

## INFORMATION SECURITY FOR ELECTRIC CARS IN ACCORDANCE WITH NIST CRITICAL INFRASTRUCTURE CYBERSECURITY FRAMEWORK

### AZ ELEKTROMOS AUTÓK INFORMÁCIÓBIZTONSÁGA A NIST KRITIKUS INFRASTRUKTÚRÁK KIBERVÉDELMI KERETRENDSZERÉNEK VONATKOZÁSÁBAN

TÓTH András

(ORCID: 0000-0001-6098-3262)

[toth.hir.andras@uni-nke.hu](mailto:toth.hir.andras@uni-nke.hu)

#### Abstract

The automotive cybersecurity environment is dynamic and is expected to change continually and, at times, rapidly. The security of the information is a mandatory requirement of all electric cars, which are connected to different networks to communicate among each others or connect to additional systems to get updates or road and traffic information. Some agencies have already developed cybersecurity framework to reach this goal. In this paper, I have specified the NIST Cybersecurity Framework core component functions as a vehicular cybersecurity solution, which supports the information security throughout the complete lifecycle of the vehicles.

 Supported BY the ÚNKP-17-4-IV-NKE-5 New National Excellence Program of the Ministry of Human Capacities”

**Keywords:** automotive cybersecurity environment, cybersecurity framework, Vehicle-to-Vehicle (V2V), Vehicle-to-Internet of Things (V2IoT), Vehicular Ad-hoc Networks (VANETs), Vehicular Cloud Computing (VCC)

#### Absztrakt

Az autóiipari kiberbiztonsági környezet dinamikus, és várhatóan folyamatosan és, napjainkban, gyorsan változik. Az információk biztonsága kötelező követelménye minden olyan elektromos gépjárműnek, amely különböző hálózatokhoz kapcsolódik, hogy ez által képesek legyenek egymás között kommunikálni, vagy olyan további rendszerekhez kapcsolódni, melyek segítségével frissítéseket vagy út- és forgalmi információkat szerezhetnek be. Egyes vállalatok már kidolgozták egy-egy kiberbiztonsági keretrendszert e cél elérése érdekében. Ebben a cikkben a NIST Cybersecurity Framework által meghatározott központi összetevők funkcióit olyan járműbiztonsági megoldásként határoztam meg, melyek a gépjármű teljes életciklusa során támogatja az információbiztonságot.

 Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-IV-NKE-5 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

**Kulcsszavak:** autóiipari kiberbiztonsági környezet, kiberbiztonsági keretrendszer, gépjárművek közötti kommunikáció (V2V), gépjármű és dolgok internete közötti kommunikáció (V2IoT), gépjárműves ad-hoc hálózatok (VANETs), gépjárműves felhő informatika (VCC)

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.30.

A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.22.

## INTRODUCTION

There was organized the International Military Information-security Conference in May 2017, where Prof. László Kovács drew attention during his presentation to the importance of the information security of critical infrastructures, including the information protection of electric cars. This raised a lot of questions in me, and then I tried to deeper into the subject, to find the rules and legislations in force that directly or indirectly deal with this topic. To get to know this, I studied and analyzed a number of domestic and foreign literatures, articles and researches.

Zsolt Haig and László Kovács, in their study, Critical Infrastructures and Critical Information Infrastructures, have pointed out that the world's leading nations have begun before the millennium to pay close attention to the protection of critical infrastructures, which was followed by more robust and defense-centric measures in the early 2000s.

