# Securing the Future of Connected Vehicles:

# An Analysis on Challenges and Market Opportunities


Xiang Li

## Table of Contents

## 1.0 Executive Summary

This paper will present a hypothetical business to address a market opportunity in the recently emerged and rapidly evolving automotive cybersecurity sector. I have spent an entire semester researching on the challenges in securing automated vehicles, reading about the major players in this emerging market and interviewing with some of my potential customers.

## 1.1 Problem

Cars and trucks today are equipped with computers overseeing every single aspect of their operation, running on million lines of codes. And just like your personal PC, these computer on wheels can be vulnerable to malicious attacks. If you think someone hacking into a car and causes it to crash is something out of a Sci-Fi movie, think again. The following is an WIRED journalist's experience in a hacked Jeep Cherokee.

> "I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold. Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass."
>
> "As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits."
>
> "As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission. Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached

> a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun."
>
> "At that point, the interstate began to slope upward, so the Jeep lost more momentum and barely crept forward. Cars lined up behind my bumper before passing me, honking. I could see an 18-wheeler approaching in my rearview mirror. I hoped its driver saw me, too, and could tell I was paralyzed on the highway."
>
> "'You're doomed!' Valasek shouted, but I couldn't make out his heckling over the blast of the radio, now pumping Kanye West. The semi loomed in the mirror, bearing down on my immobilized Jeep. I followed Miller's advice: I didn't panic. I did, however, drop any semblance of bravery, grab my iPhone with a clammy fist, and beg the hackers to make it stop."
>
> Source: WIRED[1]

Jeep Cherokee is not the only car vulnerable to hackers. Any modern vehicles equipped with tire pressure monitoring system, USB, Bluetooth or cellular connection are vulnerable to attacks like this. Many Fiat Chrysler Automotives products featuring UConnect infotainment system are affected by the same vulnerabilities as the Cherokee. One article on Bankrate.com has listed 7 other "most hackable" cars, including the Cadillac Escalade, Infiniti Q50, Toyota Prius, Ford Fusion, BMW X3, Chrysler 300 and Range Rover Evoque.[2]

Commercial trucks these days are fitted with cutting edge fleet management technologies to help fleets maximizes fuel efficiency and vehicles run time, but at the same time they could be even easier to exploit due to the standardized communication protocol known as the J1939 standard.

[1] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired. N.p., 21 July 2015. Web. 14 Mar. 2017.
[2] Strohm, Mitch. "9 Most Hackable Cars." Bankrate. N.p., 21 Mar. 2017. Web. 16 Apr. 2017.

## 1.2 Solution

In my vision, the company would eventually become a major force in securing today and tomorrow's connected motor vehicles. We would start with addressing the security concerns in fleet management technologies used in commercial motor vehicles, building a scalable/modular solution that can be implement on different platforms with little to no modifications. We will then venture into securing tomorrow's connected passenger vehicles using our expertise carried over from securing commercial vehicles.

## 1.3 Market

The beginning of the smartphone era also brings along the revolution of Internet of Things (IoTs). Phones, tablets, TVs, speaker systems, thermostats and fridges, even light bulbs are connected to the Internet. Whether you like it or not, connected vehicles are here to stay. Automakers are on the frontline of building smarter and more connected cars to attract new car buyers with cutting edge technologies such as Vehicle to Vehicle, Vehicle to Infrastructure communication, Advanced Driver Assistance System. There is an immense shortfall in securing these highly-connected vehicles and automakers are scrambling to defend their connected vehicles against cyber threats. They aren't yet keen to openly work with third party cybersecurity companies, as that would be tantamount to admitting there's a problem. Private collaboration remains the best way forward for automotive cybersecurity companies, says Ben-Noon, the CEO of Argus Cyber Security.[3]

[3] Fox-Brewster, Thomas. "Meet The Former Israeli Cyber Soldiers Hoping To Stop Hackers Causing Car Crashes." Forbes. Forbes Magazine, 05 Sept. 2014. Web. 27 Apr. 2017.

Most of the commercial vehicles on the road today are outfitted with technologies made by third-party fleet management providers such as Omnitracs and PeopleNet to help increase fleet efficiency and productivity. And according to IBISWorld Industry Report, declining barriers to enter the fleet telematics system market and strong demand for industry products will attract more players to the industry.[4] Consequently, the number of industry operators is expected to increase at an annualized rate of 6.3% to 102 companies over the five years to 2017.The vulnerabilities of commercial vehicles are getting less public exposures compared to those of passenger cars, but due to the wide deployment of fleet tracking services and J1939 standard protocol, they are at even more risks than passenger vehicle.

## 1.4 Competition

There are a few companies specialized in addressing the cybersecurity needs of connected vehicles. Some of them are raising millions in funding or getting acquired by Tier One suppliers. Most of them focus on securing passenger vehicles. We will cover more details on them in Section 3.4.

[4] Kalyani, Darshan. Fleet Telematics Systems in the US. Rep. no. OD4546. N.p.: IBISWorld, 2017. Print.

