Security issues and vulnerabilities in connected car systems

Conference Paper · June 2015

DOI: 10.1109/MTITS.2015.7223297

CITATIONS
12

READS
2,839

3 authors:

Tamás Bécsi
Budapest University of Technology and Economics
37 PUBLICATIONS **73** CITATIONS
SEE PROFILE

Szilárd Aradi
Budapest University of Technology and Economics
35 PUBLICATIONS **69** CITATIONS
SEE PROFILE

Péter Gáspár
Hungarian Academy of Sciences
402 PUBLICATIONS **2,617** CITATIONS
SEE PROFILE

2015 Models and Technologies for Intelligent Transportation Systems (MT-ITS)
3-5. June 2015. Budapest, Hungary

Security Issues and Vulnerabilities in Connected Car Systems

Tamás Bécsi
Department of Control for Transportation and Vehicle Systems
Budapest University of Technology and Economics
Budapest, Hungary
Email: becsi.tamas@mail.bme.hu

Szilárd Aradi
Department of Control for Transportation and Vehicle Systems
Budapest University of Technology and Economics
Budapest, Hungary
Email: aradi.szilard@mail.bme.hu

Péter Gáspár
Systems and Control Laboratory
Computer and Automation Research Institute
Hungarian Academy of Sciences
Budapest, Hungary
Email: gaspar.peter@sztaki.mta.hu

***Abstract*—The Connected Revolution has reached the automotive industry and the Internet penetrates into the modern vehicles. Formerly acquiring data from a vehicle was the tool of Fleet Management Systems handling commercial vehicles. In the recent years connectivity began to appear in the passenger vehicles also. The first features were infotainment and navigation, having low security needs remaining far from the vehicular networks. Then telematics and remote control, such as keyless entry appeared and created a new security threat in the vehicle. The paper shows how the connected feature changes the vehicle and also presents vulnerabilities of each element to show the importance of cautious system security design.**

Keywords*—*Connected Car; Security

I. Introduction

Today, Internet-of-Things (IoT) is one of the most popular visions of the future, where every single electronic device is connected to the internet providing data and communicating with each other. This phenomenon also means that while till nowadays the data on internet was mainly originally generated by people, from this point devices will become a major information source. How it will affect the society or everyday living is hard to tell, on the other hand it is not the focus of the recent paper.

Another vision that is one of the ultimate goals of the automotive industry is the fully automotive vehicle capable of fulfilling the transportation capabilities of a traditional car. Though recent prototype projects aim the individual sensing and sensor architecture of these vehicles, at the future this feature - as far as one can tell - will highly depend on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Some research projects that aim improved driver assistance systems also focus on these communication possibilities.

On the other hand vehicle owners and manufacturers could benefit from achieving data or communicating with the vehicles. This is an area where manufacturers can gain advantage in the competition for customers. The connected feature is an added value for the vehicle and a basis for marketing since it holds desired, modern and straightforward feature for the future buyers.

It is clear from these different approaches that there are various needs towards the appearance of Connected Cars. With the recent improvements in communication possibilities the term connected is not clear since every participant of the industry translates it to different meanings. The question can be stated as “With whom my car is connected” (see Fig. 1):

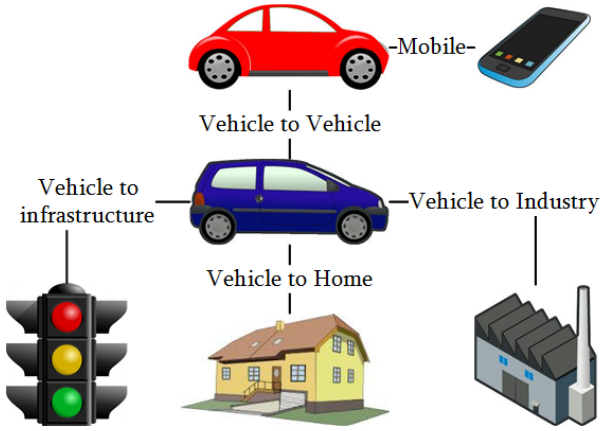

Fig. 1. Connected Car concepts

Car-to-Car communication (Vehicle-to-Vehicle): This form of connected communication is the exchange of information between two vehicles that warn each other of obstacles on the roadway, a change in the road surface, or other hazards.

