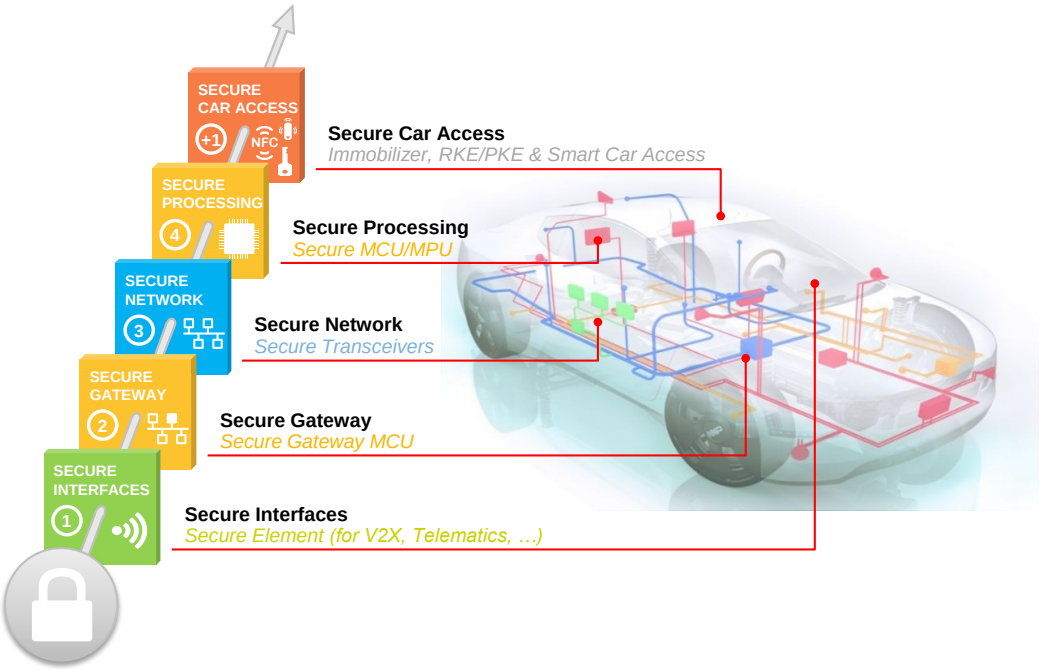
A Multi-Layer Vehicle Security Framework

Whitepaper

Authors:

Andy Birnie, Timo van Roermund
BU Automotive
NXP Semiconductors



-- This page is intentionally left blank –

Contents

-- This page is intentionally left blank –

Introduction

Vehicles are going through a rapid evolution: many mechanical systems are being (or have already been) replaced by electrical systems, leading to highly computerized vehicles. In addition, connectivity is being added for reasons of safety and convenience. But with that comes a security risk.

Until recently, cars have been isolated from their environment and from the internet. The only exception was the interface for vehicle diagnostics, but because this port is a wired interface within the vehicle, it could rely on the physical protection offered by the vehicle itself. As such, remote and scalable attacks, i.e. attacks that can be mounted from anywhere within the internet, did not play a role.

But that situation is rapidly changing. Now most modern cars allow smartphones to be paired via Bluetooth with the car radio for hands-free phone calls or to play music. And many modern cars are wirelessly connected to the internet, for example to enable additional services in the car and to provide for some limited remote control of the car, e.g. remote unlocking and starting. Aftermarket connected insurance and remote diagnostic dongles on the OBD port bring a new connected risk too, unforeseen in the original vehicle design. To improve safety, these cars will also be equipped with telematics based emergency assistance (e.g. eCall) and V2X communication technologies for accident prevention. This results in the fully connected car summarized in Figure 1 below.

