November, 2014

Automotive (R)evolution: Defining a Security Paradigm in the Age of the Connected Car

Authors:
Dr. Joerg Borchert, VP of Chip Card and Security ICs, Infineon North America
Shawn Slusser, VP of Automotive, Infineon North America

Summary

The potential for dramatic improvements in driver safety and comfort/convenience is accelerating the integration of “Connected Car” technology in passenger vehicles. Blending vehicle-to-vehicle (V2V) communications, cloud connectivity, and the integration of consumer electronics technology in vehicles will make driving safer and less stressful. But this increased connectivity calls for new data security mechanisms to ensure the integrity of automotive systems, while protecting consumers from the risk of intentional cyberattack or theft of personal data.

Addressing these security issues is a significant challenge for the broad automotive ecosystem, encompassing the manufacturing value chain, insurers, standards organizations and regulatory bodies. The industry needs to integrate security practices at the earliest stage of design, with the goal of protecting system integrity through the entire vehicle lifecycle. Two well-established and proven foundational principles for security strategy serve as a reference point in the age of the Connected Car:

1. Privacy/security by design
2. A Trust Anchor based approach

With deep experience as a provider of semiconductor solutions for both automotive electronics and security systems, Infineon has a unique perspective on the technologies and business models required to help protect against cyberattack.

The (R)evolution Has Begun

Recent announcements from all sectors of the US automotive ecosystem confirm that the age of the Connected Car has arrived.

V2V Communications: In August 2014, the NHTSA issued an Advance Notice of Proposed Rulemaking (ANPRM) regarding standards for Vehicle to Vehicle (V2V) communications. This is a potential key milestone in a process toward a federal mandate that vehicles be equipped with a V2V communications system to support collision avoidance applications, which NHTSA describes as the most important advance in driving safety since seatbelts. In September 2014, the Michigan Department of Transportation announced that it is teaming with the University of Michigan and auto manufacturers to implement a Vehicle to Infrastructure (V2x) communications system on a 120-mile highway corridor in Michigan. Also in September, General Motors announced plans to begin selling cars with integrated V2x technology in model year 2017.

Cellular/Mobile Integration: The development of integrated V2x technology is the latest example of how passenger vehicles are becoming rolling communications platforms. Cellular connectivity for safety and convenience applications already is offered by multiple OEMs. A growing number of aftermarket companies offer smartphone driven “smart car” services that monitor in-car electronics systems through the easily accessible diagnostic port. At least one manufacturer, Tesla Motors, now uses remote connectivity to update the software of electronics modules in its vehicles; by eliminating the need to visit a dealer for software updates or other services the brand owner is improving both the customer experience and its own bottom line.

WiFi on Wheels: In addition to cellular-based connectivity, manufacturers and aftermarket companies offer mobile “hot spot” capability using the same type of WiFi used for in-home wireless connectivity. Combined with cellular technology, many cars now can maintain a nearly full-time connection to the Internet and thousands of cloud-based services.

Rising to the Challenge

The automotive ecosystem is moving at a rapid pace to create enormous new functionality in how we use personal transportation. While many technology elements will need to develop in parallel, integration of complex technology is a core competency of the global automotive industry. Collectively, and in coordination with policymakers, the industry is now beginning to address the risks introduced by the connected revolution.

Building more communications access points into cars – whether through the Internet or private network connections – makes the vehicle more vulnerable to threats from “bad actors.” For the connected car to succeed, OEMs must build in security that protects the multiple automotive systems that can be accessed through connected technology from risks associated with unauthorized access.

The Connected Car also will exchange information about where and how a driver uses the car with other vehicles and with other points of contact in the transportation and service infrastructure. It is vitally important to balance the safety and convenience benefits of connectivity with provisions to protect the consumer’s right to privacy in daily life. Developing these new security and privacy architectures requires technologies and business models from outside of the automotive industry. Fortunately we can look to lessons learned from other industries in the design of security for other types of networks to design the security framework for the connected car.

