

Secure Connected Cars For a Smarter World

Whitepaper

Author:

Timo van Roermund,
Security Architect, BU Automotive
NXP Semiconductors



-- This page is intentionally left blank --

Contents

| | |
|---|----|
| Introduction..... | 1 |
| Connectivity – Driving the need for security..... | 2 |
| Potential risks..... | 3 |
| Market demand..... | 4 |
| The challenge | 5 |
| Paradigm shift..... | 6 |
| From after-thought to integral approach..... | 7 |
| Standardization | 7 |
| Security needs | 8 |
| Defense in depth | 8 |
| Securing the vehicle electronics architecture | 9 |
| Risk analysis..... | 11 |
| Life-cycle management | 12 |
| Summary | 13 |
| Hardware as a trust anchor..... | 15 |
| Secure hardware solutions..... | 16 |
| Secure Car Access solutions | 16 |
| Secure Elements..... | 17 |
| Secure MCUs | 17 |
| Smart IVN transceivers..... | 18 |
| Example use cases..... | 19 |
| V2X..... | 19 |
| Car-to-cloud communication | 20 |
| Central gateway..... | 21 |
| Conclusions..... | 23 |
| Definitions | 24 |
| References..... | 29 |
| About the author..... | 30 |
| About NXP | 30 |

-- This page is intentionally left blank --

Introduction

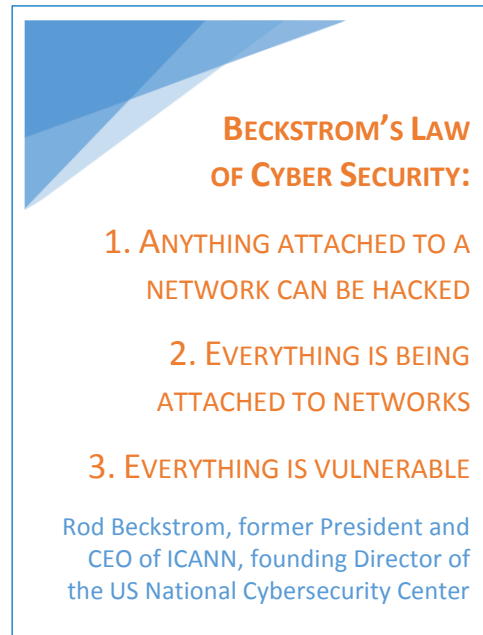
The automotive industry is rapidly evolving and NXP is at the forefront of this shift, helping transform the car from a simple mode of transport to a personalized mobile information hub. NXP brings V2X communications, telematics, and in-vehicle networking into the car, as well as wireless technologies for vehicle access, Near Field Communication (NFC) and multi-standard digital broadcast reception. NXP is also driving innovation in advanced technologies, such as car radar and advanced driver assistance systems (ADAS).

All these electronic functions bring great benefits to the driver, increasing comfort, convenience, safety and efficiency. But these features come with new risks, too. Modern vehicles are gradually turning into 'smartphones-on-wheels', which continuously generate, process, exchange and store large amounts of data. Their wireless interfaces connect the in-vehicle systems of these 'Connected Cars' to external networks such as the internet, enhancing consumer experience by enabling new features and services. But this connectivity also makes the Connected Car vulnerable to hackers who attack the vehicle by seeking and exploiting weaknesses in its computer systems or networks. In fact, several studies (e.g. [1]) have already warned some years ago that hacking into a car is possible, and more recently hackers indeed demonstrated that they

could gain remote control over vehicles [2][3]. The same day, U.S. Senators Markey and Blumenthal introduced an automotive security bill [4] that would establish federal standards to both secure vehicles and protect user privacy. This bill followed after Senator Markey's earlier report [5] that stated that the technology systems and data in today's cars and trucks are vulnerable to theft, hacking and the same invasions faced by any technical system today.

Steps need to be taken now: the Connected Car must be secured, to ensure the correct functioning of all in-vehicle systems, as well as user privacy. This implies a paradigm shift in the design of in-vehicle electronics. Traditionally, there has been a strong focus on *safety*, meaning that for example the brakes should function correctly under all circumstances. Safety will remain equally important in the future, but the increasing amount of electronics and software in vehicles will additionally require *security*, to protect the vehicle against hackers.

NXP has been developing security ICs for decades, and our best-in-class solutions are used all over the world to secure sensitive applications like electronic passports and electronic payment systems. By leveraging this expertise and deep security know-how, we have been able to create a rich portfolio of security products that helps OEMs and Tier-1s to protect their vehicles against cyber-attacks. These products allow end users to profit from all the benefits of new applications and technology, without having to worry about their personal safety and their privacy.



BECKSTROM'S LAW OF CYBER SECURITY:

1. ANYTHING ATTACHED TO A NETWORK CAN BE HACKED
2. EVERYTHING IS BEING ATTACHED TO NETWORKS
3. EVERYTHING IS VULNERABLE

Rod Beckstrom, former President and CEO of ICANN, founding Director of the US National Cybersecurity Center

Connectivity – Driving the need for security

Until recently, cars have been isolated from their environment and from the internet. The only exception was maybe the interface for vehicle diagnostics, but because this OBD-II port is a wired interface, it could rely on the physical protection offered by the vehicle's chassis, like the electronic control units (ECUs) and the in-vehicle network (IVN).

But things are changing rapidly: most modern cars already allow smartphones to be paired via Bluetooth with the car radio for hands-free phone calls or to play music. And it doesn't stop there: many modern cars are wirelessly connected to the internet, for example to enable additional services in the car and, to a certain extent, provide for remote control over the car such as remote unlocking and starting. To improve safety, these cars will furthermore be equipped with eCall and V2X communication technologies, complemented by ADAS systems that offer advanced driving assistance features and ultimately, autonomous driving.

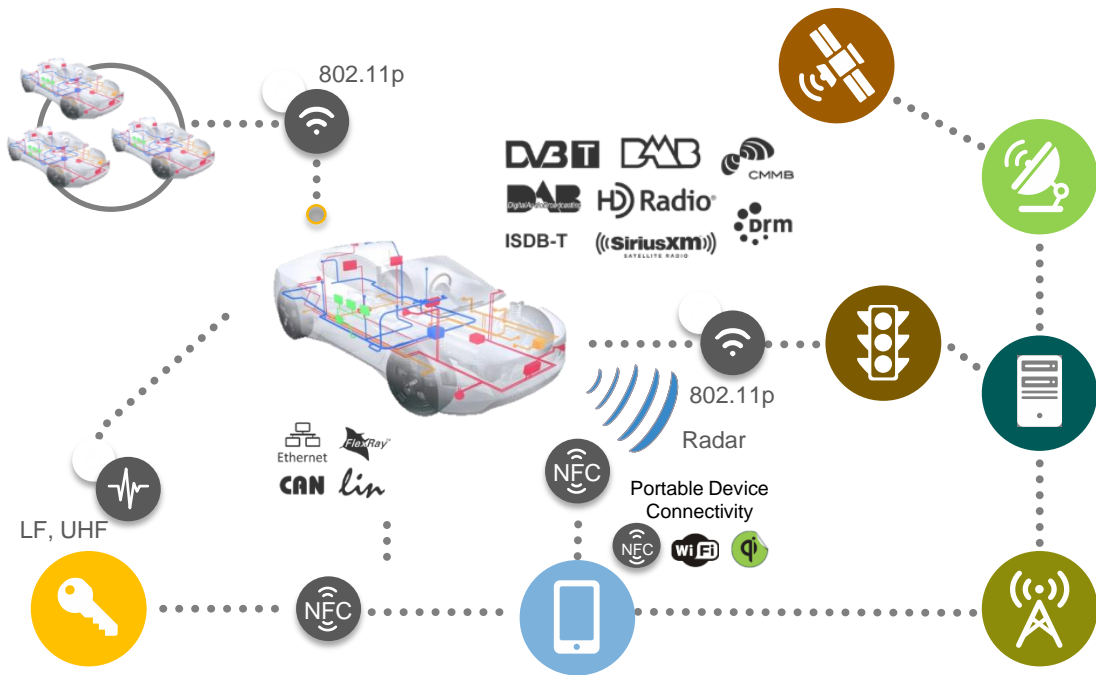


Figure 1: Various interfaces of The Connected Car

These wireless technologies bring great benefits to the driver: for example, *comfort* is increased because you can remotely enable the air conditioning systems to cool the cabin shortly before driving home, in summer time. *Convenience* can be increased because, for example, your in-car entertainment system is seamlessly synchronized with your phone and via your phone to your media collection at home. Last but certainly not least, the introduction of ADAS helps to increase *safety and efficiency*, for example by using information from nearby vehicles to prevent collisions, or by using information provided by road infrastructure or the cloud to reduce the travel time.