According to their wording, the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets was released at the beginning of 2003, which divided the critical infrastructures into the following sectors:

- agriculture and food;
- water;
- public health;
- emergency services;
- defense industrial base;
- telecommunications;
- energy;
- transportation;
- banking and finance;
- chemical industry and hazardous materials;
- postal and shipping. [1]

This division was similarly prepared by all the states, altered by merging or extending some sectors. As already seen in this compilation, the transport sector has already appeared at that time, but because of during this period there was no widespread the usage of electric cars, the transport sector did not deal with them as a critical information infrastructure. Till the last few years doctrines and standards were always not considered relevant to the automotive sector as there was no vector for cyber threats in the cars themselves. It was changed in February 2013, when the President of the United States signed an Executive Order (EO) to improve critical infrastructure cybersecurity, to counter the growing threat of cyber attacks against critical infrastructure that could threaten the economic health of the Nation and the physical safety of citizens. After this measure the leaders of other nations and international organizations started to develop their own cybersecurity framework to reduce cyber risks to critical infrastructures including e-cars.

The Barack Obama's EO was directed to the National Institute of Standards and Technology (NIST)<sup>1</sup> to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructures. NIST met with over 2,000 representatives of critical infrastructure sectors, state and local governments, international interests and other interested parties, holding workshops to develop the critical infrastructure cybersecurity

---

<sup>1</sup> NIST is an organization to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

framework. It is needed for the framework to meet several requirements. According to these, the framework must:

- include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;
- provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess and manage cyber risks,
- identify areas for improvement to be addressed through future collaboration with particular collaboration with particular sectors and standards-developing organizations;
- be consistent with voluntary international standards. [2]

This paper is focusing on the progress of the information security, in a narrower sense the cybersecurity, and how this affects the automotive industries, both for manufacturing, traditional IT and advanced cyber-physical systems, such as Vehicle-to-Vehicle (V2V), Vehicle-to-Internet / Vehicle-to-Infrastructure (V2I), Vehicle-to-Internet of Things (V2IoT) Vehicle-to-Everything (V2X) applications. In V2V communication, vehicles communicate with one another using On Board Units (OBU), through Omni-directional antennas and sensors. In V2I communication, vehicles communicate with infrastructure units along the road such as toll collection booths, traffic lights, petrol stations etc. Such road side infrastructure units are called as road side units (RSUs). The inter-vehicle communication takes place over a range of 300–500 m using IEEE 802.11 protocols, using the dedicated short range communications (DSRC) standard.

The National Highway Traffic Safety Administration Agency has formulated a guidance as a resource to supplement existing voluntary vehicle cybersecurity standards, principles, best practices, and lessons learned and help guide future industry efforts. In this the basic definitions of the topic were laid, which are used in this paper as well:

- attack surface: the set of interfaces (the “attack vectors”) where an unauthorized user can try to enter data to or extract data from a system, or modify a system’s behavior;
- attack vector: refers to the interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors enable attackers to exploit system vulnerabilities, including the human element;
- automotive: refers to “of, relating to, or concerned with motor vehicles in general”
- Controller Area Network (CAN): a dominant serial communication network protocol used for intra-vehicle communication;
- debug: the activity of discovering errors or undesirable actions within computer code;
- digital signing: a mathematical technique used to validate the authenticity and integrity of a message, software or digital document;
- Electronic Control Unit (ECU): an embedded system that provides control functions to a vehicle’s electrical system or subsystems through digital computing hardware and associated software;
- exploit: refers to an action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software and/or hardware. An example of an exploit would be using a diagnostic port vulnerability to take advantage of a buffer overflow that allows access over Internet Protocol (IP) networks;

- firmware: refers to the software code and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs (I/O) to execute those functions. Firmware may take a variety of different forms. For example, in some cases “firmware” may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled code;
- incident: is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform through the use of an exploit.
- Public Key Infrastructure (PKI): refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates;
- telematics: refers to the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management;
- vulnerability: a weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an ECU is vulnerability. [3]

## **THE FOUNDS OF NIST CYBERSECURITY FRAMEWORK IN E-CAR INFROMATION SECURITY**

In the last years the penetration of cyber security aspects in automotive industry has widely increased and the cars are transformed from a simple mode of transport to a personalized mobile information hub. Until recently, cars have been isolated from their environment and from the internet, but the electric cars use various numbers of wireless technologies, like V2V, V2I, V2IoT, V2X communications, telematics, Near Field Communication (NFC), remote diagnostics provided by Original Equipment Manufacturers, fleet management services and multi-standard digital broadcast reception, complemented by Advanced Driver Assistance Systems (ADAS) that implement autonomous driving features.

