Cybersecurity and Connected Cars

Facts and Emerging Vendors

January 7th, 2017

Contents

Contents 1

1. **Introduction to connected vehicles** 2
2. **Major Cybersecurity Issues in Connected Vehicles** 4
3. **Connected vehicle penetration points** 5
4. **Major Connected Vehicle Security Product Vendors** 8
5. **Product comparison: Secunet AG, ESCRYPT, Harman and NXP** 11
6. **Market Forecast** 12
7. **Conclusion** 13
8. **References** 14
9. **About CyberDB** 15

1. Introduction to connected vehicles

"No matter what happens, don't panic!" Greenberg, a senior writer at Wired, was told to stay calm by two hackers, Charles Miller and Chris Valasek, during a car hack demonstration in 2015. The hackers developed a software to remotely sabotage a Jeep Cherokee. The demonstration of the hack went viral on the Internet within days. Miller and Valasek succeeded in compromising the multimedia system of the vehicle which then allowed them to exploit laterally other vulnerabilities of the vehicle. Accelerating, braking and turning off the engine were several highly risky moves performed in the demonstration. Driving a hackable and hacked car on the highway can hardly be an ideal experience. The irony of assuring the driver not to panic in the demonstration is a gimmick to draw attention to a dual emerging industry: connected vehicles and automotive security solutions. Connected vehicles are designed and built based on the architecture of the Internet of Things (IoT) technology. Internet access has become a basic embedded feature for consumer goods and infrastructures. The connectivity allows the products to communicate user data constantly with a centralized network. The IoT architecture revolutionizes and rejuvenates many traditional industries such as construction, healthcare and home appliances.

Connected vehicles are one of the most notable examples in this wave of innovation. The diversity of connected vehicles is rich, such as consumer car, motorcycle, van, bus and commercial truck. According to the usage, their performance and surrounding services can be significantly optimized. One remarkable advantage is the potential of safety improvement. Driving monitoring systems such as anti-fatigue, remote braking and incident reporting can extensively help alert drivers and save lives in case of road accidents. This case is particularly true for bus and truck drivers who spend long hours driving. In addition, the connectivity can facilitate other activities of the user. For example, the driver can make financial transaction while he is driving. He can pay his take-away meal and pick it up with an estimated arrival time to shorten the delivery time. He can also purchase music for the multimedia system during a long trip. Furthermore, it is possible to adopt a centralized house management system integrated to a connected car that the driver can send

remote commands before arriving home to start running the washing machine, robot vacuum cleaner, turning on or off air condition, to name a few. Connected vehicles are not mere transport machines. They are a multipurpose platform. More importantly, in recent years, high technology giants such as Google and university research centers have demonstrated considerable resources to the research and development of fully autonomous vehicle. This foreseeable future will be likely to generate more values for the user experience.

The system of connected vehicles is more sophisticated than an airplane. A connected vehicle is reported to have approximately 300 million lines of code, whereas a Boeing 747 plane has 75 million lines. In this perspective, the challenges of securing an intelligent vehicle are much more severe than an airplane. Moreover, considering the extensive range of usage that connected cars cover, the security considerations have to be multidimensional. There are thousands of hackable computer chips in a connected vehicle. One security problem of one component can thus cause catastrophic consequences for the user. In the case of Jeep Cherokee, its manufacturer, Fiat, had to recall 1.4 million vehicles in the U.S. as a result of the exposed cybersecurity issues. The IoT technology driven industry revolution progress fast. Traditional carmakers might not have sufficient preparation to recognize and deal with the cybersecurity aspect of their product. Such circumstances reflect the gap between the ‘presumed’ and ‘required’ security for carmakers, which cybersecurity experts are required to fill. The U.S. has recognized the emergency and importance of the ascension of connected vehicles in 2015. The Security and Privacy in Your Car Act (Spy Car Act) was implemented in this year to oblige automotive manufacturers to reach appropriate compliance to build robust and secure connected vehicles. The guidelines provide cybersecurity insights for the entire product lifecycle. This legislation example reveals the complex cybersecurity threats that the industry confronts as well as the urgency to address them appropriately.

