The connected car: security boundaries

Just like computer systems, today's cars are networked with the internet and external services. As the level of networking increases, so does the risk of unauthorised access which is significantly challenging the automotive electronics sector. Elektrobit Automotive relies on a combination of established security and encryption techniques for the protection of their networked systems. However, these have to be adapted to meet the specific needs of car manufacturers.

Data protection in connected vehicles

The high proportion of electronic components in the car and the connection of vehicles to both other vehicles and external service providers increase the risk of unauthorised access to the infotainment infrastructure. Today's infotainment systems can already download content or new functions from the internet. Specific apps such as the "Connect" system in the Audi A1 run on infotainment platforms. App-supported interaction between vehicle on-board electronic systems and driver smartphones is already a reality with the "Ford Sync" system or BMW's "Connected Drive".

Future on-board systems will increasingly rely on external computing capacity and online information, such as server-based speech recognition as used by Apple's digital assistant, Siri. Cars are becoming more and more connected to infrastructure, the service network, their user's home and other vehicles.

Risk assessment for attack vectors

Although this trend is likely to enhance operating comfort and driver safety, connecting the vehicle to the internet also poses a higher risk of hacking attacks and manipulations with potentially serious consequences [1], (Fig. 1). Those who attack IT systems today rarely do so to prove their technical prowess, but rather with the intention of extracting a benefit. This can be a "proof of concept" in search of security gaps that is rewarded by the affected companies. However, the main concern is criminals who break into third-party systems for financial gain.

Payment systems and account and credit card data stored on servers are therefore popular targets. This risk should not be underestimated given the business models that are planned for the future automotive world. Also, the threat for safety-relevant vehicle systems such as brakes or engine management systems bears a high potential for blackmail for manufacturers and customers, and vehicle theft is also a very real risk.

