AUTOMOTIVE CYBER SECURITY AND MODERN SAFETY VEHICLE SYSTEM

Milan Marcinek

PhD. Lecturer Academy of the Police Force in Bratislava, Slovakia

Abstract

Author discusses the new theme of automotive cyber security in his article. Present trend of the automobile industry is to produce more modern, faster and safer vehicles. In the near future, our cars will be equipped with an electronic security system that automatically calls the emergency service operator in case of a traffic accident. These new eSafety system combine mechanical, micro electric, communication and information technology in order to ensure car safety. When you are unconscious, the system informs the rescuers where the accident happened. They arrive at the scene of the accident within a few minutes.

These intelligent vehicles take us toward a transport model that is safer and more efficient applying an interconnected driving experience. Nevertheless, there is concern that this could expose connected cars with their passengers to potential risks from online threats. Undertaken research identifies possible automotive cyber security vulnerability. It also highlights how automotive security seems to be responding to the claims that cars can really be hacked. The development for scientific themes around automotive cyber security and issues around liabilities related to automotive cyber security incidents are raising as well as possible negative influences or vehicle data misuse. Unfortunately, online identity theft and the act of capturing personal information by the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services.

Finally, the introduction of these systems into everyday life has led to the development of the modern concept of the information society. However, the growth of information society is accompanied by new and serious threats. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Online fraud and hacking attacks are just some examples of crimes that are committed on a large scale every day.

Keywords *vehicle, cybercrime, security, eCall system, car hacking, cyber security, protection*

INTRODUCTION

There are new threats for automobile industry. Car hacking has become a serious problem. An increasing number of cars are at risk from computer hackers because of the advanced Internet systems they offer. We may assume that the problem could be life-threatening. [1]

The number of electronic central units in modern cars ranges from 20 to 100. This means 100 different points of access for potential car hackers. The units do not only control services but also the operation of the engine, transmission and safety features such as stability control and anti-lock brakes. If someone hacks this system, they then have access to whole car's central unit. Currently, there are also firms working on developning a software barrier that will not prevent hackers from accessing in-car connectivity features but will stop them from being able to attack the vital electronic central units. We may lose navigation or audio, but not the car's operating and safety systems.

Since 1995 EU legislation demands that all new cars come standard with an electronic immobiliser. This device only allows the vehicle to start when it is provided the right credentials.

[1] MARCINEK, M. - DWORZECKI, J. *Technical Aspects of use of Selected Specialist Equipment Intended for Road-Side Rescuing*, p. 20.

However, thieves can wirelessly steal all of the information from a car key in seconds. They are then able to fool the car into thinking the key is present, and drive away as if they had the key.

A new car hacking study by Roel Verdult, Flavio Garcia and Baris Ege showed that thieves can disable immobilisers and drive off without a key in models from Volvo, VW, Audi and Fiat. It has found that electronic immobilisers used by 26 car manufacturers are vulnerable to hacking, putting many motorists at risk.

New electronic systems create superior safety through active technology and contribute to safety on roads by preventing vehicle collisions and consequently helping to reduce injuries and deaths on the roads. However, it goes about the computer systems which equipped the cars therefore the term of cybercrime significantly touches the theme of automotive innovation and forthcoming threats.[2]

CYBERCRIME DEFINITION

The term cybercrime defines a range of offences including traditional computer crimes as well as network crimes. These crimes differ in many ways as well as there is no single criterion that could include all acts mentioned in the different legal approaches. Cybercrime is a narrower term than computer-related crime. The term computer-related crime involves a computer network. Moreover, it covers not only offences with any relation to a network but also single computer systems. It is activity in which computers or networks are a tool, a target or a place of criminal activity. When discussing broader sense of cybercrime, there are several difficulties to define it. It would cover traditional crimes such as murder if a keyboard was used to hit and kill the victim.[3] However, there descriptions which exclude the used physical hardware but there is sometimes risk that excluding crimes that are considered as cybercrime in international agreements such as the Council of Europe Convention on Cybercrime.[4]

As a good example may be consider if a person who produces devices such as USB which contains malicious software that destroys data on computers when the device is connected. However, since the act of deleting data has not been committed through global electronic networks, it would not be qualified as cybercrime under the narrow definition above. Such acts would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference.

