09AE-0014

Introduction to Vehicular Embedded Security

André Weimerskirch
escrypt Inc.
376 Harbor Way
Ann Arbor, MI 48103, USA

Marko Wolf, Thomas Wollinger
escrypt GmbH
Lise-Meitner-Allee 4
D-44801 Bochum, Germany

ABSTRACT

For new automotive applications and services, information technology (IT) has gained central importance. IT-related costs in car manufacturing are already high, and they will increase dramatically in the future. Yet whereas the area of safety and reliability has become a relatively well-established field, the protection of vehicular IT systems against systematic manipulation or intrusion has only recently started to emerge. Nevertheless, IT security is already the base of some vehicular applications, such as immobilizers or digital tachographs. To securely enable future automotive applications and business models, IT security will be one of the central technologies for the next generation of vehicles.

After a state-of-the-art overview of IT security in vehicles, this paper will give a short introduction into cryptographic terminology and functionality. This contribution will then identify the need for automotive IT security while presenting typical attacks, resulting security objectives and characteristic constraints within the automotive area. We will introduce core security technologies and relevant security mechanisms, followed by a detailed description of critical vehicular applications, business models and components relying on IT security. We conclude our contribution with a detailed statement about challenges and opportunities for the automotive IT community for embedding IT security in vehicles.

INTRODUCTION

Information technology - we broadly define as being systems based on digital hardware and software - has gained central importance for many new automotive applications and services. The costs for software and electronics are estimated to approach the 50% margin in car manufacturing in 2015. Perhaps more importantly, there are estimates that already today more than 90% of all vehicle innovations are centered around IT software and hardware. These applications are realized as embedded systems, and range from simple control units to infotainment systems equipped with high-end processors whose computing power approaches that of current PCs. In high-end cars one can find around 70 processors that are connected by several separate buses and up to several hundred megabytes of embedded code.

Not surprisingly, many classical IT and software technologies are already well established within the automotive industry, for instance hardware-software co-design, software engineering, software component re-use, and software safety. However, one aspect of modern IT systems has received little attention in the context of automotive applications: IT security. Security is concerned with protection against malicious manipulation of IT systems. The difference between IT safety and IT security is depicted in Figure 1. Today there are niche applications in the automotive domain (e.g., immobilizers) that particularly rely on IT security technologies. Nevertheless, the majority of software and hardware systems in current cars are not protected against manipulations. The reason for this is that previous car IT systems did not need security functions because there was little incentive for malicious manipulation. Secondly, security tends to be an afterthought in any IT system, because achieving the core function is often the main focus when designing a system. As can be seen in the example of the Internet, introducing IT security as an after-thought but not from the very beginning is often doomed to failure.

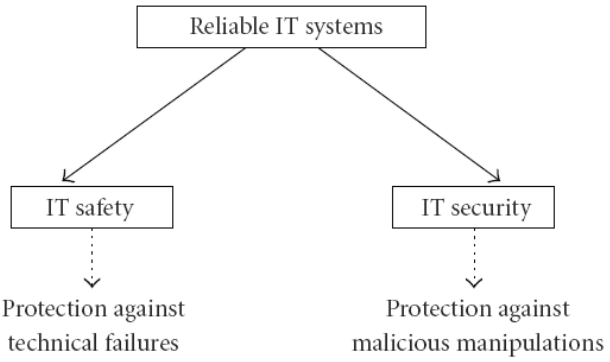

Figure 1: IT Safety and IT Security

The situation has changed dramatically, as we will show in this contribution with respect to the arguments given above. More and more vehicular systems need security functionality in order to protect the driver, the manufacturer and the component supplier. Secure software updating of electronic control units (ECUs), preventing chip tuning, preventing unauthorized change of the mileage, or assembling non-original parts are only some examples. Future cars will become even more dependent on IT security due to the following developments:

- An increasing number of ECUs will be reprogrammable and have to be protected.
- Vehicles will communicate with the environment in a wireless fashion that requires protected car-to-infrastructure communication.
- New business models (e.g., time-limited car functions or pay-per-use infotainment content) will be established, but will only be successful if abuse can be prevented.
- An increasing number of legislative requirements (e.g., secure emergency call functions)
- Increasing networking of cars enables car-to-car communication that has to be protected against abuse and violation of privacy.
- Electronic anti-theft measures will go beyond current immobilizers, e.g., by protecting individual components.