## 2.0 Products and Services

### 2.1 Problem Worth Solving

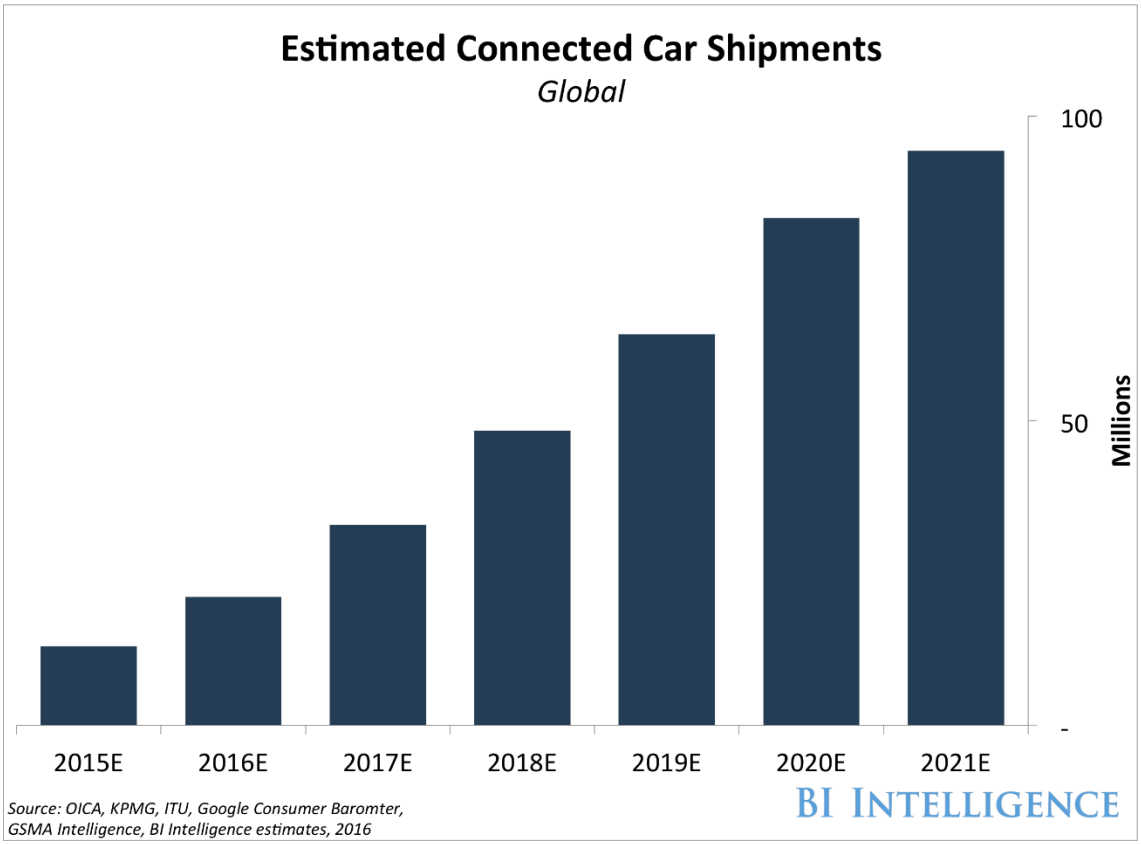
Cars and trucks used to be simple mechanical machineries requiring human overseeing every aspect of the vehicle operation. Things started to change in the 80s when automakers began to equip vehicles with computers for better dependability and more functionality. Since then vehicles have become increasingly more technologically sophisticated and are much more than moving mechanical parts. A modern vehicle's computer oversees and controls all functions of a vehicle from drivetrain components to entertainment system.

Stefan Savage, a computer science professor at the University of California, San Diego, said at the Enigma security conference in San Francisco that carmakers don't know exactly the software is inside the vehicles they sell. The way the auto industry work caused this, since car builders source components from third parties at the lowest cost, and these components' software are all hidden from the manufacturers of a vehicle. "There is nobody in the world that owns all the code in a vehicle," said Savage. "That's a big problem."[5] Working with APIs from multiple third parties without knowing the internal workings of them leave automakers in the dark on how secure these third-party components are, and whether there are security loopholes in their vehicles that can exploited by attackers.

In recent years, the concept of Internet of Things (IoTs) are also making the way into automotive industry. Today's car buyers are more interested in how their cars fit into their digital lifestyle as a gadget than the more traditional selling points such as horsepower, engine

[5] Simonite, Tom. "Your Future Self-Driving Car Will Be Way More Hackable." MIT Technology Review. N.p., 16 Mar. 2016. Web. 10 Dec. 2016.

displacement or number of cylinders. As a result, car manufacturers are building vehicles with many advanced technologies and connectivity to suit the customers' demands.




Source: BI Intelligence

Yoni Heilbronn, the vice president of marketing at Argus Cyber Security, an automotive security company, said: "The equation is very simple. If it's a computer and it connects to the outside world, then it is hackable."[6] Vehicles today as they are essentially computer on wheels travelling down highways. The now famous Jeep Cherokee hack demonstrated by Charlie Miller and Chris Valasek was a wakeup call to the car industry that car hacking is an imminent threat. OEMs are well aware of the risks associated with making their products connected to the

[6] Overly, Steven. "What We Know about Car Hacking, the CIA and Those WikiLeaks Claims." The Washington Post. WP Company, 08 Mar. 2017. Web. 09 Mar. 2017.