Car-to-Infrastructure communication (Vehicle-to-Infrastructure): This term refers to wireless communication between vehicles and components of the infrastructure. These components may be intelligent traffic signs, or nodes in the cellular network, which can be used for establishing communication with the Internet, infotainment platforms or carmakers.

ISBN 978-963-313-142-8 @ 2015 BME

Car-to-X communication: Denotes the exchange of information between vehicles, other means of transport, the infrastructure, traffic management centers and various Internet applications. In Car-to-X communication the car both sends and receives data, while other players also receive and process the information.

Cloud: Cloud computing replaces local data storage with storage in a "cloud" that can be accessed via the Internet.

Smartphone or smart device: With the wide spread of smart phones, tabs and the appearance of smart watches these units are obvious targets of the communication.

Therefore the Connected Car concept is diverse and heterogeneous with multiple standards under development and without best practices. The recent trends of the automotive industry suggest that the connected solutions will be introduced to the vehicles step-by-step, from minor or non-safety critical systems to more complicated systems.

This paper deals with the Connected Car type that is already present in several vehicles [1][2], the case when the car owner can reach its own vehicle through a mobile device and the vehicle is also connected to a Cloud service by using the connection of the mobile or its own. (see Fig. 2)

A crucial point of this type of Connected Car is the connection technology that the vehicle uses to communicate with its environment. The first question is the route of the data. As Fig. 2 shows the vehicle, the mobile device and a central server could communicate independently with each other. One possible route is that the internet connection for the vehicle is provided by the handheld device of the owner, while there exists an alternative route, where the vehicle itself can communicate with the Cloud services. Naturally these two solutions can be merged together. If we need maximal availability for direct communication between the vehicle and the Cloud only the GSM technology can be taken into consideration. The same applies to the mobile devices.

The direct communication between the vehicle and the mobile device depends on the possible technologies that are reachable today: Bluetooth, Wifi or NFC. Other means, such as IrDA or ZigBee are not supported in majority by the mobile manufacturers.

The paper is organized as follows: The following section describes how the connection to a mobile device and the appearance of wireless communication changes the requirements of the modern vehicle. In Section III the security problems identified at each element of the Connected Car are detailed.

II. How the connected feature changes the car

It can be seen from the above that it is not a question that there is a need for the Connected Vehicles. Though several problems arise that must be handled somehow:

The first important aspect is the time gap between the automotive and the mobile industry since their development and lifetime cycles differ significantly. The design time of a modern

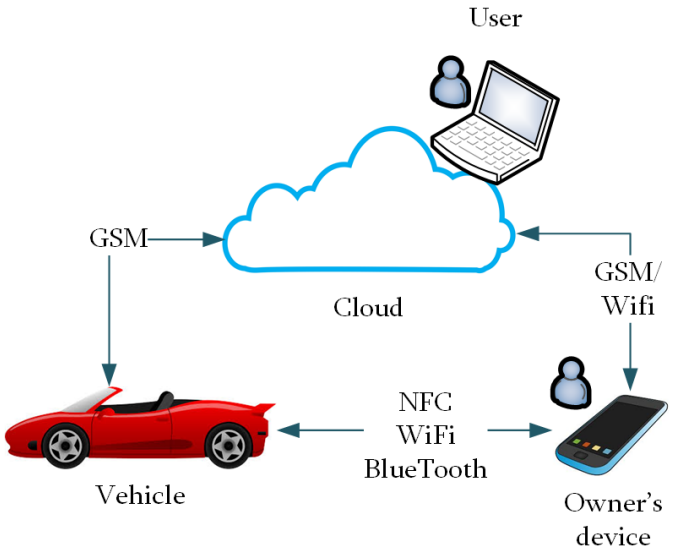

Fig. 2. Connected Car simple connections

vehicle is the same as the overall lifetime of a mobile product, let it be hardware, software or communication technology. Just imagine still using MySpace or MSN messenger on a smart phone with 412 MHz Single-core CPU. Naturally these things are not directly comparable. Though according to the European Automobile Manufacturers' Association the average age of a passenger vehicle in Europe is 8.6 years [3] and according to the US Department of Transportation it is 11.4 years in The US [4]. This means that the Connected Car developed today has to be compatible with the mobile - or who knows what kind of - device of the next 10 years. In other words the majority of the people will exchange its mobile device in every two years but will not exchange its car in under five years.

