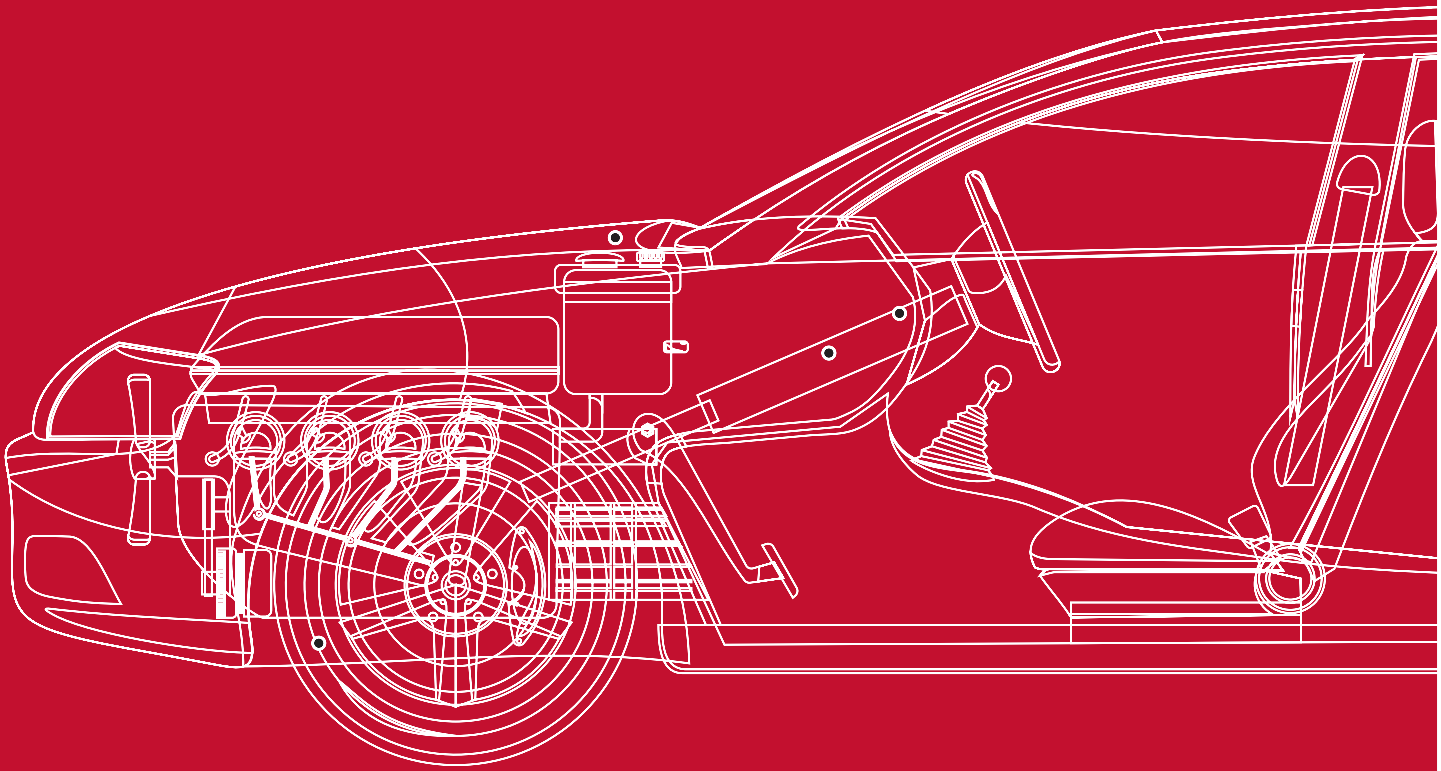


Latest threats to the connected car & intelligent transport ecosystem

CONTENTS

AUTHOR

David Clare

David is the technical lead for automotive testing and research at NCC Group. He specialises in securing embedded solutions with a focus on transport systems and in-vehicle networks. David has over ten years' experience in information security, having held numerous technical roles spanning many different industries. With a passion for electronics, mechanics and offensive and defensive cyber security, David pursues these interests both professionally and as a hobbyist.