Internet, but are very inexperienced and clueless when it comes to cybersecurity practices. These are the reasons why a global group of automakers formed the Automotive Information Sharing and Analysis Center (AUTO-ISAC). This center will let participating companies swap cyber security data and keep each other abreast of the latest hacking threats targeting vehicles. The goal is to "further enhance the industry's ongoing efforts to safeguard vehicle electronic systems and networks," explained Robert Strassburger, vice president for vehicle safety at the Alliance of Automobile Manufacturers, in a statement.[7]

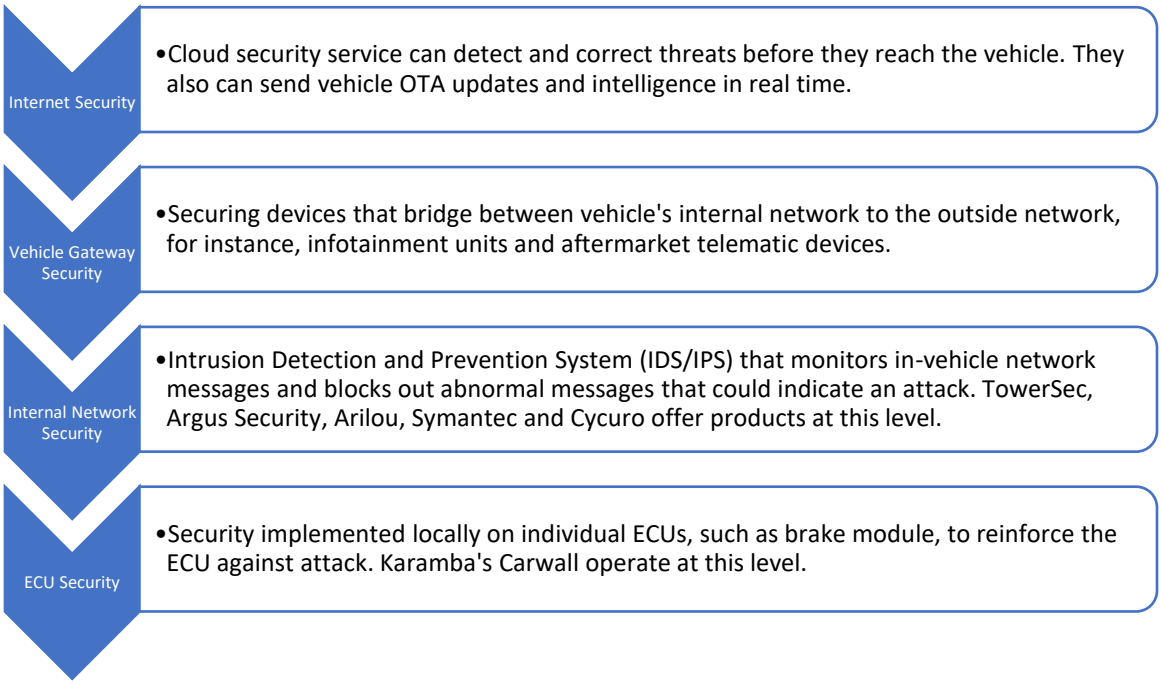
Similarly, for various aftermarket accessory makers, their connected devices designed to be installed on vehicles also bring along attack vectors for hackers. In the following Section 2.3, we included a research study demonstrating how aftermarket telematics device can be used to remotely control a vehicle.

## 2.2 Our Solution

Securing connected vehicles is an enormous task and we need to divide and conquer the big problem into smaller pieces. "The best mental model for understanding how automotive cybersecurity solutions work is to envision them as having several layers of defense," Argus Security's Yoni Heilbronn said. "Multiple solutions focused on different parts of the connected car ecosystem must be integrated in order to provide comprehensive, end-to-end protection; a

[7] Vanian, Jonathan. "Automobile Manufacturers Form Cybersecurity Information Sharing Hub." Automobile Manufacturers Form Cybersecurity Information Sharing Hub | Fortune.com. Fortune, 15 July 2015. Web. 30 Apr. 2017.

single product alone is not adequate." The list below provides a visual representation of all necessary steps to secure connected vehicles.[8]




My plan is to focus on securing vehicle gateway units. I do not have the technical expertise on testing and developing security software that can be installed on gateway units, but I am looking for technical co-founders to help me along the way and come up with a product that can be installed on different platforms.

## 2.3 Validation of Problem and Solution

While connectivity in modern vehicles provides us with comfort, convenience and safety, they also bring attack surface through which to access the vehicle's delicate Controller Area

[8] Toews, Rob. "The Biggest Threat Facing Connected Autonomous Vehicles Is cybersecurity." *TechCrunch*. N.p., 25 Aug. 2016. Web. 10 Dec. 2016.

