VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 2 pp. 218–236

Smart Cars and Information Security

Gašper Školc, Blaž Markelj

Purpose:

'Smart cars' use a great variety of data in order to operate. They obtain this from the surrounding area using sensor technology and other available resources. The drivers and passengers of such vehicles transfer different data by connecting their mobile devices with smart-vehicle systems (and by using various apps). The purpose of this paper is to investigate the problem of user data security in smart cars and to provide an insight into the general knowledge regarding such issues held by those who drive smart cars (both private and commercial users).

Methods:

The results are based on descriptive findings arising from a literature review and a research study conducted among the Slovenian population via the "1ka.si" online portal.

Findings:

The research conducted and presented in this paper shows that the use of mobile devices and their applications, which are connected to a smart car, constitute one of the biggest risks to information security in smart cars. Drivers are aware of such risks, but consider them to be a secondary concern. In addition, the lack of a uniform definition of smart cars points to a new under researched area concerning the information security of smart devices (such as cars, mobile devices etc.). Such issues pose a problem for smart car manufacturers and application developers as well as the users of mobile devices.

Research Limitations:

The main limitation of the research study is that the target population does not possess much knowledge about the discussed topic and related issues.

Practical Implications:

The research study's findings provide an insight into data security issues (which also serve as practical implications) concerning the use of smart cars.

Originality/Value:

The findings of the paper may prove useful for both the users and owners of smart vehicles in general as well as the manufacturers of mobile devices since the relevant data flows take place at the level of smart devices. The key challenge involves the owner of a single device and the level of information security knowledge they possess.

UDC: 004.056:629.331

Keywords: smart cars, information security, data security, personal data, mobile devices, connectivity

Pametni avtomobili in informacijska varnost

Namen prispevka:

Pametni avtomobili danes za svoje delovanje uporabljajo raznovrstne podatke, ki jih pridobivajo iz okolice s pomočjo senzorske tehnologije in ostalih dostopnih virov. Uporabniki pametnih avtomobilov tako prenašajo raznovrstne podatke, ko svoje mobilne naprave povezujejo s sistemi pametnih avtomobilov (tudi z uporabo različnih aplikacij). Namen prispevka je prikazati varnost uporabnikovih podatkov pri rabi pametnih avtomobilov in izpostaviti poznavanje tovrstne problematike med uporabniki pametnih avtomobilov (tako zasebnih kot poslovnih).

Metode:

Ugotovitve, predstavljene v članku, izhajajo iz deskriptivnih dognanj in raziskave, ki je bila izvedena s pomočjo spletnega vprašalnika, objavljenega na spletnem portalu »1ka.si«.

Ugotovitve:

Raziskava, izvedena v tem članku, nam je pokazala, da eno največjih tveganj informacijski varnosti pri rabi pametnih avtomobilov predstavlja uporaba mobilnih naprav in aplikacij, ki se povezujejo s pametnimi avtomobili. Vozniki tovrstna tveganja sicer poznajo, vendar so za njih sekundarnega pomena, kar tudi nakazuje, poleg neenotne definicije pametnih avtomobilov, na novo neraziskano področje informacijske varnosti pametnih naprav (avtomobili, mobilne naprave itn.). S tovrstno problematiko se srečujejo tako proizvajalci pametnih avtomobilov in mobilnih aplikacij kot tudi uporabniki pametnih naprav.

Omejitve/uporabnost raziskave:

Omejitev raziskave predstavlja predvsem pomanjkljivo znanje prebivalstva o obravnavani tematiki in njeni problematiki.

Praktična uporabnost:

Ugotovitve raziskave omogočajo vpogled v problematiko varovanja podatkov (ki prav tako služi kot praktična uporabnost) pri uporabi pametnih avtomobilov.

Izvirnost/pomembnost prispevka:

Ugotovitve prispevka so uporabne tako za vse uporabnike in lastnike pametnih avtomobilov kot tudi za proizvajalce pametnih naprav. Pretakanje podatkov namreč poteka na nivoju pametnih naprav, razlika je le, kdo je lastnik posamezne naprave in s kakšno stopnjo informacijskovarnostnega znanja posamezno napravo upravlja.

UDK: 004.056:629.331

Ključne besede: pametni avtomobili, informacijska varnost, varovanje podatkov, osebni podatki, mobilne naprave, povezljivost

1 INTRODUCTION

The impact of technological development on individuals and societies can be seen in the ways in which they transform the methods they use in their work-related activities and, thus, their lives. Nowadays, people are constantly exposed to the unstoppable development of technology in numerous fields. In the past few years, tremendous progress has been recorded as the Internet of Things (IoT) has also started to encompass vehicles. Pacheco, Satam, Hariri, Grijalva and Berkenbrock (2016) state that, apart from mobile devices and computers, the IoT has also facilitated 'smart' cities, smart homes and other smart cars. It is precisely the way these technologies are incorporated that has led to various discussions about the relatively new phenomenon of 'smart cars'. Many scientific papers attempt to definite a smart car, but none of these definitions has been universally accepted (European Union Agency for Network and Information Security [ENISA], 2016). Further, such cars also incorporate the IoT which enables their users (drivers and passengers alike) to make advanced use of the car in order to improve the user experience and increase the car's safety (ENISA, 2016). The definition used in this paper combines several different definitions (Barret, 2012; Bernik & Markelj, 2014; Chui, Löffler, & Roberts, 2010; Eskandarian, 2012; ENISA, 2016), namely: *Smart cars are vehicles which form part of the Internet of Things, function on the basis of an adapted operating system, similarly to mobile devices, and provide access to the Internet and other mobile devices without a physical connection (wirelessly). They also encompass systems that use computers, controls, communication channels and automated technologies to provide traffic safety in general and ensure transport efficiency by reducing energy consumption and the environmental impact.*