Potential risks

Despite all these advantages, these new features come with new risks, too. For example:

- Traffic information provided by infrastructure and the cloud should be trustworthy. You don't want someone to broadcast traffic jam warnings for his own route, thereby "clearing his route" and gaining time, at the cost of others.
- Autonomous Emergency Braking systems can prevent a crash or reduce the impact speed of a crash by applying the brakes independent of driver input. But it should not be possible for hackers to activate this system by sending fake V2X messages to a vehicle, or by manipulating the safety-critical communication inside the vehicle.
- eCall systems bring rapid assistance to motorists involved in a collision, by automatically sending post-crash information to the emergency call center. You don't want third parties to get access to this personal data.
- Automated Vehicle Identification allows the car to identify itself for seamless access to a parking or a toll road. When not protected, hackers could steal for example personal data including payment details.
- Car sharing systems allow access to a vehicle via a smart card or mobile device. If not protected well, a thief might be able to abuse this system to gain access to the vehicle.
- The OBD-II port offers diagnostic and reporting capabilities, allowing one to e.g. rapidly identify and remedy malfunctions within the vehicle. But attackers may use it to gain access to the in-vehicle network, potentially even remotely (via Bluetooth or cellular dongles).
- Pay-as-you-drive insurance schemes may allow you to reduce your monthly insurance premium, because you only pay for the miles you actually drive and based on your driving style. However, you don't want unauthorized third parties to get access to the same data and get insights into your driving habits.
- Car owners may want to chip-tune their engine, to increase performance of the engine. OEMs may want to protect against such manipulation by the vehicle owner, because it may have negative consequences for the reliability and the emission levels.

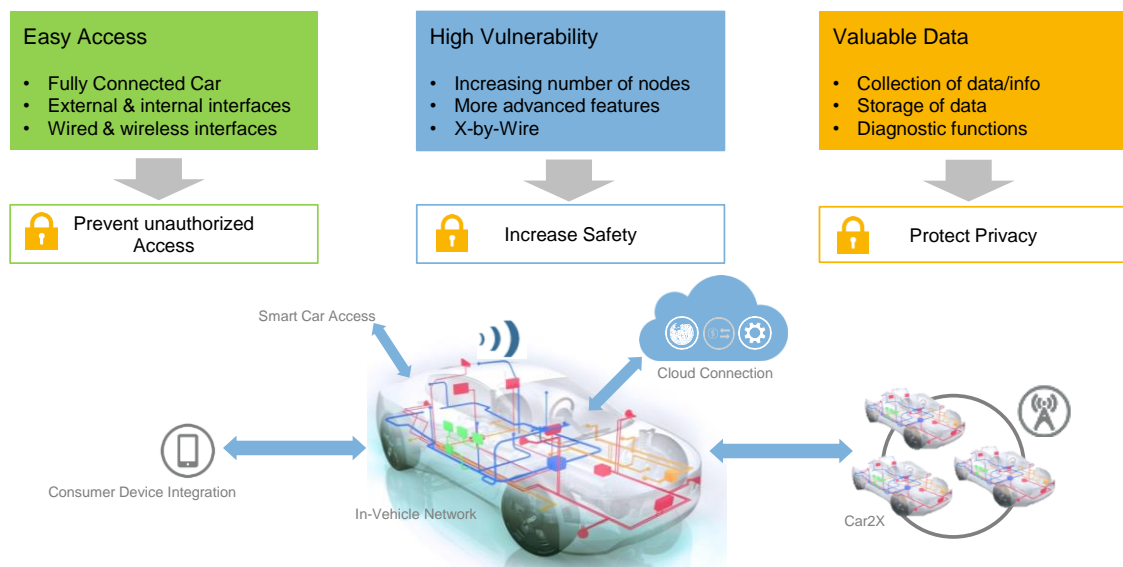


Figure 2: Security challenges for the Connected Car

These examples illustrate that the connected car contains valuable data that becomes accessible from outside the car because the in-vehicle electronics are connected to external networks, including the internet (see Figure 2). Traditionally, vehicle manufacturers have been concerned about safety – meaning that for example the brakes should function correctly under all circumstances. But more and more, they also need to take into account security and privacy – meaning that the vehicle needs to be protected against cyber-attacks by which hackers may steal (personal) data or take (partial or full) control over the vehicle.

Market demand

The hacks that were presented in the summer of 2015 at the security conferences Black Hat and DEF CON raised awareness amongst end users as well as politicians that the Connected Car needs to be well-protected against cyber-attacks. The general expectation is that this will lead to an increased demand for solutions that address the most urgent needs, providing improved security for the wireless interfaces and a first level of isolation in the in-vehicle networks. On the longer term, we expect that security will become an integral part of the design of the Connected Car and that the demand for security products will steeply increase as a consequence (see Figure 3).

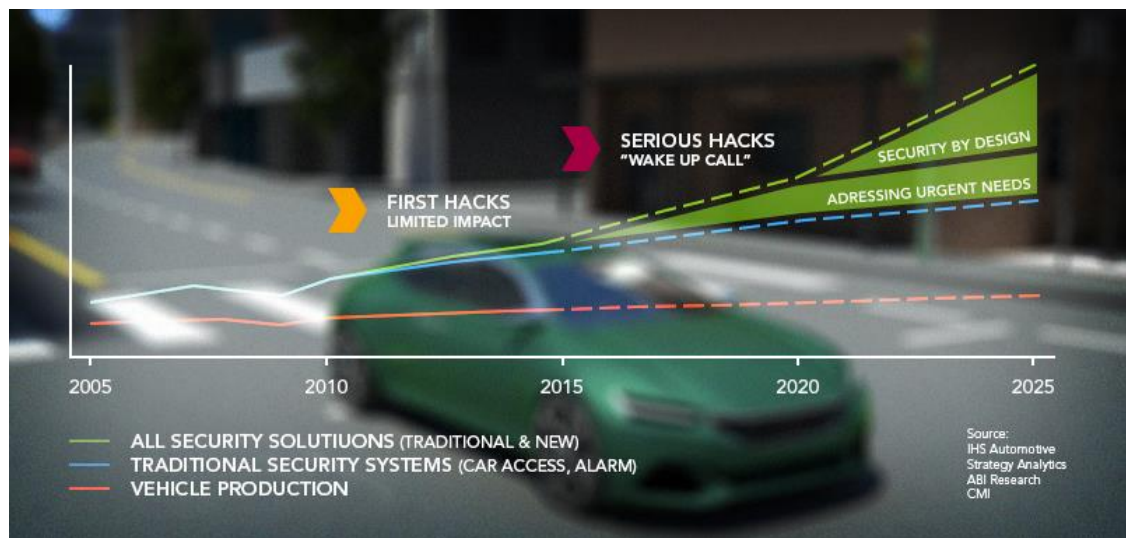


Figure 3: Recent hacking attacks will trigger a steep increase in the demand for automotive security solutions

The challenge

The range of attacks that a Connected Car faces, is extensive and diverse: it varies from relatively simple attacks, in which for example malicious messages are sent to a vehicle, to more sophisticated attacks in which hackers may open up ECUs and try to reverse engineer their microcontrollers and software.

A first reason for that is that there isn't a single, well-defined hacker. In fact, there are various attackers, with different motivations, skill levels and resources. For example, there may be (academic) researchers who try to take (partial) control over the vehicle, for scientific reasons. Or there may be (organized) criminals with large budgets that want to steal valuable data from a vehicle, for financial gain. But the threats do not only come from third parties: for example in the example of chip tuning, the car owner himself may be the 'attacker' who wants to unlock extra features or gain (engine) performance.