Network(CAN) bus. Initially developed in the 1980s by Bosch, Controller Area Network became an industry standard in cars in the 1990s and is used in virtually all cars since. Being an older technology, CAN's limitations in today's connected, Internet of Things centric automobile – e.g., low baud rate, meager peak speeds and limited bandwidth – were not deal breakers considering the favorable economics and proven track record, but are now causing many obstacles in applications of advanced features. In addition, the rise of connected cars performing tasks that could not have been foreseen during the 1980s (when CAN was brought to market) has revealed a potentially much larger issue – security.[9]

> "Kathleen Fisher, a computer science professor at Tufts University, warned that automotive computer networks are inherently weak and difficult to secure. Nearly all cars use a networking technology called the "controller area network bus," or CAN bus, developed by the German auto parts maker Robert Bosch GmbH in the 1980s. "The CAN bus is hopelessly insecure," Fisher said. It was developed decades before cars were connected to the Internet and lacks features to block malware programs or reject commands from unauthorized intruders. Fisher said it will take years and cost millions to develop more secure vehicle networking systems, and no company will do this unless its competitors do the same."[10]

In addition to the CAN's inherent deficit, a modern vehicle can incorporate up to 100 independent Engine Control Modules (ECUs) and Body Control Modules (BCM). Car makers rely heavily on outsourcing to third parties to design and manufacture these modules. It is hard for car makers to ensure all the modules from different suppliers are secure. Building a safe platform requires a holistic approach, however since no one party owns or has access to all the source codes in a vehicle, it makes securing the vehicle even harder.[11]

[9] "Connected Car Security and the Need to Replace CAN with Ethernet." Innovasic. N.p., 19 Aug. 2015. Web. 26 Feb. 2017.
[10] Bray, Hiawatha. "After Car Hack, Internet of Things Looks Riskier." The Boston Globe. BetaBoston, 3 Aug. 2015. Web. 26 Feb. 2017.
[11] Toews, Rob. "The Biggest Threat Facing Connected Autonomous Vehicles Is cybersecurity." *TechCrunch*. N.p., 25 Aug. 2016. Web. 10 Dec. 2016.

The industry is well aware of the limitation of CAN and a few of the industry leading automotive and tech companies have formed OPEN Alliance Special Interest Group to promote "the wide scale adoption of Ethernet connectivity as the standard in automotive networking applications."[12] Ali Abaye, a senior director of product marketing for Broadcom's Infrastructure and Networking Group estimated we will start seeing Ethernet replacing CAN in the early 2020s.[13] Broadcom invented BroadR-Reach technology, an Ethernet physical layer standard designed to replace the aging CAN standard. Unlike the CAN bus, BroadR-Reach is built on standard Ethernet protocol which makes implementation of security much easier than the current CAN technology.

A study published by a team of researchers at University of California San Diego studied the vulnerabilities of aftermarket telematic control unit such as the ones found distributed through insurance companies' driving behavior based saving programs (Progressive Snapshot and Liberty Mutual RightTrack) and consumer oriented smart driving assistant dongles such as Automatic Labs's Automatic dongle and Verizon backed Zubie Key. These types of devices provide a bridge between the vulnerable vehicle Controller Area Network (CAN) and the Internet, and as demonstrated by the UCSD team, can be used to remotely control vehicle's body functions (turning on windshield wipers) and brakes (selectively applying brakes and selectively disabling brakes).[14] The type of attack is not limited to just controlling windshield wipers and brakes, as having access to CAN bus makes it possible to control almost every part of the

[12] Baunfire.com, Spark CMS by. "Frequently Asked Questions." Open Alliance. Open Alliance SIG, n.d. Web. 19 Apr. 2017.
[13] Yoshida, Junko. "Ethernet Backbone in Car: Hype or Reality? | EE Times." EETimes. N.p., 6 Aug. 2013. Web. 26 Feb. 2017.
[14] Foster, Ian D., et al. "Fast and Vulnerable: A Story of Telematic Failures." WOOT. 2015.

vehicle. Telematics unit makers are aware of the security needs for their products. This is reflected in the Section 3.3 during my interview with some of the ELD solution providers.

This security problem also applies to heavy commercial vehicles. A group of researchers from University of Michigan conducted an experiment on conducting attacks on commercial vehicle's J1939 Standard CAN. In their demonstration, the researchers managed to do everything from changing the readout of the truck's instrument panel, triggering unintended acceleration, to even disabling one form of semi-trailer's brakes.[15] This is a serious public safety concern. Imagine someone disabling the truck's brakes on a long steep decline, or accelerating the big rig against driver's will. "Today there are about 4 to 4.5 million fleet management systems installed in Europe; this number is forecast to double over the coming years, resulting in a penetration rate close to 100% after 2020." -Wolfgang Bernhart, Senior Partner, Roland Berger.[16]

There are also monetary incentives for criminals to exploit these commercial vehicles. Malicious attackers could compromise an entire fleet of trucks remotely and leave them all stranded on the road and ask for ransom money to re-enable the trucks. The result of hundreds of disabled trucks in a large fleet leading to delayed deliveries and dissatisfied customers is disastrous.

[15] Greenberg, Andy. "Hackers Hijack a Big Rig Truck's Accelerator and Brakes." Wired. Conde Nast, 02 Aug. 2016. Web. 19 Mar. 2017.
[16] Thomas, India. "Special Report: Connected Trucks Published by Automotive World." Automotive World. N.p., 28 Nov. 2016. Web. 26 Apr. 2017.

### 2.4 Roadmap/Future Plans

As mentioned previously in Section 2.2, our focus is on securing vehicle gateway units. The first step is to acquire some devices to test from a few different fleet management providers and demonstrate their devices contain vulnerabilities and can be used as attack vectors and thus countermeasures should be built-in. Once the weaknesses are identified, the companies are more than likely to hire us to provide consulting and software solution to implement on their fleet management devices. The next step is to develop a more sustainable product, a modular solution that can be easily adapted to different telematic/fleet management devices.