IT security will play an important role for several future automotive technologies, and will even be an enabling technology for some future applications. The target platforms within cars which incorporate security functions are embedded systems, rather than classical PC-style computers. Some obvious differences, in comparison to common PC-based environments, are listed below.

- Embedded devices have small processors (often 8-bit or 16-bit micro-controllers) which are limited with respect to computational capabilities, memory, and power consumption. Hence, the usage of cryptographic primitives and protocols is limited.
- Embedded devices mostly have only limited possibilities and limited bandwidth for external communication. Hence, the extent and frequency of external communication, e.g., for internal updates, are limited.
- Attackers of embedded systems often have physical access to the target device itself.
- Embedded systems are often relatively cheap and cost-sensitive because they involve high-volume products. Thus, adding complex and costly security solutions is not acceptable.
- It is costly to establish the necessary organizational aspects for security products, e.g., one needs to adopt the production and life-cycle chain.

Hence, the technologies needed for securing vehicular applications mainly belong to the field of embedded security, which differs from general IT security.}

CRYPTOGRAPHIC BACKGROUND

Besides security enhancing technologies such as filtering (e.g., firewalls), anomaly detection (e.g., intrusion detection systems), or vulnerability scanning (e.g., antivirus software), cryptographic primitives for data encryption and decryption, signature generation and verification, including the necessary cryptographic protocols, are the core of virtually all security-critical IT systems. Understanding the basic functionality is essential for designing, analyzing, implementing and assessing an IT security system. In this section, we therefore identify the basic security services that can be provided by cryptography, followed by short introductions into symmetric- and public-key cryptography, cryptographic hash functions and cryptographic protocols relevant for vehicular security applications.

SECURITY PROPERTIES

Even though security depends on much more than cryptographic algorithms - a robust overall security design including secure protocols and organizational measures are needed as well - cryptographic primitives and schemes are in most cases the atomic building blocks of a security solution. In the following, we specify the security properties that properly combined cryptographic primitives and schemes are required to enable.

- *Confidentiality* is a service ensuring that information is kept secret from all but authorized parties.
- *Integrity* is a service ensuring that unauthorized parties cannot modify system assets and transmitted information. It is important to point out that integrity relates to active attacks as well as technical errors and therefore it is concerned with detection rather than prevention.
- *Authentication* is a service concerned with assuring that the origin of a message is correctly identified.
- *Identification* is a service establishing the identity of an entity (e.g., a person, PC, credit card).
- *Non-repudiation* is a service that prevents the sender of a message from denying commitments or actions.
- *Access control* is a service restricting access to resources to privileged entities.

Security services can be achieved by employing the two most important cryptographic schemes: symmetric and asymmetric cryptography. Symmetric cryptography provides the ability to securely exchange messages between two parties. This is especially important if the data should not be revealed to any third party. Authentication without non-repudiation can also be achieved if the secret key is known only to the two parties. The second family of schemes, asymmetric or public-key algorithms, provides advanced functions such as digital signatures and key distribution over insecure channels. For common automotive applications, both symmetric- and public-key algorithms are used.

Symmetric-key algorithms require both communication parties to share a secret key. Symmetric-key algorithms are typically used for encryption as well as for protecting integrity and ensuring authenticity. Popular algorithms include the Advanced Encryption Standard (AES) for encryption as well as Message Authentication Codes (MAC) for ensuring integrity and authenticity. Note that the exchange of the shared secret key between the parties should be done using a secure channel, e.g. provided by a public-key crypto-system.

Public-key cryptography is based on the idea of separating the key used to encrypt a message from the one used to decrypt it. Anyone who wants to send a message to another party, e.g., to Bob, can encrypt that message using Bob's public key. However, only Bob can decrypt the message using his private key. It is understood that the private key should be kept secret at all times whereas the public key is publicly available to everyone. Furthermore, it is impossible for anyone except Bob to derive the private key from the public key (or at least to do so in a reasonable amount of time). Public-key mechanisms can be used for key exchange, digital signatures and data encryption. While public-key algorithms provide non-repudiation, they are around three orders of magnitude slower than symmetric-key algorithms. Typical public-key algorithms are elliptic curve cryptography (ECC) and RSA.