Eskandarian (2012) distinguishes between three categories of smart cars according to their degree of autonomy, i.e. smart cars with high autonomy able to drive without any driver assistance; smart cars with moderate autonomy which assist the driver as necessary; and smart cars with low autonomy (pure driving), which completely transfer all control over the vehicle to the driver and merely warn the driver of potential errors. Activities such as the ABS and stabilisation systems along with other systems and components, which constantly measure the vehicle's condition and help provide a safe and comfortable ride, run automatically in the vehicle. Further, data regarding the vehicle as controlled by the driver, or the driver's 'personalised driving style', are also collected. Schwartz (2004) states that personal data constitute an important currency in the 21st century since personal data already have a high value that is constantly growing. The Slovenian Personal Data Protection Act (Zakon o varstvu osebnih podatkov [ZVOP-1-UPB], 2004) stipulates that every individual regardless of their nationality, race, colour, religious beliefs, ethnicity etc. shall enjoy the protection of their personal data. It also defines personal data as *any data relating to an individual, irrespective of the form in which it is expressed.*

2 THE ARCHITECTURE OF SMART CARS

The European Union Agency for Network and Information Security (ENISA, 2016) has devised the typical or general architecture of smart cars, as well as the

main elements of such architecture. Nakrani (2015) states that, along with the development of technology, the car has become a space for the use of media, i.e. both a communications centre and a working area. Consequently, the number of useful functions in these cars has been increasing. According to ENISA (2016), the majority of smart cars are made up of the following domains: *the power train sub-network*; *the chassis control sub-network*; *the body control sub-network; and the infotainment sub-network* (the infotainment domain), that are all connected through a common gateway. All of these domains bring a certain level of risk to smart cars, which can be distinguished in terms of their impacts on security and privacy. The infotainment domain, which is separate from the other domains, includes navigation (GPS), communications (phone etc.) and other entertainment services (audio/video unit – multimedia unit). The electronic control unit and the system of sensors enable passengers to manage a wide array of functions, such as the main multimedia unit, audio/video contents, navigation and telephone services. Apart from entertainment services (audio/video), this domain provides access to the Internet, access to traffic information, maps, digital recording instruments (tachographs) etc. The electronic control units in this domain run on the operating systems of mobile devices, such as Windows CE, Android, Tizen or WebOS. The infotainment domain also includes Bluetooth or Wi-Fi networks. The communications unit is primarily responsible for providing connectivity, but also contains the majority of security features for protecting communications such as firewalls, authentication services etc. This unit is used for diagnostics (error notifications, messages regarding software updates etc.), accident reporting and emergency calls, car theft or geo-positioning notifications (geo-fencing) etc. Apart from Wi-Fi and 3G connectivity, it provides other interfaces intended for long-distance communications, as well as wired and wireless interfaces for local use (ENISA, 2016).

Meola (2016) states that by 2021 82% of all cars sold will be smart cars, which he considers to be the most important element of the Internet of Things in the automotive industry. Moreover, Meola (2016) believes we will witness increasing development aimed at integrating various applications into cars, such as navigation applications (which are replacing the initial vehicle GPS systems), music applications (thus making car radios redundant) etc.

3 SECURITY IN SMART CARS

Although smart vehicles have only become well known in the past few years, there are already numerous publications regarding attacks against smart cars and their systems. This issue would be less pertinent if it did not threaten both the safety and data security of their users. Završnik (2010) emphasises that people are constantly subjected to different types of control, i.e. through their mobile phones, RFID objects and documents, as well as vehicle positioning systems. He also states that our locations, communications and, thus, our needs, desires and interests are meticulously analysed, meaning we are (potentially) subjected to profiling and exposed to several threats with respect to personal data. However, such threats not only jeopardise users but also affect manufacturers who are then forced to

deal with numerous vehicle recalls due to the emergence of threats and presence of vulnerabilities. Bernik and Meško (2011) add that knowledge of the situation and awareness of the threats existing in cyberspace (which also includes smart cars) are crucial if we wish to reduce the impact of such threats on individuals and enterprises. A range of institutions, including ENISA, are striving to persuade car manufactures to introduce so-called best practices to help ensure the highest level of smart car security and thereby protect them from the many cyber threats they are constantly exposed to. Yet, the security or protection of smart cars depends on every single component and system, which also includes cloud services, applications, vehicle components, as well as a host of maintenance and diagnostic tools. It is also worth mentioning that the cyber security of smart cars does not merely affect the security and privacy of those using such vehicles, but also has a strong impact on security generally. For the manufacturers of smart cars, cyber security continues to entail the greatest challenge and highest cost (ENISA, 2016).