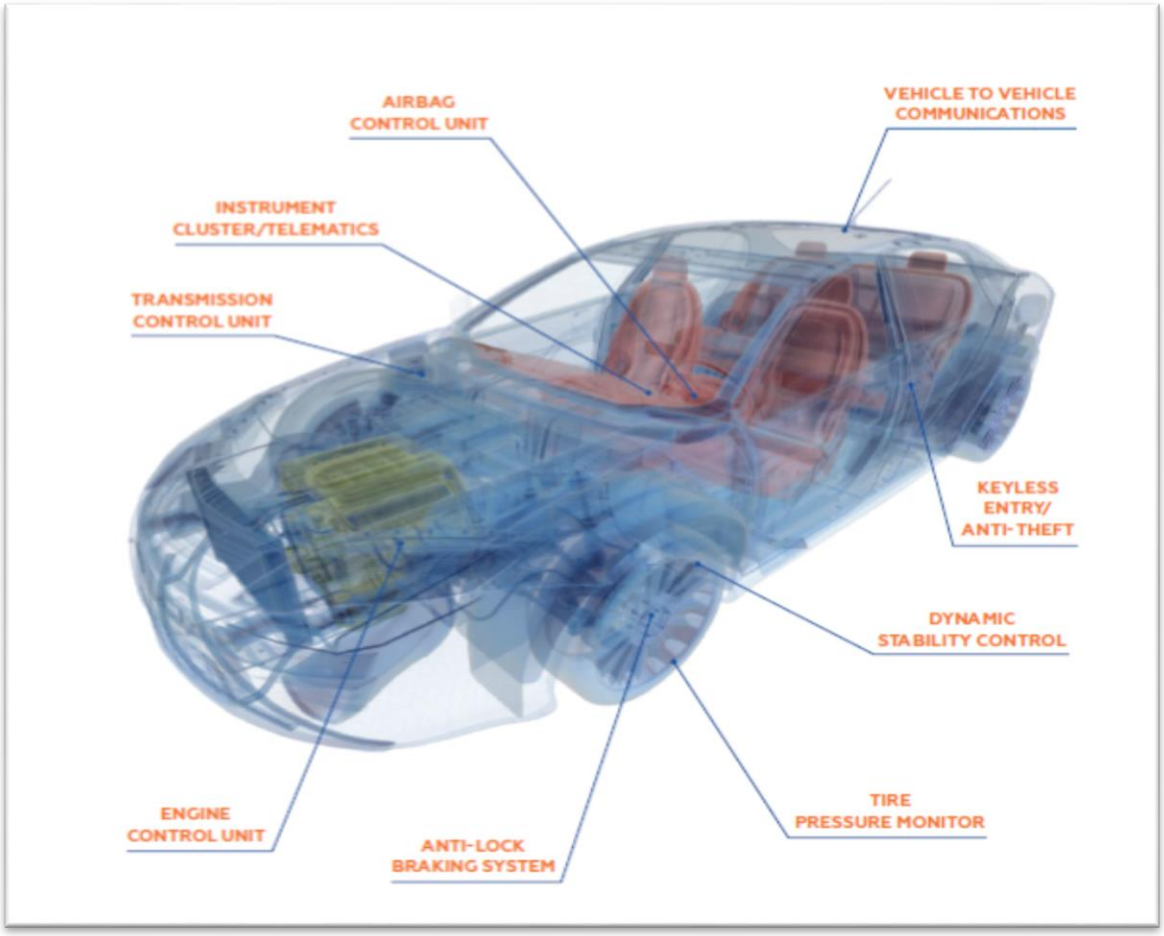
Connected vehicles evoke both risks and opportunities. It is evident that the industry is moving towards a new era which connectivity will be a necessity rather than an accessory. Thus, the main issue is to manage the risks and make the best of the opportunities. Given all the avant-garde technological advantages of connected vehicles, it is unwise to deny its adoption. Understanding

comprehensively the cybersecurity aspect in connected vehicles helps carmakers assure their customers and achieve optimal security.