Key points

- The modern vehicle has become increasingly computerised as the demand for cleaner emissions and better transport safety for drivers and pedestrians has grown.
- In the vehicle modification and security industries it has been known for some time that electronic vehicle systems contain exploitable vulnerabilities. However, it is only within the past decade that academics [1], government [2], vehicle manufacturers and the cyber security research community [3][4] have begun to focus on automotive security from a cyber perspective, as opposed to the traditional viewpoint of vehicle theft.
- Numerous initiatives are currently underway [10][20][21] to begin to address this threat and to bring the principles used within traditional enterprise environments (such as the SDL) to the automotive world.

Introduction

The modern vehicle has become increasingly computerised as the demand for cleaner emissions and better transport safety for drivers and pedestrians has grown. It now resembles a sophisticated cyber-physical control system which is capable of autonomous functions. This is enabled through the fusion of intelligent software algorithms and cutting-edge hardware, providing environmental awareness and high throughput data processing.

Modern vehicles consist of a multitude of different inter-connected process control systems which each govern a specific mechanical process. These take input from a complex array of real-time sensors and connected data sources.

Physical control of the vehicle is gradually being taken away from the driver and placed under the supervision of these embedded process control systems. These systems work together to automate the driving process in the pursuit of increased safety for drivers and other road users.

This automation is achieved by integrating Advanced Driver Assistance Systems (ADAS) with the mechanical powertrain in order to provide the vehicle with an increasing degree of awareness about its operational environment.

The ADAS systems consist of individual components such as Light Detection and Ranging (LIDAR) systems, Forward-Looking Infra-Red (FLIR) cameras, ultrasonic sensors, stereoscopic vision systems and Internet-connected data sources. These systems can communicate via a single core network such as a Controller Area Network (CAN) BUS. However, they are often segregated or segmented and are increasingly becoming mixed with newer in-vehicle network solutions such as FlexRay and Ethernet. This creates a complex mixed network with a large number of connected nodes and gateways.

We are now able to do more in our vehicles while on the move. Modern In-Vehicle Infotainment (IVI) systems allow occupants to listen to audio and watch video from a variety of local and remote sources, to make and receive phone calls, use satellite navigation, receive live traffic data, request concierge services, real-time vehicle feature updates 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 publicly-accessible communications networks such as the Internet. They are also adopting consumer communication technologies such as Bluetooth Low Energy (BLE) and ZigBee.

Telematics services being used to track vehicle movements and collect performance and diagnostic data is now a widespread practice.

These services are used by vehicle manufacturers to support warranty claims and regular vehicle maintenance as well as companies specialising in bulk data collection, in order to provide analytics services to third-parties. In addition, these are used by insurance companies looking to offer safe and resposible drivers lower premiums.

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, activating the horn to locate the vehicle, or even remotely unlocking the vehicle and starting the engine.

The prevalence of telematics in modern vehicles has enabled the European Commission to promote an initiative known as Emergency Call (eCall), which is intended to bring rapid assistance to motorists involved in a collision anywhere in the European Union. eCall will be a standard feature of all new vehicles from 2018, with a follow-up system called 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 is generated, collected, and stored on both internet-facing systems and back-end databases by Original Equipment Manufacturers (OEMs), Telematics Service Providers (TSPs), emergency and security services as well as various third-parties.

The connected relationship 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. In addidtion, there are concerns surrounding the collection of data such as consumer privacy, data ownership, data retention and both authorised and unauthorised surveillance.

The obligation to protect consumer data from unauthorised access, both when stored and in-transit, has never been more regulated. However, the demand for increased data sharing between both corporate enterprises and national government organisations is also increasing. As is the ability for the security services to tap into these data sources to support operational and threat intelligence.

These facts, together with the sheer number of vehicles in use nationally and internationally, mean that automotive systems are increasingly viewed as an attractive target by those with malicious intent. Because of this, the potential for cyber security weaknesses to exist and be exploited by malicious threat actors has never been higher.

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

- IVI systems: These connect directly to the heart of the vehicle network, exposing it to a large wireless and wired attack surface. This means that any vulnerabilities present may allow attackers to not only collect and manipulate sensitive personal data. It could also allow direct manipulation of critical vehicle functions if the attacker is able to pivot into the in-vehicle network, resulting in a cyber-physical attack.

- Telematics: Telematics services connect vehicles to Internet-facing or Internet-connected systems, allowing operational vehicle data to be collected and in some cases provide remote control of vehicle functions. If vulnerable, this could be exploited to compromise the safety or security of the vehicle.