According to ENISA (2016), numerous experts in the automotive industry and particularly in smart cars have developed three categories of best practices. These include policies, standards and organisational measures and security functions. Payne III (2017) states that a car may contain enormous quantities of data, something its user may not even be aware of. When we wish to connect our phone to a smart car, the system always displays a notification asking us whether we wish to transfer data from our phone to the system of the vehicle. Transferred data may include text messages, calls and various other data. Even if the user rejects the vehicle's offer to exchange data, the vehicle may still record data regarding the device it has connected to. Thus, a smart car data may be unaware that the vehicle may even record data on the number of times they opened or closed car doors and switched on the lights, information about the route they entered into the navigation system, their favourite locations and locations that have been saved by the vehicle. The fact such data may help in the investigation of criminal offences (for instance, terrorism) is a positive aspect of their recording and storage. Payne III (2017) also states that users are unaware of the quantity of data a smart car can store, which is why the mere sending of an image of a driver's licence, credit card or even the credit card number alone can give an unauthorised person accessing such data an opportunity to cause an unfortunate event, which could also entail identity theft or financial damage. Peppet (2014) adds that the habits, routines and everyday activities of smart car users are also recorded. He notes that insurance companies may be able to use such data to determine the quality and method of a person's driving which could, at least theoretically, reduce the costs of insurance. Silberg, Plesco, Rotman and Le (2016) emphasise that smart cars record masses of information and data concerning drivers' routines and tendencies, as well as current data about the car and its diagnostics. This enables car manufacturers to obtain new insights since they become familiar with individual drivers' specific needs, their behaviour and the ways in which they control the car. On one hand, this allows manufacturers to increase the safety and security of their vehicles, yet it also provides them with an opportunity to monetise such data. They also state that manufacturers who collect such data may be able to support their existing smart car users in not merely purchasing a vehicle, but also for other services like 'premium' parking services, car transport and rental services, battery charging and refuelling services etc.

4 THREATS

Browne (2016) contends that most people do not have any concerns regarding cyber security when using smart cars and other devices connected to the Internet of Things. The problem arises from the fact that consumers wish for ever-greater connectivity of their devices with the outside world from any location, leading to potential vulnerability of the system and, thus, of their privacy. This not only concerns smart cars, which are able to connect to home-security systems, smart TV sets, smart refrigerators and other smart devices, but also smart houses and apartments, as well as the personal data stored on such devices. All of them are connected via numerous networks, while their users are not necessarily aware of the vulnerability of these systems. Users tend to be more aware of security issues and the vulnerability of personal computers than those pertaining to mobile devices, which also include smart cars and other IoT devices.

Unauthorised persons may carry out the following activities (ENISA, 2016):

- - *damage/loss* (loss of information stored in a cloud, loss/leak of sensitive information – about payment, driving routines and similar when selling the car etc.);
- - *wiretapping/bugging/interception/hijacking* (repeating messages, when adequate protection measures are not in place, attackers can easily manage the braking, steering and other functions of a car);
- - *MITM* (man-in-the-middle) or session hijacking (potential financial loss, uploading of malware, obtaining a legitimate key in order to steal the vehicle, network data collection etc.);
- - *criminal offences/abuse* (denial of service (DoS, DDoS), which leads not only to network failure but also to unexpected behaviour of the vehicle; unauthorised access to the information system/network (attackers take over control of the vehicle));
- - *disclosure of confidential information*;
- - *identity fraud* (most often resulting from cloning the key aimed at misrepresenting the vehicle within the road infrastructure systems (toll payments etc.)); and
- - *malware/malicious activity* (exploiting well-known pathways for attacks against the Linux, Android and Windows environments. Such attacks are subsequently also carried out against smart cars).

Today's cars use hundreds of sensors linked to numerous inter-connected computers. These technologies not only provide comfort for their users while travelling but are also used to guarantee their safety and security. Hartfield (2017) claims that the integration of smart phones into cars is not due to constant pressure by IT services providers, but also arises from car manufacturers themselves. This which is evident from the development of their own technologies, such as BMW's Connected Drive, Volkswagen's Car-Net, Mercedes' mbrace etc. Other vulnerable systems include USB technologies, which increase the risk of potential attacks on smart vehicles (USB enables devices such as music players, navigation systems or charging components to be connected, while this particular interface is often targeted by attackers who are able to modify the USB hardware, which cannot be

detected by the end-user) and may also change vehicle settings, and Bluetooth technologies that are most often used to transfer directories or contacts into the car system, but can also be used to transfer passwords and applications for later use by attackers for the purposes of wiretapping or intercepting communications, stealing personal data and other malicious acts. The integration of smart phones into cars thus contributes to additional vulnerabilities hidden in communications channels, such as 3G/4G, Wi-Fi, Bluetooth etc. Further, third-party applications downloaded by users onto their smart phones could also be extremely problematic. These applications are usually allowed certain privileges which may put users at risk. Mobile platforms, which face this issue most often, include the Apple iOS and Android system (Harfield, 2017).

McAfee (2017) states that every electronic device consists of several components produced by numerous manufacturers/suppliers. Hardware, software, developer tools, testing tools and many other systems are not the product of any single manufacturer. The issues arising from the production of such devices relate to the fact that products manufactured or assembled in this way are normally cheaper and more accessible to consumers. These production processes may lead to security risks since the manufacturers of these components do not necessarily use the same level of security applied by the manufacturers of original parts. McAfee (2017) also claims that such components must be detected and security measures taken during the following steps in the supply chain: the use of authorised distribution channels for the purchase of hardware and software used for maintaining and assembling cars; the use of a tracking system which detects critical components containing security systems; continuity of supply, which is based on a long-term policy with respect to the availability of spare parts; recording of risks stemming from production processes; control over finished products and potential risks (wrong description, falsification or forgery etc.).