The starting point for securing the Connected Car is the concept of lifecycle management and protection. Security architectures for protecting electronic vehicle systems must be an integral part of the design in order to be effective for the life of a car. Establishing a unique-to-each-vehicle trust binding process among safety critical devices, including communications, early in the vehicle lifecycle is critical to future, and inevitable, software updates. Security needs to be capable of withstanding twenty plus years of evolving attacks, and that resiliency will be dependent upon strong initial trust relationships established at vehicle production and sale.

Infineon’s expertise in effective security technologies for the protection of digital information comes from long experience in trusted computing for information technology systems and in authentication and identity protection for financial cards and personal identification applications. The company is a leading manufacturer both of Trusted Platform Module (TPM) technology used to provide a hardware trust anchor in computing systems, and smart card microcontroller chips used to protect credit/debit cards and secure identification documents. These hardware security technologies are proven to be scalable in mass market applications. More than one hundred million PCs and notebooks are equipped with TPMs, more than 450 million e-Passports are in circulation, and billions of secure credit/debit cards have been issued to date.

Safety vs. Security Risk

When talking about the Connected Car, it is important to distinguish between safety risk and security risk. Safety risk refers to the danger of unintentional errors disrupting the safe operation of the vehicle. The industry is tackling safety challenges in electronic systems through the well-developed concept of functional safety, embodied in the ISO 26262 international standards.

Security risk, the focus of this paper, refers to intentional attacks on systems and software. These include the following.

1. Using unauthorized parts in a vehicle to change its operating behavior.
2. Tampering with installed electronic control units (ECUs) to subvert the manufacturer’s intended use/IP.
3. Tampering to inhibit and/or manipulate operation of the vehicle.
4. Using an electronic attack to facilitate theft of a vehicle.
5. Unauthorized extraction of personal information about the vehicle owner.
6. Using an electronic attack to maliciously alter the vehicle behavior or operation.

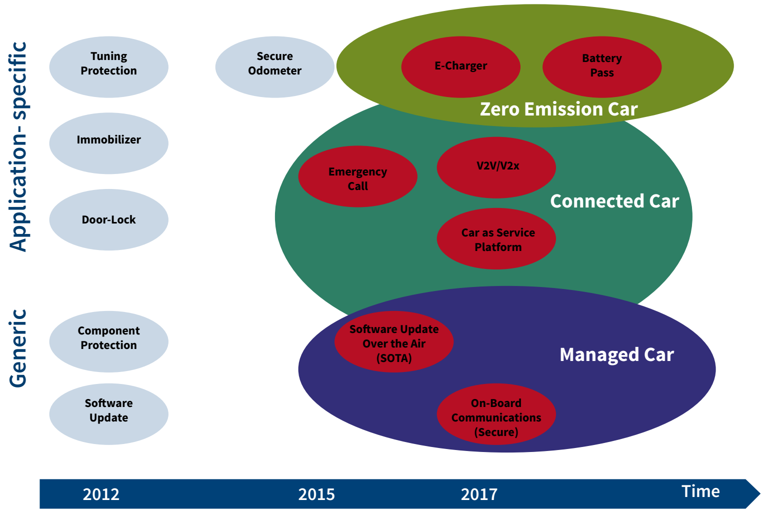

Figure 1: Security Risk in the Connected Car

Figure 1 shows the baseline conditions that exist today and different stages in the evolution of the Connected Car. It shows that certain security risks are not the result of adding network connectivity to the car. These risks, shown on the left side of the diagram, are addressed with technology that does not need to be as dynamic and flexible as techniques to deal with security in a connected environment.

As illustrated in Figure 2, the vision for the Connected Car extends beyond V2V/V2x safety and driver information applications. A vehicle with either Internet or private network connectivity is a platform for a broad range of services. Some of the future use cases that leverage connectivity to enable better care/maintenance of vehicles, improved safety, and convenience/cost saving for consumers are described below.