Some of these problems can be easily solved, though some may not. Some technologies should be extinct e.g., nothing ensures that Bluetooth will be available in a pocket device 10 years from now. Updating the software or even the hardware of the gateway between the vehicular network and the cloud could be a solution. Though beyond software upgrades this means interchangeable or mobile automotive parts which was not in common till now.

The above mentioned problem is about the management of the life-cycle of the product though there is a much more important issue that must be considered: automobile security and to consumer privacy. The Connected Car functionality enables functions that remotely operates the vehicle e.g keyless entry, window operations or preconditioning. With these features it opens a wireless entry point towards the Body Control Module (BCM) of the vehicle which is a generic gateway between the vehicular networks of the vehicle and in this way is a potential target of attacks. This means that by hacking the Connected Car at any point could not only lead to loss of private information but to the loss of the vehicle by theft. The worst case of the exploit of the Connected Car is it can be

ISBN 978-963-313-142-8 @ 2015 BME

a tool for a perfect crime by causing accidents remotely and invisibly.

There are many wired or wireless digital access points to the vehicle's network beside the Connected Car which is best summarized by Checkoway et al. [5], such as the Wireless Tire Pressure Monitoring System (TPMS), Anti-theft, Telematics, Keyless Entry, Infotainment (Radio, USB or Compact Disc) or the OBD-II port.

There has been several studies that shown the vulnerabilities of this backdoors. Miller and Valasek [6] and Koscher et al. [7] presented OBD-II exploits, Roufa et al. presented a way to force-stop a vehicle through the eavesdropping and spoofing of the TPMS messages [8]. The hacking of the BMW ConnectedDrive [9] by Spaar and the DARPA's hack of the OnStar system [10] even reached the major news channels.

III. System Elements and security threats

Three different areas can be distinguished by its physical location when examining the security aspects of the Connected Car:

- The first is obviously the group of the under-the-hood elements, e.g. the Electronic Control units (ECU), the vehicular network and the communication gateway.
- Second is the Mobile device which can not only belong to the owner, but to the service or even a third party user in case of car-sharing.
- The third is the Cloud infrastructure. The security of the cloud is not under the scope of this paper.

Beyond these, the protocol, authentication, authorization, encryption and data protection plays a significant role in the overall system security.

Fig. 3 summarizes the system elements and the identified vulnerabilities and threats.

A. Under the Hood

From security point of view one can distinguish three elements that are in the vehicle. Though these elements can not be the target of an active online attack, they can be used at the preparation phase of the attack for reverse engineering purposes.

a) ECUs.: The ECUs can be mistakenly considered "secure" since they are in the vehicle and can not be reached directly, however they are exposed to several threats. The first question is that how hard it is to reverse engineer the ECU by disassembling or probing its circuitry. The second problem is that does it provide any backdoors? The source of these backdoors could be several: The developers leave it because of debugging or inattentively, or in an intended way. We see two possible backdoor threats of the ECUs. One is, when the ECU – since its functionality is too complex – runs an operating system, and does not closes all possible intrusions. The second is that the ECU itself provides diagnostic access.