Apart from physically stopping the vehicle, messing around with the air-conditioning system, ventilators and windscreen wipers, attackers can also direct their attacks elsewhere. Such attacks include car theft or causing electronic damage/disabling car functions; falsification of car data (mileage); access to personal data (mobile phone numbers, addresses, bank details, location data etc.) to be used immediately or subsequently for the purposes of extortion; wiretapping or intercepting voice and data communication between users and their cars; and access to the manufacturer of peripherals, service provider or to data regarding application providers or applications as such (Schorer, 2015).

Based on concrete examples, one could observe that the development of information security within smart cars is still an ongoing process. The first example occurred in 2017 when Smith (2017) reported an incident that had allegedly happened in London. Unknown persons used a device which can be purchased on eBay to increase the range of a key (which was located in the victim's house) of a new BMW in order to unlock the car, start its engine and steal the vehicle. This example points to the significant vulnerability of contactless keys, even among vehicles of a higher price range.

The second example was reported by Greenberg (2016) who demonstrated how two researchers in England, namely Charlie Miller and Chris Valasek, took

over certain controls of a Jeep Cherokee manufactured by Chrysler. They conducted their first 'attack' in 2015 by using a unit, which is able to physically connect with a computer, in order to hack into the electronic control system, thereby accessing certain parts of the car and allowing them to remotely control particular elements (for instance, operate the windscreen wipers, turn off the braking system when the car drove slower than 8 km/h, turn the steering wheel when the gearshift lever was in reverse etc.). Following this 'attack', Chrysler recalled 1.4 million of its vehicles in order to install upgrades to prevent or disable such attacks. A year later, Miller and Valasek (in Greenberg, 2016) used a new method to hack the controller network of the same vehicle, which helped them circumvent certain safeguards and security elements that had prevented them from fully carrying out their 'attack' during their first attempt. By accessing the controller network, they were able to send a command to the vehicle from a remote location, which enabled them to take control of the entire vehicle (including braking at high speeds, reducing speed, turning the steering wheel while driving etc.). This case demonstrates that smart cars are just as vulnerable as personal computers or other mobile devices, yet attacks against smart cars may prove more threatening because they not only affect the data of drivers connected to such cars, but also their health and safety.

The third example shows that, despite a sound level of protection, the user data that are stored in the vehicle are not encrypted. Constantin (2017) states that a USB port can be used to enter malicious script which is then run by the system automatically and with full administrator rights. This was established by Gabriel Cîrlig (in Constantin, 2017) who also found unencrypted data belonging to the users of connected mobile devices (e.g. call history, text messages and email addresses, contact lists etc.) stored in the infotainment module. In addition to such data, he found other sensitive data like the list of favourite locations from or to which the car was travelling, the sound profiles of different commands, as well as GPS coordinates entered by users into the GPS unit of the infotainment module. This means that every security feature used by mobile devices therefore becomes superfluous as they are connected to the infotainment domain of the smart car examined by Cîrlig via a Bluetooth connection. He also claims the infotainment module of this particular vehicle was manufactured in Japan and represents a paradise for hackers since it uses both Wi-Fi and GPS and is based on Linux operating systems that provide full access to the terminal, while the module itself also contains numerous error-detection tools (including for the GPS system) which the developers had failed to protect (Constantin, 2017). This case depicts another example of potential threats against smart vehicle users since it is precisely the drivers (apart from unprotected data) who represent the most substantial risk as attackers are able to use a malicious USB key to access their data, hack through open Wi-Fi networks and gain real-time (live) access to location data.

5 SOLUTIONS

Given that numerous smart cars use the infotainment domain, car manufacturers are forced to incorporate different security features. These include unique personal

identification numbers and specific sets of radio-frequency signals, encryption, masking, scanning, detection of anomalies, use of certificates, filtering, firewalls, intrusion detection systems, whitelists, fraud detection, encryption of data regarding network connections, protection of keys and the use of closed systems which prevent the writing of code without authorised tools (Browne, 2016). The National Highway Traffic Administration (NHTSA) adopted the Security and Privacy in Your Car Act (2015) in an attempt to ensure cyber security in vehicles. They wanted to achieve adequate protection against unauthorised access to electronic controls or to any data related to driving, such as data on location and speed, as well as data regarding the owner or passengers. Moreover, they wished to prevent any unauthorised access to the data collected and stored by electronic systems built into the vehicle (Pearson, 2017). Smart cars need an occasional software upgrade just like any other smart device, from smart phones to smart robot vacuum cleaners. Anderson et al. (2014) emphasise that such vehicles may be connected with each other, with the infrastructure or the Internet, meaning they can be exposed to cyber attacks. The increasingly improved connectivity of smart cars (Internet, USB connection, mobile phones etc.) gives rise to new security challenges and therefore to an ever-greater number of entry points that can be abused for the purpose of carrying out malicious attacks against the vehicle and (the privacy of) its users. It should also be pointed out that software updates always require access to the Internet, which gives an opportunity for computer viruses to infect the system during a completely legal software update, thus misappropriating considerable quantities of personal data belonging to the user. That is why several authors stress that connections to servers must be extremely secure. Among the myriad of threats affecting smart cars, the most important threat, i.e. the human being, must not be overlooked. Technology enthusiasts always wish to have access to different systems to obtain control over elements for which car manufacturers have prevented or disabled access. In the context of mobile phones, experts point to the phenomena of 'jail breaking' and 'rooting' that enable technology enthusiasts to gain greater access to and increased flexibility of their device. Smart cars can also fall victim to these phenomena because users will want greater efficiency or wish to use their own software, even if that means they will be putting their own physical safety and security, as well as the security of their personal data, at risk (Anderson et al., 2014).