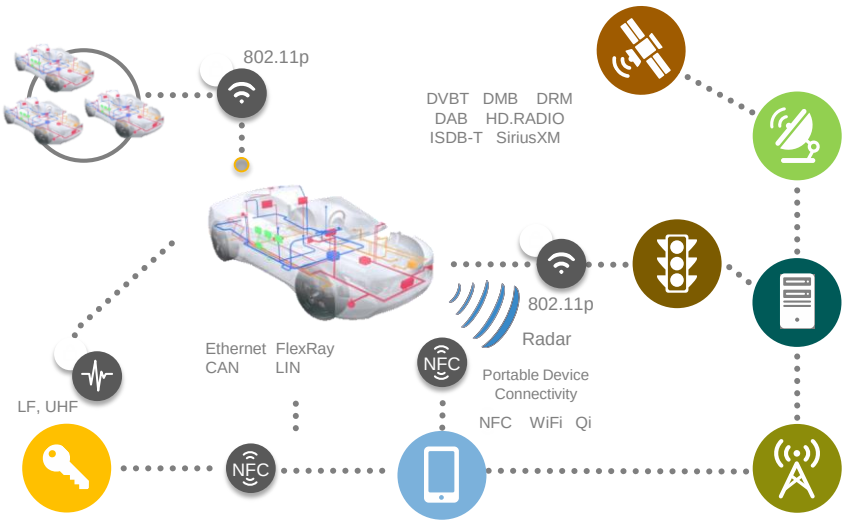


Figure 1: The interfaces of the connected car

The hacks of 2015

The hacks of 2015 reached the popular press [1][2][3], and caused some of the biggest vehicle recalls in history [4]. For the first time, the public started to understand the need for increased in-vehicle security. US politicians felt the need to get involved [5] and most recently the FBI have decided the risk is so high, they have even issued warnings to the public [6]. And recent surveys show that such steps may not be superfluous [7].

But the events of last year has also shown the world that different OEMs had different security levels in place already, and different speeds of solving the issue. As the vehicle OEMs reacted, NXP put together a framework, consisting of 4 security layers that lead to a highly secure vehicle network. Whatever their starting point, this framework will guide our customers to a quick and cost effective step function increase in security, using NXP products.

From a physical hack to a remote attack

Most security hacks, whether targeted at cars or consumer goods like smartphones, consist of linking up a number of smaller vulnerabilities. In the first stage, a hacker identifies weaknesses in the design and/or implementation of a device – often using physical attacks (reverse engineering). The next step is exploitation, in which the hacker links up a number of these vulnerabilities, which may ultimately lead to a remote and scalable attack. The Jeep hack of 2015 is a great example of this: after (physical) reverse engineering of the vehicle, they linked up weaknesses in the external network, the TCU and the programming interface of a device on the CAN network, allowing them to take full control over the vehicle. An attack that affects a complete vehicle fleet is the worst case scenario, but the Jeep hack showed us all that it is, currently, very realistic.

How to secure a vehicle

The Connected Car and the presence of hackers are now parts of life – hence security must be an integral part of the design of the Connected Car, as security is as weak as the weakest link. Vehicle security is a big topic, but we can break it down into manageable chunks.

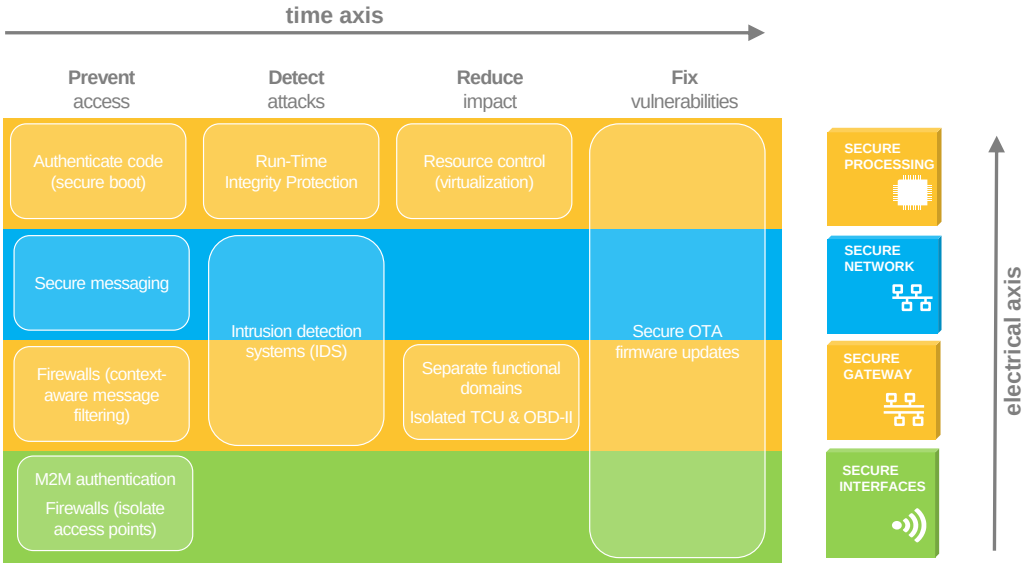


Figure 2: Breaking down the topic of vehicle network security

We can break it down on two different axes – a time axis, and an electrical axis:

The time axis

Security needs to be designed into the vehicle architecture from the very start and it must furthermore be maintained throughout the vehicle's entire lifecycle. Contrary to common belief, security is much more than prevention only. To secure a vehicle, one must:

- **Prevent access**, e.g. using machine-to-machine authentication and gateway firewalls, to ensure that hackers cannot access and tamper with the (safety critical) nodes in the vehicle
- **Detect intruders**, e.g. secure boot of the controller, to validate that the software is (and remains) genuine and trusted
- **Reduce impact** of any determined intruders who did manage to gain access, e.g. by isolating the network domains, to prevent that a compromised infotainment unit in one domain can be used to control e.g. the brakes in another domain
- **Fix vulnerabilities**, e.g. enable full vehicle OTA update capability through the secure gateway, to fix vulnerabilities before they can be exploited (at large scale) by hackers

The electrical axis

We can look at the IT industry for guidance to solve the problem of vehicle security. The key point is defence in depth – never rely on just one line of defence, but assume that has been breached, to reveal another layer of defence. Then assume that has been breached to reveal another layer, etc.

There is for example a common myth that adopting a system of individual unique secret keys for every vehicle is sufficient, but that assumes the perfect impenetrable system, and one of those hasn't been designed yet. Unique keys alone are not sufficient to protect the vehicle. At best, they prevent scaling of the attack to other vehicles.

NXP's 4+1 security framework

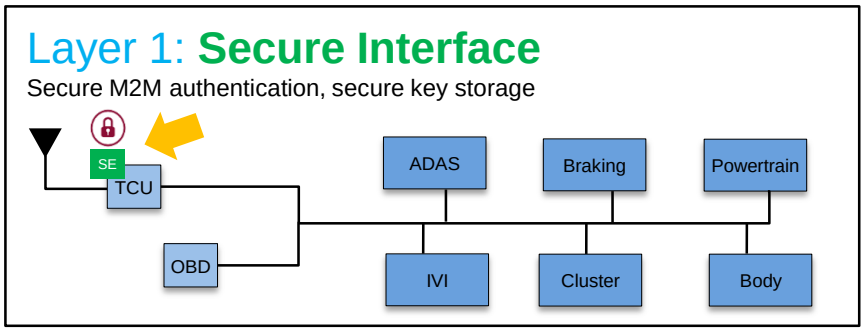
A secure vehicle architecture follows the same principles, summarized in the 4 layers of security that together provide the right level of protection:

- **Secure interfaces,** which connect the vehicle to the external world
- **Secure gateway**, which provides domain isolation (separating interfaces, infotainment, safety-critical systems etc.)
- **Secure network**, that provides secure communication between control units (ECUs)
- **Secure processing,** on the various control units that implement all the features of the connected car

These four generic layers are complemented by an additional layer, comprising the various car access and immobiliser solutions.

Let's look more closely at these layers:

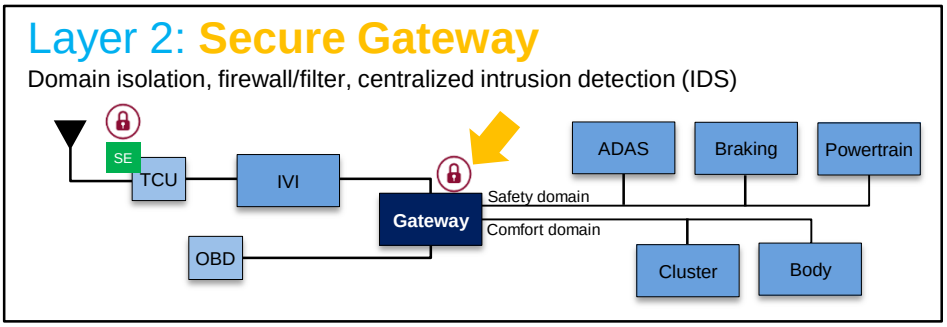
Layer 1 – Secure Interface



A common network today is completely unprotected. If a hacker gets access to the telematics control unit (TCU) or on-board diagnostics (OBD) port, he can then send spoofed CAN messages and hence control safety critical items, like brakes.