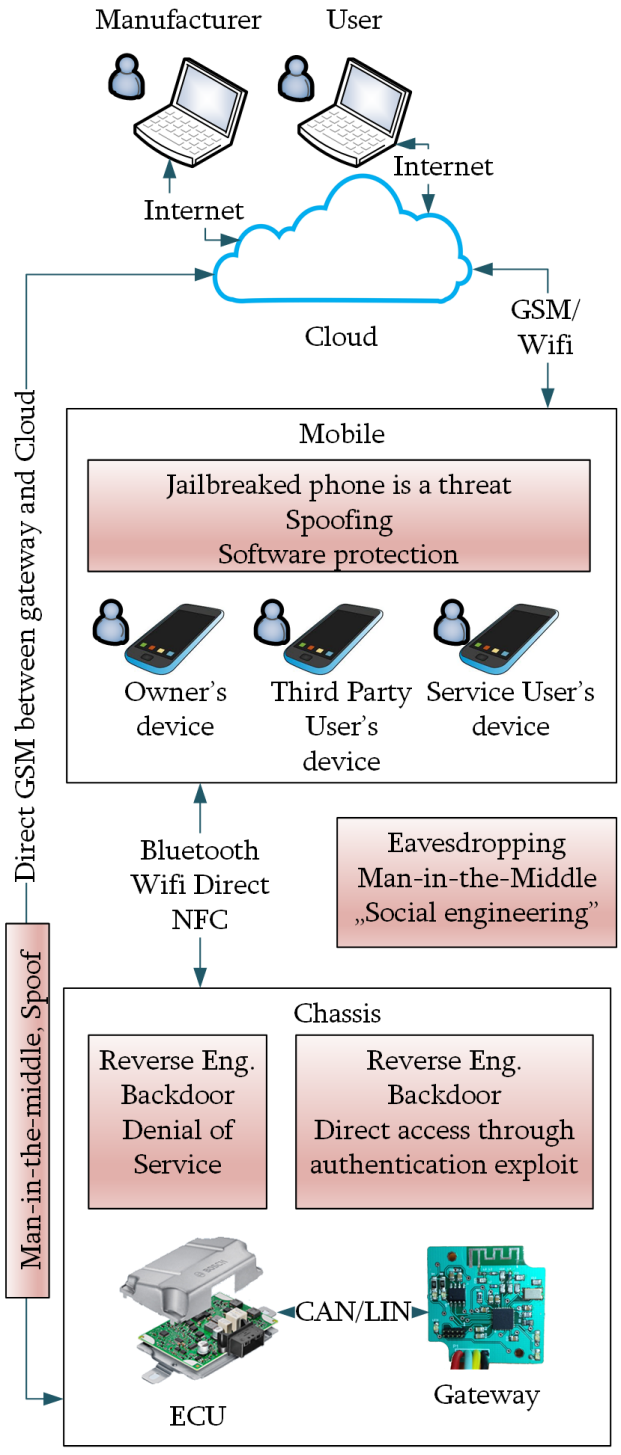

Fig. 3. Security threats

Another problem is about the integrity of the commands. The ECU itself has to apply rules to override the commands of the Connected Car system based on the state of the vehicle to evade dangerous situations.

A much more complex problem is when the ECU itself has the possibility of reflashing from an outer source. In this scenario all aspects of security arises: Does the sender is whom says (Authentication), and has the rights to reflash (Authorization). Can we prove it later that this transaction was realized? Since it holds confidential information, can we protect it? (Non-repudiation) Is the data unaltered? (Integrity) In case it is not, it is possible that an altered ECU firmware is transferred into the ECU leading to a Direct-access attack, meaning the attacker can do anything with the car he wants. Naturally this is the most difficult attacking mode, which is almost impossible without ”social hacking”, i.e. the acquisition of required information from the manufacturer in other ways than reverse engineering.

Besides the above mentioned problems, embedded security in vehicles has to deal with its automotive specific boundary conditions, e.g. computational and memory-constrains of the controllers, cost requirements, and physical security also.

b) Vehicular network.: Vehicular networks such as LIN, CAN, FlexRay or MOST play different roles in the vehicle. A brief summary can be found about the security aspects of these networks in [11] and [12].

When these technologies were born, the design targets were the reliability and cost-effectiveness. The major security design aspect of these networks was that they will not get in contact with the outer world, moreover the nodes will spend they entire life in a closed network with constant topology. Therefore they lack the protection from attacks. Though when these networks are open to the Internet, they need to fulfil the same security principles as any other ICT network [13].