Schober (2016) compares the prevention of cyber attacks on smart cars with the prevention of cyber attacks on personal computers: users must ensure their software and hardware are up to date; they should avoid installing devices or applications not authorised by the manufacturer; they should take note of any unauthorised interference with or intrusion into the vehicle since many intrusions into smart cars actually require physical access to cars (inserting a USB key etc.). Ward (2017) states that security ought to be provided throughout the life-cycle of cars and systems they use. Beltov (2016) claims the incorporation of the IoT in vehicles and use of smart cars' platforms provide an opportunity to view, control and adapt vehicle settings via smart phones, tablets and computers. Similar issues also arise when using third-party software and applications for such

manipulations as they may pose a threat to users' personal data. Zurkus (2015) states that smart cars are technologically-advanced and computer-supported devices which are connected to navigation and entertainment systems that enable them to store personal data, which can be targeted by numerous attackers. Naturally, the question arises as to who the owner of such data is, where and how the data is shared/sent and how smart car manufacturers are protecting it (Zurkus, 2015). These issues were regulated when the European General Data Protection Regulation entered into force. While discussing privacy in smart cars, it is worth asking what kind of information and data our car actually holds. Payne III (2017) states that smart car manufacturers will undoubtedly start applying methods to conceal such information, but the method they will choose to achieve this has yet to be revealed.

6 METHODS

The research study was based on the following hypotheses:

Hypothesis 1: Male car users believe that the abuse of smart cars is more likely to lead to the misappropriation of data than female users.

Hypothesis 2: Car users believe the abuse of smart cars is most likely to lead to the misappropriation of their contact details (phone numbers, e-mail addresses etc.).

The research study was conducted through an online questionnaire made publicly available on the "1KA" online portal (www.1ka.si). The questionnaire was active for 10 days in 2017. Drivers were informed about the research study via Facebook profiles and the *Avtomobilizem.net* online forum. In terms of the geographical element of the population is in line with the period, during which the data were collected; in terms of the geographical element, the population was located in Slovenia, while in terms of the content, the population included all drivers aged between 18 and 90. The questionnaire contained questions posed in such a way to enable the researchers to obtain an insight into the knowledge, awareness and use of security solutions, as well as the awareness of threats that could materialise during the use of smart cars and affect their connectivity to other devices. Data were analysed using the SPSS software, version 22. At this point, we note that our sample is not random and therefore the results of our analysis cannot be generalised to the whole population.

The sample was selected using snowball sampling, i.e. a non-probability method, and includes 113 individuals (as shown in Table 1), 87 of whom responded to the questionnaire in its entirety while in 26 cases respondents interrupted their completion of the questionnaire, thus providing a partial response. The majority of respondents were between 19 and 30 years of age (as shown in Figure 1); 64% were male and 36% female (Table 1), with the majority of respondents stating they frequently drive a car (see Figure 2).

Table 1: Descriptive statistics of the sample – respondents' gender

		Frequency – n	Valid share (%)
Valid	Male	56	64.4
	Female	31	35.6
	Total	87	100
Missing	Interrupted	25	
	Total	26	
Total		113	

Figure 1: Descriptive statistics of the sample – respondents' age

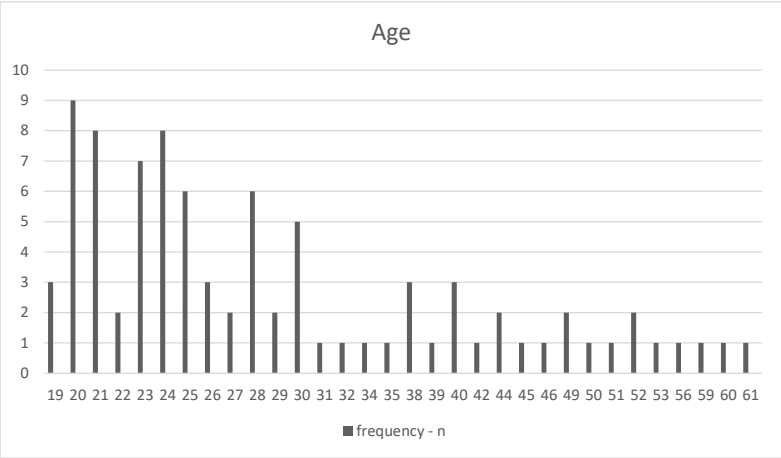
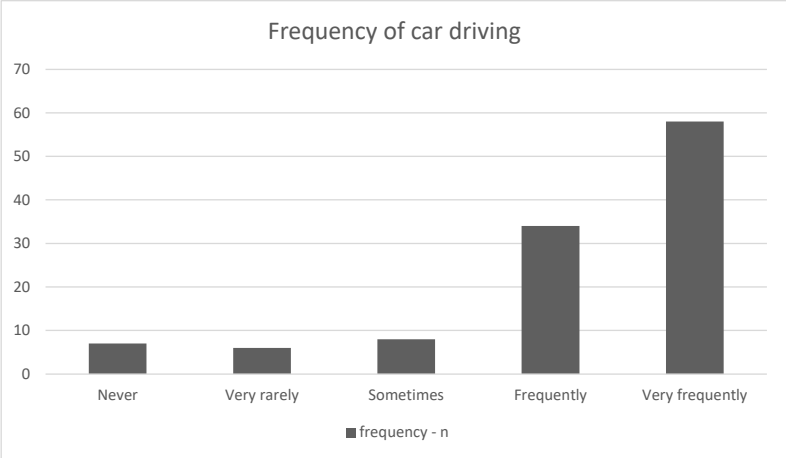


Figure 1 shows the sample mainly consisted of drivers, most of whom stated they drove cars very frequently.

