Automotive Security

Position on automotive security
Position on automotive security

Introduction

Digitization is a major innovation driver for both companies and society. The permanent availability of networked and software-based systems, for example via the Internet, is a central customer requirement that is also relevant in the vehicle. These systems have the potential to provide a variety of additional services and functions in and around the vehicle. As a result this new type of function has been increasing for years and is becoming an elementary component of the vehicle and an enabler for associated digital services. Many of these functions are already offered by vehicle manufacturers. The range of personalized functions in the vehicles, the infotainment equipment and the online services offered will represent an even greater share of the overall experience surrounding the vehicle in the future. Automated driving will also use connectivity to access external information that can be used to both refine user experience and expand the scope of automated functionality. For example, the integration of external data will make driverless vehicles possible in an urban environment. Connected vehicles therefore offer innovative features and functions that make driving and the travel experience safer, more pleasurable and more interesting.

Increased networking, additional interfaces and functionalities also increase the vulnerability of vehicles to potential attack by hackers. As the degree of vehicle automation increases, so too must the security measures to protect the vehicle functions against manipulation. In order to cope with the customer’s demands for networking and functionality in the digital age, appropriate security concepts are required that offer sufficient protection for the vehicles, connected back-end systems and customer devices.

It is important to protect both the vehicle and user data against unauthorized access and any vehicle functions against manipulation. Thus, automotive security is required to protect the privacy interests of customers and the integrity of a vehicle, its components and safe operation of its functions. It is in the fundamental interests of the automotive industry to ensure the highest safety standards and to protect the vehicle in the best possible way.

The automotive industry recognizes the need for effective automotive security and is investing in the development and validation of its products at the level necessary to ensure that the protection requirements are met. Security measures are addressed throughout the entire vehicle lifecycle and are addressed in the following three pillars.

This VDA position on Automotive Security is an extension to the existing VDA positions on „Data Privacy“ and „Access to the Vehicle and Vehicle Generated Data“. 
In order to ensure an adequate level of automotive security in new products, a uniform methodical approach to the development of vehicle systems and their networking is described and applied in the industry. This procedure includes the following process steps:

1. Identify and evaluate security risks
2. Determine appropriate risk reduction measures
3. Ensure and verify the implementation of the risk reduction measures
4. Test and release the implementation

This approach has already been proven in the field of functional safety with the industry standard ISO 26262. The VDA and its members have initiated standardization for automotive security engineering in a similar manner. Taking a global view, the Standards Organizations ISO and SAE have established a joint working group to produce the standard ISO-SAE AWI 21434 Road Vehicles - Cybersecurity Engineering. This standard will lay the foundation for making Automotive Security an integral part of the entire development process in the automotive industry. The standard will describe the relevant aspects of product definition, design, implementation, and testing. However, the standard will not prescribe specific technology.
From the perspective of the automotive industry, this standard will achieve an integrated, consistent, application-oriented and risk-based understanding of ‘security by design’, in product development and throughout the entire supply chain.

**Basic technical requirements**

The basic technical requirements are the second pillar in the holistic approach to automotive security. This addresses security protection mechanisms and cryptographic procedures. These basic requirements are based on international recommendations and standards and are applied by individual manufacturers to their respective functions and system architectures.

The fundamental technical requirements are based on established technologies and security best practices, such as cryptographic procedures as recommended by the Federal Office for Information Security (BSI) and other international institutions. This ensures that only recognized, proven and tested approaches are recommended for future developments.

In addition, the basic technical requirements and protection mechanisms are updated with expert knowledge from the automotive industry and checked for individual application at the OEM. This ensures that only state-of-the-art mechanisms are used.

Furthermore, the automotive industry contributes to the establishment and constant improvement of new automotive security mechanisms through various technical standardization committees (e.g. AUTOSAR) or publicly funded projects (e.g. EVITA).

The basic technical requirements and security mechanisms are solution elements within the framework of a holistic security architecture. This must include measures adapted to manage risk at the following levels in the vehicle environment:

- Individual components and control units (secure hardware and software)
- In-vehicle networking (data communication between internal systems)
- External interfaces and protocols (e.g. wireless communication via mobile or WLAN)
- End-2-End security for security-related services.

A security architecture includes not only the vehicle itself, but also connected systems such as backend servers or connected customer devices. The full scope of functional, system-specific conditions and requirements needs to be taken into account.
when designing the security system architecture. Consequently vehicles are not arbitrary nodes in the so-called Internet of Things (IoT), but usually part of a manufacturer managed network with clearly defined rules and access.