To secure the Connected Car, 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.
The first layer of protection adds security to the TCU, by attaching a Secure Element for maximum security. Secure elements are dedicated security microcontrollers with advanced cryptographic accelerators and proven advanced physical and electrical attack resistance – more commonly used in ePassports, bank cards and mobile phones – that can be used to establish an end-to-end secure channel to the external world, e.g. using TLS over a regular cellular or WiFi connection. They also act as an ultra-secure vault for keys and certificates.

Layer 2 – Secure Gateway



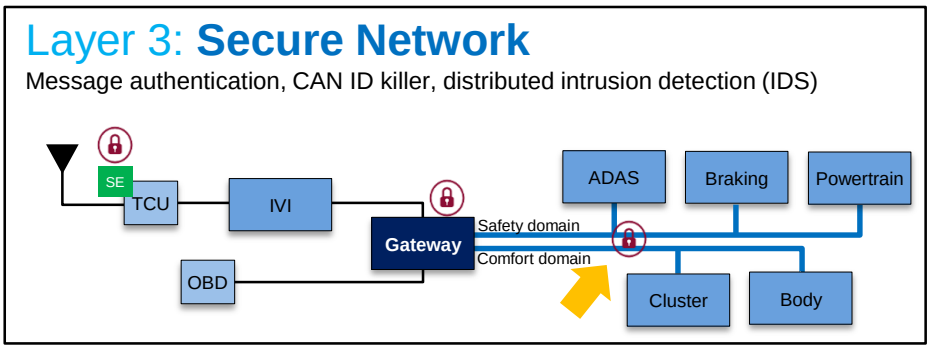
As was observed in the Jeep hack, once the hackers were on the network, they could send messages anywhere. This can be blocked by the presence of a central gateway ECU. This separates the TCU and OBD from the network and breaks up the vehicle network into functional domains, with the gateway firewall deciding what nodes can legitimately communicate with what other nodes

In the Tesla Model S hack of 2015, the protection offered by the gateway was highlighted by Marc Rogers as a key security feature for modern vehicles [3]. Where in the Jeep hack [1], Miller & Valasek could switch off brakes remotely because the Jeep did not have a gateway and associated domain isolation, in the Tesla hack, the worst they could do was sound the horn!

The first true gateway was introduced into some high-end vehicles 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, apart from isolation, its most important function is the 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 currently legitimate, and hence will be passed through the gateway onto the destination.

Layer 3 – Secure Network



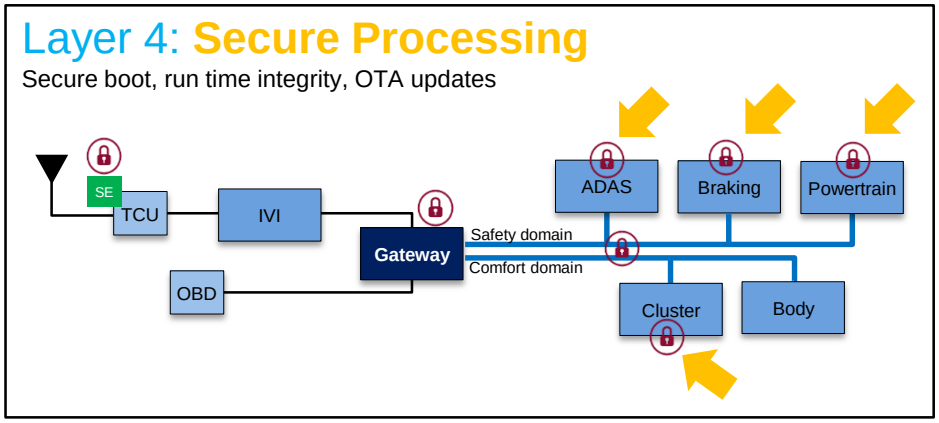
So with the network now split into domains, the attack surface of the architecture is significantly reduced. But the sub-network is still vulnerable to attacks, such as message manipulation. Layer 3 protects this sub-domain by doing 4 things:

1. adding a message authentication scheme – each message is extended with a cryptographic code to guarantee an authentic sender and also that it was received unaltered.
2. encryption – data & identity theft can be avoided by encrypting the messages that are exchanged between different ECUs inside the vehicle
3. intrusion detection – pattern recognition and rules checking to detect anomalies in the network traffic and to block malicious packets before they can even reach the microcontroller, including message rate limiting mechanisms to prevent denial-of-service attacks
4. ECU level validation – the authenticity of ECUs in the network can be verified regularly (e.g. on engine start and periodically afterwards)

These features can be enabled by security subsystems (including cryptographic accelerators) that are integrated in the microcontroller. However, 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.

An network-centric security solution is proposed as an alternative, cost-effective upgrade path. By implementing such security features at the network level, inside the transceiver, security can be retrofit to existing networks with existing ECUs, while significantly reducing the amount of ECU software re-development.

Layer 4 – Secure Processing



And finally, we need to ensure the software running on the processor is genuine and trusted, and has not been altered in any way. To achieve that, modern microcontrollers feature secure boot and real-time integrity checking schemes to guarantee the code image is authentic, trusted and unaltered. On top, mechanisms for controlled lock-down of the MCU and ECU through manufacturing are employed to lock out debug and serial download features, which would be invaluable to hackers

On top of that, a secure software upgrade mechanism is needed. Modern vehicles already feature around 40 microcontrollers (high end can be over 100) and 100 million lines of code (i.e. more than modern PCs and smartphones), and those numbers will only increase over time. That represents huge software complexity. Such complex systems *cannot* be bug free, so vulnerabilities *will* be found after the vehicle enters the road. But when a bug or security vulnerability is detected, the OEM needs to have the ability to quickly, seamlessly and of course securely, update the vehicle software, preferably without the need to visit the garage. The ability to perform OTA (Over-the-air) software updates for *every* ECU in the vehicle is now demanded, and is justified by the number and cost of vehicle recalls in the last few years.

Layer +1 – Secure Car Access

Secure car access is the traditional side of vehicle security, covering immobiliser and car access solutions. Innovations in this area include new features like remote lock & unlock, passive start, remote vehicle monitoring and car access via NFC or BTLE using a smart phone or wearable device.

Which layers to apply, and in which order?

The 4 generic layers are presented here as logical sequential 4 steps, however depending on the OEM architecture, it may be that layer 4 is instigated prior to layer 3, or indeed layer 1 is the last to be implemented relying on the security of an applications processor in the TCU, without the secure element. Decisions like that would need to be driven by individual vehicle threat analysis.