Figure 2: Descriptive statistics of the sample – frequency of car driving



7 RESULTS

The research study was based on the following hypotheses:

Hypothesis 1: Male car users believe that the abuse of smart cars is more likely to lead to the misappropriation of data than female users.

Hypothesis 2: Car users believe the abuse of smart cars is most likely to lead to the misappropriation of their contact details (phone numbers, e-mail addresses etc.).

Discriminant analysis based on two groups (males and females) was undertaken in order to test the first hypothesis. This method was used to analyse a question the responses to which were provided on a 5-point Likert scale, where 1 meant "I completely disagree" and 5 "I agree completely".

Table 2: Group statistics – Discriminant analysis based on two groups

Do you agree with the following statements? It is highly likely that the abuse of a smart car will lead to the misappropriation of my:		Average	Standard deviation	Valid N	
			Unweighted	Weighted	
Male	photo and/or video contents	3.15	1.008	53	53.000
	documents (work-related, private, confidential etc.)	3.06	1.117	53	53.000
	calendar entries (work-related, private)	2.91	1.024	53	53.000
	certificates (for online banking, access to business systems etc.)	3.06	1.247	53	53.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.11	1.235	53	53.000
	contact details (phone numbers, email addresses etc.)	3.21	1.116	53	53.000
Female	photo and/or video contents	3.45	.827	29	29.000
	documents (work-related, private, confidential etc.)	3.41	.946	29	29.000
	calendar entries (work-related, private)	3.14	.953	29	29.000
	certificates (for online banking, access to business systems etc.)	3.52	1.122	29	29.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.59	1.240	29	29.000
	contact details (phone numbers, email addresses etc.)	3.55	.910	29	29.000
Total	photo and/or video contents	3.26	.953	82	82.000
	documents (work-related, private, confidential etc.)	3.18	1.067	82	82.000
	calendar entries (work-related, private)	2.99	1.000	82	82.000
	certificates (for online banking, access to business systems etc.)	3.22	1.217	82	82.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.28	1.250	82	82.000
	contact details (phone numbers, email addresses, etc.)	3.33	1.055	82	82.000

Table 2 shows the average values and standard deviations of the variables pertaining to the two groups. Compared to the first group (males), the second group (females) exhibits higher average values and lower standard deviations with respect to all variables (with the exception of *"passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)"*, where the standard deviation is higher). These results suggest that, in comparison with their male counterparts, female respondents believe there is a greater likelihood of the abuse of smart cars leading to the misappropriation of users' data. The group of male respondents believe the abuse of a smart car is most likely to lead to the misappropriation of contact details (phone numbers, email addresses etc.), while the female respondents believe that such abuse would most likely lead to the misappropriation of passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.). The comparison of the average values of both groups shows they believe that the abuse of smart cars would most likely lead to the misappropriation of contact details (phone numbers, email addresses, etc.), which was expected since smart cars are most often connected to mobile devices which synchronise users' contact details with the systems in the car.

The second hypothesis was tested by applying descriptive statistics and the confidence interval related to the type of misappropriated data. As demonstrated in Table 3, two variables had an average value above 3, meaning that on average the car drivers included in the sample agree that the connection between smart cars on one hand and mobile devices and GPS systems on the other is secure. With respect to the variable *"The connection among smart cars is secure"*, one can observe that respondents were undecided given the average value of exactly 3. They believe that connections to wireless networks, smart homes and cities are less secure since the average value of these variables is below 3. The highest average value (3.47) was attributed to the connection between smart cars and GPS systems, while the lowest average value (2.88) was observed for the connection between smart cars and smart cities. This means the respondents believe that the use of GPS systems in smart cars is the most secure form of connectivity, while the connectivity between smart cars and smart cities is perceived as the least secure.

Table 3: Descriptive statistics – connection security*

		Connections between smart cars and mobile devices are secure	Connections between smart cars and wireless networks are secure	Connections between smart cars and GPS systems are secure	Connections among smart cars are secure	Connections between smart cars and smart homes are secure	Connections between smart cars and smart cities are secure
N	Valid	85	84	83	84	84	85
Average		3.18	2.98	3.47	3.00	2.96	2.88
Standard deviation		.833	.864	.915	.905	.898	.851

**Measured on a 1 to 5 scale, where 1 means "I completely disagree" and 5 means "I agree completely"*

Table 4 shows the majority of variables have an average value above 3, which means the car users included in the sample believe there is a high likelihood of the misappropriation of the listed data, with the exception of the variable *"Calendar entries (work-related, private)"*, where the variable's average value is below 3. It is therefore possible to conclude the respondents believe that the likelihood that abuse of a smart car would to lead to the misappropriation of data from mobile devices is high.

Table 4 also shows that *"Contacts (phone numbers, e-mails, etc.)"* were attributed with the highest average value (3.32). This value falls within the boundaries of the 95% confidence interval of the mean, which has a lower endpoint of 3.11 and an upper endpoint of 3.53. However, the confidence intervals intersect for every single variable. Nevertheless, the average value of *"Contacts (phone numbers, email addresses, etc.)"* is significantly higher than the values for other variables. These results enable us to confirm that respondents believe that smart car abuse would most likely lead to the misappropriation of contact details (phone numbers, email addresses, etc.).