Using securing commercial vehicles as a stepping stone into the automotive security field, eventually we would like to step into securing tomorrow's passenger cars as well.

## 3.0 Market Analysis Summary

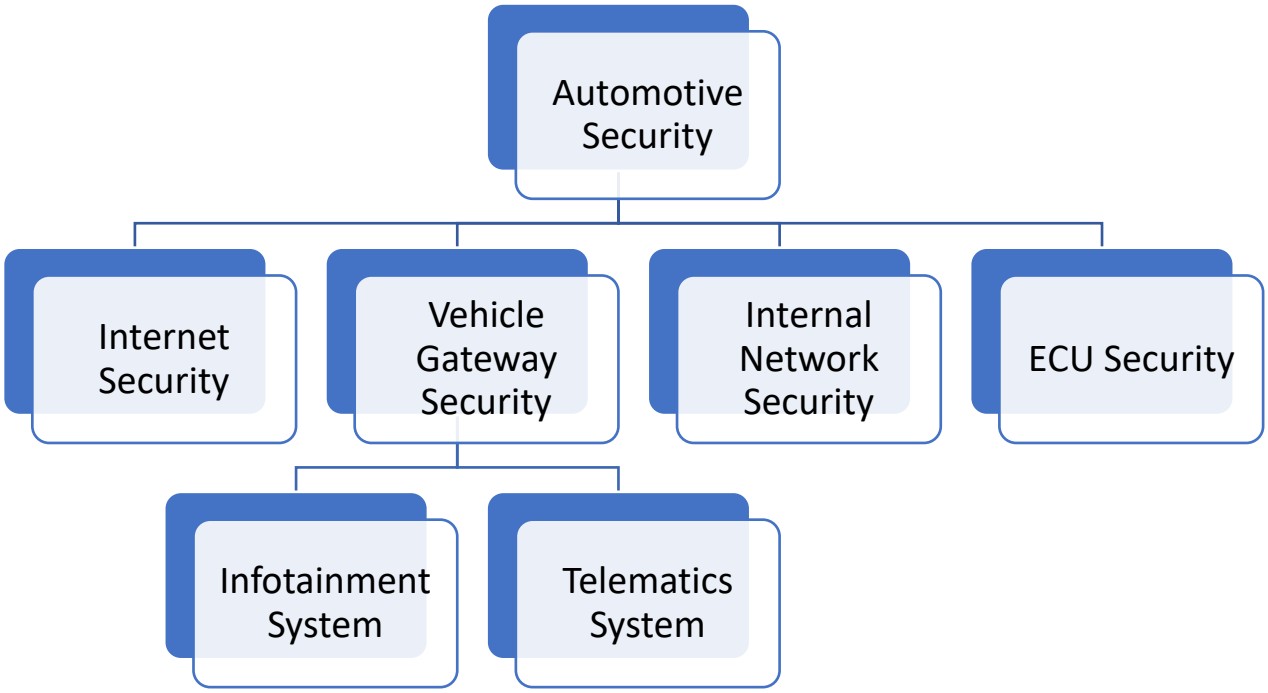
### 3.1 Market Segmentation

> "Over the next decade, as automobiles become connected and more autonomous, in-vehicle safety will expand from "active" and "passive" to yet another dimension; that of "cyber security" from threats against the vehicle's data transmissions and physical control. A layered approach is required in addition to minimum requirements of "identification, detection, prevention, response and recovery we be mandated" which will probably become mandatory over the next five years. These drivers are expected to fuel growth in the Automotive Cyber Security Market during 2015-2025."[17]

[17] "Automotive Cyber Security Market Forecast 2015–2025: The Secure Connected Car." Auto2x. N.p., n.d. Web. 26 Apr. 2017.

Due to the rise of connected vehicles, the automotive cybersecurity industry is growing rapidly for the past few years. Many companies are formed aiming to address cybersecurity issues for connected vehicles and raised millions of investments funding. Many of the big names in this field are from Israel.

As mentioned in previous sections, securing a connected vehicle requires a comprehensive approach covering multiple levels of vehicle operation. The following chart illustrates various aspects of securing a connected vehicle.




Internet Security: This is the same type of security service needed by all types of businesses, and as such, many companies provide security solutions for businesses by using firewall, installing antivirus software, deploying Virtual Private Network (VPN), managing

access control and policy. AVG, Kaspersky, Cisco, Norton are some of the big names in this field.

Internal Network Security: There are also many companies aiming to secure vehicles' internal network by using Intrusion Detection and Prevention System (IDS/IPS) and Deep Packet Inspection (DPI). TowerSec, Argus Security, Arilou, Symantec and Cycuro offer products at this level.

ECU Security: Karamba Security is a company that offers products to secure individual ECUs. Their products would be most likely sold to OEMs and Tier 1 suppliers to harden their ECUs.

## 3.2 Target Market Segment Strategy

And lastly, vehicle gateway security is the segment I would like to focus on. Vehicle gateway device is the bridge between a vehicle's internal network and the outside network, and as such is the first attack surface exposed to hackers. Under this category, there are two sub-focuses: security of infotainment systems and security of aftermarket telematic devices.