All these electronic functions bring great benefits to the driver, increasing comfort, convenience, safety and efficiency. But these features come with new risks, too. Modern vehicles continuously generate, process, exchange and store large amounts of data. Their wireless interfaces connect the in-vehicle systems of these e-cars to external networks such as the internet, which forms entry point for hackers, opening the door for remote attacks.

The transition we are living involves mainly the massive introduction of cyber security functionalities in vehicle components. Coming generations of connected cars will differ as a result of moves toward greater convergence between automotive communications technology and connections to resources beyond the confines of the car. This is needed to deal with the increase of connectivity integrated in vehicles that is progressively exposing the vehicular network to the global hacking community. Indeed the market of aftermarket devices accessing the Controller Area Network (CAN) is wide. These devices include aftermarket head units and On-Board Diagnostic (OBD) ports to dongles, which can be Bluetooth, Wi-Fi or cellular connectivity. These devices are typically connected by the vehicle owner to the OBD port hence exposing the vehicle to remote attacks. In this view the vehicle is a set of high-level functionalities integrated through in-vehicle and out-vehicle data streams and deployed in a set of computation units. This results in the integration of cyber physical systems that provide a number of functionalities by means of wired interactions between electronic control units (ECU). So an e-car is an Internet linked device, where the awareness of online threats and the

malicious hacking of computer systems could affect the use of almost any physical entity that qualifies as a connected device.

The motivations of the hackers can be the followings:

Foreseeable motives:

- Data theft – targeted data types might include:
  - Access to online automotive apps and services – that contain banking/credit records;
  - Congestion Charge or toll payment information;
  - General personal identification data – e.g., social media users names and passwords;
  - Insurance and tax data – useful for identity theft;
  - International travel permits;
  - License plates and other vehicle registration data;
  - Lifestyle information – e.g., fitness club membership;
  - Medical records – a driver suffering from a health issue may have information about their condition either stored on a vehicle or accessible via the vehicle or a mobile device temporarily connected to the vehicle;
  - Vehicle location information – which may be used to identify patterns of use or driver behavior in anticipation of offensive action against a vehicle;
  - Vehicle physical security data.
- Extortion / denial-of-service threat;
- Fraud and deception (altering or deleting schedule logs and records);
- Freight and goods theft (activating false alarms that cause goods to be left unattended);
- Automotive ‘Hactivism’ – cyber-infiltration of a vehicle’s systems that is politically- or ideologically-motivated;
- Immobilization;
- Mischief and malevolence – individual hackers testing defenses and their skills; or wanting to inflict damage and/or disruption out of spite;
- Premises security and burglary – vehicle data that reveals businesses and homes are unoccupied.

Secondary motives:

- Industrial espionage – illegal access to intellectual property;
- Infliction of political or reputational damage;
- ‘Script kiddies’ – adversarial hackers pitting their skills against the automotive software safeguards;
- Sabotage or degrading of vehicle and connected system performance;
- Terrorism – disabling vehicles as part of an attack, for instance vehicle identification re-assignment (for stolen cars). [4]

The automotive industries can use the NIST Cybersecurity Framework components to avoid or minimize the possibilities of these attacks. It allows enterprises to identify, detect, protect, respond and recover from cyber security risks and incidents, and it provides a basic baseline set of controls which companies can use to better understand, manage, and reduce its cybersecurity risks, and to help determine “which activities are most important to assure critical operations and service delivery.

