Automotive Cybersecurity

Ashish Jadhav

Introduction

Automobiles of today and of the future are a part of a well-connected network of vehicles which access multiple communication and informational services over cloud and across peers. The electrical infrastructure of a vehicle is made up of a large number of ECUs [electronic control units] communicating over multiple intra-vehicular networks. These are also connected through the in-vehicle infotainment [IVI] and telematics sub-systems to the external world over Internet-based protocols. As such the automotive world is exposed to security and privacy exploits prevalent over the cyberspace.

Automotive cybersecurity is a study of the issues of security of the automobile system and the privacy of the automobile user information in this well-connected vehicular scenario. Compared to any other consumer electronic systems like PCs, mobiles, and IoT devices, a vehicle has its own characteristics in terms of its architecture, usage, and upgrade constraints. In fact Internet of Automotive Things [IoAT] is the term that is used in the vehicular domain of things. As such classical security and privacy techniques like vulnerability and threat analysis, cryptographic security, privacy lists, Public Key Infrastructure [PKI], digital certificates, security updates, etc. need to be relooked and redesigned for the automotive systems.

In recent times various automotive vulnerabilities have been utilized, and security hacks of vehicles have been reported. An additional dimension is that an automobile is a safety critical system and the implication of such hacks in addition to the financial or time loss could also be on the life of the automobile users in the vicinity of a compromised vehicle or the pedestrians nearby. Hence providing security to an automobile user is a very important and challenging area. Automobile OEMs [Original Equipment Manufacturer] are already announcing plans for driverless

A. Jadhav (✉)
Ramrao Adik Institute of Technology, Mumbai, India

M. Kathiresh, R. Neelaveni (eds.), *Automotive Embedded Systems*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-59897-6_6

cars and ADAS [Advanced Driver Assistance System]. Such systems also would need innovative approaches for their security.

In this chapter, we begin with a description of the general principles of cybersecurity. Then we see some aspects of how automotive systems have evolved which helps us in understanding how there are differences between traditional cybersecurity and automotive cybersecurity. Next we look at the automotive cybersecurity threats and the in-vehicle infotainment system that is a crucial component from an automotive cybersecurity perspective. Next we look at the three very important standards in the automotive world from a cybersecurity view. These are AUTOSAR, ISO 26262, and ISO/SAE 21434. Finally we conclude this chapter with some very upcoming initiatives on the use of blockchains in the automotive industry and a brief about the MOBI standard.

Cybersecurity

With the evolution of computer systems, computer networks, computer programs and data, the field of computer security, network security, software security, and data security have undergone a revolution in the past few years. Today, we have computing devices which are ubiquitous, always on and always connected to the Internet. Computing systems today are in the form of mobile phones, tablets, and embedded systems in various things – Internet of Things (IoT). Their typical characteristics are huge volumes, low power consumption, and low hardware capabilities compared to a dedicated computing system like a personal computer or a server. Due to the proliferation of cheap mobile communication, the mobile computer network has innumerable devices used for various applications. Software is truly distributed across multiple devices and is also available as a service through the cloud. This is the world of information and data explosion. There are countless intelligent applications deployed which are processing information across multiple domains.

Cybersecurity deals with security of today's countless devices connected over the Internet executing distributed information processing applications to provide services to today's mobile users and things. It deals with security of the information on the computing devices with end user, cloud and embedded in things. It also deals with security of information in transit and in storage through the network. It deals with the security of flow of information from the end user to the application service provider through various intermediate service providers like hosting services, storage services, network services, etc. Cybersecurity is concerned with the procedures, processes, tools, techniques, and infrastructure required to enable security and privacy in today's world.

Cybersecurity can be further sub-divided into the following security domains from a decomposition perspective:

1. Application security: Dealing with the security of various applications providing services, user interfaces, and application interfaces which can be compromised

2. Information security: Dealing with the security of information and data that is entered, generated, measured, stored, transferred, and displayed by the application
3. Network security: Is the security of the network consisting of hardware and software components that are utilized by the distributed application for the transfer of information and data across geographically distributed application components
4. Computing system security: Is the security of the computing systems that could be personal computers, laptops, mobile phones, tablets, devices, things, etc. which are responsible for execution of the distributed application

Though we can view an application providing some service to a user, decomposition into the abovementioned security entities is important from a perspective of study, design, implementation, testing, maintaining, and upgrading a system with the objective of fulfilling security-related requirements and goals.