### 3.2.1 Market Needs

Infotainment systems and telematic devices are the most common gateway devices. Infotainment systems are usually directly controlled by car manufacturers and are highly integrated into vehicles. BlackBerry owned QNX operating system is a big name in the infotainment sector. QNX runs in more than 60 million vehicles as of the end of 2014, with over

40 automakers relying on the software platform, accounting for 47% of the market share, with its closest competitor as open-sourced Linux with about 20% of market share.[18] QNX Telematic devices are mostly installed on vehicles as aftermarket add-ons and are sold by third party service providers. These devices are used in applications such as usage based insurance (such as Progressive Snapshot), asset monitoring (XIRGO Technologies), fleet management (such as Omnitracs and Verizon Telematics) and smart driving assistant (such as Automatic and Zubie).

Both infotainment systems and telematic devices need to have built-in security measures to counter outside attack. However, for us as a small startup company without connection and reputation in the field, it would likely be very hard for us to secure a contract working directly with BlackBerry or automakers. We will likely have more success helping aftermarket telematic device makers in securing their products in the beginning.

While passenger vehicles are recently becoming connected thru services like OnStar, Uconnect, mBrace, Audi Connect etc., commercial trucks have been more pervasively connected thru satellite or cellular for telematics, fleet management and engine management applications for quite some time, therefore providing more avenues for attackers.[19]

### 3.2.2 Market Trends

Hour of Service (HOS) rules were put in place by the Federal Motor Carrier Safety Administration (FMCSA) to limit how long a commercial vehicle driver could operate legally

[18] Muoio, Danielle. "Blackberry Is Quietly Trying to Make a Comeback - but Not with Phones." Business Insider. Business Insider, 11 Jan. 2017. Web. 26 Apr. 2017.
[19] Heavy Vehicle Cyber Security Bulletin. Issue brief. Alexandria VA: National Motor Freight Traffic Association, 2016. Web. 28 Mar. 2017.

within a period of time. Drivers are required to log their Record of Duty Status (RODS) on a paper logbook, and need to have the logbook available when requested by law enforcement.

There are many ways a driver can cheat the paper logbook. It is a fairly common practice among many owner-operators and smaller fleet drivers to use tricks such as pattern logging, shaving miles, dropping trips, using multiple logbooks, etc. to cut down their on-duty hours on the logbook.[20]

To make enforcement of the HOS more effective, FMCSA's final Electronic Logging Device rule was published on December 2015. The ruling requires all eligible commercial vehicles to be outfitted with Electronic Logging Devices (ELDs) by December of 2017. Electronic Logging Device is a telematic device that is connected to the commercial vehicle's CAN to track and record Hour of Service compliance, replacing the paper logbook. Cheating of HOS will be much hard since ELD device is connected directly to truck engine, recording hours automatically when the truck is driven.

ELD mandate is a highly controversial issue in the trucking industry, and most owner-operators and drivers from small fleets have strong resentment against the ELD mandate. Owner Operator Independent Drivers Association, or OOIDA has challenged the ELD mandate in superior court and lost the case in October of 2016. At the time of writing, OOIDA has just filed a petition with the U.S. Supreme Court asking the judicial branch to review its case against

[20] "Exposing Log Book Tricks." TruckersReport.com Trucking Forum | #1 CDL Truck Driver Message Board. N.p., 1 Jan. 2008. Web. 19 Apr. 2017.

electronic logging devices, claiming ELD mandate violate truckers' Fourth Amendment rights and constitute "warrantless searches" to "uncover evidence of criminal activity."[21]

### 3.2.3 Market Growth

Regardless of the reception and legality of the ELD mandate, the mandate will go into effect on December 18, 2017. According to my interview with some of the ELD service providers, many trucks out on the road are still not compliant yet. The market demand for the ELD compliant device is rapidly growing and we might even see a situation where supply does not meet the demand towards later part of the 2017.

## 3.3 Key Customers

The ELD mandate brought along a proliferation of companies making ELD compliant devices. I have included a table all fleet management companies that currently offer ELD solutions.

| | | |
|---|---|---|
| Apollo Solutions | ATS Fleet Management Solutions | BigRoad |
| Blue Ink Technology | Blue Tree Systems | CarrierWeb |
| Cartasite | Continental | Dispatching Solutions DriverTech |
| Eclipse Software | E-Log Plus | EROAD |
| Fleet Complete | FleetUp | Forward Thinking Systems |

[21] OOIDA Appeals to U.S. Supreme Court on ELD Mandate Lawsuit. OOIDA. Owner-Operator Independent Drivers Association, 13 Apr. 2017. Web. 18 Apr. 2017.

| | | |
|---|---|---|
| GeoSpace Labs | Geotab | Gorilla Safety |
| GPS Insight | HOS 247 | HOS Reporter |
| Hutch | iGlobal | ISE Fleet Services |
| J.J. Keller | KeepTruckin | Konexial |
| Load Logistics | M2M in Motion | MiX Telematics |
| Mobile Warrior | Nero Global Tracking | Omnitracs |
| Pedigree Technologies | Pegasus TransTech | PeopleNet |
| Quartix | Rand McNally | Simple Truck ELD |
| Spireon | Teletrac Navman | Telogis |
| Zed Connect | Zonar | |

I have spoken with three of my potential customers, one small, one medium, and one large companies from the list above to find out more about their offerings and the current steps they have taken to ensure security on their products.