Cybercrime and cybersecurity are then issues that can hardly be separated in an interconnected environment. The fact that the 2010 United Nations General Assembly resolution on cybersecurity addresses cybercrime as one major challenge underlines this.

Cybersecurity plays an important role in the ongoing development of information technology. Enhancing cybersecurity and protecting critical information infrastructures are essential to each national security. Making the Internet safer the users are protected. It has become crucial to the development of new services in government policy. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy.

In particular, this includes the adoption of appropriate legislation against the misuse of the intelligent transport system for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.

Cybersecurity strategies help to reduce the risk of cybercrime. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by the issue of cybersecurity are global and farreaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. The World Summit on the Information Society recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime.

The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas:

[2] MARCINEK, M. - DWORZECKI, J. General Vehicle Safety Systems overview. p. 11-21.
[3] Another broader definition is provided in the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism which points out that cybercrime refers to acts in respect to cybersystems.
[4] ETS 185 – Convention on Cybercrime.

- Legal measures - focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.
- Technical and procedural measures - focuses on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards.
- Organizational structures - focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems.
- Capacity building - focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda.
- International cooperation - focuses on international cooperation, dialogue and coordination in dealing with cyberthreats.[5]

As it seems, a comprehensive approach against cybercrime is needed. Considering only the technical measures, any crimes cannot be prevented. International cooperation, such as international dialogues, cooperation and coordination in dealing with possible future cyberthreats, in this area is also crucial. Sufficient legislation and legal framework is an essential part of each cybersecurity strategy. This requires substantive criminal law provisions to criminalize activities related to computer fraud, illegal access or data interference. Moreover, the cybercrime tools for investigation are needed. The perpetrators can act from different part of the world and even their real identity may be masked. Therefore the tools and instruments needed for cybercrime investigation can be quite different from the other tools.[6]

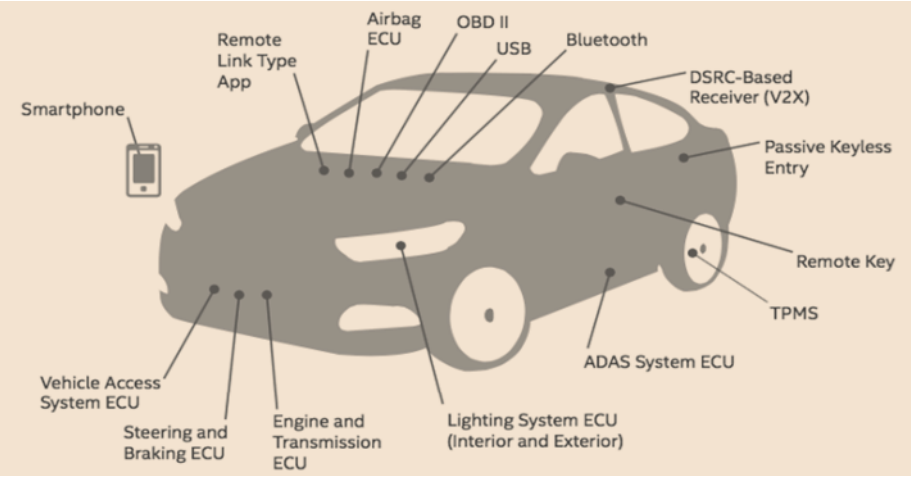

Figure 1 The most hackable parts on a next generation vehicles.
Source: Own source

DIMENSIONS OF CYBERCRIME

Cybercrime often has an international dimension. The illegal content often passes through a number of countries during the transfer from a consignor to a consignee. A number of countries base their mutual legal assistance regime on the principle of dual criminality.[7] Investigations on a global level are generally limited to those crimes that are criminalized in all participating countries. The criminalization of illegal content differs in various countries. Material that can lawfully be distributed in one country can easily be illegal in another country. Apart from language issues and power adapters, there is a very little difference between the computer systems and cell phones sold in Asia and those which are sold in Europe. Due to standardization, the network protocols used in countries on the African continent are the

[5] Source:
<www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html> [online 02.05.2017]
[6] For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website.
[7] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

same as those used for example in the United States. This standardization enables users around the world to access the same services over the Internet. The question is what effect the harmonization of global technical standards has on the development of the national criminal law. Although the Internet may not recognize border controls, there are means to restrict access to certain information. The access provider can generally block certain websites and the service provider that stores a website can prevent access to information for those users on the basis of IP-addresses linked to a certain country.