Threats to cybersecurity are caused when security aspects like confidentiality, integrity, and availability of system or data are compromised by a malicious user. Confidentiality of data implies that only the intended user can access the data. Integrity deals with the property that the data has not been tampered or changed by an adversary. Availability of the system and data deals with providing the legitimate users access to the system and data.

The objectives of cybersecurity are to ensure confidentiality, integrity, and availability to the users of the application or system. Attacks and hacks are carried out by adversaries to compromise the confidentiality, integrity, or availability of a system or application by exploiting various vulnerabilities present in the system or the application. These could be either in the system/application or in the information database or the network or the systems hosting the application.

This could lead to cybercrimes committed to genuine system users, to cyberattacks which are planned operations with a motive to compromise the system or data for some intention, or to more serious cyberterrorism which is used to cause unrest and panic by compromising security of the applications and data.

Cybercriminals use malicious code (malware) to exploit vulnerabilities and compromise systems and steal data. Some common types of malware include virus, Trojan, ransomware, adware, and botnets. Some cyberattack techniques include SQL injection, phishing, man-in-the middle attack, denial-of-service attack, etc.

Some cybersecurity techniques to protect systems from cyberattacks are as follows:

1. Employing cryptographic techniques for system and application security. Recently quantum computing has been demonstrated, and quantum cryptography is also an upcoming technology that could have a major impact on the implementation of cybersecurity in future systems.
2. Using secure protocols for communication and storage of data.
3. Regularly updating operating systems and application software with the security fixes.
4. Having a strong antivirus software and keeping it up-to-date.
5. Having strong passwords and regularly changing them.

6. Avoid opening emails and clicking on links and executables from unknown sources.
7. Avoid connecting computing systems to public insecure Internet connections.

To ensure that the goals of cybersecurity are satisfied in a system or application, cybersecurity has to be included as an integral part of the software development and deployment process for the application:

1. Cybersecurity requirements are to be included in addition to the functional requirements of the system/application.
2. Cybersecurity considerations to be considered in the system architecture design.
3. Cybersecurity considerations to be included in the coding of the software and the design of the data bases.
4. Cybersecurity testing, verification, and validation activities to be carried out. At times penetration testing and ethical hacking too needs to be performed to ascertain the security of the developed system or the application.

Automotive System Evolution

Automobiles have gone through a major transformation from mechanical machines to electronics vehicles. Olden vehicles had very few electrical parts for starting, ignition, headlights, and blinkers. The earlier vehicles had a very simple electrical battery-driven supplementary system to support the internal combustion engine as the primary locomotive power in the vehicle. Later some sensors and cluster meters used electronics followed by the tuner/radio and audio systems. From those elementary electronics systems in olden day cars, today's vehicles have hundreds of ECUs interconnected with multiple communication networks. Due to the complexity of the implementation today, it is popular to use multicore ECUs [1]. The tuner has been transformed into a complex in-vehicle infotainment system which has diverse communication capabilities and interconnectivity.

Today, cars run multiple applications which enable the vehicle to be networked to other cars or with the infrastructure. As part of these information processing applications, it is necessary for the vehicle to communicate over the Internet. The automotive system can be further sub-divided into the following sub-systems:

1. Body and chassis
2. Powertrain
3. Engine
4. Climate control
5. Braking
6. Steering
7. Exhaust
8. Infotainment and cluster

All the sub-systems have ECUs, software components, and communication abilities to interact with other vehicular sub-systems.

The amount of electronics and software in cars having advanced safety features and autonomous driving capabilities is high to enable drive-by-wire capabilities. In fact modern cars are very complex real-time embedded software-controlled and information-driven mechanical systems. More than 50% of the cost of today's cars is of electronics and the software that goes in it. Across the multiple ECUs, there could be more than 100 million lines of code. Today's cars are truly software driven.

A car is a safety-critical system, and the mechanical, electronics, and software components together have to satisfy the safety goals required for the vehicle. The electronics equipment and all the systems in the car are designed to operate under severe environmental conditions like cold, hot, and dusty situations.

Typically the sub-systems of an automotive system are designed to have a working life-span of greater than 10 years. The infotainment system is typically built to interface with mobile devices and external interfaces. These typically evolve at a faster rate. These are consumer electronic devices and are typically replaced in 2–5 years. Integrating such diverse systems and providing applications in a vehicle which are safety-critical is one of the biggest challenges of automotive system design.