The vehicular network’s security threats come in two ways: One is that with a corrupted gateway device, the network could be disabled with a Denial of Service attack, and in case it is the same network which transfers other functionalities between different ECUs, the vehicle could become inoperable. The vehicular network can be used for reverse engineering purposes also. Naturally secure protocols and solutions exists over the original technologies for protecting diagnostics data, firmware update, or critical commands, though during the design of a complex Connected Car architecture these tools must be integrated into the overall solution.

c) Gateway.: The gateway is the point where the standardized public communications, (let them be over GSM, Bluetooth or WiFi) and the vehicular networks meet. This means that the gateway has a translation and interpretation task which leads to that the gateway ”knows” a lot about the encryption data protection and data semantics. This makes it a perfect target of the attack. The gateway does not need to be an individual ECU in the vehicle, generally it can be the built-in infotainment ECU, or it can be part of the BCM for example.

Actually one of the known Connected Car hacks, the hacking of the BMW ConnectedDrive [9] used many design failures of the gateway called Combox (see Fig. 4). The unit was originally designed for infotainment purposes and the handling of emergency calls hence it had minor security requirements. Maybe because of the need for fast development of the ConnectedDrive application, this module was connected to the vehicular network of the car to provide telemetry and remote control features. Though because of the low security standards the desolderable and readable program flash provided excellent information source for the hacker. This happened at the BMW study also, attacking the gateway with reverse engineering revealed many aspects of the ConnectedDrive application. Gateways are the perfect backdoor points of such systems also. In case the gateway has its own operating system or the possibility of remote reflashing, a spoofing attack can place harmful software on it and it becomes a perfect centre of a Direct-access attack, or as it was mentioned above for a Denial of Service attack towards the vehicle also.

Moreover the unprotected communication inside the ECU between different microcontrollers gives advantage to the attacker by providing ”plaintexts”. The best practice in this area would be the utilization of closed, individually designed electronic elements (such as ASICs) and an ECU that is almost impossible to disassemble.

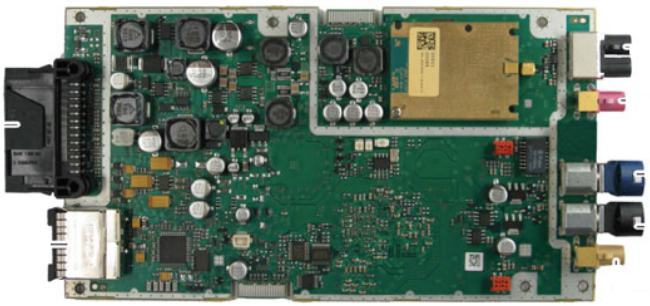

Fig. 4. Combox, the Communication Gateway of BMW

B. Mobile Devices

Automotive security usually concerns systems (e.g. vehicle) as a closed system, whose security can be ensured inherently. Moreover, the vehicle’s communication and control system usually remains unchanged after marketing it. Connecting a mobile device to the vehicle violates these rules in many way.

As mentioned before the fluctuation in mobile industry is way faster, meaning that new generations and platforms arise and fall under the life-cycle of a single car model. Moreover people are using many versions of the operational systems (see Table I) coming from various manufacturers running on different processors.

The continuous development and the multipurpose property of the operating systems leads to the constant appearance of security threats [14]. The lack of upgrading makes this a serious issue. (see Fig. 5) Furthermore the support of older versions stops after a certain time means the newly found vulnerabilities remain unfixed.

TABLE I. ANDROID PLATFORM VERSION DISTRIBUTION AS OF 03.2015 [15]

Version	Codename	API	Distribution
2.2	Froyo	8	0.4%
2.3.3 -2.3.7	Gingerbread	10	6.9%
4.0.3 -4.0.4	Ice Cream Sandwich	15	5.9%
4.1.x	Jelly Bean	16	17.3%
4.2.x		17	19.4%
4.3		18	5.9%
4.4	KitKat	19	40.9%
5.0	Lollipop	21	3.3%

Through the kernel, or permission system, the sandboxed software running environment can be attacked, leaving the application unprotected, e.g. through the permission system [16]. Different misguidance and deception techniques could lead to the exchange of the original software with malware product [17]. Changing the OS arbitrary by the user (”jailbreaking” or ”rooting”) could open the gates of application and data protection. The lack of knowledge or motivation of the users on security makes the mobile platforms vulnerable. In some cases code and stored data can be reverse engineered.