Table 1 puts the public-key and symmetric-key bit length in perspective. However, choosing the appropriate key length depends largely on the kind and security of the targets of the application in question. Highly security-critical vehicular applications, such as digital tachographs, motor control units, or immobilizers, have to provide at least middle-term security, whereas less security-critical applications such as personalized presets or customer information services could apply even short-term security.

Security	***AES/DES***	***ECC***	***RSA***
Short-term	64 bit	128 bit	700 bit
Middle-term	80 bit	160 bit	1024 bit
Long-term	128 bit	256 bit	4096 bit

Table 1: Recommended key length for public-key and symmetric-key cryptography

AUTOMOTIVE ATTACKS, SECURITY OBJECTIVES AND CHARACTERISTIC CONSTRAINTS

In the following, we first provide an overview of specific attacks and attackers in the automotive environment that differ from common PC-based IT systems. We then deduce overall automotive security objectives, along with the characteristic automotive technical and organizational constraints.

ATTACKERS IN THE AUTOMOTIVE AREA

Today attackers within the automotive area usually either want to steal a vehicle or a certain valuable component (e.g., the navigation system) or - at the owner's disposition - want to modify certain critical components. These modifications include, for instance, manipulating the mileage for a higher resale value (reduced mileage) or a higher tax return (increased mileage), manipulating the motor control unit (chip tuning) for unauthorized driving parameters, or manipulating the tachograph to circumvent legal driving restrictions or to conceal potential previous infringements. With future electronic applications such as electronic license plates, event data recorders, car communication, and copyrighted infotainment, misuse potentialities will obviously increase further. Finally, there have been non-negligible, partially quite extensive, efforts to steal competitors' expertise and intellectual property in order to advance a company's own developments or, more likely, to illegally produce marketable counterfeits.

Since automotive IT systems, compared to common (PC-based) IT systems, have specific characteristics, attacks on vehicular IT systems differ from attacks on ordinary computer systems. Attackers of a computer system seldom have physical access to the target system, whereas attackers in the automotive sector mostly have physical access to all built-in electronics. If no further protection measures have been integrated, attackers can manipulate or replace all built-in components. Moreover, vulnerabilities are much harder to fix if they are discovered after hundreds and thousands of vehicles have already been sold. Finally, automotive attacks are usually "offline attacks", where attackers have almost unlimited time to make unlimited trials to succeed.

According to the two different attacking objectives - theft and modification - we identify four different groups of attackers as shown in Table 2. In case of theft, the thief may have considerable technical expertise and some appropriate tools. However, a thief usually has only limited physical access and limited time. Three typical kinds of attackers can be identified within an attacking group wanting to modify the system. The first group includes individuals such as the car owner. They normally have only a little technical expertise, a few appropriate devices as well as restricted financial resources for an attack. Skilled (OEM) garage employees are the second group of attackers. They have

appropriate tools, have the necessary technical expertise and have considerable insider information. They would even invest money if an attack promised appropriate revenues, i.e., if it were easy to attack many automobiles. The third group of attackers includes competing manufacturers, counterfeiters and organized crime that may have immense technical and financial resources limited only be the potential economic gain. The motivation of this group is to gain competitors' intellectual property (IP) or to exploit the outcome of an attack commercially, e.g., by selling counterfeits or providing tools and expertise on the Internet.

Target	***Systematic Modification***			***Theft***
Attacker	Individual Owner	Mechanic, Garage Personnel	Organized Crime, Competitor, Faker	Thief
Technical Resources	Varied (Generally low)	High	Very high	Varied
Financial Resources	Low	Medium	Very high	Low
Physical Access	Full	Full	Full	Limited
Risk	Low	Medium	Very high	Medium

Table 2: Attackers in the automotive area

Since the group of counterfeiters and people in organized crime is the most powerful and dangerous one, all actions to protect automotive IT should particularly try to resist attacks from them in such a way that the costs of a successful attack will exceed the potential gain. More importantly, a single successful attack on an automotive device must not be able to break all other devices as well, e.g., by revealing a global identical secret.