Automotive Cybersecurity

Consider the diagram given in Fig. 1, which shows the block diagram of a connected vehicular network.

Compared to a computer network or a mobile ad hoc network, there is a major difference when we consider the vehicular networks. Whereas the node in a computer or mobile network is typically a computing device which is connected, it is much more complex in the case of vehicles. The vehicle which is connected to the

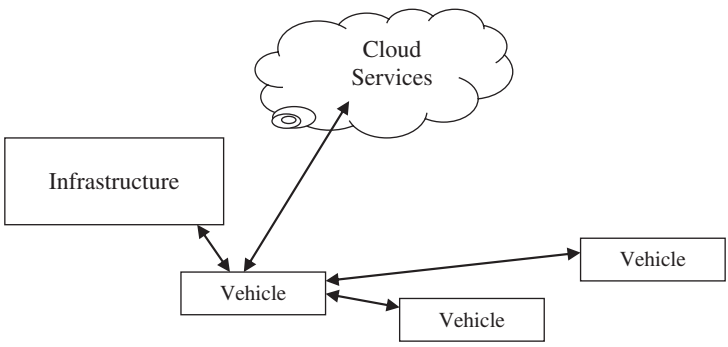

Fig. 1 Connected vehicular network

network is in turn consisting of hundreds of ECUs interconnected by diverse networks like the following:

1. Control Area Network [CAN] typically used for powertrain, engine control, etc.
2. Local Interconnect Network [LIN] typically used for powered windows, seat belts, climate control, door locks, etc.
3. Media Oriented Systems Transport [MOST] typically used for multimedia communication and infotainment systems
4. FlexRay typically used for steer-by-wire, brake-by-wire, etc.
5. Ethernet typically used for telematics applications
6. Dedicated Short-Range Communication [DSRC] for vehicle-to-vehicle and vehicle-to-infrastructure communication, etc.

Most of the ECUs are running real-time critical applications, and a failure or malfunction can be fatal in this safety-critical system. Typically, a secure gateway device is used for interconnecting these diverse networks, and a firewall is used for the Ethernet connection to the external world. Automotive systems can also have intrusion detection systems [IDS] to detect anomalous activity in the network. A diagram of these systems is shown in Fig. 2.

One more challenge from a cybersecurity perspective in an automotive system is that of software updates. While we are used to have automated updates and planned updates in computing systems and mobile systems for fixing security loopholes, updating software in a vehicle is a challenge [2] due to the time-critical nature of the systems and the safety and availability requirements.

Another consideration which cannot be taken lightly in terms of an automotive system is that we cannot say that a system is 100% secure. The same is true about safety, we cannot say that a system is 100% safe. There have been reported cases in the past of accidents that have been caused due to safety failures. Safety processes have matured over the years, and by using techniques like redundancy in the system, the chances of failures can be reduced to satisfy the practical purpose of system

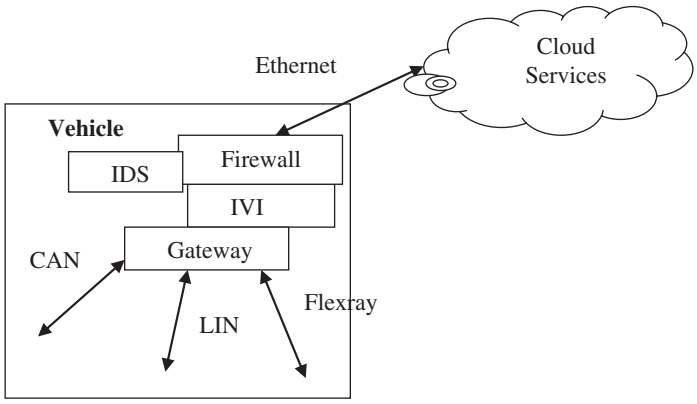

Fig. 2 Automotive cybersecurity system organization

usage. Also, a safety failure is due to some component failure, misbehavior, or environmental factors that can be either predicted or analyzed. The difference in security is that the accidents caused by security breaches are intentional and are cybercrimes. They are caused by an intelligent adversary who hacks into the system and is responsible for the failure caused to the system which could in turn lead even to a safety failure. So indirectly the safety of the system has been manipulated by an intelligent adversary.