Furthermore the attack surface, i.e. the sum of the different points (the "attack vectors") where an unauthorized user can attack the system, is large: attacks may be mounted directly from the in-vehicle electronics network, from user devices such as smartphones that are coupled to the infotainment system, from external devices in proximity such as other V2X-equipped vehicles, or from the cloud.

Finally, the impact of a successful hacking attack may also widely differ. In certain cases, a hacker may target a specific vehicle, causing (limited) damage to that vehicle only. But a hacker may also find an exploit that can be abused over complete series of cars. When such an attack can easily be reproduced by others, for example because the hacker publishes tools and instructions on the internet, the impact, and likely also the (financial) damage, is obviously much larger. For example, a large-scale attack at random vehicles could easily have an economic impact, because it has the potential to severely disturb traffic in a large geographical region. Also, the costs for car manufacturers could be high, because of potential recalls and associated brand damage.

The big challenge for vehicle manufacturers is therefore to implement solutions that block this wide variety of hackers, with different motivations, resources and skill levels, and using many different attack vectors, in a cost-effective way.

Paradigm shift

System performance and reliability has had (and will always have) high attention from vehicle manufacturers, with a strong focus on safety hazards. By adding wireless interfaces to their cars and connecting their vehicles to external networks, manufacturers are however all of a sudden confronted with new threats that stem from an uncontrolled and evolving environment. They are faced with intentional hazards caused by hackers who do not obey to any rule. On the contrary, they will do whatever it takes to achieve their goal. Also, their attacks will only get better over time: their knowledge level continuously increases and also their (hardware and software) tools get more and more sophisticated.

Like safety, security is a quality aspect – threats of either type can have a negative impact on the reliability and safety of the Connected Car. But there are also important differences.

The ISO 26262 standard addresses systematic failures and random hardware failures. Such safety threats are quite predictable – systematic failures are deterministic and random hardware failure rates can be predicted with reasonable accuracy – and the nature of the hazards will not change over time. Furthermore, the likelihood that multiple failures occur simultaneously, is considered to be rather unlikely in safety engineering.

Security threats on the other hand are generally less predictable and they will also change over time. Furthermore, hackers do not hesitate to manipulate various parts of a system simultaneously, if that increases the chance of a successful attack. As a consequence, security threats are not necessarily covered within a safety framework such as ISO 26262.

Security threats thus form a largely unexplored field for the automotive industry. Outside the automotive industry, standardized frameworks such as Common Criteria are used to provide customers assurance that a product's security attributes can be trusted and that the customer's security needs are protected. Such frameworks are however fairly new to the automotive industry and it will likely take some time, as was the case with functional safety, before they are widely embraced.

SAFETY & SECURITY

SAFETY THREATS

Unintentional hazards that either result from natural phenomena (e.g. extreme temperatures or humidity levels), or from human negligence or ignorance (e.g. improper design or use).

SECURITY THREATS

Intentional hazards that result from attacks planned and carried out by humans.

THREAT EVALUATION

The ISO 26262 norm is a risk-based safety standard that focuses on systematic or random hardware failures in automotive equipment that would lead to a risk to humans.

The ISO 14508 norm, based on Common Criteria, defines a framework that provides customers assurance that a product's security attributes can be trusted and that the customer's security needs are protected.

Both norms aim to address hazards throughout the entire lifecycle of a product.

From after-thought to integral approach

To successfully protect the Connected Car from attacks, a paradigm shift is needed in automotive vehicle design: security must become part of the entire lifecycle of the vehicle. It needs to become an *integral* part of the design process, as opposed to an afterthought, because security is only as strong as the weakest link. Furthermore, the security architecture requires regular maintenance.

This calls for security-by-design and privacy-by-design, which may also have a significant impact on the architecture and on the in-vehicle electronics. For example, in-vehicle networks may need to be adapted such, that systems with similar criticality are clustered in separate networks, to better isolate highly critical safety systems from e.g. the in-car entertainment systems.

Standardization

There is also a need for standardization, both for processes as well as for implementations. On the process side, one can think of standardized lifecycle management, from development, via deployment to maintenance. Something based on or comparable to Common Criteria could form the basis for such framework, but automotive-specific adaptations may be needed, as was also the case for ISO 26262 which was derived from a generic safety standard, IEC 61508.

But also technical specifications are a must-have. It's not uncommon for straightforward mistakes to be made in security architectures and implementations. A seamless integration of features like secure boot and secure communication into a well-reviewed specification like the AUTOSAR software stack is therefore highly beneficial.

The standardization bodies are currently taking initial steps to create such standards. For example, the SAE Vehicle Electrical System Security Committee [6] is working on a cybersecurity guidebook (J3061) and requirements for hardware-protected security (J3101), and ISO's TC22 plans to identify the need for communication channels between functional safety and cybersecurity in ISO 26262 Edition 2.

SECURITY & PRIVACY

SECURITY AND PRIVACY BY DESIGN

Design the right level of security and privacy into a solution, right from the requirements phase, and address them throughout the complete lifecycle.

THE WEAKEST LINK

Attackers don't obey the rules and simply find the easiest way to achieve their goal. They will therefore search for the weakest spot in the system. Security is therefore only as strong as the weakest link.

SECURITY VS. PRIVACY

Security is about secrecy of information, privacy is about control over personal data.

PERSONAL DATA

Personal Data, or Personally Identifiable Information (PII), is information that conflicts (to a greater or lesser extent) with people's need for privacy when it is disclosed or revealed.

Security needs

Wireless interfaces impose the biggest risk to the Connected Car, because they open the door for *remote* attacks: one does not need to be in direct proximity of the vehicle in order to gain access to its internal systems. In other words, manufacturers can no longer solely rely on the physical protection offered by the vehicle's chassis.

The fact that one can remotely access in-vehicle systems also implies that these systems face security threats coming from the outside world. And thus, there is a risk that these systems are hacked and that data contained therein is stolen. This poses a threat to the reliability and safety of the car – the hacker can potentially take control over the car – as well as to the privacy of the driver – the vehicle data can be used to build a profile of its user(s).

Defense in depth

Most vehicle hacks consists of a number of smaller steps. It usually starts with finding a vulnerability (a 'bug') in a system that is remotely accessible. But once you get for example into a car's telematics unit, you have a good chance of getting into just about any other part of the car such as the ECUs that control engine speed, braking, cruise control, valet parking etc.

It is good practice to use multiple security techniques to mitigate the risk of one component of the defense being compromised or circumvented. In the example above, the first line of defense is to protect the telematics unit itself. But the security architecture should furthermore be designed in a way that an attack on an individual ECU does not scale to other ECUs in the vehicle. For example, by isolating critical ECUs and their networks from non-critical ECUs and their networks using firewalls.

In the next sections, we will go through the complete car electronics architecture, starting from the external interfaces, via the in-vehicle networks down to the individual ECUs, and sketch the possible countermeasures that can be applied on each level. Figure 4 gives a brief overview of some of the possible countermeasures per layer.

ATTACK CLASSIFICATION

REMOTE ATTACKS

Attacks that are executed at a distance, typically via a network, by sending messages to exploit weaknesses in a system's design or its implementation (e.g. software bugs).

PHYSICAL (IC) ATTACKS

Sophisticated attacks that can only be executed by an attacker with physical access to a system or an IC. Examples of physical IC attacks are fault injection attacks, micro probing, chip delayering, reverse engineering and side-channel analysis.

SIDE-CHANNEL ANALYSIS

A non-invasive attack, in which the behavior of an IC or system is observed. Examples are timing analysis, static and dynamic power analysis (SPA/DPA), electromagnetic analysis (EMA) and photo emission analysis. Usually physical access is needed, although there have also been real-life examples of timing attacks against networked devices such as cloud servers.