### *Chris Riegel with Blue Ink Technology*

Blue Ink Technology is one of the ELD vendors that sells adapter that plugs into diagnostic port of trucks and tracks Hour of Service compliance. The company has about 25 employees, and used to be in the business of GPS fleet tracking service. I was informed by Chris who works there. He told me most trucks do not yet have them installed, and in fact there is a strong sentiment and hostility towards FMCSA's ELD push. Many fleets are still waiting till the last minute to install ELD devices in their trucks. On the other hand, ELD vendors do not have

enough stocks in inventory to supply the market demand towards the end of the year before mandate goes into effect.

Their product utilizes Bring Your Own Device(BYOD) approach. It is a simple dongle that "can be installed in seconds with no tools required. Simply plug it into the cab's 6-pin or 9-pin diagnostic port near the driver's foot well." It works by using Bluetooth communication to transmit vehicle data to a smartphone or tablet with cellular service running their App to track hour-of-service compliance. Chris told me when the team initially designed the device, they considered the possibility of hackers attacking the device, and intentionally made the device at a hardware level simple and therefore presents very little attack vectors. Software update can only be performed through the use of physical USB connection, so unless someone has physical access to the dongle, they cannot modify the firmware of the dongle. Furthermore, Chris told me the dongle is at a hardware level not able to send packets on the vehicle CAN bus, making a replay attack impossible.

A small ELD provider like Blue Ink Technology's products featuring limited functionalities do not have enough attack vectors for cybersecurity to be a big concern. Therefore, companies like this are not our primary target customers.

*Ryan Johns with KeepTruckin*


KeepTruckin is a startup based in San Francisco backed by Google Ventures. The company raised $2.3 Million in seed funding in 0213 and $8M in Series A funding from Index Ventures. Currently it has around 100 employees. I spoke with the CTO Ryan John.

Their website shows the device as a simple plug and play solution that works together with the driver's smartphone. This led me to believe KeepTruckin's offering is similar to Blue Ink Technology's offering where there is not many attack vectors present. Contrary to what I believed, Ryan told their device has superior computation ability, large memory and storage as well as GPS hardware built-in, when compared to competing products. In addition, KeepTruckin is developing a third iteration of the hardware that has built-in cellular connection using AT&T's network so the device can access the outside network and perform a OTA update without needing a smartphone connection. The powerful hardware and connected nature of their product means there are more attack vectors available for hackers to exploit.

Ryan told me most of the resistance against ELD push is by owner-operators and smaller fleets. The drivers there have more wiggle room and is more likely to cheat the Hour of Service regulation. Larger fleets are more in favor of the ELD push because it levels the playing ground for them. Majority of KeepTruckin's customer base are owner/operators and small to medium sized fleets ranging from 30 to 500 trucks. Many fleets like the self-service model KeepTruckin'

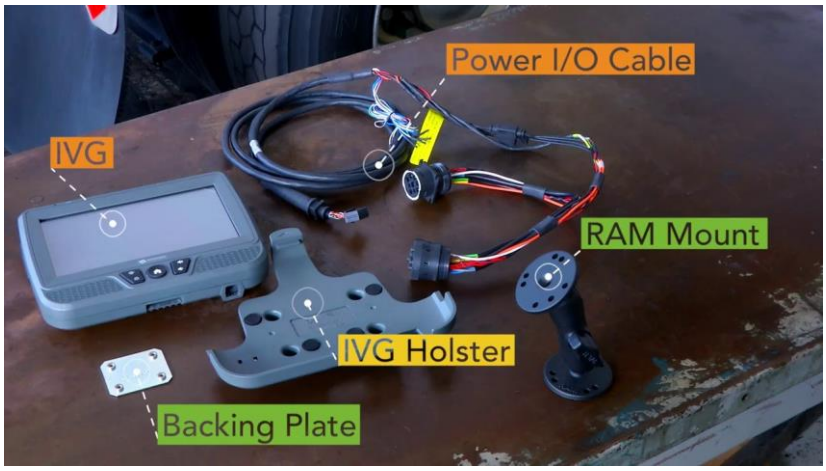
provide, cutting out dealing with salesperson and complicated customization out of the equation. Almost none of the customers see telematics device security as a priority while making purchase decision. Larger fleets sometimes would ask for their data center security to ensure fleet data is kept private (this is later brought up in my interview with Omnitracs as well). KeepTruckin uses Amazon Web Service to handle backend service. Ryan also stated inventory concern towards end of 2017 when all the owner/operators make purchase at last minute to stay compliant. KeepTruckin is ramping up the production of devices and increasing inventory level to face the market demand at the end of the year.

Towards the end of the interview, I brought up to Ryan that I am interested in pursuing a business in consulting security solutions for Electronic Logging Device manufacturers and he said while he does not have much experience in cyber security consulting, he could see a need at his company for service like that. It is a validation of my business idea.

A fleet management provider company like KeepTruckin has more employees and capacity to develop more complicated software and hardware for more advanced fleet management functionalities than smaller competitors. The increased software and hardware complexity adds more attack vectors that could be exploited by attackers. KeepTruckin does not currently hire outside security firm for consulting service and product, but they could benefit from outside security expertise and software to secure their products.