AUTOMOTIVE ATTACKS

This section provides an overview of specific hardware and software attacks in the automotive environment that typically differ from attacks on common PC-based IT systems.

Attacks on Automotive Hardware

Attacks on automotive hardware are usually attacks to replace critical components with unauthorized components or to illegally modify existing components. Usually, most hardware components provide no further protection mechanisms beyond some more or less sophisticated tags. They can be easily cloned, modified or replaced by unauthorized components. However, a few critical components, such as the tachograph, the speedometer or airbags, provide some basic (cryptographic) mechanisms to prevent or at least detect unauthorized modifications, replacements, or misuse. In such cases hardware attacks aim at circumventing or breaking these protections by readout of secret keys, deactivation of alarm channels, or wiretapping its operation or communication.

Attacks on Automotive Software

Today's vehicles hold several dozen electronic control units (ECUs) that control almost anything, such as air conditioning, electric windows, engine, and brake system. Several of these ECUs allow downloading an updated program and data code to apply bug fixes, to improve existing functionality, to renew underlying data, or to install/activate new software features. The software update might be performed over a diagnostic channel, other available communication channels such as Bluetooth and GSM, or by using a storage medium such as a CD-ROM or a USB device.

However, current automotive IT systems are mostly unprotected against malicious software attacks. Often, for example, an ECU's memory can be accessed without any further restrictions using its regular interface. Others may be compromised by employing unprotected diagnostic or communication interfaces. Finally, all ECUs without additional tamper-resistant features can be dismounted and analyzed offline using sophisticated equipment. Obfuscation techniques and pure software encryption (without hardware support) provide only minimal additional protection, since all programs have to be decrypted during run time, and hence will be stored decrypted at some point. The program code can then be read out at this point and analyzed by attackers with only moderate technical understanding. Moreover, most encryption keys are stored somewhere unprotected or can be guessed easily. Disabling even sophisticated software protection measures by re-engineering the "decisive validation branch" within the binary enables circumvention of almost all available software protection mechanisms.

Important (software) security vulnerabilities could also originate from inadequate OEM-internal software protection management. Thus, employees should not be able to disclose software to competitors or other unauthorized persons (unconsciously or maliciously) if adequate organizational security precautions are established and executed.

OVERALL SECURITY OBJECTIVES

To guarantee road safety and operational reliability of vehicles, and to sufficiently protect business models based on the security of the vehicular platform, we define the following overall automotive security objectives.

- Confidentiality of data: Unauthorized access to protected data must be unfeasible.
- Integrity of data: Unauthorized modification of data must be unfeasible or at least detectable.
- Hardware and software integrity: Unauthorized modifications to vehicular hardware and software must be unfeasible or at least detectable (by the vehicle).
- Availability: Authorized hardware and software components must have proper access to their dedicated data and services.

- Uniqueness: Unauthorized cloning of a hardware component must be unfeasible or at least detectable as non authentic.

TECHNICAL CONSTRAINTS

The application of complex IT systems in automotive environments is subject to some characteristic technical constraints. Automotive computing resources are -- in comparison to usual computer systems -- rather limited. Nevertheless, automotive applications are often required to provide (hard) real-time capabilities. This leads to severe requirements on complexity, memory size and run-time efficiency for automotive implementations that also often have to cope with lots of specific architectural restrictions.

Vehicular IT systems are often subject to specific physical constraints, such as high variations in temperature, moisture or particular mechanical loads. They usually have to cope with these conditions over a product life cycle of up to 20 years in which only minimal maintenance efforts are acceptable. Moreover, vehicular IT systems usually have only limited communication resources to e.g., exchange cryptographic keys or update software. Thus, virtually all vehicular functionality has to work properly, even with an external communication functionality severely limited in capacity and frequency. Since typical computer users can mostly employ ergonomic input and output devices, users within the automotive environment are restricted to only a few ergonomically designed peripheral devices. To demand only a minimum of user interactions, virtually all vehicular applications are required to run almost completely autonomously.