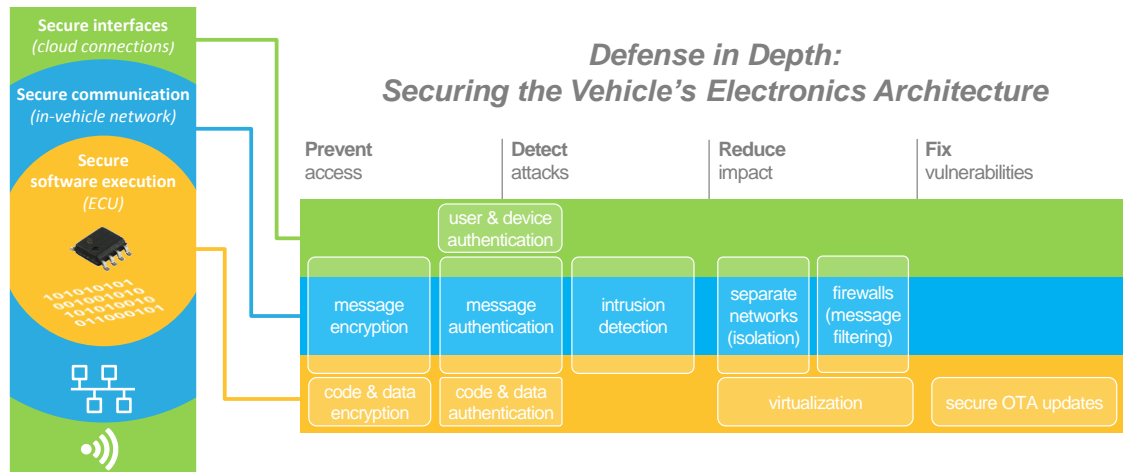


Figure 4: Example countermeasures per layer of the car electronics architecture

Securing the vehicle electronics architecture

Traditionally, the automotive industry has been conservative in adopting features offered by consumer electronics. But the Connected Car is finally becoming a reality, and it will likely redefine the entire automotive industry. Vehicle manufacturers have to find ways to deliver the advanced features their customers demand, into their 'smartphones-on-wheels'.

They will also need to embrace security solutions that are widely used in smartphones and IT infrastructures, but that are relatively new to the automotive world. Examples of such technologies are firewalls, intrusion detection and prevention systems, virtualization technologies and secure firmware updates.

External interfaces

To secure the Connected Car, one has to start with the external interfaces themselves. First of all, the communication channels needs to be protected against *data theft*, e.g. by encrypting the data, and against *manipulation*, e.g. by authenticating the messages that are exchanged to protect their authenticity and integrity.

Furthermore, the interfaces need to prevent unauthorized access. This involves processes such as machine-to-machine authentication to check that you are communicating with a known or authorized device.

CYBER SECURITY

CYBER-PHYSICAL SYSTEM

A system of collaborating computational elements controlling physical entities.

CYBER-SECURITY

All technologies, processes and practices by which digital equipment (computers and networks), information (programs and data) and services are protected from unauthorized access, attack, manipulation and damage. It can for example be a combination of physical security, information security, policies, standards, legislation, and risk mitigation strategies.

In-vehicle networks

Securing the interfaces is a critical requirement, but on its own may not be enough to stop hackers. For example, they could compromise and impersonate a trusted device and use this to bypass access control.

Therefore, one has to apply additional lines of defense. One logical place to do so is in the in-vehicle network, which forms the “spine” of the vehicle and connects all the different parts of the “brains” (ECUs). For example, countermeasures may need to be implemented on the network level to protect against:

- *Data theft*, for example by encrypting the messages that are exchanged between different ECUs inside the vehicle
- *Message manipulation* and *replay attacks* on the in-vehicle network, by authenticating the messages that are exchanged between different ECUs inside the vehicle
- *Network manipulation*, by authenticating the ECUs regularly (e.g. on engine start and periodically afterwards)
- *Inside attacks*, where one compromised ECU is used to attack other ECUs inside the vehicle’s network, by physically or logically isolating ECUs from one another (e.g. by placing ECUs with different criticalities on different networks and by filtering network traffic using firewalls)

Electronic Control Units (ECUs)

Once the external interfaces and internal networks are secured, the “brains” of the Connected Car must also be protected. These brains are formed by up to (and in some cases, over) a hundred individual computers (ECUs) that together implement the control functions in the car, including many advanced (automated) driving functions. These ECUs continuously generate, process, exchange and store large amounts of valuable (sensitive) data. As such, these ECUs and their data form an attractive target for hackers and need to be protected against:

SECURITY BASICS: PART 1

ENCRYPTION PROTECTS SECRETS

Encryption prevents data from being read by unauthorized parties, to protect sensitive data such as intellectual property or your navigation history.

Encryption can be realized with symmetric crypto, as well as with public-key crypto algorithms (see next page).

AUTHENTICATION PROVIDES TRUST

Authentication provides trust, in identities or in messages.

User or device authentication:

Confirm the claimed identity of a person or a device.

Message authentication:

Confirm that a message is not modified and that it originates from a particular entity.

Authentication can be realized using Message Authentication Codes or digital signatures: the first are usually based on symmetric block ciphers (CMAC) or hash functions (HMAC) and digital signatures employ public-key crypto.

- *Data theft*, for example by encrypting the memory contents (code and data)
- *Manipulation of the software* that is running on various systems, e.g. by implementing secure boot

But this is not enough. To understand this, we need to have a look at the software complexity: a modern high-end car already features around 100 million lines of code (i.e. more than modern PCs and smartphones!), and the number is only expected to increase over time. Such complex systems *cannot* be bug free, and vulnerabilities *will* be found after the vehicle enters the road.

Another logical consequence of the fast growth of software in vehicles, is a trend to reuse hardware [7], by integrating multiple software stacks, sometimes with different criticalities and often originating from different vendors, on the same microcontroller or CPU.

To manage such complex software systems and to enable hardware reuse in a secure way, ECUs additionally need:

- *Secure Firmware-Over-The-Air updates*: to prevent known vulnerabilities from being exploited, they need to be patched as soon as possible after their discovery, using firmware updates that are delivered over the air to vehicles in the field
- *Process and resource isolation*, i.e. multiple software stacks running on the same microcontroller or CPU should be isolated from each other, for example using virtualization techniques, to prevent that one vulnerable software stack can be misused to attack the other software stacks.

Risk analysis

In the previous sections we sketched how the in-vehicle electronics architecture of the Connected Car can be secured in the future. But security always comes at a cost. Basically, it is an insurance premium you pay upfront to prevent damage that may otherwise result later on, if the vehicle would be attacked.

To ensure that costs and benefits are well-balanced, one needs to perform a risk assessment upfront when

SECURITY BASICS: PART 2

SYMMETRIC CRYPTO

Conventional cryptography, which relies on the same key for encryption and decryption.

Examples: 3DES and AES.

PUBLIC-KEY CRYPTO

The class of cryptographic algorithms that require two separate keys to perform two opposite cryptographic functions, one of which is secret and one of which is public.

Examples: RSA and ECC.

WHICH TO USE?

The main advantage of public-key cryptography is that only a non-secret key needs to be shared with the other side, whereas symmetric crypto requires both sides to agree on the same secret key before initiating communication.

Because symmetric key algorithms are nearly always much less computationally intensive than public-key ones, it is common to exchange a symmetric key using public-key crypto and then use that key and symmetric crypto to protect further data.

designing an actual vehicle electronics architecture. Since security risks are a function of threats, vulnerabilities and potential impact, one needs to identify all possible threats and assess, for each threat, the potential impact of a successful attack as well as the vulnerability of the device to such attack (see also [8]) and possible countermeasures. Finally, one must set priorities for the different risks to determine which risks to address first.

One popular method for reasoning about computer security threats is the STRIDE system, developed by Microsoft. It provides a mnemonic for security threats in six categories: Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service and Elevation of privilege.

Life-cycle management

If is not enough to only *design* a secure vehicle electronics architecture, it must also be maintained during deployment of the vehicle. The IT systems of the Connected Car are highly-complex and need active maintenance, including key management and secure firmware updates.