Lifecycle Management

The third pillar, lifecycle management, is important because the effectiveness of security measures can change over the entire life cycle of the product. Various external influences can lead to a reduction of the security level over time. In this respect, for example, the following circumstances have to be considered:

- A decrease in the effectiveness of technical security mechanisms such as cryptographic algorithms, as a result of technical advances (e.g. the scale of computing power available to the hacker) and overall progress (e.g. the development of new analysis tools or methods).
- New vulnerabilities and attack possibilities are discovered and disseminated.
- New tools emerge from the hacker community, making complex and time-consuming attacks easier or more automated over time.

In order to meet these security challenges throughout the product life cycle, the VDA members provide appropriate and recognized measures.

A basic measure is field observation. This means that any attacks will be identified and analyzed through both technical and non-technical measures. In addition to existing technical solutions from classic IT, the automotive industry also uses social media, automotive-oriented web forums or vulnerability databases to identify potential threats. Results from field observation are incorporated into the security measures for newly developed products in order to continuously improve the level of protection.

In addition to these individual solutions, platforms have been established within the industry which enable the exchange of information on security topics so that threats can be dealt with as quickly as possible e.g. the AUTO-ISAC1 in the USA and expert committees in the VDA. Security experts are actively involved in these platforms, as well as in research, development and specialist conferences.

As a further measure, the manufacturers and suppliers of relevant components and system product security operate Incident Management2 in order to be able to react appropriately to security incidents. In addition to the manufacturers, the VDA is also a contact point for reporting security weaknesses. The information is directed to the responsible contacts in the member companies in order to enable further rapid analysis and, if necessary, initiation of countermeasures.

Classification of further approaches

The application of the three pillars: security engineering, basic technical requirements and lifecycle management, describes a holistic approach that is suitable for meeting the specific requirements of networked vehicle security. Demands from the political arena focus on certification of security measures and processes or prescribed standard technical solutions in conjunction with regulatory requirements. The VDA approach has a broader scope for the following reasons:

Certification of security measures and processes

Common Criteria (CC) certification typically develops its strength in highly standardized products and regulated markets, especially in clearly defined, manageable and differentiated systems with clear security requirements.

In contrast, vehicles are characterized by diverse functionalities that evolve over time and manufacturer specific security architectures. A certification approach for such diverse and complex systems can only illuminate limited aspects (and therefore not guarantee overall security). Central requirements would inhibit innovation and increase cost since individual solutions that are appropriately optimized may not be compliant.

Compulsory certification introduces the risk that solutions will be designed to simply conform with a security profile, rather than to risk-adjusted measures. In this sense, the certification conveys a false sense of security and does not improve the actual security of the systems. Against this background, compulsory certification is not recommended by the automotive industry for the protection of the owners, drivers and occupants of vehicles.

Demand for technical standard solutions and regulatory requirements for security measures

Standard technical solutions can provide a unified, industry-wide basis for meeting security protection needs. However, they only make sense if their security can be proven, for example in the case of cryptographic procedures.

Industry-wide standardization of solutions at system and architecture level would make it easier to scale attacks on vehicles across multiple product lines and manufacturers. Furthermore, when considering complex vehicle systems or indeed complete vehicles, it cannot be assumed that requirements for various manufacturers and models are the same. Over-standardization will also limit the pace of product innovation.

The automotive industry shares and supports the legitimate social interest that vehicles have an adequate level of automotive security. Regulatory requirements would only make sense if the goals of this regulation are not achieved by the market itself.
Therefore, regulation should only define appropriate security objectives and not technical measures. The concrete solutions to achieve these goals should be designed and implemented by the individual manufacturers in the context of the overall system security architecture.

The VDA and its members consider that the three pillared approach that they have adopted and described in the sections above is appropriate and in everyone’s interest. It will ensure the security of vehicles and vehicle-related services and enable continuous improvement.

1. Backend describes the part of a software application that runs on the server and manages the data.
2. The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations and develops international standards.
3. SAE International, formerly known as the Society of Automotive Engineers (SAE), is a non-profit organization for technology and science dedicated to the advancement of mobility technology.
4. AUTO-ISAC: Automotive Information Sharing and Analysis Center
5. Incident Management: organizational and technical process for responding to detected or suspected security incidents or disruptions