There is one more important difference in an automotive system from the point of view of implementation of cryptography to provide cybersecurity. Security heavily relies on cryptographic algorithms. The cryptographic algorithms that implement cybersecurity are basically open algorithms in the sense that the algorithm is publicly known to everyone. The strength of the algorithm primarily depends on the cryptographic key that is used by the algorithm. The symmetric key has to be kept secret in case of a symmetric key-based cryptography between the two parties exchanging secure information. The private key has to be kept secret in case of asymmetric key-based cryptography. Usually the secret key is associated with a user in case of a computational system like PC or mobile and is protected by the password or passphrase which is known and entered by the user for cryptographic operations. In an automotive scenario, this is difficult. As an automotive system is in turn a distributed network of ECUs, the sub-systems would have to communicate securely without human intervention. It is also not possible for the user to enter the password while simultaneously driving the vehicle. The vehicle has to have built-in mechanism to store the secret key and use it without human intervention. So to ensure this secrecy in automobiles, hardware-based mechanisms like a Hardware Security Module [HSM] or on-chip security implementation are used. If a hacker tries to hack the secret key from the hardware module or the on-chip store, the hardware is destructed and fails and has to usually be replaced.

Ethical hackers have taken full control of vehicles in the past and have demonstrated the importance of automotive cybersecurity.

There are a plethora of SAE, ISO, AUTOSAR, and IEEE standards which deal with security of various aspects and components of an automotive system right from ECUs, vehicular networks, to communication protocols. Of special interest is the ISO/SAE 21434 joint standard for cybersecurity of automotive systems, and we will consider this in details in a later section.

Automotive Cybersecurity Threats

The three major threats that exist in any connected vehicle system are threats dealing with the following:

1. Confidentiality—An attacker can gain access to the confidential vehicular data. Data could be belonging to the vehicular driver, connected phone, vehicular data, or OEM-related data.

2. Integrity—An attacker can modify the data in the vehicle. This could be programs in the ECUs. Malicious code can be introduced.
3. Availability—An attacker can prevent the data from the vehicle to be accessed by a legitimate connected external vehicle or a user.

The threat of hacking a car could lead to the following scenarios:

1. Injecting malicious code in the vehicle
2. Getting remote access and taking over the controls of a vehicle, i.e., the driver or the controller of the vehicle is unable to control the vehicle
3. Theft of information flowing from the vehicle to another vehicle, to the infrastructural computer, or to the cloud
4. Getting access to the back-end systems of the OEM or service providers of the vehicle

Traditional security uses a connected system to frequently update security patches. Automotive systems unlike consumer electronics systems have certain challenges and complications in the application of software updates:

1. Automotive system might not be always connected. There could be regions and durations where connectivity does not exist.
2. Difficulty of updating software in automotive systems. The system cannot take time to update, and it needs to start immediately. It cannot start an update when it is being driven as it is a real-time safety-critical system.
3. Unlike a PC or a mobile phone, an automotive system could have software scattered into multiple ECUs and processors connected over diverse networks. Handling distributed updates across the system is complex.

The major threats to a vehicle from a cybersecurity perspective are the following:

1. Brought-in devices. Mobile phones, tablets, and computers which have their own connectivity and which are in turn connected to any of the vehicular system.
2. Vehicular wireless connections like Bluetooth and Wi-Fi, required for infotainment and telematics applications. These could include vehicle-to-vehicle, vehicle-to-infrastructure, or vehicle-to-cloud connectivity.
3. Physical thefts of a chip or module from the vehicle.

A popular threat model in use is briefly described here. The Microsoft STRIDE model [3] classifies potential threats according to the types of exploits that are used:

1. Spoofing—is a threat on the authentication and involves impersonating a legitimate user
2. Tampering—is a threat on the integrity of data and involves modification of data or code by an unauthorized entity
3. Repudiation—is an threat to non-repudiation and involves improper claim on performing some actions
4. Information disclosure—is a threat on the confidentiality of information and involves unauthorized access to information

5. Denial of service—is a threat to the availability of the services to the legitimate users
6. Elevation of privilege—is a threat to authorization and involves illegitimate ways to get authority

For an automotive system threat modeling, the STRIDE threats are considered against each component of the system that is exposed as a threat surface, as well as from the interest of an attacker in exploiting the threat. There are variants of the STRIDE model which are also popularly used by OEMs and suppliers.