Key management and crypto agility

To prevent attacks from being scaled from one device (or vehicle) to a complete network of devices (or vehicle fleets), ECUs will need unique cryptographic device keys. These keys need to be managed during their lifecycle. For example, existing keys may need to be replaced with newly created keys every now and then, and the existing keys need to be destroyed. In some cases, the new keys are created outside the vehicle, e.g. in a cloud server, and need to be securely distributed from these cloud servers into the vehicles.

And also cryptographic algorithms eventually may become obsolete and be replaced with new ones. Vehicles shall be sufficiently protected during their entire lifetime, which is approximately 15 years. The use of open and preferably standardized crypto algorithms and security protocols as well as the key sizes that are

SECURITY BASICS: PART 3

CRYPTOGRAPHIC KEY

Secret data that is used in cryptographic algorithms to encrypt or decrypt or to create or verify digital signatures or MACs.

KEY SIZE AND CRYPTOGRAPHIC SECURITY

The key size of a cryptographic algorithm is the size measured in bits of the key used by the algorithm.

Its cryptographic security (or strength) is a measure of the fastest known attack on the algorithm, also measured in bits. It cannot exceed the key size, but it can be smaller.

Example: 3DES has a key size of 168 bits, but provides at most 112 bits of security.

CRYPTO-AGILITY

Over time, hackers get access to more computing power and new weaknesses may be found in existing crypto algorithms. Therefore, longer key sizes and potentially also different crypto algorithms may be needed in the future.

generally expected to be sufficiently secure during the vehicle's entire lifetime, is of course a good starting point. But sooner or later, a move to larger key sizes will be needed.

Key management and cryptographic algorithm agility are thus important aspects of the lifecycle management of a Connected Car.

Firmware management

Another clear example where active maintenance is needed, is when security vulnerabilities are found after initial deployment and need to be fixed. Security flaws can affect individual models, or even worse, complete series of cars or even all cars. Worst case, flaws might be discovered in widely-used security protocols. Recently, quite a serious few flaws have been discovered in the Transport Layer Security (TLS) specification as well as its implementations [9][10][11]. This affected many internet-connected devices, which all became vulnerable from one day to another and needed to be patched urgently. Also the Connected Car, being a complex IT system, will need to be patched every now and then and secure firmware updates are therefore a must-have.

Summary

The Connected Car is a complex IT system on wheels, consisting of many ECUs (forming the vehicle's "brains") that are linked together via the in-vehicle network (its "spine"). To secure all of this, an integral approach is needed where countermeasures are applied at all levels. Most prominently, the Connected Car needs:

- Secure external interfaces, with strong M2M authentication to prevent unauthorized access
- Secure in-vehicle networks and secure communication on these networks, as well as on its external interfaces, to prevent data theft and manipulation
- Secure ECUs with firmware protection and update provisioning, in the form of secure boot and secure OTA updates

SECURITY BASICS: PART 4

PLAIN TEXT & CIPHER TEXT

In an encryption scheme, the unencrypted message or information is referred to as plaintext, as opposed to ciphertext that can only be read if decrypted.

HASH FUNCTIONS

Functions that can be used to map digital data of arbitrary size to hash values (or message digests) of fixed size. These hash values can be used to uniquely identify secret information.

Examples: SHA-2 and SHA-3.

The exact security requirements for a specific vehicle shall be determined using a thorough risk analysis that must be part of its design process. Furthermore, the security architecture and its implementation needs to be managed during its entire lifecycle, which means that it requires for example active key management and secure firmware updates.

Hardware as a trust anchor

System integration and bring-up will be the major time-to-market challenge for many OEMs. It is also likely that improvements are needed during the lifetime of the car, not only because its complex systems will need to be fine-tuned over time, but also because the Connected Car is actively interacting with its environment, which will evolve during the lifetime of the vehicle. As a consequence, many of the features of modern cars will need to be implemented in software, rather than hardware, because it not only reduces the development time (and cost), but also significantly reduces the need for expensive recalls because firmware updates can be provided over-the-air.

The same holds for the security architecture and its implementation: for some parts, software is the better choice, for example because of the need for updatability in the field. Nevertheless, a certain level of hardware support is needed in virtually any case: this may be because of performance reasons, but more often also for security reasons: updatability of software is, on the one hand, a powerful feature that allows the manufacturer to manage the product during its entire lifecycle. But on the other hand, the same updatability also provides hackers with a means to manipulate the product.

In general, securing systems with software only is not possible. At the very least, the security implementation would need to be isolated from other, less-trusted code, for example by executing the security software at a higher privilege level (system vs. user mode), enforced by hardware. Other examples include side-channel resistant crypto implementations, which usually need specific hardware, and on-chip security implementations such as HSMs that protect cryptographic keys from software attacks by moving the control over those keys to the hardware domain. These examples illustrate that dedicated security hardware is needed as a basis, or as “trust anchor”, for protecting the system.

HARDWARE SECURITY & SECURITY EVALUATION

TAMPER-RESISTANCE

Resistance to tampering the device by normal users or systems or others with physical access to it. The amount of resistance is usually ‘proven’ via third party evaluation according to Common Criteria.

COMMON CRITERIA (ISO 15408)

A standardized framework that provides customers assurance that a product’s security attributes can be trusted and that the customer’s security needs are protected.

HIS SHE, EVITA HSM

The Secure Hardware Extension (SHE), as well the Hardware Security Module (HSM), is an on-chip extension to any given microcontroller, which can be used to protect software (secure boot, secure update) and data (secure storage, secure communication). It moves the control over cryptographic keys from the software domain into the hardware domain to protect those keys from software attacks. The specification does not require tamper resistance.

The main difference is that a HSM is programmable, while a SHE module is only configurable.

Secure hardware solutions

NXP's security portfolio is the perfect fit to the needs of the automotive industry for securing the Connected Car, as well as to enable new end-user device oriented use cases.

NXP has been developing security ICs for decades, and our best-in-class solutions are used all over the world to secure sensitive applications like electronic identification with e-passports and electronic payment with bank cards and smartphones. And NXP is also worldwide the number one provider of reliable and secure solutions for car access and in-vehicle networking, it has been putting security features onto its MCUs for over 10 years now, it was the first semiconductor supplier to implement SHE & HSM compliant security modules on silicon and it is now also the first to bring a secure V2X solution to the market.

By leveraging all this expertise and deep know-how, we have been able to create a rich portfolio of security products that helps OEMs and Tier-1s to protect their vehicles and systems against cyber-attacks, thereby allowing end users to profit from all the benefits of new applications and technology, without having to worry about their personal safety and privacy.

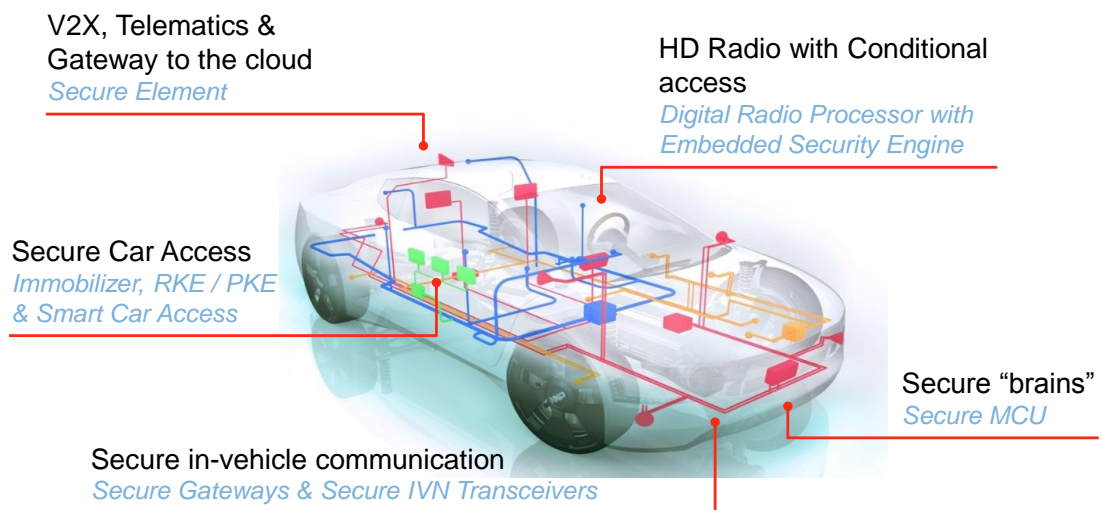


Figure 5: NXP's automotive hardware security solutions are key in securing the vehicle's entire E&E architecture

Secure Car Access solutions

NXP is the leading automotive supplier of chipset solutions for passive keyless entry (PKE) and passive keyless go (PKG) systems worldwide. Our solutions for PKE and PKG systems provide maximum comfort, security and performance. They also minimize power consumption, printed circuit board (PCB) space and overall system cost. A large range of additional interfaces, such as NFC or bi-directional radio frequency links are available, creating the ultimate end-user experience.