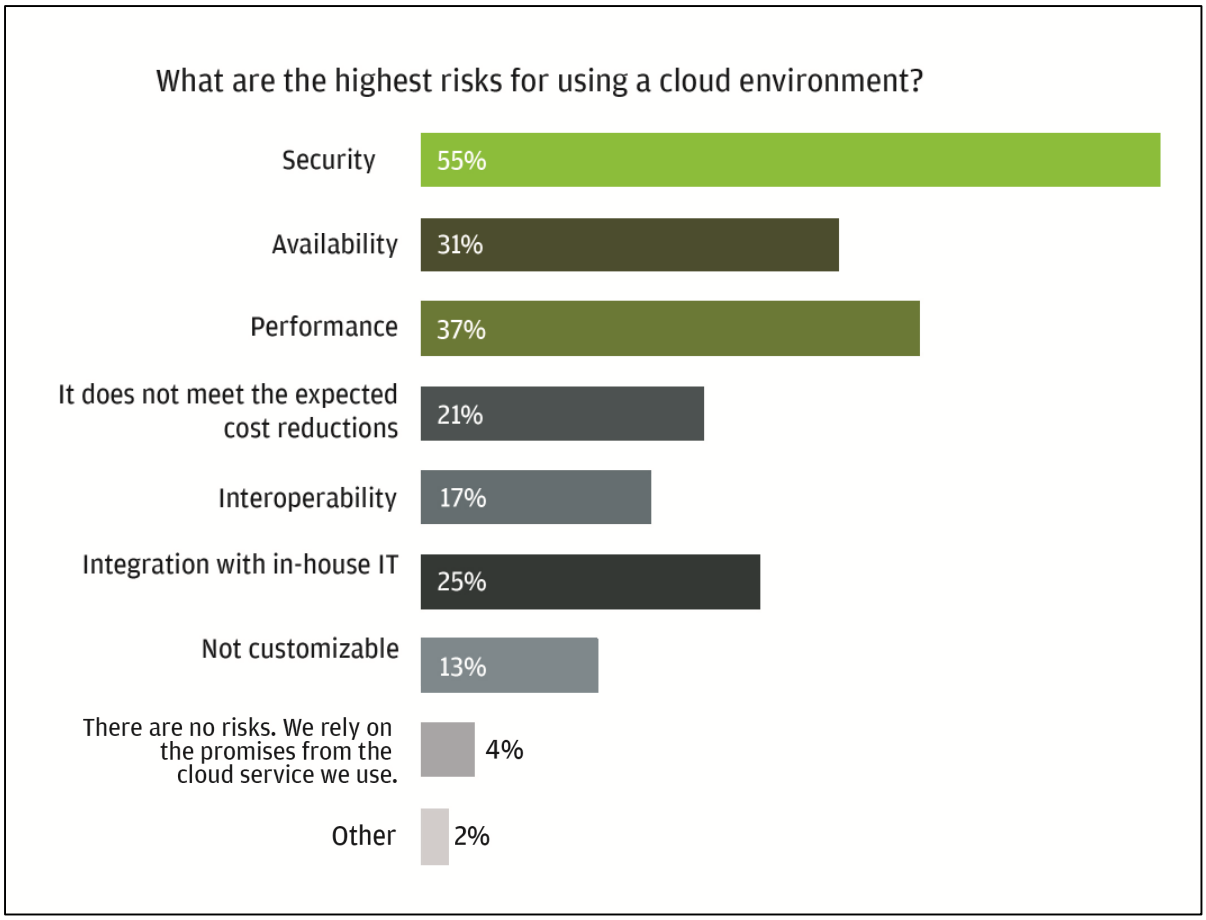

Figure 1: *Security risks are the most important consideration in the use of cloud environments (Source: Capgemini, Sogeti, HP)*

Confidentiality is not the solution

The connection of vehicles with the internet is unstoppable despite all the known dangers and risks, which means that car makers and suppliers are required to provide reliable security solutions for the networked systems. However, the solution cannot be "security by obscurity", i.e. keeping standards and interfaces secret. As early as 1949, the information theorist Claude Shannon laid the foundation for modern security architectures in his maxim "the enemy knows the system" [2]: the system must still be reliably protected even if an attacker knows all its technical details. So, for example, it doesn't matter if the IP address, the port or encryption algorithm is known, as long as the *key itself* remains secret.

In this context the embedded electronics specialist Elektrobit Automotive considers the encryption of data, for instance by means of asymmetric cryptography using the public/private key principle, to be a fundamental prerequisite for modern security solutions. The encryption of data and transmission paths is based on signatures whereby one key is publicly accessible ("public") and another is only known to the user or component ("private").

High security with asymmetric cryptography

The public key enables the originator of a file or transmission to be authenticated and its digital signatures verified. Furthermore, the sender can use the public key to encode data for the recipient. To decrypt an enciphered file or transmission, however, the recipient requires its own private key that is undisclosed to anyone (Fig. 2).

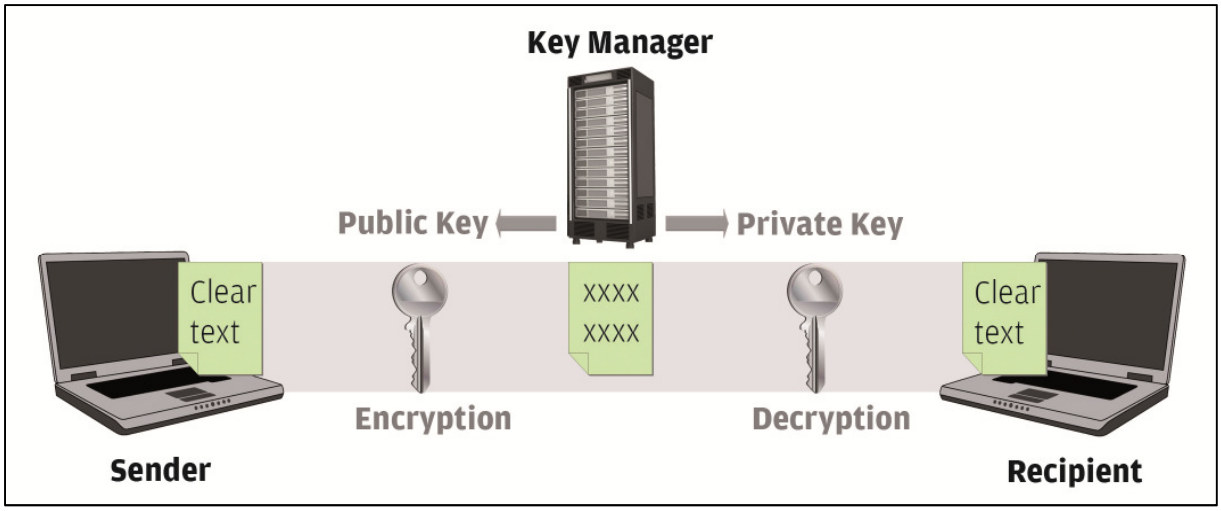

Figure 2: *Asymmetric encryption under the public/private key principle is the most important foundation of today's security solutions*

If the key is sufficiently long (for example the 1024-bit keys used in the automotive sector), this principle also protects against "brute-force attacks", that is, where all conceivable keys are tried.

However, security mechanisms need to be implemented on all system levels (Fig. 3) to provide adequate protection of the car.

Level	Safety precaution
Chips, bus systems	- Signature verification on chip level - „Tamper proof"-components - „Trust architecture"
Automotive components	- Component protection - Signature verification on component level
Software/apps/content	- Proof of source and integrity - Authentification of software components
Transmission path, online access	- VPN tunnel, end-to-end encryption - Identity verification of servers (SSL/TLS)

Figure 3: *Security measures at all levels of information processing protect the systems in the car from manipulation*

Elektrobit has tested special measures for this and deployed them in the field of electronic control unit (ECU) security. They can be individually combined for each module, from the bus system through to data transmission. This enables, for example, EB's software engineers to ensure that navigation systems based on the EB street director navigation solution can securely access the latest map material and traffic information.