- Vehicle diagnostics and software: Software is often publically available but is unfortunately often poorly developed. This is due to international regulation designed to ensure that non-franchised and third-party dealerships are able to diagnose and repair vehicle faults.

- Authentication between diagnostic software and vehicle Electornic Control Units (ECUs): This is often based on challenge/response algorithms which are stored client-side within the diagnostic software. The software can be reverse engineered by an attacker to uncover sensitive information, allowing legitimate diagnostic services to be exploited in order 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 they often do not contain a signature to verify the authenticity of the message. This means that it can easily be manipulated and used to control almost all critical vehicle functions via injection and spoofing of a message.

- Secure Development Lifecycle: The automotive industry is largely unfamiliar with the principles of a SDL when it comes to embedded systems and control modules. This leads to vulnerabilities being introduced into automotive systems during the design and development phases as new features are requested and added.

  The reliance on coding guidelines specific to safety applications such as MISRA-C, are not necessarily suitable when the solution is being developed. It requires a high security profile and results in insecure code being re-used across the industry.

- Physical vehicle security: External access to internal vehicle network wiring allows attackers to compromise the security of the vehicle from the outside when the vehicle is locked and alarmed.

  Convenience technologies such as Remote Keyless Entry (RKE) and keyless start are vulnerable to Relay Station Attacks (RSA) and amplification attacks which are difficult to defend against.

- Intelligent Transportation Systems (ITS): Future plans for a fully integrated and resilient 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.

- ADAS and autonomous vehicles: The increased attack surface and inter-connected nature of these new systems means that deploying them within modern vehicles can have unforeseen consequences, introducing new attack vectors into the vehicle network.

- Academics and security researchers: Are beginning to explore and discover weaknesses in sensors and environmental awareness technologies used in autonomous vehicles [12].

Automotive cyber security

In the vehicle modification and security industries it has been known for some time that electronic vehicle systems contain exploitable vulnerabilities. However, it is only within the past decade that academics [1], government [2], vehicle manufacturers and the cyber security research community [3][4] 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 they are accustomed to, and often possessing a much higher technical skillset.

In-Vehicle Infotainment

The IVI system typically represents the component with the largest attack surface within the vehicle network. It provides occupants with the ability to access telephony, audio, video, satellite navigation and live traffic information. Sometimes it even provides Internet connectivity and access to concierge services.

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 while some are exposed remotely. These include the Human-Machine Interface (HMI), USB ports, disk drives, auxiliary audio connectors, Bluetooth or Wi-Fi wireless communications channels and Internet-connected telematics services.

An IVI system is usually based around a system-on-chip or Field-Programmable Gate Array (FPGA) that features an ARM or x86 microprocessor and is supported by numerous smaller systems containing specialised microcontrollers and firmware required to support its primary function.

The software component of the IVI system is typically an Operating System (OS) designed specifically for an automotive application. It is often 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. For example, 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 [5].

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 and it represents a significant risk to the security profile of the vehicle. Since there is 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 core vehicle network could have catastrophic consequences for the safety or the vehicle's occupants.

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 or accesses media originating from an untrusted resource. Such resources could contain malicious code which is triggered when the IVI system accesses the infected resource.

Malicious applications masquerading as an official application could also be unwittingly installed on a user's smartphone or onto the IVI itself. This in-turn provides an attack path both to the user's mobile device and the in-vehicle network.

Telematics

Historically, telematics systems were deployed only on large commercial fleets and heavy goods vehicles. However, 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 head-end telematics systems under the control of a Telematics Service Provider (TSP), and to receive data from manufacturer systems or other third-party service providers.

The majority 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 then 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 the vehicle horn and lights or even remotely unlock the doors to the vehicle.

The on-board telematics system is connected to critical vehicle subsystems via the core vehicle network and consists of numerous smaller electronic systems. Wireless communication takes place over 2G, 3G and even 4G networks (depending upon availability). It 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 Next Generation Telematics Pattern (NGTP) messages. This is because the telematics solution provider relies solely upon the theoretical security provided by the underlying telecommunications network and it does not add any further authentication or encryption to the communications protocol at layers above.

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 Identification Number (VIN) which can be obtained through other techniques, this can present a risk. Not just to a single vehicle but to an entire fleet or model range.