NXP also provides the ingredients for a new generation of NFC based Smart Car Access Systems. This allows NFC devices like smartphones to be used in conjunction with traditional car access systems, enabling new use cases like car sharing, temporary car access and many more.

Secure Elements

NXP is the recognized market leader for Secure Elements, with more than 2 billion SmartMX controllers shipped worldwide. Also, many of the countries that deploy electronic passports are using NXP's secure hardware. Its IntegralSecurity™ architecture with more than 100 patented security features offers state-of-the-art security to protect against side channel attacks, physical attacks and reverse-engineering. The security of these products is also proven via third party security assessments: the SmartMX2 family of products and associated software libraries have been awarded the Common Criteria EAL6+ certification for a secure microcontroller.

The NXP SmartMX products are therefore the perfect candidates for securing access to the Connected Car from the cloud (internet services), from the vehicle's direct environment (e.g. V2X) and physically via NFC based Smart Car Access Systems (see previous section). NXP offers a broad hardware and package portfolio and full solutions, including Java Card OS & applets. Furthermore, NXP offers a one-stop-shop solution where needed and strong customer support.

Secure MCUs

To secure the "brains" of the car, the newest microcontrollers in the market, offered by NXP, are already equipped with implementations of the SHE and HSM specifications. The NXP implementation of SHE, called CSE (Crypto Services Engine), is a programmable sub-system meaning that its functionality can be modified when enhancements are identified. Every 32-bit microcontroller introduced by NXP in the last 3 years has included a crypto module meeting the SHE or HSM specification. Even the recently announced S32K family that addresses the low-end market, will be SHE compliant.

As such, these microcontrollers allow secure verification and execution of code, as well as high-performance (line-speed) message protection on the in-vehicle networks and the external interfaces of the Connected Car. These are some of the fundamental building blocks that will protect the in-vehicle electronics networks of the future.

Of course, security is more than just cryptography and associated key storage. NXP's microcontrollers therefore also provide security features like:

- life cycle management that controls access to the device, gradually locking down the device as it passes from NXP to Tier 1 to OEM to the field, through the manufacturing cycle
- secure debug access
- basic tamper resistance, including voltage supply and clock monitoring and SPA/DPA resistance.

Smart IVN transceivers

As a leader in in-vehicle networking solutions, we realize that it is impossible for OEMs and Tier-1s to apply a security upgrade to all existing microcontrollers and their software from one vehicle model to another. The associated cost for validation and verification of the modified hardware and software would simply be too high. Therefore, we propose an IVN centric security solution as an alternative, cost-effective upgrade path.

Our smart IVN transceivers provide a flexible and cost-effective platform that can be used to implement security features at network level, such as:

- transparent authentication and encryption of the IVN messages, allowing the network to be protected against message manipulation and data theft,
- intrusion detection and prevention systems (IDS/IPS), to detect anomalies in the network traffic and to block malicious packets before they can even reach the microcontroller
- rate limiting mechanisms to prevent denial-of-service attacks

By implementing such security features at the network level, security can be retrofitted to existing networks with existing ECUs, while avoiding (or at least, reducing) the need for re-verification and re-validation of the ECU's microcontroller hardware and software.

Example use cases

It is usually easier to understand the security needs of a Connected Car, when one thinks of a concrete use case. Therefore, we will present three use cases that will soon be supported by a large part of all new, connected vehicles.

V2X

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication technology, commonly referred to as V2X, is about to enter our vehicles and our streets. In 2014, USA's National Highway Traffic Safety Administration (NHTSA) judged that "these technologies may prove to be the next game-changer as we look at the future of auto safety" [12] and is currently working on a proposed mandate that will detail the required implementation schedule for V2X technology into every new vehicle. In anticipation of this mandate, GM announced in September 2014 that the new MY 2017 Cadillac CTS will be the first production vehicle to offer built-in V2X systems, based upon NXP's secure 802.11p technology.

V2X-enabled vehicles and road-side units (RSUs) broadcast messages that can be received by any vehicle equipped with a V2X receiver that is within range. The receiving vehicle can use these messages to predict hazardous situations and to alert the driver, or try to prevent accidents autonomously.



Figure 6: The Connected Car, interacting securely with its environment

Of course, the trustworthiness of these messages must be ensured. Therefore, messages are authenticated using digital signatures, proving their origin and integrity to the receiver.

Due to the ad-hoc nature of the application – others are not known upfront – keys for verification need to be exchanged dynamically. The use of public-key crypto simplifies that, because only the non-secret public key is exchanged. Certificate authorities (CAs), as part of a larger Public Key Infrastructure (PKI), authorize vehicles and road side units to send messages by issuing certificates describing their digital identity and their permissions.

Also, the privacy of the driver must be protected. Each vehicle can regularly change its identifier (“pseudonym”) to make it harder to identify or follow a specific vehicle. All these identities need to be managed by the PKI and once operational, it will likely be the largest of its kind in terms of the number of nodes (vehicles, RSUs) and the number of managed identities.

The vehicle implementation also has to deal with some challenging requirements. The sender must ensure that the secret (private) keys that it uses to create the digital signatures, cannot leak. Otherwise, they could be misused to send fake messages that go undetected. Such attacks could easily be scaled: a single compromised key could be cloned and be misused to affect smart traffic systems across a large geographic region, such as a complete state or country. A tamper-resistant Secure Element therefore provides the right level of protection for such keys.

On the receiver side, the main challenge is performance. Each individual vehicle sends messages at a fairly low rate – in typical situations, no more than ten per second – but due to the broadcast nature of V2X, a receiver can receive hundreds of messages per second in crowded traffic situations with many nearby vehicles and RSUs. The signature verification for these messages imposes a big computational load and requires high-speed crypto accelerators to be integrated into the receiver.

Car-to-cloud communication

The Connected Car will also have an internet connection, providing access to cloud services such as remote diagnostics services to monitor the current condition of vehicles, or remote software updates. The remote diagnostic function will improve safety and reliability by early detection of potential components or system failures. As an added benefit, service time can be reduced because spare parts can be ordered upfront, before the car arrives at the service center. The remote software update or over-the-air update as it is known, also has significant benefits for the user as critical software improvements can be provided on a real-time basis, without requiring a trip to the dealership or other user actions.



Figure 7: Cloud-based services entering the Connected Car

We also expect that more and more third parties will offer a variety of cloud services to the connected car, especially when it offers autonomous driving features that allow one to use the travel time for work or leisure. It is therefore likely that cloud-based business solutions will, in one way or another, become available in the Connected Car, as illustrated in Figure 7.

All of these use cases are examples of big data. And in all cases, sensitive data is exchanged with the cloud. Hence, it is very important that only authorized cloud services can get access to (part of) the car network and (part of) the data contained therein. NXP's Secure Elements can be used to implement tamper-proof machine-to-machine authentication, offering the right level of protection for protecting access to the valuable data contained in the Connected Car.

Furthermore, it is likely that existing IT security technologies such as HTTPS and TLS will be used to protect the data that is exchanged between the vehicle and the cloud and that secure software updates will be needed to regularly improve the vehicle's complex self-driving algorithms. For example, the OEM could offer cloud-based services to continuously improve the capabilities of its vehicles, by processing data collected from its vehicles in the cloud, using advanced machine learning algorithms, and sending back improved algorithms and configuration data to the vehicles via software updates. These updates should be secured in a way that others cannot misuse the same mechanism to flash malicious software versions that could affect the reliability and safety of the vehicle. A Secure MCU with an integrated Hardware Security Module enables hardware-backed secure software update mechanisms, as well as high-speed data encryption and authentication.