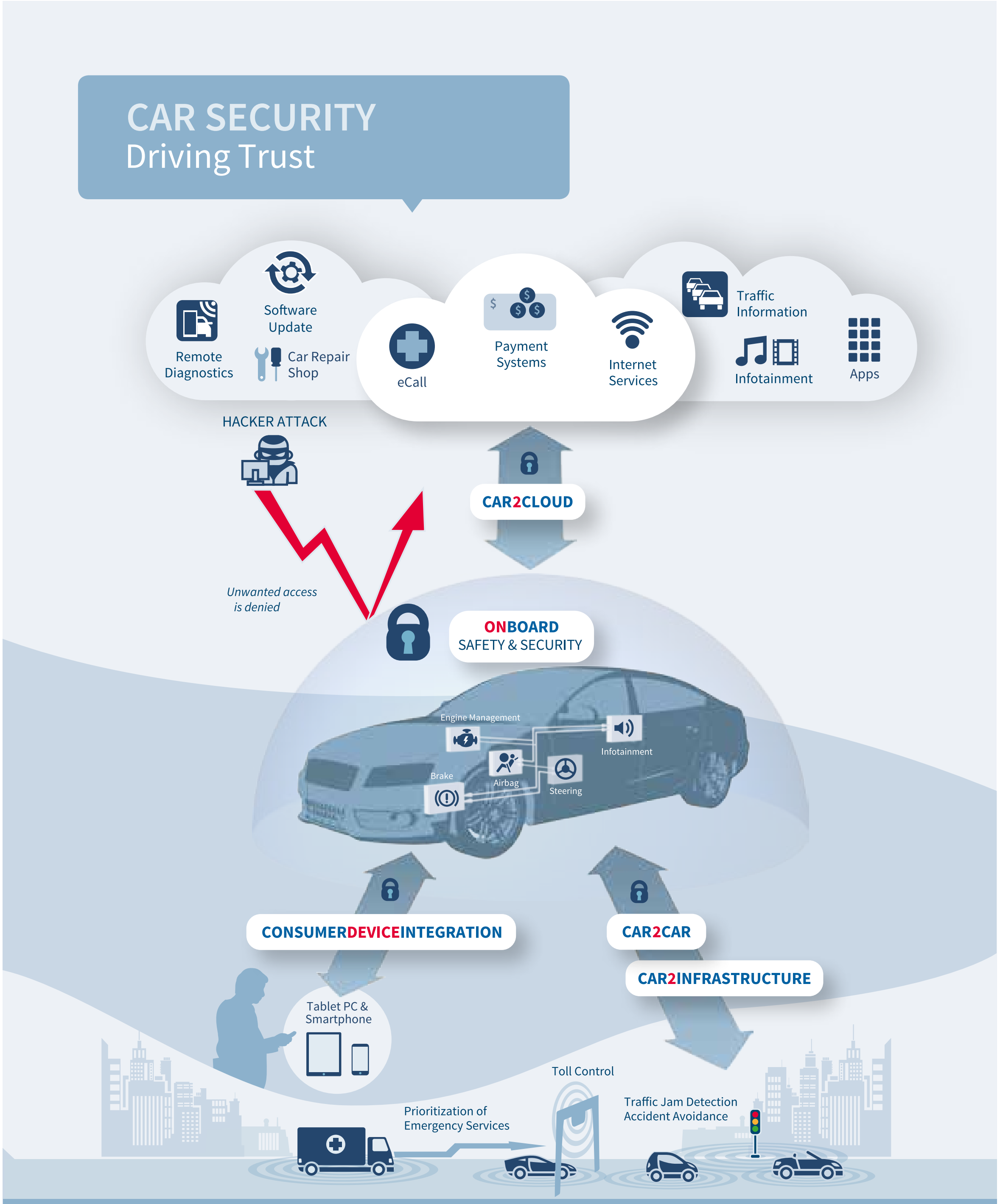

Figure 2: Connected Car Use Cases

1. Automated updates to in-vehicle electronics by transmitting software over the air (SOTA), in the same way that computer/software companies update applications and operating systems and smartphone and tablet apps are upgraded using the cellular network. Given the serviceable life of the car, it is reasonable that some form of software updates will be required over the lifetime of the vehicle.