NON-TECHNICAL CONSTRAINTS

Beyond the technical constraints, automotive IT systems are also subject to some particular organizational and legal constraints that may substantially differ from legal constraints for ordinary computer systems.

A possible public key and certificates infrastructure (PKI) for instance requires complex and costly organizational structures, particular within the automotive context with a multitude of involved parties (e.g., manufacturer, supplier, OEM, garage personnel, content provider, etc.) and only limited (end user) security understanding. Another important key factor is interoperability to existing infrastructures and devices to enable end users to integrate their existing devices (e.g., mobile navigation systems, smart phones, multimedia players, etc.) as simple and holistically as possible.

Since vehicular IT systems - in comparison to e.g., ordinary operating system software - have only limited possibilities for maintenance, compatibility, stability, safety and reliability of deployed hardware and software are requirements. In particular, the corresponding support infrastructure must be available during the complete typical life cycle of the vehicle, i.e., up to two decades. Finally, as vehicular IT systems are often involved in highly safety-critical modules (e.g., steering wheel lock, drive-by-wire systems), they cannot be released 'without warranty' and 'exclusion of any damages', as most PC software usually is. Legally binding warranties are mandatory for providing operating safety and legal security,. However, warranty statements are usually only based on complex and expensive internal and external certification procedures. Thus corresponding documentation, models, tests, and assessments, as well as the development process itself, even has to be prepared for possible certifications at the beginning of any development process.

SECURITY MODULE

A security module, which is also called a security anchor, provides necessary security-relevant methods such as encryption and decryption, generation and verification of signatures, hashing, and secure storage of cryptographic keys. Such a module might be implemented in software or hardware. Clearly, a hardware solution provides higher performance and a far higher security level. It is possible to deploy a single central security module in a vehicle (e.g., at a central control unit) or to implement it in each control unit that has a need for security. In the first case, a hardware implementation is appropriate to securely protect numerous critical assets, whereas in the later case a software implementation could sometimes be adequate.

A security module must fulfill the following requirements:

- *Unclonable*: A security module must be unclonable. It is desirable to bind the identity of a vehicle to the security module in such a way that it cannot be faked, manipulated, or cloned. In addition, it must be impossible to install the security module in another car in order to change its identity.
- *Secure key storage*: A security module must be able to store keys in a secret and protected way. It must protect secret keys from being read and public keys from being altered.
- *Secure computations*: The security module must be able to securely (and efficiently) perform cryptographic operations to prevent leakage of cryptographic secrets into unprotected areas.
- *Alarm channel*: In case of a security breach, the security module must be able to notify people. For instance, such an alarm channel might be provided during diagnostics.

A security module can be based on a customized security controller, a Trusted Platform Module (TPM), or an FPGA. A TPM provides a compatible standard interface more suited to the PC office world, whereas a customized security controller approach can be adapted in a flexible way. Both approaches provide a highly secure computing environment as well as secure key storage. An approach based on FPGAs provides a very flexible way, but at higher cost. The properties of various security module solutions are summarized in Table 3:

	TPM	Custom specific	
		ASIC	FPGA
Standardized	Yes	No	No
Flexibility	No	Yes	Yes
Prize	Medium	Low (for high volumes)	High
Security level	High	Adaptable to required level	Medium - high

Table 3: Security Module Properties

Using a security module purely based on software, run-time attacks exploiting available software interfaces can usually be avoided if an implementation as secure and small as possible is used. Run-time or online attacks are limited to using software interfaces provided and try, for instance, to inject malicious code. However, hardware modifications based on manipulation, exchange, and addition of hardware components probing communication lines cannot be prevented (or even detected) by pure software security modules. Most attacks can at least be detected by applying solutions based on a hardware security module and plausibility checks. Hence, the main achievements of a security module are as follows:

- A single security module might save code size and hence reduce costs.
- A solution based on a software security module can prevent at least run-time software attacks (such as injecting malicious code).
- A solution based on a hardware security module is able to prevent software attacks and detect hardware-based attacks (such as hardware manipulation).

SECURITY MECHANISMS AND APPLICATIONS

In the following, we present mechanisms based on cryptographic methods and the security module that allow components and business models described in the subsequent section to be secured. We start by presenting mechanisms to ensure hardware and software integrity as well as to secure communication channels.