Asymmetric encryption as a basis for many concepts

The principle is to deploy asymmetric encryption at all levels of protectable systems. In the field of automotive electronics, this extends right down to communication between components such as chips and bus systems. In these elements, cryptographic signature checks at chip level are frequently used to guarantee the certification and integrity of other components on the data bus. With the Autosar-based ECU operating system EB tresos Safety OS, the signature check is done at chip level via what is known as a Crypto Primitives Library or a Crypto Service Manager, for instance. Additionally, crypto processors are fitted with protective devices to prevent sabotage or unauthorised access ("tamper-resistant" or "tamper-proof"). Because of the complexity of the algorithms and the strict security requirements, these security mechanisms are developed in close conjunction with the semiconductor manufacturers.

Data transfers between ECUs that are connected via the on-board network can be used as a gateway for data manipulation, so these components also need protecting. What is known as component protection (EB tresos Safety E2E Protection) also prevents ECUs or other elements from being replaced with substitutes that may be compromised. The systems then only communicate with one another if they are notified via a signature check.

Protection against harmful components

This prevents components modified with malicious intent from attacking the bus system from within or intercepting its data. Cryptographic authentication is also used at software level, e.g. for the infotainment and user interface systems. Updates, apps or system-relevant content need a signature to demonstrate that they originate from a trustworthy source (usually the vehicle manufacturer) before they are installed and executed.

A state-of-the-art encryption process that is attuned to their application and security requirements is typically used for this purpose. This is usually implemented in the Autosar 4.0 crypto module, for which Elektrobit assumed coordination in the Autosar consortium on behalf of BMW. Last but not least, the transmission route (e.g. via the mobile phone network) and the on-board system's access to servers on the internet need asymmetric encryption. In this way, on-board systems verify whether they are connected to the authentic central server.

This protection can be enhanced by hard-coded server addresses that make it harder to reroute the on-board system to a rigged-up, false remote station as the source of data and updates. Encryption on the transmission route also prevents "man in the middle" attacks whereby an attacker infiltrates the communication between client (vehicle) and server (Fig. 4).

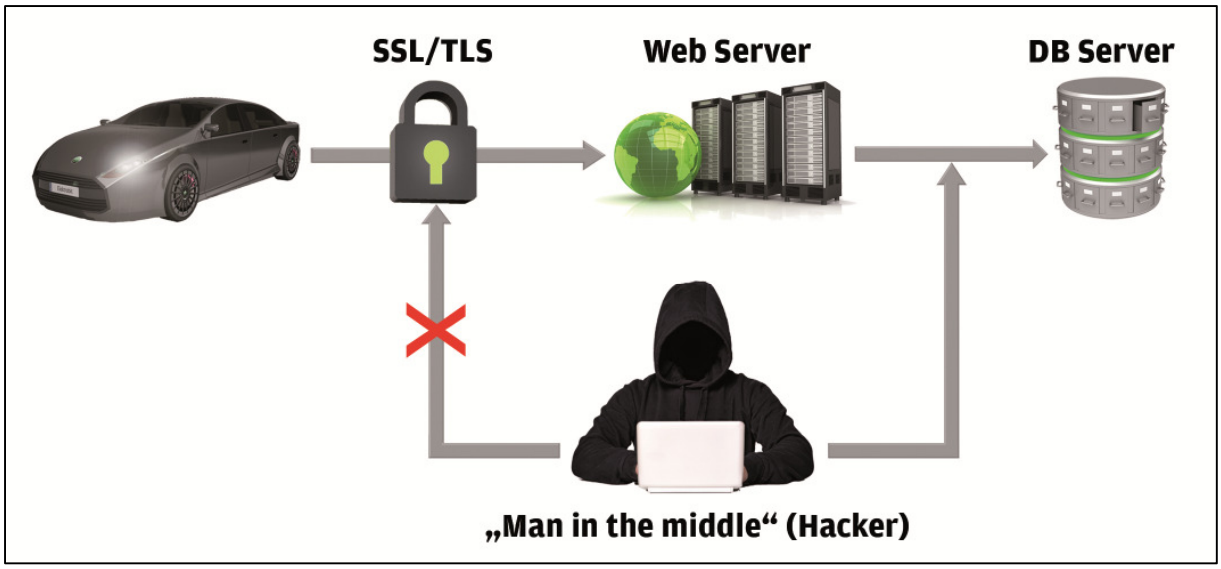

Figure 4: *Encryption (SSL/TLS) of data transfer prevents “man in the middle” attacks in which an attacker manipulates the communication between vehicle and server*

The encryption of the transmission route via VPN (virtual private network) or the identity check of the server with SSL (Secure Sockets Layer) is the responsibility of the server operator (usually the OEM).