2. V2V Communications: Collision Avoidance, Platooning and Autonomous Driving applications will use a combination of vehicle sensors (e.g., cameras, radar) to observe conditions within line-of-sight and Digital Short Range Communications (DSRC) to learn about approaching vehicles not yet visible to sensors. An added element is the potential to communicate with non-moving objects (traffic lights, etc.) to improve traffic flow.

3. Opt-In features such as toll paying (electronic transactions), sharing vehicle telematics with insurers (for rate setting), location-based advertising, etc., are envisioned as both new convenience and cost-saving features that can be offered to vehicle owners. It’s likely that additional use cases and business models that we cannot anticipate today will be developed. Making provisions for a secure, trusted and maintainable vehicle platform now will allow the industry the greatest possible flexibility going forward.

Possible Threats and Attacks

In the past two years, “black hat” research teams have demonstrated successful attacks on automotive electronics systems that allowed them to control vehicle acceleration and braking. These attacks were orchestrated through the vehicle diagnostics port, which is used by service technicians to analyze electronic systems connected via a car’s internal wiring network. It is reasonable to believe that similar attacks using wireless network access to the same automotive network systems are feasible and that these may become broadly distributed, just as many exploits are made available to bad actors today. The potential threat to consumers (and the commercial impact on any manufacturer) from such attacks requires a security strategy to:

1. Effectively protect the hardware and software of a vehicle from intentional attack.

2. Protect personal information about the vehicle owner.

3. Finally, and importantly, to make the Connected Car successful in the global marketplace, a security solution should work for the widest possible range of use cases at the best possible cost to the manufacturer, and ultimately to the consumer.

As noted earlier in reference to Figure 1, the industry already addresses a number of security risks inherent in the use of advanced electronics, such as use of unauthorized parts and tampering with odometers. The Connected Car (Figure 2) contains new points of access for potential attackers. In such areas as V2x communications and the vision of the auto as a service platform, market success is dependent on securing all potentially exposed systems against both risk of attack and loss of privacy.