The European Commission has been promoting a telematics-based system known as eCall which aims to provide emergency assistance to motorists involved in a vehicle collision anywhere in the EU. When vehicle systems detect a crash event has occurred the vehicle automatically opens a voice channel to the emergency services and transmits critical, potentially sensitive data via a separate communication channel. This data includes information such as vehicle location, direction, status, VIN, 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 called 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 TSPs, all with different approaches to system architecture 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 were to be compromised, it could potentially allow an attacker to launch attacks against thousands of vehicles at once. This could have 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.

Recent attacks targeting the legacy telephony signalling protocol set, Signalling System No 7 (SS7), could also affect certain vehicle telematics systems and serves as a wake-up call for solution designers implementing the next generation of telematics services. While attacks targeting SS7 have been known about for decades[13][14][15], the telephony industry has been slow to address issues affecting this protocol standard. This problem has only recently caught the attention of government ministers due to high profile research[16][17] and real-world criminal exploitation[18].

Attacks against SS7 can allow the subscriber's location to be identified, SMS messages to be intercepted and re-routed, the subscriber service to be blocked (DoS), incoming calls to be redirected and outgoing calls to be intercepted.

In July 2016 the National Institute for Standards and Technology (NIST) declared that SMS-based two-factor authentication should be abandoned in favour of token-based access [19]. This was due to the vulnerabilities present in SS7 which allowed attackers to reroute authentication codes sent via SMS to victim devices and to mobile devices under their control.

While these issues and the resultant NIST recommendation largely affect the enterprise IT arena and specifically the banking sector, some poorly implemented telematics systems use SMS messages for Command and Control (C&C) or even telematics module authentication with head-end TSP systems. While real-world criminal exploitation of vehicle telematics systems using SS7 has not yet been reported publicly, it is highly likely that security researchers and malicious actors alike will begin to apply these exploit techniques to the automotive sector.

Location and tracking of high-value vehicles and Ultra High Net-Worth Individuals (UHNWI) would be of significant interest to criminal actors. Additionally, the ability for attackers to intercept and reroute C&C messages used within telematics solutions to enable attacks against fleets of vehicles poses a significant risk. SMS messages were often chosen for critical functions in legacy systems due to their low bandwidth requirements and poor connectivity in many geographic areas. However with improvement of 3G and 4G coverage, SMS can be deprecated and fully encrypted end-to-end communication channels can be established for all data in transit.

Big data

Data is increasingly viewed as being the world's most valuable commodity, and collections of extremely large data sets (collectively known as big data) can be analysed to reveal patterns, trends, and associations, especially relating to human behaviour. This includees interactions between individuals or interactions between individuals and online services and systems. This has serious implications for TSPs with regard to the type and quantity of data collected, where and how it is stored and whether the data can be considered as Personally Identifiable Information (PII).

This concern also affects system level implementations collecting smaller datasets, due to the system architects and developers needing to ensure that data is securely stored and the end-user has the capability to securely erase all collected data when they desire to do so.

Unfortunately many implementations either do not erase collected data at all or do so in an insecure manner, where the data can still be recovered by an attacker with sufficient knowledge of the system implementation. This results in significant implications for the rental and used car markets where a single vehicle can amass data associated with many individuals. PII such as phone numbers, SMS messages addresses and travel locations can fetch a high price on the black market, especially when the data pertains to Ultra-High Net-Worth Individuals (UHNWI) which are a high value target for attackers.

An EU initiative called the General Data Protection Regulation (GDPR) [11] has been created with the intention of strengthening and unifying data protection for all individuals within the EU and addresses the export of personal data outside of the EU. This particular initiative has far-reaching implications for the transport industry as a whole regarding the either intentional or unintentional collection of data via connected vehicle systems.

Vehicle diagnostics & software

Diagnostic software is produced by manufacturers to aid both franchised dealers and non-franchised 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 through a dedicated hardware interface. This allows almost every vehicle subsystem to be interrogated and modified.

As diagnostic software is able to modify any vehicle subsystem or component virtually, it can be used by those with malicious intent to compromise the safety or security of the vehicle. For example, by programming new keys to the vehicle security module, disabling the vehicle alarm systems, uploading modified calibration data to the Engine Control Module (ECM) or even disabling airbags and Supplementary Restraint System (SRS) components.