HARDWARE PROTECTION

An easy way to provide basic protection against hardware manipulations can be achieved by mechanical countermeasures deploying special component constructions. Such special constructions could be proprietary constructions that fit only into cars of a single manufacturer or constructions that require proprietary (not publicly available) tools and equipment. However, that solution is uncomfortable and provides only minimal hardware security.

More reliable approaches [5] for detecting faked or bogus vehicle components use small computing tags attached to each crucial component in order to logically link security- and safety-related parts to a specially protected central security module. Such component identification schemes rely on the tamper evidence of the computing tags that are tightly integrated (non-removable) into critical components that can communicate with each other and on the tamper resistance of the central security module. The component identification protocol works even without the need of a central tamper resistant security module by distributing its task to the (of course) more powerful computing tags.

To protect hardware (and particularly hardware IP) effectively, all critical hardware cores have to be integrated completely into a single protected chip. Although there are (physical and chemical) methods to comprise even such a System on a Chip (SoC), these are highly sophisticated and expensive methods. Thus, attacks on SoC hardware today can comprise only a small amount of data and are not applicable to a large amount of hardware. However, if the outcome is worthwhile enough, e.g., if a SoC contains a globally similar secret key that enables easy attacks on a large scale, even sophisticated and expensive attacks are feasible.

SOFTWARE PROTECTION

In order to provide effective software protection:

1. Only original software must be accepted by the vehicle: No manipulated or malicious software must be downloaded to the car. In particular, no software must be downloaded to the ECU that alters the defined behavior of the vehicle (e.g., due to software version conflicts).
2. Only authenticated parties are able to alter data, e.g., parameters, stored in the vehicle.

Furthermore, the following is desired for an actual security design:

- The compromise of a single control unit does not affect the entire system, i.e., a single successful attack does not lead to a global system break.
- The required computational performance on the side of the control unit shall be minimal.

A solution for this problem in general is quite simple. Based on digital signatures, the issuer of the software signs the program code, and the control unit in the

vehicle verifies it. Hence, the issuer holds a secret key for signing the program code, and the control units hold the corresponding public key for verifying it. More details are described in [4].

ELECTRONIC IMMOBILIZER

The electronic immobilizers, as well as the keyless entry to a vehicle, are probably the oldest applications of cryptography in vehicles. The electronic immobilizer usually works in the following way: The vehicle sends a challenge to a passive battery-less transponder integrated in the vehicle key, which then answers by a response. Transponder and vehicle share a secret key. Only if the transponder knows the secret key then the vehicle will start. Hence, a vehicle's key that has the appropriate physical properties (i.e., that is an exact physical copy of the original key) but does not know the secret cryptographic key will not make the vehicle start. This is shown in Figure 2. Here, *f* is a cryptographic function such as a keyed hash function that takes as input the challenge *r* as well as a key *k* and returns the response. A general approach for an electronic immobilizer was presented in [2].

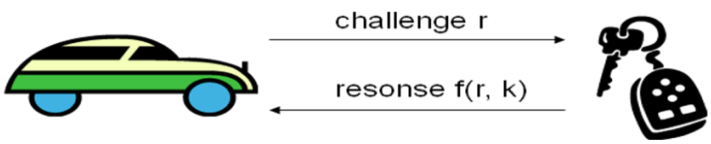

Figure 2: Electronic immobilizer

For the electronic immobilizer, attacks at the hardware layer must be considered. Such a hardware attack can never be prevented at reasonable cost. The goal is to make such an attack impossible for a rational attacker, i.e., the cost of an attack should exceed the gain of the stolen car on the black market. Hence, the goal is to achieve economic security. A hardware security module is an appropriate platform to provide such security goals. It is able to securely store the secret keys and to link the key's transponder to the vehicle by means of the security module. The immobilizer links a crucial control unit (usually the engine control unit) to the vehicle's key. Hence, the engine control unit is only activated if the proper key is presented. There are several weaknesses though. The crucial control unit can simply be replaced by one that is always activated, i.e., by one that implements exactly the same functions but without the key verification. Hence, avoiding malicious software updates of the firmware is absolutely necessary. Furthermore, a so-called Mafia attack is possible. Here, the vehicle's signal is forwarded over an external channel (say, a wireless LAN) to the vehicle's key. This is particularly dangerous in combination with a keyless entry system where an adversary establishes a channel between the victim's vehicle and the victim such that the vehicle's doors unlock and the engine starts. Usually, once the vehicle starts, the engine will not turn off, even if the key's signal is lost.