SYSTEM eCALL

Among the other intelligent transport systems in road transport, the system eCall consists of information and communication technology located either in a vehicle or transport infrastructure. It serves to optimize and manage road transport, increase road safety and continuity, improve the management and maintenance of roads, improve public transport services and reduce the negative impact on the enivornment.

It provides transmission, collecting, processing and exchange of information among service providers, traffic information providers and transport infrastructure users. [8]

According to the European Commission, the system will greatly diminish emergency service response times in 50%. That means that this faster response time will reduce the severity of injuries and save lives. It will automatically contact emergency responders in the event of a serious road accident, send GPS coordinates to local emergency services, and wirelessly send airbag-deployment and impact-sensor information.

System eCall is a European initiative intended to bring rapid assistance to motorists involved in a collision anywhere in the European Union. The system eCall will be mandatory in all new cars sold within EU after April 2018.

The concept of eCall was presented in 1999 by European civil servant Luc Tytgat, at the launching of the Galileo project, by the European Commission. The year before, 170 experts met in Brussels, invited by the Commission, to analyse the European dependence on the American GPS system but also to gather civilian applications propositions.[9]

In 2001, the project was first presented as a European calling system, in the context of the German youth science competition Jugend forscht to keep delayed for the next several years. The project started again by the European Commission in 2011. Nonetheless, the development of eCall is at its beginning comparing to countries where similar concepts have existed for years.[10]

Historically, the first European country to monitor and control its traffic was Germany. It was with its Autofahrer Leit und Informationsystem (ALI) project, which it launched in the 1970s. The system enabled authorities to obtain data about the vehicles on the roads and even communicate with them. At the moment there are several national intelligent transport systems around Europe. The Eropean Union considers them fragmented and uncoordinated with minimal possibility to provide correct geographical continuity throughout the European Union at its external borders." [11]

Therefore, EU aims to accelerate the deployment of more innovative transport technologies and coordinate their implementation in the European states. The member states had the freedom to choose which systems they wanted to invest in. Before the directive the EC also passed an Action Plan, which suggested a number of targeted measures, including the proposal for passing the directive of implementation of ITS. The directive stipulates that the EC has to adopt the specifications of the functional, technical, and organisational or services provisions of ITSs by 2017 to address the compatibility, interoperability and continuity of ITS solutions across the EU. To the first priorities belong traffic and travel information, the eCall emergency system and intelligent truck parking. The national traffic information centres should cooperate and exchange information about road accidents or alternate routes with one another, according to the agreement passed at the meeting of EU transport ministers held in Cyprus in July 2012.

As it seems, these plans aim to mandatory introduction of eCall across the EU. In generally, all new models of passenger cars and light commercial vehicles will be equipped with eCall system as

[8] MARCINEK. M. *Simulation of crisis situations of the national and international crisis management as a support for crisis managers' education*. p. 33-35.
[9] MARCINEK, M. *Linka tiesňového volania eCall v podmienkach Slovenskej republiky /The emergency line eCall in the Slovak Republic*. p. 161-165.
[10] The first nation to implement a system similar to eCall was Japan. Its Comprehensive Automobile Traffic Control System (CACS) was implemented around 1970. It was designed to control the traffic in Tokyo.
[11] Directive 2010/40/EU passed by the European bodies in July 2010.

well as the necessary infrastructure in order to properly receive and process eCall. Data obtained through eCall enable rescue services to provide assistance to drivers and passengers faster.

The European Commission introduced eCall, a groundbreaking initiative intended to bring rapid and automatic assistance to motorists involved in incidents anywhere in the European Union. Industry coalitions such as ERTICO, Europe's Intelligent Transportation System organization, European Member States and ITS industry leaders around the globe are working hard to develop and deploy new technologies and strategies to meet the eCall challenge.