The National Highway Traffic Safety Administration Agency created a paper in this topic in 2014 (National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles), but it only looked at the subject from the risk

management side. The Agency's multilayered approach to cybersecurity has the following goals:

- expand the knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
- facilitate the implementation of effective, industry-based best practices and voluntary standards for cybersecurity and cybersecurity information-sharing forums;
- foster the development of new system solutions for automotive cybersecurity;
- research the feasibility of developing minimum performance requirements for automotive cybersecurity;
- gather foundational research data and facts to inform potential future Federal policy and regulatory activities. [5]

They specify 6 risk management framework steps for the vehicle sector to define criticality/sensitivity of information systems, select baseline security and supplement controls, implement security controls for applying security configuration settings, determine security control effectiveness and continuously track changes to the information systems. The 6 steps are the following:

- assess threat model/use cases;
- categorize vehicle systems;
- select security controls;
- implement security controls;
- assess security controls;
- monitor security controls.

They define that the security controls are the management, operational and technical safeguards (or countermeasures) prescribed for a system to protect the confidentiality, integrity and availability of the system and its information. Security controls, also known as security requirements, will be needed to implement security controls to protect vehicles (based on safety criticality considerations. [6]

I analyzed the vehicle sector from the NIST Cybersecurity Framework core component functions, which contain cybersecurity activities and informative references and organized around particular outcomes. It is possible to identify the following areas with the five steps of the functions:

- What processes and assets need protection?
- What safeguards are available?
- What techniques can identify incidents?
- What techniques can contain impacts of incidents?
- What techniques can restore capabilities?

Functions organize basic cybersecurity activities at their highest level. These functions are identify, protect, detect, respond, and recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. [7]



**Figure 1.** The NIST Cybersecurity Framework core component [8]

The first step, as shown on Figure 1, is to identify what processes and assets need to protect. The companies have to do an asset management, where they can find the physical devices, the internal and external information systems, the software platforms and applications, what they have to protect against a possible attack. Also very important to do a risk assessment (as it is specified in the National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles) to identify the possibly threats, the asset vulnerabilities, likelihoods and the impacts. Specific attacks are address for instance the cyber physical systems integrated in the vehicle. They depend on the vehicle and aim to measure the security of vehicle functions. Typical examples are traction control, ABS, automatic transmission. The likelihood is measured on the basis of five aspects which are:

- expertise needed by an attacker to implement the threat;
- motivation of the attacker;
- cost of the tools needed to implement the threat;
- effort needed by an attacker with specified expertise to implement the threat;
- availability of public available information (e.g. non-deep internet) describing the vulnerability.

The impact is measured on the basis of two aspects which are:

- impact on system functionality;
- impact on human beings interacting with the system.

The next step is the protection. When the threats are identified the companies can focus for the protection to minimize the possibility of occurrence. The users of the e-cars can use access control, where the main assets and associated facilities are limited just to authorized users, processes, or devices, and to authorized activities and transactions. It means that the access permission is managed, so the owner and other persons, who have the right to use the car, can set up for example a code for the access to the ECU, so without the car is unusable. More important questions are the data security and the information protection. The companies have to focus on the protection of the confidentiality, integrity and availability of information. To reach this it is needed to build up proper security policies, processes, and procedures, which

are maintained and used to manage protection of information systems and assets. Protecting cars against cyber threats requires disciplines and collaborations in applying security principles at each level and layer of the system. The protection is a critical layer in the overall cybersecurity defense system of the car, because it represents the border between the vehicle's internal network and the external world.