2. Major Cybersecurity Issues in Connected Vehicles

To begin with, neither vehicles nor cybersecurity products are new to consumers. However, combining cybersecurity to connected vehicles is a great challenge to both security software developers and carmakers. A 2015 joint survey published by Ponemon Institute and RogueWave software studied this gap between these two actors regarding connected vehicles. The survey identifies three key obstacles hindering the two parties from collaborating seamlessly. They are: 1) the lack of trust of carmakers to expose potential product vulnerabilities to white hat hackers and security researchers. 2) the insufficient training for carmakers to approach and address security as software developers. 3) the inadequate emphasis on security in product development. This industry background further suggest significant cybersecurity risk in interoperability and endpoint because automotive manufacturing ecosystem involves a wide range of components from different suppliers. The complexity of the global supply chain of automobile manufacturers and industry compliance is critical. The failure of one component can generate catastrophic domino effects. It is not unimaginable that a competitor adopts cyberattack strategies to succeed in the market. In this context, one crucial perspective is to alert and forbid OEM hardware suppliers and software developers to collaborate with a competitor. However, establishing standardized security protocols to require every stakeholder to respect and comply is a demanding and ambitious endeavor. The following diagram shows several examples of penetration points of a connected vehicle.

3. Connected vehicle penetration points



(Ponemon Institute & RogueWave Software, 2015)

This illustration implies the consequences in case of the malfunctioning of one or multiple parts in the vehicle. For examples, hacking the antitheft system can lead to property loss; hijacking the brake and engine can cause traffic accidents. Provided that the IoT architecture plays a significant role in connected vehicles, its common vulnerable areas, such as insecure default password, data interception and untrustworthy third party firmware, also apply to connected vehicles. More significantly, the connectivity of a connected vehicle is complex. It can be wireless, Bluetooth, cellular, electronic control units (ECU) or a mix of the four. Each connectivity approach has their own weaknesses. For instance, according to Miller and Valasek (2014), Bluetooth is "one of the

biggest and most viable attack surfaces on the modern automobile, due to the complexity of protocol and underlying data." In addition, connected vehicles is not necessarily an equivalence of new vehicles. Nowadays, additional accessories with connectivity can be added to old vehicles so as to connect them to the entire IoT framework for connected vehicles. This enlarges the population of connected vehicles and thus complicates the security solution research and development.

Then, the popular stunts of hijacking the driver control to remotely control the steering wheel, brake or turn off the engine of a connected vehicle suggest risks other than a road accident. One scenario can be stopping a vehicle in a particular place to assault, rob, kidnap and murder the passengers and driver in the vehicle. This concerns vehicles like bus that brings children to school and truck that carries valuable goods. Besides, hacking connected vehicles can be politically motivated, notably hostage and assassination. Hacking one vehicle might be car theft whereas hijacking ten thousands can cause overwhelming public order and security consequences. Such a scenario is similar to a critical infrastructure attack. For instance, the attacker can manipulate the vehicles to crash a government institution as if he commands a real army. Cybersecurity does generate physical security impact.

In addition, the risk of connected vehicle data is unprecedentedly high today. It concerns two sets of information: the operation data of the vehicle and personal data of the user. The former ensures the proper functioning of the vehicle. Vehicle performance can be constantly checked and monitored for follow-up maintenance and reparation purposes. In case of either an accident or remote seize of control, this data is imperative for forensic personnel to trace the origin of the problem and restore the event scene. The latter covers a wide range of personal information ranging from social security number, bank account to home address. As connected vehicles are also serving as a key platform for financial transaction, such information is eventually highly profitable both on individual and corporate level. In particular, commercial trucks and fleets that transport goods worth of trillions of U.S. dollars, the corporate information notably, payroll, tax information and delivery schedule are at stake. Losing this data to either criminals or competitors is damaging to multiple actors: carmaker, logistics provider, sender and receiver.

The scale of cybersecurity in connected vehicles is large. The domino effect can go uncontrolled fast and easily if the security risk is mis- or unmanaged. For many customers, safety is the priority. For carmakers, safety cannot be ensured without security. Thus, recognizing the risks, both on hardware and software level, can help address the gap between carmakers and security software developers is essential to provide safe products to the market.