In-Vehicle Infotainment Systems [IVI] and Cybersecurity

With the growing demand for touch-based smart entertainment systems in vehicles, the infotainment system is a very important component which has now become a major differentiator in vehicles. In many countries people spend a major amount of time travelling in vehicles, and an IVI system is popular in reducing the boredom of the journey and providing the driver with an easy interface to access vehicular controls and information with minimal distraction from driving. As the system provides a user-friendly HMI which is also driver-friendly, it is rich in features and a complex system having hardware and software components. It usually provides personalization and customizations to the vehicle user.

The infotainment system hosts the telematics interface of the vehicle and is connected to various other sub-systems of the vehicle. It is a very critical component from the cybersecurity perspective of an automobile. Usually a gateway is used to isolate this system having critical cybersecurity threats from the safety-critical ECUs of the vehicle which could be interconnected over diverse intra-vehicular networks as shown in Fig. 2. Usually all connections to the outside world are channeled through the IVI system. At times firewalls and IDS systems are also used as cybersecurity mechanisms to take care of the threats which are exposed by the IVI system.

Usually the IVI system is feature-rich and rich in the sense that it provides a lot of attack surfaces in a vehicle. Some of the attack surfaces are as follows:

1. USB ports—Usually a mobile device or external pen drives are connected and can easily compromise the security of the system or introduce malware. There have been cases where the USB has been used to attack the IVI system by updating the firmware of the system with a malicious code.
2. Diagnostic port—Allows access to outsiders during maintenance and servicing of the vehicle. An attacker can use this port to carry out an attack on integrity and confidentiality.
3. Multimedia playback systems like software radio and audio players can be used to carry out certain types of attacks.
4. Short-range communication—like Bluetooth or Wi-Fi can be used to carry out attacks related with confidential system information or malware injection.

5. Long-range communication—for data connectivity through a mobile communication channel; usually connects to the Internet, from which remote hackers can carry out various types of attacks. GPS connectivity can also be used to hack into an IVI system.

Fortunately techniques used for securing the IVI system in a vehicle are similar to cybersecurity of computing systems and mobile devices, and lots of best practices, tools, and products are available. And intrusion detection systems, firewalls, gateways and other cryptographic tools, and secure protocols are used to take care of the cybersecurity threats posed by the IVI.

AUTOSAR and Automotive Cybersecurity

Automotive Open Software Architecture [AUTOSAR] is an international standard for development of the software stack for an automotive ECU. The objective of this standard is to ensure interoperability among different ECU suppliers supplying the ECU hardware which has tied up basic software stacks and other system and application software components to OEMs. One more major objective of this standard is to reduce the complexity by standardization so that the suppliers can focus on building more complex application over the standardized stack.

Throughout the development of the AUTOSAR standard, the focus has been on defining the interfaces and verification of the conformance of a developed system, with respect to the standard, by performing conformance testing. As this standard development began almost two decades back, there have been various instances where security considerations have been discussed and have been incorporated into the standard in its various releases. The security focus of AUTOSAR has been to define procedures and interfaces for secure onboard communication. The security-related AUTOSAR [4] components of the basic software stack are distributed as follows:

1. Cryptographic Service Manager [CSM] which is a component of the system services layer
2. Cryptographic Abstraction Library [CAL] which is also a component of the system service layer
3. Secure On-board Communication [Sec-Oc] module which is part of the communication services

These modules are responsible to implement secure communication services by providing the following functionalities:

1. Standard interfaces for providing cryptographic services
2. Cryptographic functionality for which support is provided for Hardware Security Module [HSM] or Software Library
3. APIs for carrying out secure on-board communication through the multiple buses supported by the ECU

ISO 26262 and Automotive Cybersecurity

The ISO 26262 standard [5] deals with the functional safety of automotive systems. A vehicle, overall, is a safety-critical system as a malfunction can lead to losses of lives. All the safety-critical sub-systems in an automobile inherently need to be secure. A compromise on the security of the sub-system can easily compromise the safety of the operation of the system. Functional safety and reliability for an automobile system are well-understood domains having standards, tools and techniques. The overlap between cybersecurity and functional safety is an area that is of interest and further research.