Since 1996 all vehicles have been required to support a minimum set of diagnostic information from the OBD-II standard [6] 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 communication with vehicle systems. The authentication mechanisms available are weak and in some cases can easily be bypassed altogether.

Pirated diagnostic software is easily obtained from online auction sites, or in some cases legitimate copies can be downloaded from the OEM online technical services website. Diagnostic software is often not developed in line with best practice methods such as a SDL, and can contain large amounts of active and redundant code, written in multiple languages. This software can be reverse-engineered, to reveal sensitive data about the internals of the vehicle network and associated subsystems known as ECUs. This can aid in further attacks against the vehicle.

Sensitive assets such as seed/key algorithms used for challenge/response authentication with vehicle ECUs can be retrieved from the diagnostic software. Once authentication has taken place with an ECU, it is possible to perform sensitive actions such as re-flashing ECU firmware, modifying data in memory and running manufacturer diagnostic routines.

These actions are often exploited by the tuning community to improve performance. They can also 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 or falsifying vehicle mileage.

There is also a further risk posed by vehicle diagnostics to the safety of the vehicle while in motion. This is because some Unified Diagnostic Services (UDS) functions can be accessed while the vehicle is being driven. Certain diagnostic services allow the state of I/O lines to be controlled and provide the ability to test motors, solenoids and actuators which can have a disastrous effect on vehicle safety if executed during vehicle operation. For any given vehicle it is often possible to cause an ECU to reset or to become unresponsive through the use of basic diagnostic services, which do not require authentication or via uniquely constructed malicious messages. This can for example, result in the engine and electronic systems turning off and complete loss of power.

The fact that these issues are common among almost all vehicles demontrates that it is imperative OEMs urgently begin to implement thorough testing of all diagnostic and engineering functions under various different vehicle operational conditions.

Low-level measurement and calibration protocols such as CAN Calibration Protocol (CCP) and Universal Measurement and Calibration Protocol (XCP) are often used during the ECU development process or in EOL End-Of-Line (EOL) programming and calibration tools and then disabled on production systems. However these protocols are often accidentally left enabled or can be re-activated through a UDS diagnostic routine. The protocols provide low level access to ECU volatile and non-volatile memory and allow live tuning of parameters to take place in real-time.

While significant knowledge of the embedded device and memory structure is required to perform data acquisition or alter ECU calibration, sometimes it is possible to determine certain properties by reverse-engineering OEM diagnostic software. This is due to the fact that developers often do not correctly separate code intended for internal or development use, only from the code used in production software.
In many cases, engineering and development code or data is still resident in OEM dealership-level software but just not directly used by the software application. Such issues such have been exploited by the tuning and modification community to alter the calibration of ECUs, which could not be tuned by simply flashing modified firmware via UDS.

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. Also from actuators to ECUs that govern a specific mechanical or environmental process. Currently, most vehicles use CAN-BUS as their core vehicle network [7] and used as the primary communications medium between almost all control modules. It is supported by other wired networks such as the Local Interconnect Network bus, FlexRay, and Ethernet. Some wireless communications channels in the Ultra-High Frequency (UHF) and Low Frequency (LF) ranges are also employed for communications with Tyre Pressure Monitoring Systems (TPMS), remote sensors as well as key fob features such as keyless ignition and Remote Keyless Entry (RKE).

Newer vehicles are described as being 'Multi-CAN', which means 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. This 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 in order to filter out invalid frames. This is not a security measure and is used only to maintain system stability in the event of random bit-flipping caused by interference. 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. This includes 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 injecting CAN messages into the network. As long as the data bytes of the message (including any counters and checksum values) are correct, and the injected message is being transmitted at a quicker rate than the target message being overwritten by the attacker, the modules connected to the CAN-BUS network will accept the attacker's message as valid. This is obviously unsafe and can have a serious effect on the operational safety of the vehicle.

Third party aftermarket devices which interface with the OBD connector [8] and use diagnostic protocols in order to provide information to the end user on a mobile device are now commonly available. Such devices have not, from our experience, been subjected to appropriate testing and review, and any security vulnerabilities present in products such as these may 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 with a remotely accessible wireless interface. 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.