Central gateway

The first true gateway was introduced into vehicles about 8 years ago. Since then, as the amount of data being transferred between ECUs in the vehicle has significantly increased, the gateway functionality has become more complex, and also more common place in our vehicles. In its current form, the central gateway provides many functions, linking data and signals from the various nodes around the vehicle, converting the plethora of automotive communication protocols.

From a security view point it's most important function is its firewall that separates the external interfaces from the safety-critical inner vehicle network. The gateway engine is a contextually aware routing function that determines, by a number of increasingly sophisticated checks, which messages are legitimate, and hence will be passed through the gateway onto the destination.

As well as the firewall, the presence of the gateway immediately introduces a physical network isolation, particularly in reference to some of the recent vehicle hacks, where the externally connected head unit was on the same network domain as safety critical ECUs controlling braking, chassis, powertrain etc. By separating OBD diagnostics port and head unit into their own domains, any message to the safety domains need to pass through the gateway and hence pass through the firewall to be checked for validity.

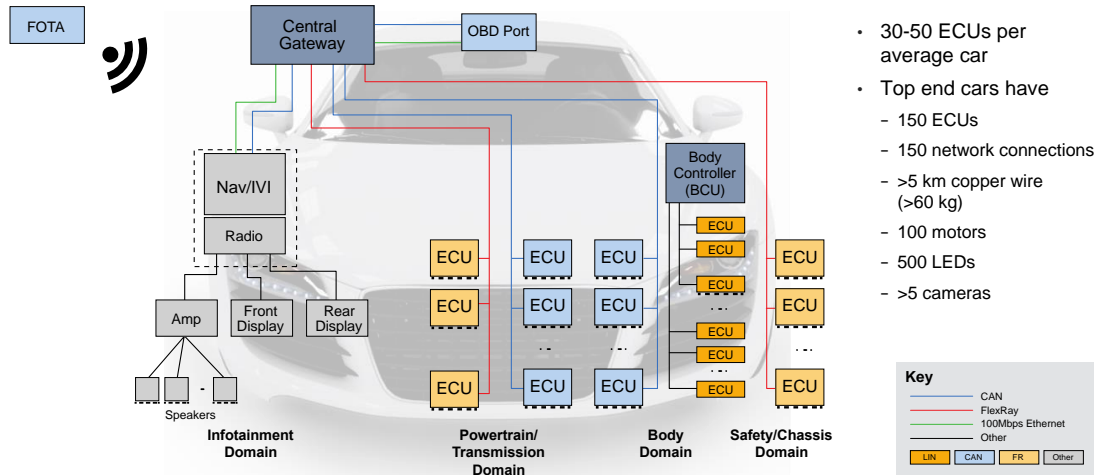


Figure 8: The role of the central gateway in a typical vehicle network architecture

Being central to the vehicle architecture, the node is holder of most information about the status of the vehicle, so it also gets involved in strategy functions, like user settings (sport or eco mode), energy management etc.

As has been mentioned before, OTA programming of ECU firmware is vital to maintain security levels through the lifetime of the car, as well as to avoid recalls for other software bug fixes. Currently, being able to perform OTA updates of the head unit is common place, but the ability to perform this update function on ECUs deep into the vehicle network is rare. The gateway becomes key when doing this deep OTA update, managing the update process by ensuring availability, authenticity and confidentiality throughout the process of updating the individual ECUs inside the network, with each firmware image being signed (and encrypted) specifically for the target ECU.

Conclusions

The Connected Car, as part of a Smarter World, is highly connected to and constantly interacting with its environment. It brings enormous promises for increased comfort, safety and efficiency. But it also raises questions regarding security and privacy: like all connected device, it also becomes a target for attackers. As such, the key points to consider and address are:

- system integrity, to create safe and reliable networks inside and outside the vehicle
- user privacy, to maintain our social values
- and brand protection, to encourage quality and protect business investments

NXP's products secure the Connected Car against cyberattacks and allow its users to be in full control of their data, making the Connected Car an opportunity for business and society, rather than a threat to us all!

Definitions

| | |
|--------------------------------|--|
| AES | Advanced Encryption Standard. It is a specification for the encryption of electronic data, standardized by NIST in 2001 which is widely used for data encryption and decryption. It is a symmetric crypto algorithm, meaning the same key is used for both encrypting and decrypting the data. |
| Asymmetric cryptography | See 'public-key' cryptography. |
| Attack surface | The sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to attack a system. |
| Attack vector | The path or means by which a hacker can gain (unauthorized) access to a system. |
| Authentication | The process of determining whether someone or something is, in fact, who or what it is declared to be. See also 'user authentication', 'device authentication' and 'message authentication'. |
| CA | A Certificate Authority (CA) is a trusted third party that issues digital certificates. Many public-key infrastructure (PKI) schemes feature CAs. |
| Ciphertext | In an encryption scheme, the encrypted message or information is referred to as ciphertext that can only be read if decrypted. |
| Common Criteria | A framework that provides customers assurance that a product's security attributes can be trusted and that the customer's security needs are protected. As the basis for the international standards ISO/IEC 15408 and ISO/IEC 18045, Common Criteria provides assurance that the process of specification, implementation and evaluation of products has been conducted in a rigorous, standard, achievable, repeatable and testable manner at a level that is commensurate with the target environment for use. |
| Cyber-physical system | A system of collaborating computational elements controlling physical entities |
| Cyber-security | All processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction. It can for example be a combination of physical security, information security, standards, legislation, policies, and risk mitigation strategies. |
| Decryption | The process of decoding unreadable ciphertext into readable plaintext. |
| Device authentication | The process of confirming the claimed identity of a device. |
| Digest | The hash value of a message is often called the message digest, or simply the digest. (See 'hash function') |

| | |
|----------------------------|---|
| Digital certificate | A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or on assertions made using the corresponding private key that is owned by (and only known to) the named subject. |
| Digital signature | A digital signature is used to verify that digital information has not been altered. It is especially important for assuring that data were not corrupted or altered during transport and for authenticating data such as digital signatures and passwords. Digital signatures are created and verified using public-key crypto systems such as RSA or ECC, as opposed to MACs which are created and verified using the same key. |
| Encryption | The process of encoding readable plaintext into unreadable ciphertext, such that that only authorized parties can read it. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors. |
| EVITA | EVITA was a project co-funded by the European Union within the Seventh Framework Programme for research and technological development. Its objective was to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise. |
| Hash function | A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size, called hash values, hash codes, hash sums, digest, or simply hashes. These hash values can be used to uniquely identify secret information, because it is considered practically impossible to find a second message that maps to the same value (collision resistant) or to reconstruct the original message from the hash value (non-invertible). Hash functions play a role in data or message authentication, where they are used to “compress” a larger message into a smaller MAC or digital signature that ensures the authenticity and integrity of the data or message. |
| HIS | Herstellerinitiative Software (German for ‘OEM software initiative’) is an interest group consisting of the car manufacturers Audi, BMW, Daimler AG, Porsche and Volkswagen. This group created the SHE specification. |
| HSM | In the Automotive context, a Hardware Security Module is a security unit, typically integrated in a microcontroller, which can be used to protect software (secure boot, secure firmware update) and data (secure storage, secure communication). It typically consists of a programmable microcontroller, one or more hardware accelerators (e.g. AES, SHA2) and dedicated storage for crypto keys. The HSM |