The latter attack can hardly be avoided on a cryptographic layer. A countermeasure is to use so-called distance bounding. Here, the protocol can make sure that the vehicle's key is inside a well-defined geographical area. However, due to timing problems and the wavelength of the transponder, this might be too imprecise. Further countermeasures can be provided on the physical level. For instance, multi-frequency hopping is already applied today. Clearly, each electronic immobilizer can be compromised. However, the objective is not to set up a perfectly secure system but an economically secure system - breaking into a single vehicle should be more expensive than the gain of the attacker.

COUNTERFEIT AND EXPERTISE PROTECTION

Today large amounts of an OEM's capital investments are spent on software and electronic development that - without further protection - could easily be copied, analyzed and reused by simply buying the corresponding components or vehicles. Thus, reliable counterfeit and intellectual property (IP) protection should prevent copyright infringement or expertise theft by potential competitors and particularly prevent mass production of unauthorized counterfeits of vehicle components.

- *Counterfeit protection*: Illegally produced replacement parts cause a worldwide loss of about 3 billion dollars [1] per month. The professional organized manipulation of automotive electronics causes considerable damage to the manufacturers and to the economics caused by unwarranted claims, brand damage and undermined business models. Moreover, counterfeits endanger the safety of all motorists and cyclists. Traditional methods to prevent counterfeits use tags, e.g., holographic stickers that are supposed to be unforgeable. However, there are illegal businesses that create boxes, labels and other significant trademark logos and emblems to let counterfeits look like real parts.

- *IP and expertise protection*: Automotive OEMs and suppliers always have a comprehensible interest to find out valuable expertise from their potential competitors. Moreover, even though intellectual property rights are legally effective in most countries in the world, there are large domestic markets, such as China, where IP thefts and infringements are virtually untraceable and therefore unprosecutable. Therefore, expertise leakage and IP theft is a serious problem. Today mostly software and firmware, but even complex hardware, can be copied when it is profitable enough. Expertise leakage and IP theft has to be tackled primarily by applying organizational security measures such as scrutinizing potential partners and preventing employees from unintentional (or intentional) exposures. However, (cryptographic) technologies also exist that can help protect IP and expertise or make a theft or leakage at least detectable.

FEATURE ACTIVATION

The production of vehicular components is moving from various small amounts of different, individually adjusted components towards large-scale production of only a small number of uniform standard components. Thus many of the various vehicle versions today internally consist of mostly the same components. On the other hand, providing many individual vehicle configurations is now crucial. To solve these conflicting requirements, car manufacturers could cost-efficiently build parts identical in construction with most features already built-in, but individually activated. Moreover, it is possible to individually activate (or deactivate) built-in hardware components or software after sales for an additional charge that would bind the customer long-term to the OEM. Features that would be capable of aftermarket activation could be, for instance, special setups for engine, gear or chassis control, enhanced board computer and comfort diagnostic functions, additional driving assistance and infotainment capabilities or certain features that can be personalized. However, capable security measures are required to prevent unauthorized feature activation that may undermine the underlying business model. Such mechanisms are described in [3].

INFOTAINMENT

Maybe the most exciting new applications in the automotive industry are driven by new infotainment business models distributing digital content. This area ranges from individual software upgrade packages, OEM premium content and newscasts, up to various multimedia files including music, video or games. Today, most medium-sized cars are already equipped with multimedia-capable on-board computers and radio systems. Upcoming integrated wireless broadband communication promises a brisk market for automotive-related on-demand sales. Embedding a reliable digital rights management (DRM) enables business models for usage-metered and on-demand utilization of digital contents, software and even hardware beyond the classical lump-sum model. Some possible examples are provided below.