System protection through sandboxing and other principles

However, encryption is not the only concept that protects connected vehicle and infotainment systems from attacks. Here the automotive sector has learnt from the IT world. The operating systems used in vehicle systems, such as the Unix-based QNX [3], have storage protection mechanisms. The so-called sandboxing (Fig. 5) prevents subprograms running in parallel from accessing and changing the memory sectors of neighbouring programs.

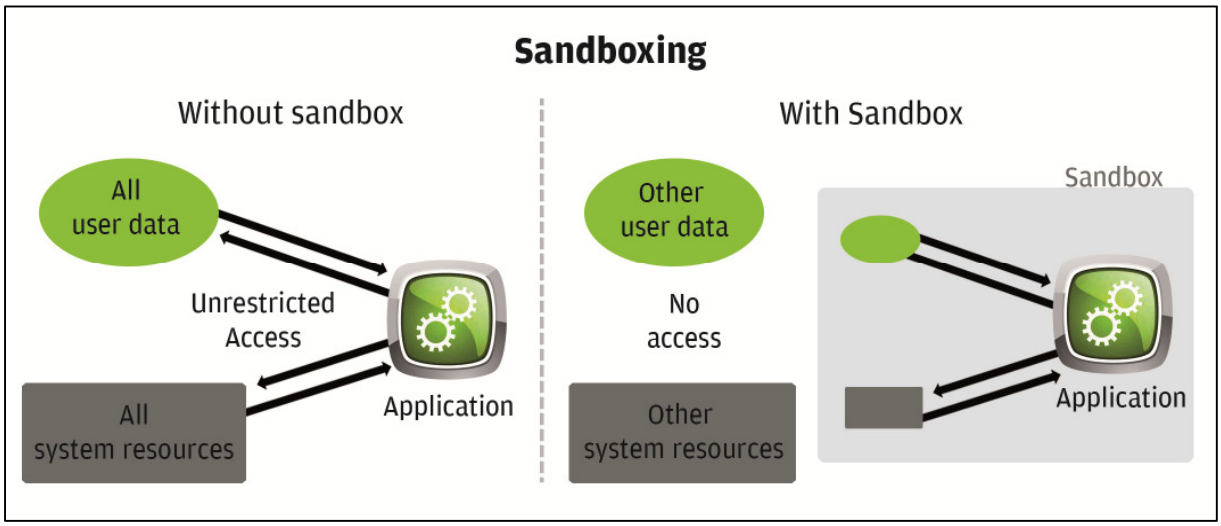

Figure 5: *Sandboxing prevents subprograms running in parallel from being able to access the memory sectors of neighboring programs*

A similar principle is used in the infotainment systems where nowadays web browsers are more and more used to display both operating interfaces and web content. Multiple instances of the browser are run so that manipulated content of a displayed web page cannot infiltrate the operating system. However, because many of these solutions are based on open-source components, the software may contain security loopholes. For that reason security updates also need to become standard in vehicle systems to remedy “zero day exploits”, which are a familiar feature on PCs today.
Zero day exploits refer to the exploitation of specific weaknesses or known malfunctions of a computer program that have only recently become known so that developers have had next to no time to protect the software and its users. Usually the security loopholes are not notified to the software manufacturer. Hackers therefore often keep zero day exploits secret for some time. However, because this gateway exists on the server side, servers need to be protected just as much as the vehicle and the transmission channel.
Therefore a holistic security architecture is necessary. The key components of this include rapid remedying of identified loopholes, security-conscious design of services and processes and the critical assessment of all provided apps, updates and content.

Outlook

As vehicles become more and more connected, the automotive sector also needs to gear up for the cat-and-mouse game between attackers and defenders around security issues. This also includes faster update cycles to satisfy the increased security requirements for vehicles and systems already sold. However, new guidelines, such as ISO standard 27034-1 for the development of safe cloud applications or the planned expansion of the Autosar standard with the definition of additional aspects of secure communication, show the significance of cloud security in the industry.

Author:

Dr. phil. Dipl.-Ling. Nicole Beringer
is coordinator for the Connect segment
in the client/server environment
at Elektrobit Automotive GmbH
in Erlangen.

References

[1] Cloud Security Alliance: Cloud Computing Vulnerability Incidents, A Statistical Overview. In: https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/,2013
[2] Claude Elwood Shannon: Communication Theory of Secrecy Systems. In: Bell System Technical Journal. 28 (1949), Nr. 4, S. 656–715 (http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
[3] http://www.qnx.com/developers/articles/article_300_2.html, 2013