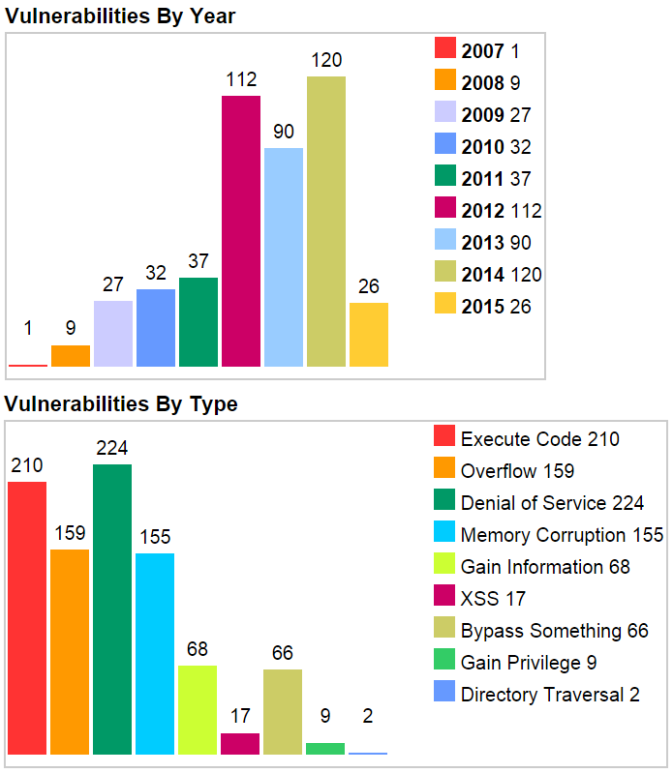

Fig. 5. Apple iOS Vulnerability Statistics [18]

Mobile security in general is very worrisome. Threats are coming continuously from apps, SMS, Web browsers and other holes that malicious hackers can exploit. Until the mobile security space becomes an area of concern for users and security companies alike, it’s hard to see how things will get any better.

The main problem with the mobile devices (as it was already mentioned before) that they are not designed for maximal security. The ”rooting” or ”jailbreaking” of these devices would lead to at least the possibility of eavesdropping their communication easily and of course it enables direct-access attacks also. Though the keys for these are stored in the mobile device. For example in case of Android, Wifi information can be found in the unencrypted text file *”/data/misc/wifi/wpa_supplicant.conf”*, though this file can only be accessed by the super user which is impossible with the recent version without the intended ”rooting” of the owner but nothing ensures that it won’t change in the future, and when the device is ”rooted”, any application could reach these information.

Though the code can be protected in several ways, mobile devices will always be the most vulnerable points of this communication chain in our opinion. The role of these devices makes them the ideal target for spoofing, since technically it is the easiest to pretend. Carefully designed authentication is a key point in protecting the mobile’s actions.

C. Communication

d) Wifi or Bluetooth.: Two major technological choices exists when the mobile device directly communicates with the vehicle: WiFi and Bluetooth from which Bluetooth based technologies dominate the area of mobile-car communication. Both solutions have versions designed with respect to IoT needs Bluetooth Low Energy and WiFi Direct.

Eavesdropping or hacking these communications are not trivial in case they don’t use basic unprotected pairing modes, though in some cases it is feasible [19][20]. Of the two available wireless communication modes, the Wifi or Wifi direct (with WPA2) can be considered more secure. Bluetooth is easier to hack, though neither is trivial. Anyway our intention is that the security of the wireless communication can not be the final line of protection in a Connected Car Application.

e) GSM.: GSM communication can be used between the cloud service and either the vehicle or the mobile. As the other wireless communication techniques it also has vulnerabilities that can be exploited. Details can be found in several papers, such as [21][22]. By using the vulnerabilities of the GSM technology, spoofing and man-in-the-middle attack is also possible.