- *Time-limited utilization*: Up-to-date navigation and traffic data may be available on demand for any place in the world (e.g., for a two weeks vacation trip in the respective area).
- *Quantity-limited utilization*: Movies, music tracks, or games can be bought for utilization for only n times.
- *Device-bound utilization*: Extra software can be installed on a particular device or a particular vehicle only. Certain car functions are only performed via a certain authentication device such as a driver's key, dealer token or personal cellular phone.
- *Usage-metered utilization*: Navigation routes can be charged for the distance actually traveled. Movies or music tracks can be charged for the actual viewing time.
- *Subscription services*: Audio, video or information broadcast services can be received as long as a valid subscription to the corresponding service exists.

Furthermore, almost arbitrary combinations are possible. For instance, an afterwards activated enhanced comfort sensor (e.g., tire air pressure sensor) may be enabled as a free sample for 4 weeks. Business models using digital content that has usage or access restrictions are only possible with a secure and reliably implemented DRM system. As it could be seen in various (non-automotive) DRM scenarios such as Pay TV, online music stores, or video game consoles, having no such secure module the business model will certainly fail.

CONCLUSION: CHALLENGES AND OPPORTUNITIES FOR THE AUTOMOTIVE IT COMMUNITY

In this contribution we presented a state-of-the-art overview of IT security in vehicles. After a short introduction into cryptographic terminology and functionality, we identified the need for automotive IT security while presenting the specific attackers and attacks within the automotive area. We introduced core security technologies and relevant security mechanisms required to protect current and future vehicular applications, business models and components that rely on IT security. In summary, it can be stated that embedding IT security in vehicles:

1. protects against manipulations by outsiders, owners and maintenance personnel,
2. increases the safety and reliability of a vehicular system,
3. enables new IT-based automotive applications and business models.

As sketched above, there are several difficulties to overcome in order to develop strong embedded security solutions. We would like to give an outlook on the future of IT security in cars in the form of the following recommendations and conclusions:

- IT security will be a necessary requirement for many future automotive applications.
- IT security will allow a multitude of new IT-based business models, e.g., location-based services or fee-based flashing. For such systems, security will be an enabling technology.
- IT security will be integrated invisibly in embedded devices. Embedded security technologies will be a field in which manufacturers and part suppliers need to develop expertise.
- IT security solutions have to be designed extremely carefully. A single “minor" flaw in the system design can render the entire solution insecure. This is quite different from engineering in most other technical systems: a single non-optimum component usually does not invalidate the entire system. One example is the Content Scrambling System (CSS) for DVD content protection, which was broken easily once it was reverse engineered.

- Embedded security in vehicles has to deal with very specific boundary conditions: computationally and memory constrained processors, tight cost requirements, and physical security.
- The multi-tier manufacturing chain for modern vehicles (OEMs and possibly several layers of suppliers) can have implications for the security design. It is, for instance, relevant who designs a security architecture and, most importantly, who has control over the cryptographic keys.
- Merging the automotive IT and the embedded security community will allow many new applications. However, there are also several challenges: security and cryptography has historically been a field dominated by theoreticians, whereas the automotive IT is usually done by engineers. The culture in those two communities is quite different at times, and both sides have to put effort into understanding each other's way of thinking and communicating.

REFERENCES

1. Gieschen Consultancy, “Report: IP theft up 22%, massive $3 trillion counterfeits”. www.bascap.com, May 2005.
2. Ahmad-Reza Sadeghi, Christian Stüble, and Kerstin Lemke, “An open approach for designing secure electronic immobilizers. In *Information Security Practice and Experience, First International Conference, ISPEC 2005.*
3. Kai Schramm and Marko Wolf, “Secure Feature Activation“. *SAE World Congress 2009*, Detroit, USA, 2008.
4. Andre Weimerskirch, “Secure Software Flashing”. *SAE World Congress 2009*, Detroit, USA, 2008.
5. Andre Weimerskirch, Christof Paar, and Marko Wolf, “Cryptographic component identification: Enabler for secure vehicles. In *IEEE 62nd Vehicular Technology Conference,* Dallas, USA, 2005.

CONTACT

André Weimerskirch
escrypt Inc.
376 Harbor Way
Ann Arbor, MI 48103
USA
aweimerskirch@escrypt.com