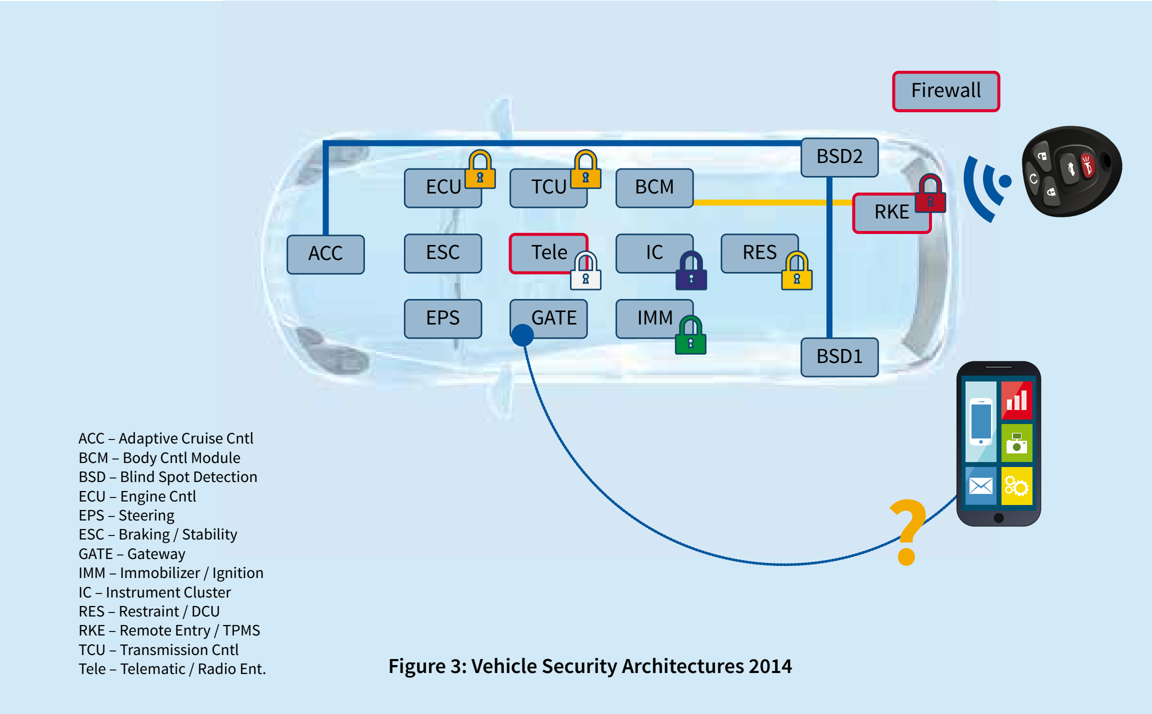

Figure 3: Vehicle Security Architectures 2014

A simplified view of today's automotive electronics architecture illustrates current industry practice. Connectivity is limited to only a few functions, such as simple Remote Key Entry (RKE) and the integrated telematics/entertainment unit in the dashboard. As seen in Figure 3, some of these integrated elements are protected with security mechanisms. Additional mechanisms for protecting electronic modules from physical tampering (including unauthorized changes in software code or exchange of original components for modified units) are also in use.

As external communications links that can access the in-car network are added, component-level security does not adequately address the heightened risk of attack. A multi-level approach is illustrated in Figure 4. Here, all critical systems are protected by security at the module level, and a protected and trusted gateway is implemented to provide additional protection for the entire hierarchy of electronic elements in the auto. Security at the component level may be enabled as part of a microcontroller, in the case of an Engine Control or Transmission Control Unit (ECU/TCU), or be implemented as a separate security microcontroller.

