technologies used by telematics services, such as 2G and 3G, are inherently insecure due to their support for plain-text data transmission or weak encryption and lack of mutual authentication between the mobile device and the cellular base station.

This means that some poorly-implemented telematics solutions are vulnerable to attack by fooling the vehicle into connecting to a malicious cellular base station and then injecting NGTP (next generation telematics protocol) messages. This is due to the telematics solution provider relying solely upon the theoretical security provided by the underlying telecommunications network and not adding any further authentication or encryption to the communications protocol. Issues like this can present a risk not just to a single vehicle, but to an entire fleet or model range, if encryption keys that normally secure the wireless communications between the vehicle and telematics head-end systems are not guaranteed to be unique per vehicle or consist of predictable information such as the vehicle VIN which can be obtained through other techniques.

The European Commission has been promoting a telematics-based system known as Emergency Call (eCall), which aims to provide emergency assistance to motorists involved in a vehicle collision anywhere in the European Union. When vehicle systems detect a crash event has occurred, the vehicle automatically places the occupants in contact with the emergency services via the nearest public-safety answering point, and transmits critical sensitive data via a separate communication channel. This data includes information such as vehicle location, direction, status, vehicle identification number, vehicle propulsion storage type, and whether the call was triggered automatically or manually. eCall will be a standard feature of all new vehicles from 2018, with a follow-up system named Breakdown Call (bCall) following shortly after.

As with many complex vehicle systems, each component of an end-to-end telematics solution will be developed by different third-party manufacturers and telematics service providers (TSPs), all with different approaches to system security and secure software and firmware development. It is vital that not only the on-board electronics comprising the vehicle telematics system, but also the Internet-facing head-end systems of the TSP, are penetration tested and evaluated. If a TSP environment was compromised, it could potentially allow an attacker to launch attacks against thousands of vehicles at once, with disastrous consequences. Similarly any application that is designed to be deployed on a mobile device should be subjected to rigorous analysis and code review, as it communicates with the head-end telematics servers of the TSP. It is therefore important that the application does not reveal sensitive data such as encryption keys, or other information relating to the head-end server systems that could aid attackers in compromising the TSP.

[1] http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[2] http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf
[3] https://www.nccgroup.trust/media/481597/usb_under_the_bonnet_andy_davis_ncc_group_slides-2.pdf
[4] https://msdn.microsoft.com/en-us/library/bb288454.aspx

All Rights Reserved. © NCC Group 2015

Vehicle diagnostics and software

Diagnostic software is produced by manufacturers to aid both franchised dealers and independent garages in servicing the vehicle. The diagnostic software runs on a computer and connects directly to the vehicle network via the on-board diagnostics (OBD) connector, allowing virtually every vehicle subsystem to be interrogated and modified. As diagnostic software is able to modify virtually any vehicle subsystem or component, it can be used by those with malicious intent to compromise the security of the vehicle, for instance by programming new keys or disabling the immobiliser once the attacker has gained access to the cabin.

Since 1996 all vehicles are required to support a minimum set of diagnostic information from the OBD-II standard [5], using a standardised connector; however, there are numerous diagnostic protocols in use by different manufacturers today. None of these protocols provide an encrypted transport mechanism for communications with vehicle systems, and the authentication mechanisms available are weak and in some cases can easily be bypassed altogether.

Unfortunately, diagnostic software is easily obtained from online auction sites, or in some cases can be downloaded from the manufacturer. Diagnostic software is often not developed in line with best practice methods for security such as a secure development lifecycle, and can contain large amounts of both active and redundant code, written in multiple languages. This software can be reverse-engineered by both criminals and security professionals, to reveal sensitive data about the internals of the vehicle network and associated subsystems known as electronic control units (ECUs), which can aid in further attacks against the vehicle.

Sensitive data such as “SecurityAccess codes” used for authentication with specific ECUs can be retrieved from the diagnostic software. Once authenticated with an ECU it is possible to perform sensitive actions such as modifying ECU firmware, modifying data in memory, and launching manufacturer diagnostic routines. These actions are often exploited by the tuning community to improve performance, but can be used to alter the behaviour of safety-critical systems, which could have serious implications for the operational safety of the vehicle . Legitimate features of the software can also be used by attackers to compromise the safety or security of the vehicle, for example by disabling critical safety and security systems or by programming extra keys.

There is a further risk posed by vehicle diagnostics to the safety of the vehicle while in motion, some ECU diagnostic services can be accessed while driving, and can cause the ECU to become non-responsive or reset the ECU altogether, which has a dramatic impact upon the safety of the vehicle.

“Diagnostic software is often not developed in line with best practice methods for security such as a secure development lifecycle, and can contain large amounts of both active and redundant code, written in multiple languages.”

Internal vehicle networks

Most modern vehicles contain multiple interconnected wired and wireless networks, for transporting messages between individual ECUs and transmitting data from auxiliary sensors and actuators to ECUs governing a specific mechanical or environmental process. The core of the modern vehicle is the CAN-BUS network [6] which is used as the primary communications medium between almost all control modules, and is supported by other wired networks such as the Local Interconnect Network bus, FlexRay, and even Ethernet. Some wireless communications channels in the UHF (ultra-high frequency) and VLF (very low frequency) ranges are also employed for communications with tyre pressure monitoring systems (TPMS) and key fob features such as keyless ignition or remote locking.