To meet the challenge of developing a Pan-European eCall program, ERTICO and its member organizations supported the EU funded the Harmonized European eCall Pilot programms, also known as HeERO. The HeERO1, HeERO 2 and iHeERO programms began in 2011 and will continue, features interoperable eCall programs in all participating EU regions, which are synchronized across country and network borders. Due to HeERO eCall has been sucessfully pre-deployed in several regions according European Norms using 112 as the pan-European PSAP emergency call number. The 112 based emergency call relies on an automatically established two-way emergency call to a Public Safety Answering Point (PSAP) call center immediately following an incident or after manual activation. The Cinterion Machine-to-Machine (M2M) module solution reliably sends the collected MSD to a PSAP via cellular networks. In addition, the module establishes an automatic handsfree voice call so PSAP staff can gather additional information from the involved passengers. The call helps determine what emergency services are needed so early responders arrive at the scene of an incident fully informed and prepared to help as needed.[12]

ECall works on an upgraded European wide interoperable PSAP infrastructure, and installed or embedded M2M communication devices in all vehicles. In the event of a serious road incident, the In-Vehicle Equipment (IVE) must be able to automatically dial 112 and reliably communicate incident details over wireless networks.

These details are collectively defined as the minimum set of data (MSD) and include:

- time of the incident,
- cause of activation,
- GPS coordinates, and
- VIN.[13]

The eCall can also be activated manually. The mobile network operator (MNO) identifies that the 112 call is an eCall from the "eCall flag" inserted by the vehicle's communication module. The MNO handles the eCall like any other 112 call and routes the call to the most appropriate emergency response centre - Public Safety Answering Point (PSAP). The PSAP operator will receive both the voice call and the MSD. The information provided by the MSD will be decoded and displayed in the PSAP operator screen. At the same time, the operator will be able to hear what is happening in the vehicle and talk with the occupants of the vehicle if possible. This will help the operator ascertain which emergency services are needed at the accident scene (ambulance, fire, police) and to rapidly dispatch the alert and all relevant information to the right service. The European standards do not specify whether eCall is provided by using an embedded network access device (GSM module) or using nomadic or portable equipment, f. i. mobile phone.[14]

[12] The European Commission estimates that eCall is expected to reduce emergency response times by 50% in rural areas and 40% in urban areas.
[13] MARCINEK, M. *Euro-NCAP a simulácie nárazov automobilov - crashtesty*. p. 210-214.
[14] MARCINEK, M. *Linka tiesňového volania eCall v podmienkach Slovenskej republiky /The emergency line eCall in the Slovak Republic*. p. 161-165.

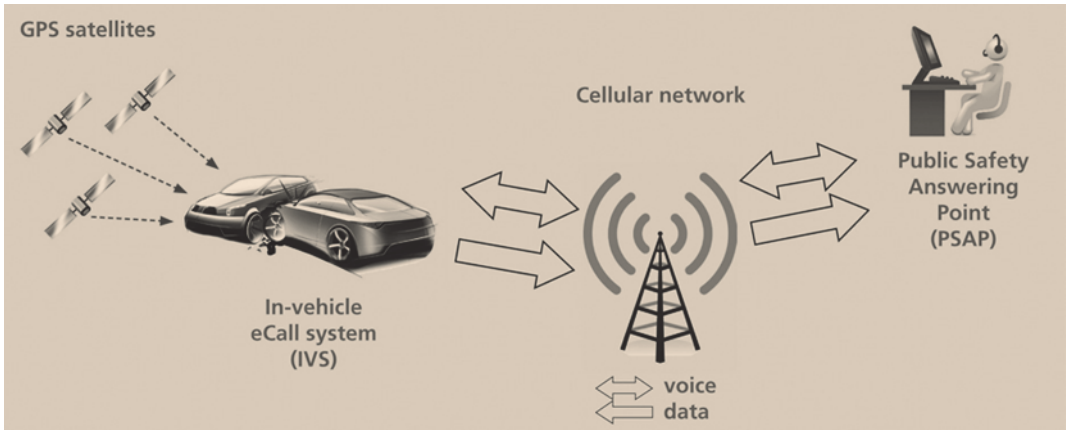

Figure 2 The eCall System operation.
Source: Own source

However, in the pan European eCall operating requirements it is defined that:

- the solution is robust and will normally survive a crash;
- the quality of service of the in-vehicle equipment, including communications equipment, is reliable.[15]

PRIVACY AND DATA PROTECTION OF IN-VEHICLE SYSTEMS

On 26 November 2012 the European Commission produced a draft Regulation regarding the *"harmonised provision for an interoperable EU-wide eCall"* to take place by 1 October 2015.[16] In some European countries appeared discussion regarding the impact eCall on privacy and data protection. Moreover, other discussions deal with mandatory installation of Event Data Recorders (EDR) which would be a move that goes against principles of liberty and freedom of choice in Great Britain.