The use of multi-protocol Gateway Modules (GWMs) to segregate and segment the vehicle network is becoming commonplace among most new vehicles. The wide-scale deployment of these devices represents a positive step in the right direction with regards to OEMs recognising the need for security in the vehicle network, they should only be viewed as a stepping-stone to more secure in-vehicle networks designed upon an Ethernet physical layer. The superior bandwidth of Ethernet combined with the many access-control and firewall filtering techniques that can be employed against layers two through seven provides a superior network environment where messages can be more easily signed, authenticated and encrypted.

Ethernet is gradually becoming more common in automotive systems and is being used for both in-vehicle network communications and diagnostics over IP. It is expected that Ethernet will eventually replace (CAN) BUS as the core vehicle network medium. However, it is vital that the industry does not repeat the same mistakes made during the early days of Ethernet and TCP/IP deployment. This led to various types of attacks being possible against communications stacks due to it being trivial for an attacker to spoof either IP addresses or MAC addresses to bypass access control rulesets. Implementations that allow VLAN tagging need to be subjected to thorough review and testing to ensure that attackers cannot perform VLAN hopping attacks and pivot around the in-vehicle network.

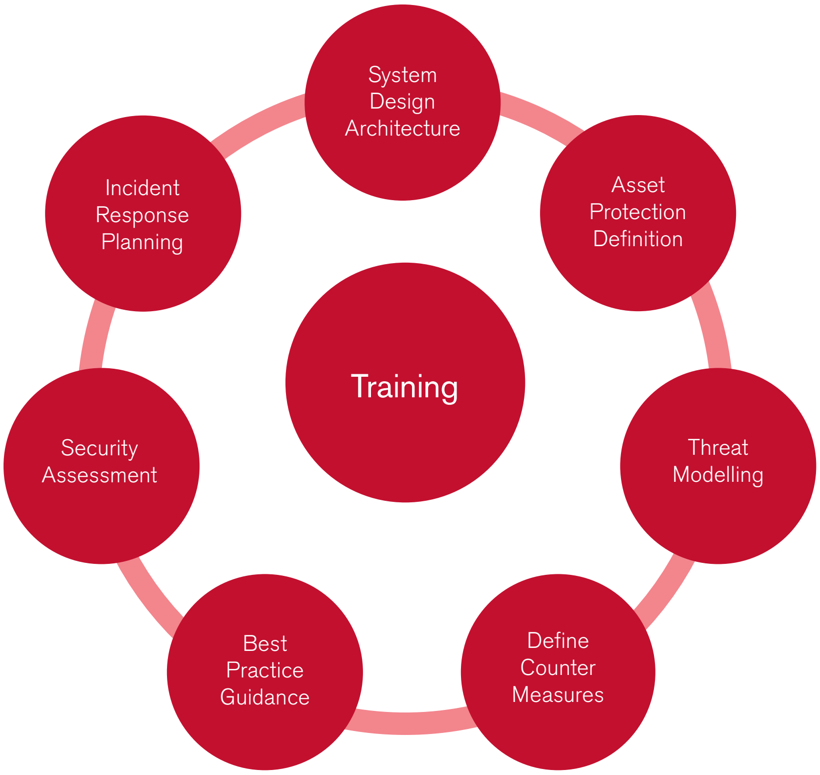
SDL

NCC Group actively engages with the automotive industry in order to encourage them to safeguard their vehicles from attack through the implementation of secure development practices within the organisation.

These practices include threat modelling of both individual vehicle components and entire end-to-end solutions, training developers in secure code development, code reviews for software and firmware developed in-house and by third parties, regular penetration testing of supporting infrastructure and “white box” and “black box” security assessments of vehicles and vehicle subsystems. This could be in isolation or when deployed in a final end-to-end solution.

The SDL provides security assurance at each stage of the development lifecycle for systems and components. The approach ensures that system-level attack points are recognised and departments within an organisation can agree upon who implements each countermeasure.

Some vehicle manufacturers and 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 SDL are missing and where additional help is required.



Physical vehicle security

It is vital that components with connections to the internal vehicle network wiring itself cannot be trivially accessed from outside the vehicle. This is due to the damage that can be caused by an attacker with access to the core vehicle network.

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 wiring can be accessed from the outside, it is often possible to exploit this attack vector to gain access to the vehicle interior by waking up the (CAN) BUS network and authenticating to the module which stores the vehicle Car Configuration File (CCF). The properties are then modified to disable vehicle security mechanisms, where further diagnostic routines can then be executed. This can provide potential entry to the vehicle interior and allow the attacker to enter the vehicle undetected. In some cases, an attacker can then programme a new key to the vehicle via the OBD port resulting in vehicle theft.