Table 4: The likelihood that smart car abuse would lead to the misappropriation of data*

		Photo and/or video contents	Documents (work-related, private, confidential etc.)	Calendar entries (work--related, private)	Certificates (for online banking, access to business systems etc.)	Passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/ debit cards etc.)	Contact details (phone numbers, email addresses etc.)
N	Valid	102	101	99	99	99	100
Average		3.21	3.19	2.97	3.23	3.29	3.35
Standard deviation		.968	1.084	1.015	1.194	1.223	1.058
95% confidence interval of the mean	Lower endpoint	2.97	2.95	2.75	2.97	3.03	3.11
	Upper endpoint	3.36	3.38	3.16	3.46	3.53	3.53
5% truncated mean		3.19	3.18	2.96	3.24	3.31	3.36

**Measured on a 1 to 5 scale, where 1 stands for a very low likelihood and 5 for a very high likelihood*

8 DISCUSSION

The purpose and objectives of the presented research study were achieved by applying the selected methods and obtaining the results explained in the previous section. We were able to measure the views of smart car users. The following statements represent the key findings of our research: Respondents believe that smart cars are relatively safe since they do not seem to be aware of potential threats. They also hold relatively positive views concerning the use and usefulness of smart cars. This result can be further substantiated by the fact that many respondents expressed enthusiasm for and interest in the research study and the response rate was quite high given the large number of completed questionnaires. The second finding, which is quite surprising, relates to the fact that male respondents believe smart cars are safer than female respondents do. Nevertheless, male respondents still believe the possibilities of such threats materialising are more likely in comparison with the females. By conducting discriminant analysis, the first hypothesis was rejected because the results of the analysis show that, compared with men, women recorded higher mean values in relation to all variables, except one. This means the female respondents believe the abuse of smart cars is more likely to lead to the misappropriation of data compared with their male counterparts.

The second hypothesis was tested by applying descriptive statistics and using the sample to deduce the characteristics of the population or, to put it differently, by calculating the confidence interval for the average values of individual variables. The results show the respondents believe that their contact details (phone numbers, email addresses, etc.) would most likely be misappropriated in the event of abuse involving a smart car, which is not surprising. This means the second hypothesis may be accepted. It is, however, interesting that the respondents do not believe there would be a higher likelihood of misappropriation for passwords given that people tend to be the most protective of data that could open the gateway to other personal or business information.

At this point, we wish to reiterate that our sample is not random and therefore the results of our analysis cannot be generalised to the whole population.

The results of this research study lead to the following recommendations: The issue of information security in smart cars is widely recognised by drivers, even though the topic is relatively new and under-researched. The results show that smart cars are considered as secure, yet the respondents believe there is a high likelihood of their data being misappropriated when smart cars are abused, so it makes sense to introduce additional measures to secure the connections between smart cars and other elements of the Internet of Things (e.g. by certifying the devices connecting to the cars). Users should also be advised not to download or store important data on their mobile devices, unless it is unavoidable. However, they should ensure their devices, data and connections with a smart car are properly protected with several security features such as data and connection encryption, coupled with the use of strong passwords that allow access to individual parts of mobile devices and their data.

The number of drivers who use smart cars very frequently is quite high, indicating the great demand for such vehicles, although this might also be a

consequence of the sampling method used. Trends in the automotive industry show that it will become very difficult not to drive a smart car, which is why the level of safety and security within such cars will have to grow along with the ease and simplicity of their use. The increase in safety and security should not merely include physical safety, i.e. by improving collision-warning systems and similar solutions, but also focus on information security since a number of cases show the abuse of the car's information system can allow such a vehicle to be controlled remotely, which may lead to drivers' physical injury/death.

Nevertheless, there is still a widespread belief it is highly likely that users can have their smart car misappropriated or stolen, which is why it is advised to not only improve the security of connections, but also to increase the level of security against physical intrusions permitted by a cyber attack (for instance, by copying keys via a mobile device, remotely unlocking the car using a signal amplifier etc.) and create the possibility of a security-clearance procedure before starting the engine. In doing so, the level of security will undoubtedly rise but it must be emphasised that the users of many devices do not regard such additional security elements as a good idea since they restrict use of the device, and this also applies to smart cars. Therefore, we believe that users ought to be informed and made aware of the importance of information security in smart cars.

Naturally, it is up to the car owners to decide whether to provide a greater information security in smart cars, and how. Our findings point to the fact that the likelihood of such threats materialising and the subsequent misappropriation of data remains high.

9 CONCLUSION

Smart cars are one of the latest topics of discussion regarding the IoT and smart devices, and remain an under-researched area in Slovenia. Experts have been paying ever greater attention to this issue lately as the threats and risks affecting smart cars have been growing in proportion to the introduction of these new technologies and their use. The infotainment domain or system used to display and connect to various entertainment contents that drivers do not actually need, but wish to have available in the car, remains the biggest problem in terms of protecting or securing a smart car. By attacking the infotainment domain with malicious code and/or exploiting a driver's own carelessness, attackers are able to cause greater damage than by hacking into personal computers (instead of merely stealing personal data, which may lead to significant damage, as it could jeopardise our identity, the abuse of a vehicle might also endanger the physical well-being and safety of both drivers and passengers). Since smart cars will become more accessible to everyone, the protection of drivers and passengers and the data they store on their mobile devices should not only be accompanied by introducing security features for devices and cars, but also by providing adequate training and awareness raising to all users who use smart cars in their everyday lives. Despite the abundance of security and protection mechanisms, humans remain the weakest link in providing information security in general and smart cars in particular. It is also important for the devices used by drivers and passengers and

smart cars alike (that are typically manufactured by several manufacturers), to be certified to ensure a higher level of protection. At the same time, drivers should be informed of these issues when buying or selling such cars. Smart cars should be used cautiously and safely, just like any other mobile devices or computers.