4. Major Connected Vehicle Security Product Vendors

Company	Country	Connected Vehicle Security products	Solution summary
Argus Cyber Security Ltd	Israel	Argus Connectivity Protection Argus In-Vehicle Network Protection Argus ECU Protection Argus Lifepan Protection Argus Aftermarket Protection	Argus solution suite offers a comprehensive protection. It includes stopping malware from installing and spreading to other programs in the vehicle, detecting in-vehicle network and ECU anomalies, and retrofitting vehicles and fleets to monitor their cyberhealth.
Karamba Security	Israel	Carwall	Carwall emphasizes on preventing hackers from exploiting software bugs. It offers real-time check on the various ECUs in the vehicle. It obliges all programs to run according to factory default setting. In order words, in case of non-compliance, it stops the anomaly from running immediately. Intrusion attempts are then reported automatically.
Cisco Systems Inc	U.S.	Cisco AutoGuard	Cisco utilizes its pioneering network technologies to closely monitor the cyberhealth of the connected vehicle. It uses over-the-air downloads to ensure the software is updated and bug fixed without sending the vehicle to a service garage. The solution of Cisco partners with OEMs to ensure the components facilitate security solution deployment.
Secunet AG	Germany	In-Vehicle Security E-Mobility Security Security for connected vehicles	Secunet ensures a comprehensive security check to verify the authenticity of the software in the connected vehicle. It also secures the application control unit by monitoring the data and protocol layers of the network to prevent cyberattacks.

Company	Country	Connected Vehicle Security products	Solution summary
Arilou Technologies (acquired by Harman)	Israel	Integration Services Penetration Testing	Arilou focus on the pre-sale security service. The company works on consulting secure development and implementation of the embedded systems. It also conducts in-depth penetration testing for ECUs and the entire system. A detailed bugs and fixes report is generated after the tests.
Harman International	U.S.	Harman 5+1 Cyber Security Framework ECUShield TCUShield	Harman introduces rigorous protection to harden the hardware platforms and in-vehicle connectivity parts that store and communicate security certificates and passwords. Sandboxing technology is also implemented to isolate each application. ECUShield and TCUShield are further employed to provide intrusion detection and prevention features on the network.
NXP Semiconductors	U.S.	Secure Vehicle Architecture Secure Car Access In-Vehicle Networks	NXP suggests the concept of defense-in-depth ranging from vehicle perimeter (interfaces) to the ECUs. The emphasis is to monitor the ECUs and networks to prevent data theft and unauthorized intrusions.

ESCRYPT Embedded Systems	Germany	CycurHSM	Escrypt develops CycurHSM to cope with the inadequacy of software security for ECUs. It uses hardware security modules (HSM) to complement the integrity of the software. CycurHSM has been proven by Bosch and it reduces the costs of integrating external ECUs while lowing the attack probability.

Other players in this market are:

- **Infineon Technologies AG**
- **Telenor**
- **Tesla Motors**
- **Verizon**
- **Visteon**
- **CyMotive**
- **GuardKnox**

5. Product comparison: Secunet AG, ESCRYPT, Harman and NXP

The following shows a **sample comparison** of selected number of the above mentioned players

Vendor & Product Name		Secunet AG	ESCRYPT	Harman International	NXP Semiconductors
Product specifications	Engine Control Unit (ECU) protection	√	√	√	√
	Hardware Security Module (HSM) protection		√	√	√
	In/Ext-vehicle network protection	√		√	√
	Embedded connectivity protection			√	√
	Automatic security update			√	
	OS protection			√	
	Real-time monitoring	√			
	Infotainment	√		√	√
	Telematics			√	
	VR & AR (360° vision) support			√	
	Penetration testing	√			
	Multi-silicon vendor support		√	√	

Other major players in this industry such as Cisco, Argus and Karamba are not shown in this table since this report does not pretend to be a comprehensive market analysis report. **For further information, please contact us at info@cyberdb.co and we will be happy to provide additional info**

6. Market Forecast

Connected vehicles and their security products have created an interdependent market. It is therefore important to relate the numbers of one market to another to have an overview. On the one hand, the number of connected vehicles will expand rapidly. In 2015, a newly manufactured vehicle already consisted of approximately 30 microprocessors on average. Business Insider estimates over 380 million connected cars by 2021 in a 2015 forecast. And, by 2020, over 75% of the vehicles will have pre-installed connectivity devices. The anticipations of Gartner are more conservative. A 2015 Gartner IoT future report suggests that 150 million connected vehicles will be on the road and a total of 250 million by 2020. The numbers of both research institutes indicate the huge market of connected vehicles in the coming few years.