The term of a black box is known to people especially from the aircrafts as a flight data place. In the car the term may be similar to the term with a camera. Nonethless, there really is the black car box that record your every move. It contains important information about the course of the flight, when we use the flight accident as an example, which can reveal what has happened. When dealing with cars and black boxes, we use the term of. Truthfully, EDR has been in the car for a longer time.

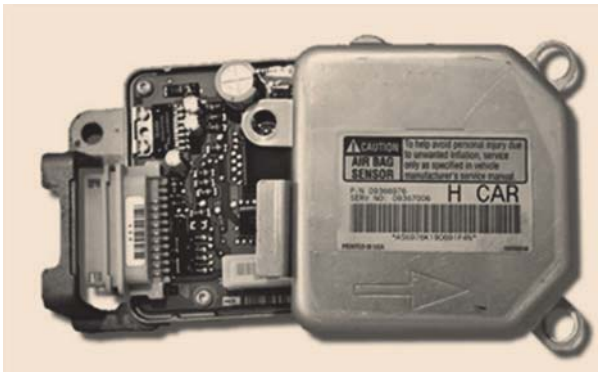

Figure 3 Event data recorder.
Source: Own source

EDR served mainly as a source of information for airbags in order to activate them. Consequently, the unit improved and began to collect a lot of other information. Nowadays, we can learn not only vehicle´s speed and location but also the pedal position or the position of a steering wheel.

[15] The most reliable solution is a fully embedded system with an embedded GSM module, embedded SIM, and the ability to manage devices over the air.
[16] European Union, *Draft Regulation no 305/2013*.
Source:
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0305&from=EN>
[online 02.05.2017]

Moreover, in the United States there is mandatory deployment of EDR units for cars. There is similar situation with either EDR or eCall system in Europe. However, some manufacturers have already put EDR into their cars even in Europe. Certainly, most companies do not discuss this integrated mystery. The problem with EDR is also how to access the data. That does not only mean special software and hardware but also real knowledge of the issue.[17]

EDR is probably installed in the most modern cars. The data are collected only for automakers to help them improve the vehicles. It is essential to also explain an important distinction to be made between eCall and the EDRs. Whilst the eCall system may not record the location of the car constantly, the EDR does have that capability. There are concerns that the EDRs ability to gather extensive data can and will be misused as:

- the data could be accessed by hackers to track individuals' location.
- insurance companies can use this to promote personalised insurance quotes by recording how individuals drive.
- police forces have already been using eCall systems to track suspicious motorists.

The European Commission has stated that the purpose of eCall is to help mitigate the consequences of serious road accidents across the EU.[18] Both systems are, however, similar to each other. Therefore the data misuse may happen similary to eCall system.

Naturally, there is an important distinction to be made between eCall and EDR. The eCall system is designed to send in-vehicle emergency calls using the EU-emergency telephone number 112. Whereas an EDR is firstly fitted in vehicles. The eCall system may be instal on it only then. EDR can also not be switched off once they have been installed in the vehicle. It is important to note that technology similar to eCall can already be purchased by individuals if they wish to voluntarily install it in their vehicle.[19]

The European Commission has stated that the MSD includes the exact location of the crash, time and vehicle description. According to a report by the EuropeanTelecommunications Standards Institute, the MSD also includes driving direction resulting from accurate satellite-based data. This data is necessary in order to enable the emergency services to assess the seriousness of the accident. Additionally, the report states that the EDR will record for 20 seconds before the accident and 10 seconds after. The European Commission has not made any remarks regarding what recording will take place before and after an event. The opinions say that it is unclear whether or not this data will be included in the MSD as standard. If the MSD does include data before and after the incident this means that the EDR is not latent. In order to obtain data prior to the incident the EDR must be recording and erasing continuously. As the EDR has the ability to record the vehicle's exact location, if it was hacked detailed information about the driver's location and journey details would be then available.[20]

SUMMARY

Safety has become a top interest for both new-car manufacturers and customers. Car manufacturers have been developing technology to help prevent accidents or significantly reduce the risk of injury and death in the event that you are involved in a collision. It is important that your vehicle can provide you with maximum protection in an accident. How safe a car is can be determined by a number of factors. Following the measures foreseen in the Transport White Paper

[17] In some US states, EDR data may be used to investigate an accident in a court, some of which may be used without the consent of the owner of the vehicle. In Europe, however, such a possibility does not yet exist, even though this theme is becoming more frequent.