REFERENCES

Anderson, M. J., Kalra, N., Stanley, D. K., Sorensen, P., Samaras, C., & Oluwatola, A. O. (2014). *Autonomous vehicle technology: A guide for policymakers*. Santa Monica: RAND Corporation.

Barret, J. (October 5, 2012). *The internet of things TEDxCIT* [Video]. Retrieved from https://www.youtube.com/watch?v=QaTIt1C5R-M

Beltov, M. (2016). *Smart cars and security - the game of risks.* Retrieved from https://bestsecuritysearch.com/smart-cars-security-game-risks/

Bernik, I., & Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo [Ensuring the security of information by understanding user behaviour on a mobile device]. *Varstvoslovje, 16*(1), 5–15.

Bernik, I., & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto [Internet study of familiarity with cyber threats and fear of cybercrime]. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Browne, W. (2016). *Internet of things devices increases cyber vulnerability of vehicles* (Master's thesis). Utica: Faculty of Utica College.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. *McKinsey Quarterly*, (March). Retrieved from https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

Constantin, L. (November 16, 2017). Researchers hack car infotainment system and find sensitive user data inside. *Motherboard.* Retrieved from https://motherboard.vice.com/en_us/article/3kvw8y/researchers-hack-car-infotainment-system-and-find-sensitive-user-data-inside

Eskandarian, A. (2012). Introduction to smart vehicles. In A. Eskandarian (Ed.), *Handbook of smart vehicles* (pp. 2–13). Washington: Center for Smart Systems Research in the George Washington University.

European Union Agency for Network and Information Security [ENISA]. (2016). *Cyber security and resilience of smart cars: Good practises and recommendations.* Retrieved from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport

Greenberg, A. (January 8, 2016). The Jeep hackers are back to prove car hacking can get much worse. *Wired.* Retrieved from https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Hartfield, S. R. (2017). *21st century automobiles: Vulnerabilities, threats, cyber security and digital forensics* (Master's thesis). Utica: Faculty of Utica College.

McAfee. (2017). *Automotive security best practises.* Retrieved from https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Meola, A. (December 20, 2016). Automotive industry trends: IoT connected smart cars & vehicles. *Business Insider*. Retrieved from http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10

Nakrani, P. K. (2015). *Smart car technologies: A comprehensive study of the state of the art with analysis and trends* (Master's thesis). Tucson: University of Arizona.

Pacheco, J., Satam, S., Hariri, S., Grijalva, C., & Berkenbrock, H. (2016). IoT security development framework for building trustworthy smart car services. In L. Zhou, L. Kaati, W. Mao, & G. A. Wang (Eds.), *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data* (pp. 237–242). Piscataway: IEEE.

Payne III., L. R. (2017). *Vehicle manipulation and forensics* (Master's thesis). Utica: Faculty of Utica College.

Pearson, T. E. (2017). *The need for encryption and secure systems within vehicles* (Master's thesis). Utica: Faculty of Utica College.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(85), 85–178.

Schober, S. (2016). *Cybersecurity and the future of smart cars*. Retrieved from http://www.ibmbigdatahub.com/blog/cybersecurity-and-future-smart-cars

Schorer, M. (2015). *Connected car business brief series*. Retrieved from https://www.vmware.com/ciovantage/wp-content/uploads/2015/12/ConnectedCar-2-Security.pdf

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harward Law Review, 117*(7), 2056–2128.

Security and Privacy in Your Car Act (SPY Car Act). (2015). *Library of Congress (114th Congress).* Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/1806

Silberg, G., Plesco, R., Rotman, D., & Le, D. (2016). *Your connected car is talking. Who's listening?* Delaware: KPMG LLP. Retrieved from https://assets.kpmg.com/content/dam/kpmg/id/pdf/2017/04/id-your-connected-car-is-talking.pdf

Smith, L. J. (October 17, 2017). Car thieves steal £50,000 BMW in seconds – is your car at risk too? *Express.* Retrieved from https://www.express.co.uk/life-style/cars/866987/car-theft-hack-keyless-entry-video-BMW-stolen

Ward, B. D. (2017). *Automotive cybersecurity - redifining war driving* (Master's thesis). Utica: Faculty of Utica College.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) [Data Protection Act]. (2004, 2005, 2007). *Uradni list RS,* (86/04, 113/05, 51/07, 67/07).

Završnik, A. (2010). Tehnično nadzorovanje vsakodnevnega življenja – postdisciplinske teoretične perspektive [Technical surveillance of everyday life – "post disciplinary" theoretical perspectives]. *Revija za kriminalistiko in kriminologijo, 61*(2), 178–190.

Zurkus, K. (March 25, 2015). Are smart cars putting our safety at risk? *CSO.* Retrieved from https://www.csoonline.com/article/2900654/data-protection/are-smart-cars-putting-our-safety-at-risk.html

About the Authors:

Gašper Školc, B.A. in Information Security Studies, master's student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: gasper.skolc@student.um.si

Blaž Markelj, PhD, assistant professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: blaz.markelj@fvv.uni-mb.si