Are security countermeasures sufficient to ensure the safety of an automotive system? To answer such questions; people, tools and techniques from different domains need to come together. Some questions that are relevant in this regard are as follows:

1. Is it necessary to design the system having distinct safety and security goals and approaches?
2. Should safety + security be considered together in the design of the system?
3. At a component level, can a component which is not having critical safety level be compromised by security and can be used to compromise the safety of the system as a via media?
4. Can a security attack lead to a safety hazard?

As illustrated in Fig. 3 all safety-critical systems need to be secure. In case of a cyberattack, the hacker can intentionally cause the failure of the safety-critical component. There could be systems which need to be secure and which are not safety-critical. We could also have systems that are non-safety-critical and not secure in an automotive system.

ISO 26262 [5] defines the safety levels for vehicular components and provides practices to design a safety-critical system in the presence of hazards, whereas ISO/SAE 21434 [7] defines the risk associated with security threats to the system. Is there a need to combine these parameters and together come up with a safety + security number? Ahmad [6] has given a detailed analysis of how security and safety are dealt with in standards like the AUTOSAR. The challenge of managing security is the unpredictable nature of cyberattacks. Whereas in safety we deal with hazards, the cybersecurity attack is active and adaptive as we are dealing with an intelligent adversary.

Fig. 3 Safety and security

ISO/SAE 21434 Automotive Cybersecurity Standard

The need to have an automotive standard for cybersecurity stems from the fact that multiple parties are involved in the manufacture of a vehicle. The OEM has numerous tier 1 and in turn tier 2 suppliers who supply parts including mechanical, hardware, and software parts that go in a particular vehicle make. As automotive cybersecurity involves security across these components assembled and working together as a system, it is necessary to have seamless implementation of security across these sub-systems. This calls for a standardized approach to cybersecurity.

The standards are usually enforced by the OEMs on their suppliers and ensure that the final integrated vehicular system satisfies commonly defined goals on cybersecurity. Standards like the joint ISO/SAE 21434 [7] play a very important goal in fulfilling the following cybersecurity requirements:

1. Clear understanding of automotive cybersecurity terminology across all parties involved in the system development
2. Defining common cybersecurity goals that the system should meet which in turn leads to security goals for the sub-systems designed, implemented, and integrated by diverse parties
3. Creating cybersecurity requirements from the goals for the specific parts of the system made by a supplier
4. Having a trail of documentation related to design, implementation, and testing that can be traced for specific security goals and requirements
5. Satisfying security requirements across sub-system boundaries and software interfaces
6. Verification and validation of cybersecurity at the sub-system and at the system levels
7. Ensuring conformance and auditing that the delivered part satisfies the required level of cybersecurity

Initially SAE came up with J3061 [8] guidelines for cybersecurity. Then later ISO and SAE started work on jointly developing the standard ISO/SAE 21434. Various automotive OEMs, ECU suppliers, chip designers, and cybersecurity companies have come together for the development of this standard which is about to be released. This standard will be applicable for cybersecurity for all road vehicles. The standard defines the activities to be performed and processes to be followed for all the phases of the vehicular lifecycle. Typical vehicular lifecycle stages and the impact of security in these phases are as follows:

1. Research and development—It is good to identify the security threats and their implications to the proposed application.
2. Design and engineering— Security requirements influence the design and implementation of the hardware and the software components of the system. Security requirements, design principles, and test cases are to be used in this phase.
3. Production—The engineered security components are preserved and replicated without compromise of the security.

4. Operation by customer—At this phase the system is open for different threats and attacks. The security provided is able to successfully combat the attacks.
5. Maintenance and service—is when the security-related updates and fixes can be applied to ensure continued security of the system.
6. Decommissioning—is when privacy-related threats are high and security credentials can be misused or stolen for attacks on other systems.

The ISO/SAE 21434 standard does not get into the following requirements:

1. Trying to enforce or recommend any specific security solution, technology, or product
2. Remedial solutions and techniques
3. Telecommunication services, systems, or products
4. Servers, back-office techniques, and their connections
5. Electric vehicle charging technologies and services
6. Requirements that are specific to autonomous and driverless vehicles

The standard deals with three different structured layers. The top layer consists of cybersecurity management across various phases. Next is the risk management across the different phases, and finally there are supporting cybersecurity processes. The approach taken is a security risk-based methodology and risk assessment and prioritization approach.