[18] The European Commission, *eCall: automated emergency call for road accidents mandatory in cars from 2015.* Source: http://ec.europa.eu/commission_2010-2014/kallas/headlines/news/2013/06/ecall_en.htm [online 04.05.2017]

[19] The Daily Mail, EU to bug every car in UK with tracker chips – and Ministers admit they are powerless to stop the Big Brother technology.
Source:
<http://www.dailymail.co.uk/news/article-2625244/EU-bug-car-UK-tracker-chips-Ministers-admit-powerless-stop-Big-Brother-technology.html>
[online 04.05.2017]

[20] It is stated that this type of data has already been used by the police to track motorists according to the article in The Sunday Times which states that some of INTERPOL members are using the eCall system for surveillance operations.

2001, situation of road safety has improved. Road fatalities have declined by more than 19% since 2013 in the EU.

However, with thousands of deaths and millions injured, roads remain the least safe mode of transport. New vehicle technology offers potential benefits but the driver is a critical factor, especially among teens and older drivers. Vehicle safety features have become a part of almost any car models. Car manufacturers integrated different safety system units in order to provide occupant protection. There are also systems to theft protection. One single unit is installed with some improvisations in order to make impossible for the thieves to disable these systems.

Furthermore, new visions plan new technologies that would reduce the deaths and injuries caused by road accidents. One of the goals is to integrate advanced technology into cars to prevent driving accidents caused by alcohol. Sensors in the car's seats and gearshift will detect alcohol through the driver's perspiration and prevent the vehicle from being driven. Additionally, a camera will watch the driver's eyes. If it detects signs of drowsiness or drunkenness, the car will issue a voice alert to the driver and tightens the seat belt as a wake-up call. While this futuristic concept car may not be hitting the highways just yet, it is interesting to wait what future brings in car security systems in order to prevent outside threat on the roads.

Connected vehicles take us toward a mode of transport that is safer and more efficient, by enabling an interconnected driving experience. One way cars are interconnecting is via the Internet, but there is concern that this could expose connected cars and the people in them to potential risks from online threats. Research undertaken to identify possible automotive cyber security vulnerabilities

are highlighted, how automotive security seems to be responding to the claims that cars can be 'hacked. We need to adapt complex activities to prevent cyber crime. Good computer security, implementation of effective policies, standards and practices, as well as correct security architectures and countermeasures, and a good level of security awareness.

Finally, no connected computer system is 100% guaranteed secure in terms of invulnerability or the integrity of the data it holds. One reason why computer systems cannot really be totally secure is because of the demands of maintaining security. Some of the risk can be balanced by allocating security resources to where it is needed most at any given period. Identifying the motivating factors behind cyber-attacks can prove an effective stratagem in countering cyber-crime and other targeted malevolent Internet-based attacks. For the automotive sector such motives might include, f. i. access to online automotive apps and services that contain banking records, general personal identification data as social media users names and passwords, insurance and tax data useful for identity theft or international travel permits etc. These motives may also include, f. i. industrial espionage and illegal access to intellectual property, sabotage or degrading of vehicle and connected system performance, terrorism with disabling vehicles as part of an attack or vehicle identification re-assignment in case of stolen cars.

A series of events should be proposed to identify these common challenges and threats in modern automotive industry and cybersecurity's issues across all modes of transport. These events should provide an environment for encouraging collaboration and research within industry in order to provide safety, security and innovation of the 21st century.

REFERENCES

[1] MARCINEK, M. - DWORZECKI, J. Technical Aspects of use of Selected Specialist Equipment Intended for Road-Side Rescuing, 1. edition. - New York: Iglobal Writer Inc., Pro Pomerania Foundation Poland, 2015. - 175 s. - ISBN 978-83-63680-77-0.