IV. CONCLUSION

With the appearance of wireless communication in the car, and the connection of the under-the-hood elements with the outer world, new security threats arise on the area of Connected Cars. ICT security needs penetrate into the vehicles. Because of this, privacy and security of the owner must be handled and the well known security principles must be taken into account during the design of such system: confidentiality, integrity, authenticity, availability and non-repudiation [23].

The case of the ConnectedDrive hack, and a recent survey asking 15 major vehicle manufacturers by the staff of U.S.

Senator Edward J. Markey [24] showed that vehicle manufacturers in the competition of *"Who has the newest and more sensational Connected feature?"* don't pay enough attention on security issues. As Wolf et al. states [25] automotive engineers don't have the knowledge of modern ICT security, still the vehicle manufacturers have to become IT companies also.

After reviewing the possibilities the first thing that must be stated that it does not matter what communication technology the system intends to utilize, it can not be the only protection. The defense should be designed in a layered mode [26].

Neither communication path can be stated as totally reliable on its own, spoofing and man-in-the-middle attacks could occur in case the attacker possesses the required information.

REFERENCES

[1] Onstar. [Online]. Available: https://www.onstar.com/us/en/home.html

[2] Bmw connecteddrive. [Online]. Available: http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/

[3] European automobile manufacturers' association (acea). the automobile industry pocket guide 2014–2015. [Online]. Available: http://www.acea.be/uploads/publications/POCKET_GUIDE_2014-1.pdf

[4] U.S. Department of Transportation, Bureau of Transportation Statistics, "National transportation statistics 2014," 2014.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security Symposium*. San Francisco, 2011.

[6] C. Miller and C. Valasek. Adventures in automotive networks and control units. [Online]. Available: http://illmatics.com/car_hacking.pdf

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.

[8] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington DC*, 2010, pp. 11–13.

[9] D. Spaar. Beemer, open thyself! security vulnerabilities in bmw's connecteddrive, c't magazin. [Online]. Available: http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

[10] Autoevolution. Darpa hacked a chevy impala through its onstar system. [Online]. Available: http://www.autoevolution.com/news/darpa-hacked-a-chevy-impala-through-its-onstar-system-video-92194.html

[11] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, June 2011, pp. 528–533.

[12] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars*, 2004.

[13] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol flexray," in *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08*. Springer, 2009, pp. 84–91.

[14] H. Shewale, S. Patil, V. Deshmukh, and P. Singh, "Analysis of android vulnerabilities and modern exploitation techniques." *ICTACT Journal on Communication Technology*, vol. 5, no. 1, 2014.

[15] Android Developers. Dashboards. [Online]. Available: https://developer.android.com/about/dashboards/index.html

[16] Z. Fang, W. Han, and Y. Li, "Permission based android security: Issues and countermeasures," *computers & security*, vol. 43, pp. 205–218, 2014.

[17] C. XIAO, "Wirelurker: A new era in ios and os x malware."

[18] CVE Details. Apple iphone os : Vulnerability statistics. [Online]. Available: http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

[19] M. Ryan, "Bluetooth: With low energy comes low security." in *WOOT*, 2013.

[20] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001, pp. 180–189.

[21] V. Bocan and B. Cretu, "Threats and countermeasures in gsm networks," *Journal of Networks*, vol. 1, no. 6, pp. 18–27, 2006.

[22] D. Fischer, B. Markscheffel, S. Frosch, and D. Büttner, "A survey of threats and security measures for data transmission over gsm/umts networks," in *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012, pp. 477–482.

[23] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks—practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 11–25, 2011.

[24] Staff of Ed Markey. Tracking & hacking: Security & privacy gaps put american drivers at risk. [Online]. Available: http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity .pdf

[25] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," *EURASIP Journal on Embedded Systems*, vol. 2007, 2007.

[26] R. Moalla, B. Lonc, H. Labiod, and N. Simoni, "Towards a cooperative its vehicle application oriented security framework," in *Intelligent Vehicles Symposium Proceedings, 2014 IEEE*, June 2014, pp. 1043–1048.