[5] http://en.wikipedia.org/wiki/On-board_diagnostics
[6] http://www.computer-solutions.co.uk/info/Embedded_tutorials/can_tutorial.htm

Newer vehicles are described as being ‘Multi-CAN’, meaning they contain more than one CAN-BUS network. Networks can run at high (500 kbit/s), medium (250 kbit/s) or low speed (125 kbit/s), and are usually grouped by the control processes governed by their attached modules such as powertrain, chassis, body, and comfort/auxiliary, but are all interconnected. A CAN-BUS network is broadcast by nature, and control modules transmit messages onto the CAN-BUS network using a unique arbitration ID which identifies each message and indicates its priority. Each control module is programmed to only process specific CAN messages with IDs relevant to its operational function. CAN messages are not encrypted, but some manufacturers will use an additional application layer checksum for safety-critical messages to filter out invalid frames. Depending on the function of the module and the content of a CAN message, when the message is processed it may result in a physical action, for example activating or modulating a discrete electronic component such as an injector, relay, actuator, or motor in order to control a process.

Most vehicle functions are controlled via CAN messages, so if the correct message is known it is possible to control most aspects of vehicle behaviour such as unlocking doors, moving mirrors, and even interfacing with powertrain control processes to actuate the steering, accelerate the vehicle, or activate the brakes. This is easily accomplished by physically connecting a computer with a CAN-BUS adaptor to the CAN-BUS network via the OBD connector, or another location which exposes the CAN wiring, and sending CAN messages onto the network. This is obviously unsafe, and can have a serious effect on the operational safety of the vehicle.

Third-party devices which interface with the OBD connector [7] and use diagnostic protocols in order to provide information to the end user on a mobile device are also sold. Such devices are sometimes not subjected to appropriate testing and review, and any security vulnerabilities present in products such as these may in some cases be exploited by an attacker to gain control of the vehicle via the CAN-BUS network. The scenario is the same for any individual vehicle subsystem; if, for example, the IVI system or telematics control module is compromised by a remote attacker, it could be possible to interface with the CAN-BUS network and take control of the vehicle.

Other technologies such as FlexRay and Ethernet are gradually being introduced into the automotive environment to allow for communications and even diagnostics over IP. However, it is vital that the industry does not repeat the same mistakes made during the early days of Ethernet and TCP/IP deployment, which led to various types of attacks being possible against the Ethernet and TCP/IP communications stacks.

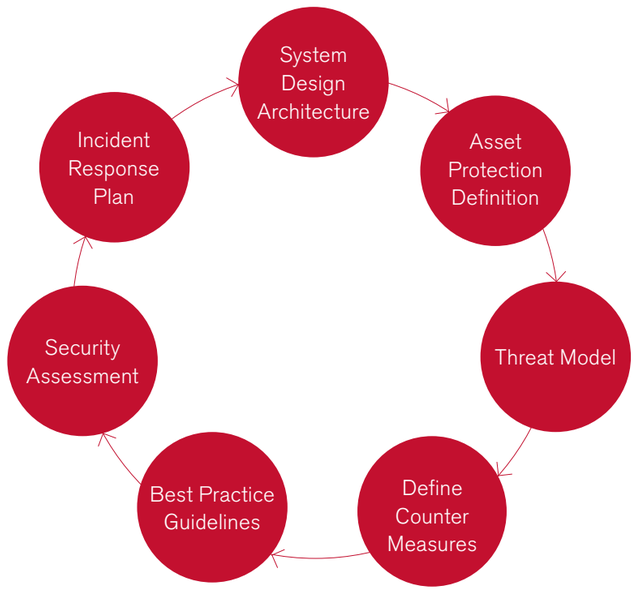
“Most vehicle functions are controlled via CAN messages, so if the correct message is known it is possible to control most aspects of vehicle behaviour such as unlocking doors, moving mirrors, and even interfacing with powertrain control processes....”

[7] http://www.amazon.co.uk/Supper-Bluetooth-Compatible-Android-Support/dp/B009NPAORC/

ASDL – Automotive Secure Development Lifecycle

NCC Group is actively engaging with members of the automotive industry, to encourage them to can safeguard their vehicles from attack by implementing secure development practices within the organisation. These practices include thorough threat modelling of both individual vehicle components and entire end-to-end solutions, training developers in secure code development, code review for software and firmware developed in house and by third parties, regular penetration testing of supporting infrastructure, and white- and black-box security assessments of vehicles and vehicle subsystems, both in isolation and when deployed in a final end-to-end solution.

The Automotive Secure Development Lifecycle is a cost-effective hardware and software engineering approach to cyber-security assurance, covering the entire development lifecycle within the automotive world. The model is intended to provide security assurance at each stage in the development lifecycle of vehicles and vehicle components. The ASDL consists of seven stages; however, all of them are underpinned with training, as this is seen as a core component of the model. The ASDL should be considered as a framework, rather than as a solution that replaces standards such as ISO 17799 or ISO 26262. The seven stages are shown below:



Clearly some OEMs and tier-one suppliers already perform security assurance activities within their business; therefore a first step is often to perform a gap analysis in order to identify which stages of the ASDL are missing and where additional help is required.