Symantec, a security software and solution company, specifies four cornerstones for protecting e-cars:

- protecting communications: particularly any modems for in-vehicle infotainment (IVI) or in on-board diagnostics (OBD);
- protecting each module: sensors, actuators, and anything with microcontrollers (MCU), and microprocessors;
- over the air (OTA) management: from the cloud to each car;
- mitigating advanced threats: analytics in the car and in the cloud. [9]

The third step is the detection, when a well-organized and built security continuous monitoring procedures help to monitor the networks, the information systems, the physical environment and personnel activities to detect potential cybersecurity events. It also can alert when a malicious code or unauthorized mobile code is detected to enter to the ECU of the car. To reach these it is needed to monitor continuously for unauthorized personnel, connections, devices and software is performed. The problem is with the e-cars, that antivirus, firewalls (they only have software-controlled firewalls in the gateways) and anomaly detection are not yet implemented in the electric vehicle, largely because of the complexity of updating policies and software regularly and frequently. Units inside vehicles have limited resources, which are often already fully utilized by the vehicle's functions. The detection is usually solved by software, applications or authentications. One of these is the Message Authentication Code (MAC), which works in the following way: each pair of nodes has a shared secret key, which helps the sender to compute a MAC and broadcast the message with it. Then all receivers compute also a MAC with the secret key and compare it with the receiving MAC. The e-cars use HMAC, which is more secured than MAC, because with it the key and the message are hashed in separate steps.

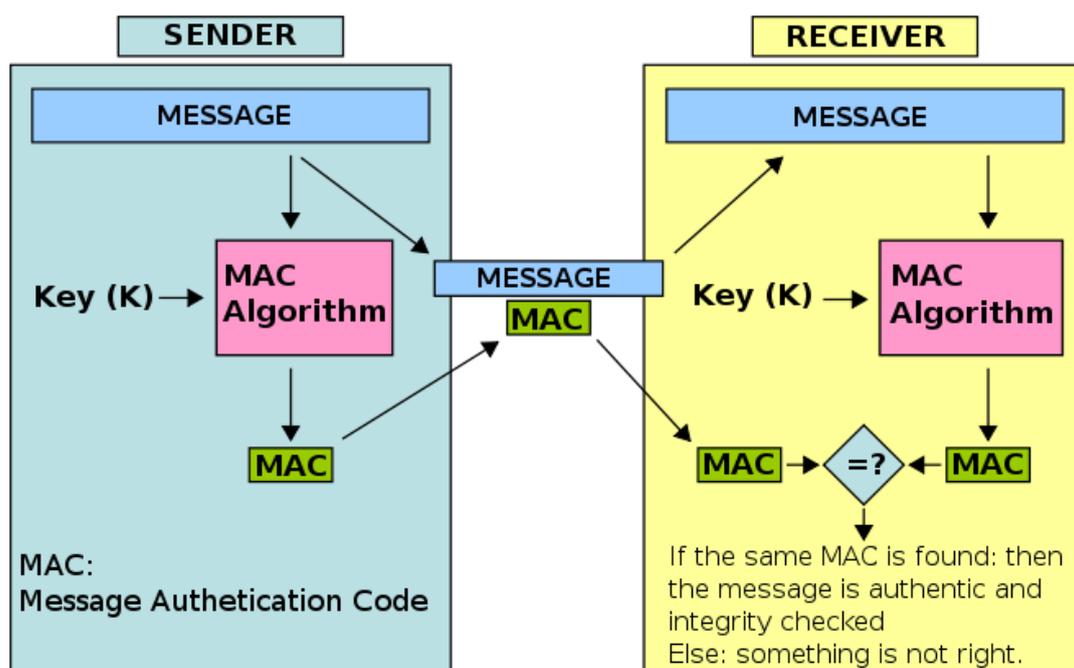


Figure 2. HMAC authentication [10]

As shown on Figure 2, during the HMAC process the sender sends a message with a MAC. When the monitor node receives this message, it can detect whether it has a MAC. If the received message has a MAC, the monitor node immediately starts to calculate the HMAC and validates the MAC on the message. If the same MAC found the authentication is done, the receiver receives the message. If the monitor node detects a MAC error, it will prevent the unauthorized frame by overwriting an error frame. This technique guarantees authentication of on-board communication proven to be resistant to spoofing and Man In The Middle and remote attack techniques, as network reconnaissance and information gathering with unauthorized access to information system/network.