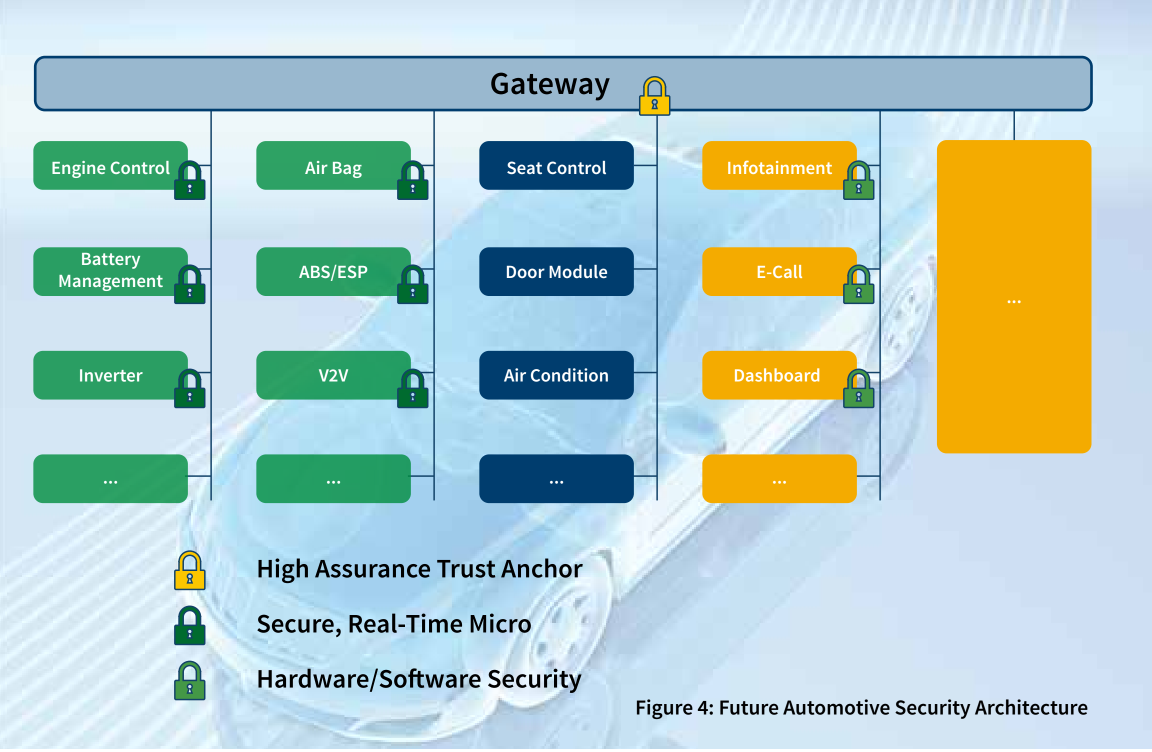

Figure 4: Future Automotive Security Architecture

At the ECU/TCU level, the priority function is for fault-free, real-time performance of automotive electronics. At the higher level of the protected gateway, a High Assurance Hardware Trust Anchor is used to enforce security policies set by the OEM for the entire vehicle. The features of the Trust Anchor include secure memory to store password and certificate information, cryptography capability, authentication to verify messages and revocation capability that allows access to be denied if a potential attack is detected.

In some respects, this architecture is analogous to physical security features in a bank. Security systems such as closed-circuit cameras, electronic access controls, motion sensors and other technologies are installed throughout the bank. The ultimate protection is the bank vault.

In a secure automotive electronic system, the High Assurance Hardware Trust Anchor is equivalent to the bank vault. It guards the secrets that control access to other systems on various in car networks. It also is the nexus for execution of a security control called transitive trust. As the system wakes up (is turned on), the Trust Anchor goes through a series of checks with each electronic component to assure that no tampering has occurred.

Use of a High Assurance Trust Anchor in a multi-level system gives manufacturers the flexibility to implement different levels of security. They often will be able to scale different component level solutions using one of the two common cryptography approaches used to “lock” information held on the security chip.

- Symmetric cryptography systems share a key between all of the devices in a system. This is an effective technique when access to the secret key can be tightly controlled, which makes the key distribution process complex in large scale systems. Its benefit is faster operation, which makes it useful in many component level applications operating solely within the vehicle's internal communications networks.

- Asymmetric cryptography combines a public key that can be shared among back office systems, and serves to unlock a private key secured within the vehicle Trust Anchor. The resulting Public Key Infrastructure (PKI) is very effective at enforcing the trust relationship established early on in the lifecycle of the vehicle, provides for a robust targeted vehicle authentication for communication and updates, and reduces the risk of key exposure typically found in symmetrical based infrastructures. Because secret keys do not have to be shared between devices, no complex distribution mechanism like that used for symmetric cryptography systems is required.

Asymmetric cryptography and PKI systems are used for nearly all secure ID/authentication systems in use today. In fact, the proposed security architecture for the NHTSA's proposed V2V implementation (discussed on page 11 of this paper) uses asymmetric security architectures.

The gateway architecture also provides flexibility for manufacturers to modify or add electronic systems on different sub-networks without consequent changes to the overall security architecture. This will enable a fast rate of innovation and incorporation of new capabilities as the Connected Car evolves.

The Task Ahead

It is critical to think about design for security as an integral part of the electronics system design, not as an add-on to existing system architecture. The task the automotive industry faces as it designs Connected Car security architectures is to determine the level of security technology required for different automotive systems and how they will interact. We have seen that it is likely that an optimal system will utilize different security hardware for different modules in the car, but the system level architecture decisions have to be established early in the vehicle design process.

An equally important part of security architecture is the development of business practices beyond the physical design of the car itself. In the current application areas for cryptographic and security microcontrollers, an ecosystem of institutions that provides validation of security practices and other bodies that manage evaluation of security claims has evolved. This ecosystem includes:

- The Common Criteria for Information Technology Security Evaluation, which provides guidelines for certification of security products based on an international standard. The Common Criteria guidelines in turn are used by authorized testing laboratories to validate that products meet agreed on requirements for security implementation.

- Cryptography guidelines are typically established by government institutions, such as those defined by the U.S. National Institute of Standards and Technology.