The concept phase for J3061 begins with "Threat Assessment and Risk Analysis" [TARA] [9]. TARA is crucial for recognition of risks early in the development phase and prioritizing the risk levels. The three fundamental security parameters of confidentiality, integrity, and availability are used for assessing the threats and analyzing those. E-Safety Vehicle Intrusion Protected Applications [EVITA] [10] provide the mechanism for risk assessment at the system level. Threat and operational analysis [THROP] uses a threat- and hazard-based analysis approach for risk assessment. Threat Vulnerability and Risk Analysis [TVRA] and Operational Critical Threat, Asset, and Vulnerability Evaluation [OCTAVE] are some other risk assessment techniques that can be used for security assessment.

Blockchain Technologies for Automotive Cybersecurity

Blockchain technologies for automotive [11] domain are one of the most recent trends getting popular. Blockchain offers a secure distributed ledger and is suitable for taking care of secure storage and integrity of information in the automotive domain. Right from OEM and supplier-specific information to information related to spare parts, insurance, vehicle history, ownership, maintenance repair, etc., blockchains can play a major role in securing applications, since they are dealing with distributed information. It is anticipated that in the coming days the usage of blockchains in the auto industry is going to increase many folds.

Some of the benefits of using blockchain in the auto industry [11] are as follows:

1. Tamper-proof data—Which is reliable.
2. No single point of failure in the system—As shared by multiple parties.
3. Transparency of the data—Everyone can see the entity and the changes made.
4. Identity management—Transactions made by an entity are tied to the identity.
5. Irreversible—Changes made cannot be reversed surreptitiously.
6. Information security—Confidentiality, integrity, and availability.

Automotive blockchain consortium Mobility Open Blockchain Initiative [MOBI] [12] is working on an initiative to standardize the automotive blockchain for vehicular identification [VID]. The objective of VID is to be able to identify a vehicle uniquely across OEMs and make and use the unique ID for other applications for tracking the vehicle like ownership changes, repairs, warranty, etc. The standardization effort also aims to improve vehicular on-road safety and emission norms and looks at techniques for reducing on-road congestions.

References

1. S. Abinesh, M. Kathiresh, R. Neelavenik, Analysis of multicore architecture for automotive applications, in *Conference on Embedded Systems (ICES)*, (Coimbatore, India, 2014), pp. 76–79
2. M. Kathiresh, R. Neelaveni, S. Vismitha, An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air, in *Computers and Electrical Engineering*, vol. 71, (Elsevier, Amsterdam, 2018), pp. 578–593
3. A. Shostack, *Threat Modeling: Designing for Security* (Wiley, Hoboken, 2014). isbn:978-1-118-80999-0
4. AUTOSAR CP. Specification of Secure Onboard Communication. AUTOSAR CP Release 4.3.1, Document id: 654.
5. ISO26262 Standard. Road vehicles – Functional safety (2018)
6. A.M.K. Nasser Securing Safety Critical Automotive Systems, PhD thesis, University of Michigan, 2019
7. C. Schmittner, G. Griessnig, Z. Ma, Status of the development of ISO/SAE 21434, in *25th European Conference, EuroSPI*, (Springer, Bilbao, Spain, 2018), pp. 504–513
8. M. Steger, M. Karner, J. Hillebrand, W. Rom, K. Römer, A security metric for structured security analysis of cyber-physical systems supporting SAE J3061, in *IEEE International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, (2016), pp. 1–6
9. ISO-SAE 21434. Road Vehicles – Cybersecurity Engineering: General Overview. https://www.iso.org/standard/70918.html. Accessed 30 Apr 2020
10. O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, T. Wollinger, Securing Vehicular On-Board IT Systems: The EVITA Project. https://evita-project.org/Publications/HRSW09.pdf. Accessed 30 Apr 2020
11. P. Fragma-Lamas, T.M. Fernandez-Carames, A review on blockchain technologies for an advanced and cyber-resilient automotive industry, in *IEEE Access, Special Section on Advanced Software and Data Engineering for Secure Societies*, vol. 7, (2019)
12. M.M. Castorillo, The World's Largest Automakers, Along with MOBI, Announce a Joint Proof of Concept for the First Vehicle Identity on Blockchain. (2019). https://dlt.mobi/. Accessed 30 Apr 2020.