New convenience features such as RKE are being widely exploited by organised criminal gangs using devices built with low-cost Commercial-Off-The-Shelf (COTS) products. RKE systems are vulnerable to what is known as RSA and various amplification attacks.

A relay station attack proxies the LF signal which is sent by the vehicle to determine if the key-fob is nearby. This is done through one relay device being positioned near to the vehicle, transmitting a second relay device which is held by an attacker within range of the vehicle key-fob.

The key-fob does not have the capability to determine if it is really in close-proximity to the vehicle or if the LF signal it received is being relayed. It therefore trusts the LF signal regardless. The key-fob then transmits the UHF unlock code back to the car. The attacker can now enter the vehicle and relay a second LF signal used for starting the ignition over to the key-fob. This responds in the same way, allowing the attacker to start the engine and steal the vehicle. This attack does work over long distances and is only limited in range by the strength of the carrier signal used to relay the original LF signal emitted by the vehicle and the two relay stations.

An amplification attack uses a device to greatly amplify the LF signal emitted by the vehicle such that if the key-fob is nearby, it will pick up this LF signal and send the UHF signal back to the car to unlock the doors. The attacker can then enter the vehicle and amplify the signal used to locate the key and start the ignition sequence in the same way.

RSA and Amplification attacks are extremely difficult to defend against, as the delay incurred by relaying or amplifying the signal is extremely small (around 10ns). This makes detection of delay via sampling the authentication sequence almost impossible for embedded processors that are not fast enough to detect a difference that small.

Intelligent Transportation Systems (ITS)

ITS are advanced applications which aim to provide new services for public transportation systems, enabling users to make safer, smarter, and more co-ordinated use of transport networks. EU directive 2010/40/EU [9] defines an ITS as a system in which information and communication technologies are applied in the field of road transport. This includes infrastructure, vehicles users, in traffic and mobility management and 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 as well as traffic incident alerting and management. These applications are possible through the use of numerous underlying wireless technologies including 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 in order to ensure the solution as a whole is robust.

If any part of the ITS infrastructure is compromised, this places all other components at risk from attack due to the interconnected nature of the end-to-end solution. It also 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.

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 LIDAR systems, laser range finders, forward-looking infra-red (FLIR) cameras, ultrasonic sensors and stereoscopic vision systems.

These are all 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, as well as 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. Therefore, exposing the vehicle to attacks that use legitimate features of these systems in order to attack the vehicle or the driver.

For example, the Radio Frequency (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 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 & conclusions

The increasing threat to the automotive industry has been recognised by government, manufacturers, and cyber security service providers alike. Numerous initiatives are currently underway [10][20][21] to begin to address this threat and to bring the principles used within traditional enterprise environments (such as the SDL) to the automotive world.

NCC Group is a strategic cyber security and assurance partner to many of the world's OEMs and Tier Ones. We help with the development of robust security programmes designed to ensure that security is considered at every stage of product development.

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

References

[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/uk/our-research/usb-under-the-bonnet-implications-of-usb-security-vulnerabilities-in-vehicle-systems/ [4] http://illmatics.com/Remote%20Car%20Hacking.pdf

[5] https://msdn.microsoft.com/en-us/library/bb288454.aspx

[6] http://en.wikipedia.org/wiki/On-board_diagnostics

[7] https://elearning.vector.com/vl_can_introduction_en.html

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

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

[10] https://www.nccgroup.trust/uk/our-research/usb-under-the-bonnet-implications-of-usb-security-vulnerabilities-in-vehicle-systems/ [11] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

[12] https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles.pdf

[13] http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf

[14] http://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf

[15] http://www.rdc.cz/en/publications/publications/dufkova07ss7tracker.pdf

[16] https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

[17] https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf

[18] http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[19] https://pages.nist.gov/800-63-3/sp800-63b.html

[20] http://standards.sae.org/wip/j3061/

[21] https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Contact

0161 209 5111
AutomotiveSecurity@nccgroup.trust
@nccgroupplc
www.nccgroup.trust/automotive

www.nccgroup.trust
@nccgroupplc