On the other hand, an IHS automotive report forecasts the **cybersecurity market size** of connected vehicles to be $759 million by 2023. Motor Intelligence makes a bolder estimation in a five-year forecast suggesting that the cybersecurity products for connected vehicles will grow to $1.2 Billion by 2020, at a **CAGR of 102.62%.**

The different research findings might subject to the methodologies of the research institute. Nevertheless, the scale of these numbers represents the potentials of a new market for both cybersecurity solution development and automotive industry. Moreover, given some high technology companies, notably Google and Apple, devote significant resources to push the limits of connected vehicles to autonomous ones. The demand for appropriate cybersecurity products will definitely expand hand in hand with the evolution of the connected vehicles. The real needs of secure connected vehicles will thus diversify and be promoted to every phase of the manufacturing process, especially secure design and third-party parts integration.

7. Conclusion

Connected vehicles and cybersecurity are the two sides of the same coin. As long as the demand for connected vehicles remains strong, the cybersecurity aspect will have to complement the safety and robust design requirements. The example of Jeep Cherokee demonstrates the costly consequences of neglecting cybersecurity prior to introducing the product to the market. Connected vehicles is an unstoppable trend of automotive revolution. The capacities of recognizing and addressing the vulnerabilities of connected vehicles determine the success for both automobile manufacturers and cybersecurity solution providers.

8. References

Martin, R., 2016. Connected Car Hacking and Cyber Security Solutions - Ignite.

Smith, M., 2016. Report examines the massive future cybersecurity problem of connected cars [WWW Document]. Network World. URL http://www.networkworld.com/article/3031092/security/report-examines-the-massive-future-cybersecurity-problem-of-connected-cars.html (accessed 1.12.17).

Singh, S., 2015. SPY Car Act Is Crucial First Step In Securing Our Cars From Hackers [WWW Document]. Forbes. URL http://www.forbes.com/sites/sarwantsingh/2015/09/08/spy-car-act-securing-our-cars-from-hackers/ (accessed 1.13.17).

Rivera, J., van der Meulen, R., 2015. Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities [WWW Document]. URL http://www.gartner.com/newsroom/id/2970017 (accessed 1.17.17).

Miller, C., Valasek, C., 2014. Survey of Remote Attack Surfaces | Hacker (Computer Security) [WWW Document]. Scribd. URL https://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces (accessed 1.14.17).

Viereckl, R., Assmann, J., Radüge, C., 2014. The Bright Future of Connected Cars.

Automotive World, 2014. Connected cars in a connected era - Automotive World.

Greenberg, A, 2014. How Hackable Is Your Car? Consult This Handy Chart [WWW Document]. WIRED. URL https://www.wired.com/2014/08/car-hacking-chart/ (accessed 1.14.17).

9. About CyberDB

CyberDB (www.cyberdb.co) is the leading global research databank for Cyber solutions and vendors.

CyberDB database includes over 1,200 vendors and 5,000 products, categorized into 8 main cyber categories and 146 sub-categories. The company publishes market researches and summaries on bi-weekly basis on cyber categories.

The database is being used by VC's, multinationals, CISO's and system integrators worldwide to help them navigate through the dynamic cyber landscape.

In addition, CyberDB offers its customers Consulting Services for Cyber Product Strategy, Cyber Technology Scouting and tailored Market researches.

CyberDB is established by the founders of Stratechy, strategy consulting practice that has been working with management teams of Hi-Tech vendors to shape their product strategy turn-around and design and execute their Go-To-Market plan. Among its customers, are NEC Corporation, Samsung, Rafael, Amdocs, Nice, Adallom (Microsoft), Brother, Cyberbit (Elbit) and S21Sec

Please contact CyberDB at **info@cyberDB.co** or visit us in **www.cyberdb.co**, on **Twitter** or **LinkedIn**