The next step is the response processes and procedures, which are executed and maintained to ensure timely response to the detected cybersecurity events. It is needed to develop increased awareness and capabilities to establish communication protocols among automotive manufacturers, suppliers, cybersecurity researchers, and government agencies could assist industry stakeholders in coordinated efforts to address discovered vulnerabilities and enhance product security. If the detection system of the car is well-organized and setup, the incoming attacks are blocked, and the driver can not realize anything during the trip. The car stores this report with information of the attack, and it is able to share it with other cars in Vehicular Ad-hoc Networks (VANETs), where vehicles communicate with each other through V2V communications. Also, in VANETs, vehicles exchange data with RSUs / Infrastructure through V2I communications. With this solution the cars build up a Vehicular Cloud Computing (VCC) network with DSRC links, where RSUs act as a Gateway for the VANET to access Public Cloud. In this way the cars can share all information according the roads, traffic and executed hacker attacks, so the other cars can be prepared to reject every incoming message from the attacker. [11]

The last step is the recovery. The development of protocols for recovering from cybersecurity incidents is important for ensuring consistent approaches for making available updates to vehicles in a reliable and expeditious manner based on specific circumstances. The procedure can be a self-recovery, when the attack did not cause a huge damage in the car, and the car has an additional storage to store recovery data. For instance, when a man-in-the-middle attacker execute endless data attacks on ECUs, that have only enough space to keep the actual image of data, they can start to compare this data with the stored info. If this attacker sends an ECU random data instead of an actual image, then it is unable to boot to a working image, even though the bootloader can verify that that the random data does not match with the latest downloaded metadata. In order to solve this problem, the ECU will use the additional storage (not it's own storage), where it has enough storage to maintain not only a previous image, but also the latest downloaded image, so it can work without fail. If the damage caused so big issues that the car is not able to continue to work, it can inform the automotive manufacturers, stakeholders, suppliers or mechanics on the established communication links. They can go to the location to fix the problem, or they can try to solve it across the carcloud to update the attacked ECUs to the right version.

## **SECURITY FRAMEWORKS TO SUPPORT E-CAR PROTECTION**

In the last few years several testing were made to analyze the security of electric cars, and to find the weakest point to strengthen the protection mechanism of the entire system against hacker attacks. One of the first and most well-known tests was when hackers killed remotely a Jeep on the highway in the US.

Examining electric cars, we conclude that typical attacks are the same as the attacks against other networks, devices or terminals. Accordingly, the attacks can be:

- data theft: user's personal data, phone numbers, other contacts, bank details;

- man-in-the-middle attack: uploading misleading information into the communications cloud used by cars, thus disrupting traffic;
- DDOS attack: thereby blocking the car's central computer and making it impossible to move;
- stealing location information: thereby tracking the driver's location;
- taking control over the vehicle: causing an accident, causing possibly attack against another vehicle or person;
- penetration: unauthorized access to resources, what can be included under the total control by the intruder, consequently modify the managed data, steal information, install malicious software on the hardware.

The above mentioned test was executed by two security researchers, and they have exposed the security vulnerabilities in automobiles by penetration tests. They have attacked an adjacent chip in the car's head unit, and rewriting the chip's firmware to plant their code. That rewritten firmware were able to send commands through the car's internal network (CAN bus) to its physical components like the engine and wheels. With the attack they could take the control over the vehicle from the radio and the windshield wipers through the accelerator to the engine. After the test the automotive industry has provided software update for the customers to secure vehicles against any potential vulnerability. [12]

It is one of the solutions against the cyberattacks, but it is much better when the industries focus on the defense and security solutions till the cars are still in the factory. There are a lot of different practices, techniques, guidelines and frameworks in this topic from companies, governments and standardization organizations. Usually there are 4 specified security layers that lead to a highly secure vehicle network:

- secure interfaces: which connect the vehicle to the external world;
- secure gateway: which provides domain isolation (separating interfaces, infotainment, safety-critical systems etc.);
- secure network: that provides secure communication between control units (ECUs);
- secure processing units: that implement all the features of the connected car.