[2] MARCINEK. M. Simulation of crisis situations of the national and international crisis management as a support for crisis managers' education. In: Nehody s hromadným postihnutím osôb, 2011 Žilina, International Congress, ISBN 978-80-969219-8-0

[3] MARCINEK, M. Organizacja, funkcjonowanie i perspektiwy rozwoju zintegrowanego systemu ratownictwa na terenie Republiki Slowackiej / aut. Milan Marcinek, rec. Jan Klimek, rec. Antoni Olak, rec. Žanna Poplawska. In: Konkurency jność podmiotów gospodarczych i jej determinanty : Katowice : Wyzsza szkola zarzadzania marketingowego i jezyków obcych w Katowicach, 2013. - ISBN 978-83-87296-64-3. - S. 551-558

[4] MARCINEK, M. - DWORZECKI, J. General Vehicle Safety Systems overview: chapter I. In: Safety Engineering: Selected Aspects - New York: IGLOBAL WRITER Inc., PRO POMERANIA FOUNDATION POLAND, 2014. - ISBN 978-83-63680-13-8. p. 11-21.

[5] MARCINEK, M. Linka tiesňového volania eCall v podmienkach Slovenskej republiky/The emergency line eCall in the Slovak Republic. In: Bezpečnostné fórum 2015. I. zväzok : zborník vedeckých prác. - Banská Bystrica : Belianum. Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, 2015. - ISBN 978-80-557-0849-2. - S. 161-165.

[6] MARCINEK, M. MARKOVÁ, I. Working Effectiveness of Hydraulic Rescue Equipments for Firefighters In: Advanced Materials Research. - ISSN 1022-6680. - Vol. 1001 (2014), pp. 517-525. Plný text: <Spôsob prístupu: http://www.scopus.com/record/=Working+effectiveness+of+hydraulic+rescue+equipments+for+firefighters&sid=5AE8CD94DF72E1297BF6E9BA302CACDA.kg

[7] MARCINEK, M. Inovácia materiálno-technického zabezpečenia dobrovoľných hasičských zborov v rámci Integrovaného záchranného systému Slovenskej republiky = Material and Technical Facilities Innovation of Volunteer Fire Brigades in the Integrated Rescue System of the Slovak Republic In: Košická bezpečnostná revue [elektronický zdroj] : polročník VŠBM v Košiciach. - ISSN 1338-6956. - Roč. 6, č. 2 (2016), online, s. 238-243

[8] MARCINEK, M. Analýza zodpovednosti pri preprave nebezpečných látok cestnou nákladnou dopravou podľa Dohody ADR a Dohovoru CMR = Responsibility Analysis in the Transport of Dangerous Substances by Road under the ADR Agreement and CMR Convention In: Ochrana obyvatelstva - Nebezpečné látky 2017 [elektronický zdroj] : sborník přednášek XVI. ročníku mezinárodní konference : [1. - 2. únor 2017, Ostrava]. - ISSN 1803-7372. - č. 1 (2017), CD-ROM, s. 90-97.

[9] MARCINEK, M The Current Situation in Vehicle Safety System In: "Dani Arčibalda Rajsa" = "Archibald Reiss Days" : tematski zbornik radova medunarodnog značaja = Thematic Conference Proceedings of International Significance : Tom II = Volume II : Beograd, 10 - 11. mart 2016 = Belgrade, 10 - 11 March 2016. - Beograd = Belgrade : Kriminalističko-policijska akademija = Academy of Criminalistic and Police Studies, 2016. - ISBN 978-86-7020-357-0. - pp. 462-472.

[10] MARCINEK, M Štatistická analýza zásahovej činnosti jednotiek HaZZ s výskytom nebezpečných látok = Statistical Analysis of Fire and Rescue Corpus Intervention Involving Dangerous Substances In: Ochrana obyvatelstva - nebezpečné látky 2015 [elektronický zdroj] : sborník přednášek XIV. ročníku mezinárodní konference : VŠB - TU Ostrava : 4. - 5. únor 2015 . - Ostrava : Sdružení požárního a bezpečnostního inženýrství, 2015. - ISBN 978-80-7385-158-3. - CD-ROM, S. 86-90.

Electronic sources

http://eur-lex.europa.eu
http://ec.europa.eu/commission.htm
www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html

Acts

- ETS 185 – Convention on Cybercrime
- The EU legislation in the Directive 2012/36/EU