| | |
|-------------------------------|--|
| | <p>specification can be seen as the successor of the SHE specification.</p> <p>This specification should not be confused with the definition that is commonly used outside the Automotive domain. There, this term is used for a tamper-proof physical computing device that is often used to safeguard and manages digital keys for and provides crypto-processing to a mission-critical infrastructure such as a public key infrastructure or an online banking application.</p> |
| ICANN | The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization that is amongst others responsible for ensuring the stable and secure operation of the internet. |
| IDS/IPS | Intrusion Detection (and Prevention) Systems are systems that monitor network and/or system activities for malicious activity and report it (or attempt to block it). The detection mechanisms can vary widely, from simple network protocol analysis to advanced statistical anomaly detection based on machine learning. |
| Key | Data that is used in cryptographic algorithms to encrypt or decrypt or to create or verify digital signatures or MACs. |
| M2M authentication | Machine-to-machine authentication is a form of mutual authentication between two devices. |
| MAC | <p>A Message Authentication Code is used to verify that digital information has not been altered. It is especially important for assuring that data were not corrupted or altered during transport and for authenticating data such as digital signatures and passwords.</p> <p>MACs differ from digital signatures as MAC values are both generated and verified using the same secret key, as is the case with symmetric cryptography.</p> |
| Message authentication | The process of confirming that a message has not been modified while in transit (data integrity) and verification of the source (origin) of the message by the receiving party. |
| Mutual authentication | The term “mutual authentication” indicates that two parties involved in a transaction (or communication) verify each other’s identity. |
| Physical attack | Attacks that can only be executed by an attacker with physical access to a system or an IC. Examples of physical IC attacks are fault injection attacks, micro probing, chip delayering, reverse engineering and side channel analysis. |
| PII | Personally Identifiable Information (PII) or Personal Data is information with the specific property that its disclosure or revelation conflicts (to a greater or lesser extent) with people's need for privacy. Such information is thus relating to one or more identified or identifiable natural persons and is describing one or more factors specific to their personal, |

| | |
|--------------------------------|--|
| | physical, physiological, mental, economic, cultural or social identity or to their behavior, interests or whereabouts. |
| Plaintext | In an encryption scheme, the unencrypted message or information is referred to as plaintext, as opposed to ciphertext that can only be read if decrypted. |
| Privacy-by-design | Design the right level of privacy into a solution, right from the requirements phase, and address them throughout the complete lifecycle. See also security-by-design. |
| Public-key cryptography | <p>A class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used, for example, to encrypt plaintext or to verify a digital signature; whereas the private key is used for the opposite operation, in these examples to decrypt ciphertext or to create a digital signature. There is no need for the sender and receiver of a message to agree on the same key before initiating communications.</p> <p>The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both.</p> |
| PKI | A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. |
| Remote attack | Attacks that are executed at a distance, typically via a network, by sending messages to exploit weaknesses in a system's design or its implementation (e.g. software bugs). |
| RSA | A widely used algorithm for public-key cryptography. RSA is one of the first practical public-key cryptosystems and the acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. |
| SE | <p>A Secure Element is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.</p> <p>The management of applications on a Secure Element is usually done in accordance with the GlobalPlatform Card Specification.</p> |
| Security-by-design | Design the right level of privacy into a solution, right from the requirements phase, and address them throughout the complete lifecycle. See also privacy-by-design. |

| | |
|-------------------------------|---|
| SHE | The Secure Hardware Extension (SHE) is an on-chip extension to any given microcontroller. It is intended to move the control over cryptographic keys from the software domain into the hardware domain and therefore protect those keys from software attacks. It consists of a state machine, an AES accelerators and dedicated storage for crypto keys. It is not meant to replace highly secure solutions like TPM chips or smart cards, i.e. no tamper resistance is required by the specification. The SHE specification was created in 2008 by the HIS consortium and can be seen as a subset of the newer HSM specification. |
| Side-channel analysis | A non-invasive attack, in which the behavior of an IC or system is observed. Examples are timing analysis, static and dynamic power analysis (SPA/DPA), electromagnetic analysis (EMA) and photo emission analysis. Usually physical access is needed, although there have also been real-life examples of timing attacks against networked devices. |
| Symmetric cryptography | In symmetric cryptography, the same key is used for both encryption of plaintext and decryption of ciphertext, or for generation as well as verification of a MAC. This implies that the sender and receiver of a message must agree on the same key before initiating communications. The term "symmetric" stems from the use of the same key to perform these inverse functions, each the inverse of the other – as contrasted with public-key ("asymmetric") cryptography which uses different, but paired, keys for the opposite operations. |
| Tamper-resistance | Resistance to tampering the device by normal users or systems or others with physical access to it. It ranges from simple features like screws with special heads to complex devices (e.g. ICs) which can withstand even the most sophisticated attacks. |
| TLS | Transport Layer Security protocol. A cryptographic protocol that provides communications security over a computer network. It used public-key cryptography to authenticate the counterparty and to negotiate a symmetric session key. This session key is then used to encrypt and authenticate data flowing between the parties, providing data confidentiality, data integrity and message authentication. |
| User authentication | The process of confirming the claimed identity of a person. |

References

| | |
|------|---|
| [1] | <p>“Comprehensive Experimental Analyses of Automotive Attack Surfaces”; CAESS; August 2011. http://www.autosec.org/publications.html.</p> |
| [2] | <p>“Hackers Remotely Kill a Jeep on the Highway - With Me in It”; WIRED. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/</p> |
| [3] | <p>“Remote Exploitation of an Unaltered Passenger Vehicle”; Dr. Charlie Miller and Chris Valasek. http://illmatics.com/Remote%20Car%20Hacking.pdf</p> |
| [4] | <p>“Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & “Cyber Dashboard” Rating System”. http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system</p> |
| [5] | <p>“Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk.”; Ed Markey, United States Senator for Massachusetts; February 2015. http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf</p> |
| [6] | <p>Vehicle Electrical System Security Committee. http://www.sae.org/works/committeeHome.do?comtID=TEVEES18.</p> |
| [7] | <p>“Consolidation in vehicle electronic architectures”; Roland Berger Strategy Consultants. http://www.rolandberger.com/media/publications/2015-07-23-rbsc-pub-consolidation_in_vehicle_electronics_architecture.html</p> |
| [8] | <p>“Threat Modeling for Secure Embedded Software”; Security Innovation & Klocwork; 2011. http://web.securityinnovation.com/threat-modeling-embedded/</p> |
| [9] | <p>“The 'Heartbleed' security flaw that affects most of the Internet”; CNN.com. http://edition.cnn.com/2014/04/08/tech/web/heartbleed-openssl/</p> |
| [10] | <p>“How the Poodle computer bug impacts business”; Fortune.com. http://fortune.com/2014/11/12/poodle-bug/</p> |
| [11] | <p>“FREAKing hell: ALL Windows versions vulnerable to SSL snoop”; The Register. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204</p> |
| [12] | <p>New DOT Research Shows Drivers Support Connected Vehicle Technology, Appreciate Potential Safety Benefits. http://www.nhtsa.gov/About+NHTSA/Press+Releases/2012/New+DOT+Research+Shows+Drivers+Support+Connected+Vehicle+Technology,+Appreciate+Potential+Safety+Benefits</p> |

About the author

Timo van Roermund is security architect in NXP's business unit Automotive with deep expertise in applied security for embedded devices, such as Vehicle-to-X communication systems, in-vehicle networks, Internet-of-Things appliances, mobile phones and wearable devices. His external contributions include for example his membership of the programme committee of the Cyber Secure Car 2015 conference in Dresden and his active contribution to the ITS (V2X) security standards via the Car-2-Car Communication Consortium's working group Security, the ETSI TC-ITS working group Security and the IEEE 1609 working group. Timo received the MSc degree in Computer Science and Engineering from the Eindhoven University of Technology.

About NXP

NXP Semiconductors N.V. (NASDAQ:NXPI) enables secure connections and infrastructure for a smarter world, advancing solutions that make lives easier, better and safer. As the world leader in secure connectivity solutions for embedded applications, NXP is driving innovation in the secure connected vehicle, end-to-end security & privacy and smart connected solutions markets. Built on more than 60 years of combined experience and expertise, the company has 45,000 employees in more than 35 countries. Find out more at www.nxp.com.

-- This page is intentionally left blank --

www.nxp.com/automotivesecurity

© 2015 NXP B.V.
All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner.
The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use.
Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

Date of release: December 2015