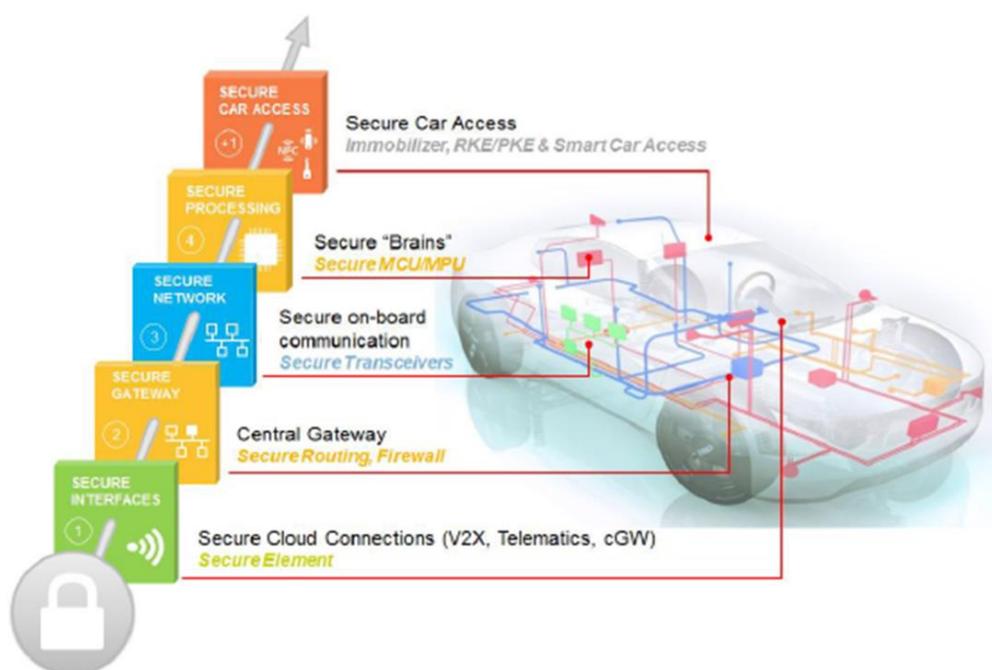


Figure 3. Automotive security framework [13]

There are also some organizations and individuals who informed the automotive industries that vehicle safety issues can be caused by cybersecurity issues, and offer security research community support. One of these was the I Am The Cavalry, which gave five recommendations for the industries in the Five Star Automotive Cyber Safety Framework. These recommendations are:

- Safety by Design – anticipate failure and plan mitigation;
  - o does the industry have a published attestation of its secure software development lifecycle, summarizing the industry’s design, development, and adversarial resilience testing programs for the industry’s products and supply chain?
- Third-Party Collaboration – engage willing allies;
  - o does the industry have a published coordinated disclosure policy inviting the assistance of third-party researchers acting in good faith?
- Evidence Capture – observe and learn from failure;
  - o do the industry’s vehicle systems provide tamper evident, forensically sound logging and evidence capture to facilitate safety investigations?
- Security Updates – respond quickly to issues discovered;
  - o can the industry’s vehicles be securely updated in a prompt and agile manner?
- Segmentation & Isolation – prevent cascading failure;
  - o does the industry have a published attestation of the physical and logical isolation measures the industry has implemented to separate critical systems from non-critical systems? [14]

Examining the above issues and frameworks, and added the NIST Cybersecurity Framework, the industries can provide a well-secured network and information system to their vehicles. With a well-developed secure software development lifecycle and management, the entire system can be protected against external attacks.