Physical vehicle security

Due to the damage that can be caused by an attacker with access to the vehicle CAN-BUS network, it is vital that components with connections to the internal vehicle network wiring itself cannot be trivially accessed from outside the vehicle. Unfortunately, the location of vehicle network wiring is not always identified as a security risk, and is instead viewed from a traditional engineering perspective, prioritising shortest routes, ease of assembly, and maximum commonality between models to reduce costs. This can result both in wiring being located in areas which are easy to access from the vehicle exterior and in redundant wiring which would normally connect to optional equipment on a higher-tier model being included on a base-model vehicle.

If the vehicle network can be accessed from outside, it may be possible to exploit this attack vector to gain access to the vehicle interior and use diagnostic software with the OBD connector to program new keys.

Intelligent Transportation Systems (ITS)

Intelligent Transportation Systems are advanced applications which aim to provide new services for public transportation systems and enable users to make safer, smarter, and more co-ordinated use of transport networks. EU directive 2010/40/EU [8] defines an ITS as a system in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport.

Applications, some of which are already deployed, include emergency vehicle notification systems, automatic speed enforcement, variable speed limits, collision avoidance systems, adaptive traffic management, smart traffic signals, electronic payment and toll management, and traffic incident alerting and management. These applications are possible using numerous underlying wireless technologies vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) communications.

Because of the vast number of interconnected systems within the ITS, and the use of numerous communications protocols (some of which are still being standardised) to support it, integrating the different components is inherently risky. Each application, protocol, and system must be developed in line with industry best practice guidelines for secure development, and the security rigorously tested to ensure the solution as a whole is not riddled with vulnerabilities. If any part of the intelligent transportation system infrastructure is compromised, this places all other components at risk from attack due to the interconnected nature of the end-to-end solution, and may allow attacks to spread throughout the network. This means that secure network architecture design and both physical and logical segregation of communications channels are crucial.

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF

Advanced Driver Assistance Systems (ADAS)

ADAS systems are designed to automate and enhance the driving process in the pursuit of safety and better driving. ADAS systems are technologies such as light detection and ranging (LIDAR) systems, laser range finders, forward looking infra-red (FLIR) cameras, ultrasonic sensors, and stereoscopic vision systems, all of which are interconnected via the internal vehicle network. Some ADAS systems can also communicate wirelessly between compatible vehicles (V2V) and with ITS infrastructure (V2I).

ADAS systems currently available include lane-keep assist, collision avoidance systems, adaptive cruise control, tyre pressure monitoring systems, and road sign recognition systems. When designed in conjunction with a safe human-machine interface, they should increase safety for vehicle occupants and other road users, and reduce collisions.

However, when added to a vehicle, these systems bring with them additional attack vectors and can increase the attack surface of the vehicle significantly, exposing the vehicle to attacks that use legitimate features of these systems to attack the vehicle or the driver.

For example, the RF communication channels used by these features can be analysed and exploited using software-defined radios (SDR) and open source software. In the case of some TPMS implementations, it is possible to perform a simple replay attack using an SDR and force the vehicle to display a TPMS low pressure event warning to the driver when in fact all tyres are inflated correctly. This could present a significant risk to the occupants of the vehicle if, for example, a VIP was on board and it was necessary to minimise the number of stops on the journey to avoid being exposed to attack.

Additionally, the interconnected nature of the ADAS, when deployed within a vehicle capable of V2V and V2I/I2V communications, means that there is now a logical path between vehicles and transport infrastructure. If one system in the chain becomes compromised this puts other systems at risk and may allow attacks to spread throughout the interconnected network.

Current status and conclusions

The increasing threat to the automotive industry has been recognised by government, manufacturers, and cyber security service providers alike, and numerous initiatives are currently underway [9] to begin to address this threat and to bring principles used within traditional enterprise environments (such as the secure development lifecycle) to the automotive world.

NCC Group has joined forces with automotive technology experts SBD to create a unique and strategic partnership and improve automotive cyber-security. The partnership combines the expertise of SBD in connected car architectures and automotive security with NCC Group's expertise in cyber security testing. Together they have created the Automotive Secure Development Lifecycle (ASDL), to help vehicle manufacturers and their suppliers mitigate cyber-security risks when developing connected cars.

These are the first steps to securing the automotive landscape; however, much more needs to be done to ensure that automotive systems and associated infrastructure cannot be exploited by those with malicious intent.

CONTACT US

0161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Manchester - Head office
Basingstoke
Cambridge
Cheltenham
Edinburgh
Glasgow
Leatherhead
Leeds
London
Milton Keynes
Wetherby

Europe

Amsterdam
Copenhagen
Luxembourg
Munich
Zurich

North America

Atlanta
Austin
Chicago
New York
San Francisco
Seattle
Sunnyvale

Asia Pacific

Sydney

www.nccgroup.trust
@nccgroupplc