- A Certificate Authority is a trusted third-party organization that certifies the authenticity of digital signatures used in PKI systems and provides for revocation of issued vehicle or signing certificates.

In Common Criteria certification of security products, the security integrity of a supplier's processes are explicitly evaluated and verified by independent accredited laboratories. Every step of a manufacturing process is typically audited to assure that information that must be protected is not exposed at any point in the process.

The automotive industry already has a practice of comprehensive monitoring of component and materials manufacturing for quality assurance purposes, so the concept of end-to-end or lifecycle monitoring for security purposes has some parallel. In some cases, such as monitoring for component re-use, security information about a system may be needed even after a vehicle is taken out of service (and after the security certification is revoked). Clearly, design for security will introduce new, data intensive processes and a new set of practices for every participant in the automotive value chain.

As noted at the start of this paper, the age of the Connected Car has begun. The potential for enhanced safety, new services offering an improved customer experience, and operating and maintenance benefits that improve manufacturer's bottom line make the Connected Car a win-win proposition for the industry and its customers. To successfully manage this revolutionary change, design for security and lifetime security trust relationship practices must become a part of the development cycle and the IT infrastructure of manufacturers. Fortunately, there are models from other industries that can be adapted to suit the unique requirements of the automotive industry and make security an integral part of future vehicle architectures.

About Infineon

Infineon Technologies AG, Neubiberg, Germany, is a global supplier of semiconductor and system solutions addressing three central challenges to modern society: energy efficiency, mobility and security. The company has been the market share leading supplier of security microcontrollers for 15 consecutive years and has more than 40 years of experience in the automotive sector. Today, Infineon offers a broad and growing portfolio of cost-effective automotive security solutions. Product offerings include hardware components such as 32-bit microcontrollers with embedded hardware security modules, security controllers for SIM cards, and Trust Anchors based on dedicated secure microcontrollers, as well as software and systems expertise.

Challenges on the Road to V2V in the United States

The US National Highway Traffic Safety Administration (NHTSA) has begun a process to define requirements for Vehicle to Vehicle (V2V) communications systems supporting collision avoidance applications in passenger vehicles. After several years of intensive study and limited-scale field tests of V2V technologies, the agency invited comment on its Advance Notice of Proposed Rulemaking (ANRPM) in August 2014.

The Readiness Report accompanying the ANRPM includes discussion of a security architecture designed to protect both the integrity of the vehicle electronic systems and individual privacy. The proposed architecture, which utilizes asymmetric cryptography and Public Key Infrastructure (PKI), introduces a complex system in which a large number of secure certificates are loaded into vehicle memory at initial point of manufacture and every three subsequent years of the vehicle’s lifetime. This is an enormous task in terms of both the security credentialing infrastructure and the computing requirements of the security architecture needed for each vehicle. The proposed system also does not contain any provision for hardware-based protection of the integrity of private keys (an essential component of PKI systems).

Infineon believes that V2V communications security based on Hardware Assured Trust Anchors within each vehicle can reduce system complexity by reducing the overall number of certificates required for each vehicle. Reducing complexity without sacrificing effectiveness is a desirable goal for any systems engineering problem, as less complex systems will be less costly to implement and maintain and be able to scale to larger numbers than more complex systems.

The Hardware Assured Trust Anchor approach is proven to be effective in securing systems with hundreds of millions of connected devices. As the transition to a Connected Car ecosystem accelerates, the benefits of this approach deserve careful evaluation. With decades of experience in automotive and security systems, Infineon stands ready to help architect, develop and implement effective solutions to secure V2V communications.

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

© 2014 Infineon Technologies AG.
All Rights Reserved.

Visit us:
www.infineon.com

ATTENTION PLEASE!
The information given in this document shall in no event be regarded as a guarantee of conditions or character-istics (“Beschaffenheitsgarantie”). With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

INFORMATION
For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office (www.infineon.com).

WARNINGS
Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office. Infineon Technologies Compo-nents may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.