## **CONCLUSION**

The information of the e-cars and their owners are always shared among elements of the connected vehicle systems, and unfortunately it is vital, that as a user we always know who we’re talking to and can be sure, that any information send or received is legitimate. The vehicle, as a member of the Internet of Things (IoT), needs to be able to authenticate itself in order to achieve accountability and so does everything in its environment. This is the only way updates, protection of intellectual property, driver identification, etc. can be carried out securely. Every vehicle owner wants to be sure, that only the online updates that he or she has tested and provided are accepted by the vehicle, and that only eligible vehicles receive updates or upgrades.

To reach this security goal the automotive industries can use the NIST Cybersecurity Framework core component functions to be sure that the information security is considered throughout the complete lifecycle of the vehicles, from the earliest stages right through to decommissioning. So they can be sure, that they protect all the necessary processes and assets, the mandatory safeguards are available, and they have all the compulsory techniques to identify incidents, contain impacts of incidents and restore capabilities.

## BIBLIOGRAPHY

- [1] HAIG ZS., KOVÁCS L.: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*, tanulmány, TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ), Nemzeti Közszolgálati Egyetem, (2012) p. 183.
- [2] LIGHTMAN, S: *The Future of the Cybersecurity Framework for Critical Infrastructure and How It May Affect the Automotive Industry*, [https://www.escar.info/images/Datastore/2016\\_escar\\_usa/PAPER\\_2016/Lightman\\_Suzanne\\_NIST\\_PAPER.pdf](https://www.escar.info/images/Datastore/2016_escar_usa/PAPER_2016/Lightman_Suzanne_NIST_PAPER.pdf) (letöltve: 2017.07.17.)
- [3] National Highway Traffic Safety Administration: *Cybersecurity best practices for modern vehicles*, (Report No. DOT HS 812 333), Washington, DC: Author (2016)
- [4] The Institution of Engineering and Technology: *Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles*, <http://www.theiet.org/sectors/transport/documents/automotive-cs.cfm> (letöltve: 2017.07.17.)
- [5] National Highway Traffic Safety Administration: *NHTSA and vehicle cybersecurity*, <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf> (letöltve: 2017.07.18.)
- [6] McCarthy, C., & Harnett, K. *National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles*. (Report No. DOT HS 812), Washington, DC: National Highway Traffic Safety Administration, (2014)
- [7] National Institute of Standards and Technology: *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (2014) p.7.
- [8] Night Lion Security: *A Baseline IT Risk Management Framework*, <https://www.nightlionsecurity.com/blog/grc/2016/cyber-security-framework-csf-security-controls-download-xls-csv/> (letöltve: 2017.07.18.)
- [9] FACHOT, M: *Protecting road vehicles from cyber attacks*, <http://ieccetech.org/issue/2017-03/Protecting-road-vehicles-from-cyber-attacks> (letöltve: 2017.07.19.)
- [10] Stack Overflow: *Clarification on HMAC authentication with WCF*, <https://stackoverflow.com/questions/9922085/clarification-on-hmac-authentication-with-wcf> (letöltve: 2017. 07. 19.)
- [11] MARVY B. M., CHERIF S., HODA K. M., SHERIF A. H.: *CARCLOUD: A Secure Architecture for Vehicular Cloud Computing*, [https://www.escar.info/images/Datastore/2016\\_escar\\_EU/PAPER\\_2016/Mary\\_Badr\\_Mounir\\_Mansour\\_CARCLOUD\\_A\\_Secure\\_Architecture\\_for\\_Vehicular\\_Cloud\\_Computing\\_PAPER.pdf](https://www.escar.info/images/Datastore/2016_escar_EU/PAPER_2016/Mary_Badr_Mounir_Mansour_CARCLOUD_A_Secure_Architecture_for_Vehicular_Cloud_Computing_PAPER.pdf) (letöltve: 2017.07.21.)
- [12] GREENBERG, A: *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (letöltve: 2017.08.30.)
- [13] I Am The Cavalry: *Five Star Automotive Cyber Safety Framework*, <https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf> (letöltve: 2017. 09. 05.)