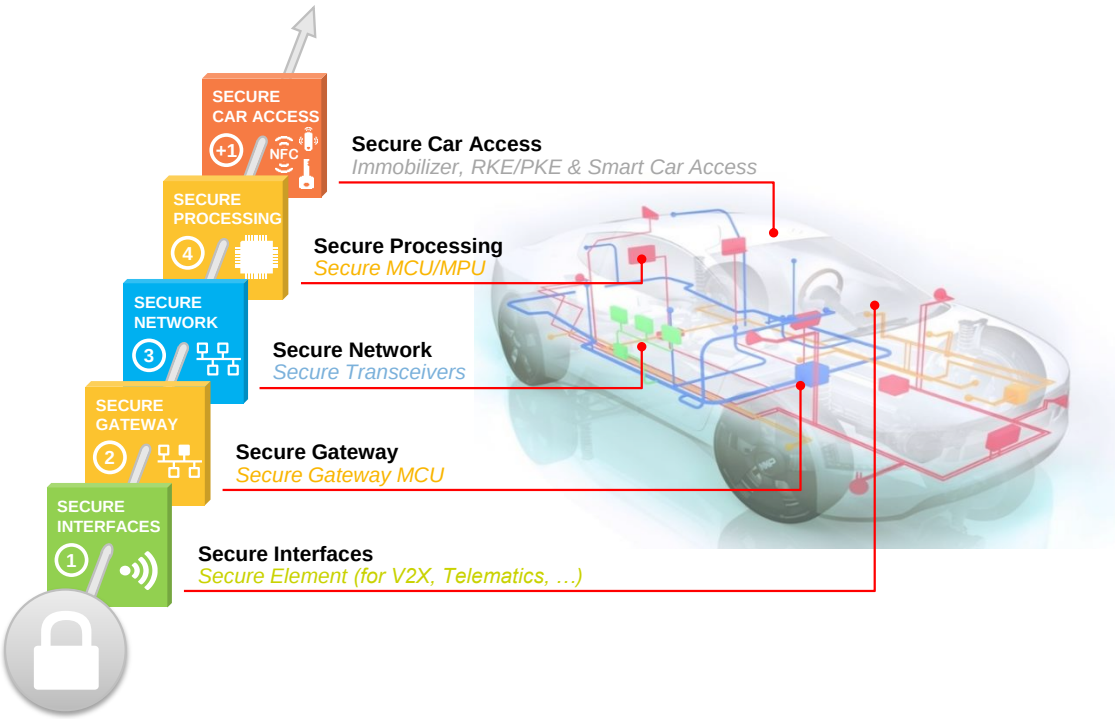
Conclusions

We are in a new era of vehicle complexity and connectivity. But that has also brought a new era of ingenuity and resourcefulness of car hackers. However, the security of the vehicle electrical architecture is vital to ensure the safety of the vehicle occupants so we need to respond to this threat.

NXP has devised a multi-layered approach, that we call our 4+1 layer security framework which provides a holistic approach, for securing the complete vehicle architecture. This builds on our automotive heritage, with deep and wide automotive application knowledge (in-vehicle networking, ADAS, infotainment, body, powertrain, etc) and leverages innovation from our market leading smartcard products used in secure applications like banking, ePassports etc.

This framework applies a defense-in-depth strategy, assuming that a determined hacker can get access through individual layers. These layers of protections are:

- **secure interfaces**, using a secure element as a tamper-proof trust anchor,
- physically & electrically isolated networks using a **central gateway** with firewall
- **secure networks** with the bus monitoring and cryptographic capabilities of a secure transceiver or microcontroller for message authentication,
- **secure processing** on the microcontrollers, with trusted software running in a protected environment.
- And of course, the "+1" layer – the **secure car access** solutions



References

[1]	"Hackers Remotely Kill a Jeep on the Highway - With Me in It"; WIRED; July 21, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[2]	"OnStar hack remotely starts cars, GM working on a fix"; WIRED; July 30, 2015. http://www.engadget.com/2015/07/30/onstar-hack-gm-fixed/
[3]	"Researchers Hacked a Model S, But Tesla's Already Released a Patch"; WIRED; August 6, 2015. http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/
[4]	"Fiat Chrysler recalls 1.4 million cars after Jeep hack"; BBC; July 24, 2015. http://www.bbc.com/news/technology-33650491
[5]	"Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System"; July 21, 2015. 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
[6]	"Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits"; FBI, U.S. DoT and NHTSA; March 17, 2016. http://www.ic3.gov/media/2016/160317.aspx
[7]	"Only One in 4 Americans Remembers Last Year's Epic Jeep Hack"; WIRED; August 3, 2016. http://www.wired.com/2016/03/survey-finds-one-4-americans-remembers-jeep-hack/

About the authors

After graduating from the University of Glasgow, Andy Birnie had various roles in product & technology development, but is currently Systems Engineering Manager for Automotive Microcontrollers and Processors within NXP. In this role Andy is responsible for working with Tier1s and OEMs to understand market trends and customer demands, to define the next generation of microcontrollers and security solutions, keeping NXP at the forefront of automotive electronics systems technology. Andy sits on the OPEN Alliance steering group, pushing adoption of Ethernet into automotive, and was a founder member of the AESIN (Automotive Electronic Systems Innovation Network) consortium in the UK.

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 conference 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 –

-- This page is intentionally left blank –

www.nxp.com/automotivesecurity

Date of release: May 2016