*Sharon Reynolds with Omnitracs*

Omnitracs LLC is one of the largest player in trucking fleet management service and is the original company that started this technology all the way back in 1988, said Sharon, the Chief Infomration Security Officer at Omnitracs. Most of Omnitracs' customers are medium to large fleets, while recently they are also selling to more smaller fleets and Owner/Operators due to the ELD requirement. Their latest flagship offering for fleet management, Intelligent Vehicle Gateway (IVG) replaces the previous flagship model MCP and provides simpler one device, one cable installation. It has built-in ELD functionality, along with many other standard features you'd expect from an industry leading ELD are available: logs, DVIR, messaging, navigation, engine diagnostics, etc. Users of the top shelf MCP models (110/200) will also recognize the more advanced capabilities that continue to be available with IVG such as in-cab scanning, tire pressure monitoring, dash cams. In addition, drivers can link their own smart phone to the IVG via Wi-Fi or Bluetooth, allowing them to perform certain tasks while away from the truck. A driver could send and receive dispatch messages, update trip progress, and even capture signatures or document images remotely from their phone. Also onboard is a voice command system. A future update will even bring Wi-Fi hotspot functionality, allowing drivers to connect



their personal tablet or phone to access Internet.[22] It is a fully-fledged fleet management computer that represents state-of-the-art technology in the industry.

Omnitracs works with a few external vendors for security testing in addition to conducting their own internal testing. I asked Sharon why they have a few different companies they use for security testing, and she told me that different security companies have different researchers with different strengths/weaknesses and by rotating thru these companies they could cover multiple aspects of their devices to ensure the security integrity. I asked for the names of the companies they work with, and she could not tell me due to company policy. When I asked whether Omnitracs' customers consider cybersecurity of telematics service when making purchase decisions, Reynolds said many larger fleets are concerned about fleet data privacy but not so much from a vehicle security aspect.

Omnitracs being a large privately owned company in this field has the resource to develop highly advanced and complex fleet management products. Their fully featured devices offer a lot of functionalities compared to offerings from smaller competitors, but that also provides more attack vectors for hackers. They do use a few outside security companies to audit their software to ensure cybersecurity integrity. The interview with Omnitracs's Chief Security Officer validates the need for cybersecurity service in fleet management industry, and leave me believe that Omnitracs could be one of my most important customers. Interesting to note, Omnitracs has just recently invested $60M in a truck platooning startup Peloton Technology as of April 5, 2017.

[22] Ratings, ELD. "Omnitracs IVG." ELD Ratings. Tandem Technology, 06 Apr. 2017. Web. 19 Apr. 2017.

### 3.3.1 Customer Acquisition

Generally speaking, there are two different types of fleet owners out there: smaller guys such as O/Os and small fleets who are reluctant to adopt new technologies and larger fleets who are willing to invest in technologies to increase profit margin and gain competitive edge against competitors.

My customers are the fleet management telematics providers such as KeepTruckin and Omnitracs. Their customers are commercial LTL and FTL truck fleets. One of the things brought up by both Omnitracs and KeepTruckin is many large fleets are concerned about data security associated with using telematics services. As another fleet management company Geotab puts it,

> "Telematics generates a vast amount of data, including a detailed history of vehicle and driver activities and operations. This type of data is extremely useful within an organization for controlling fuel and maintenance costs, increasing productivity and safety, and minimizing risk. Using telematics for accident reconstruction or benchmarking can generate even greater insight. Protecting that valuable data is essential. If accessed by a malicious party, there could be serious consequences, potentially jeopardizing customer accounts, schedules, shipments, location of assets, and personal information."[23]

[23] Nikonov, Gleb, Melanie Serr, Alex Sukhov, and Scott Sutarik. "Best Practices for Cybersecurity Management in Telematics." (2017): n. pag. Print.le

Telematics providers need to satisfy their customers demand by making sure the fleet data are secured properly from cyber-attacks. However, not many fleets are aware that not only their precious fleet data can be targeted by cybercrimes, but their trucks, the very core of their business assets can be targeted by attackers. Similar to how pharmaceutical industry advertises directly to consumers to ask their doctors about a medication, instead of to doctors themselves who have the ultimate power to prescribe a drug, we need to raise fleet managers' awareness of cybersecurity threat on their fleets. By demonstrating our ability to hack fleets thru onboard telematic devices, we can have these fleets to inquire and pressure the telematics makers to use our security products to safeguard their fleets.

### 3.3.2 The Right Customer

Comparing to their larger counterparts, smaller fleet telematics companies have less resources and expertise. They tend to develop products with less functionalities and system complexity, and therefore not having as many attack vectors than more complex units. In addition, they might not have the financial ability to purchase cybersecurity solutions from outside firms like us. Eventually this may change as the cybersecurity become a necessity instead of an option in connected telematics services, but for the time being we should focus on selling to larger companies with the financial ability to spend on cybersecurity solutions.

## 3.4 Competitors

Automotive cybersecurity is an emerging market that has only been around for about five years. It is rapidly evolving, with some major players already forming quickly standing out from the rest. Some Tier One suppliers have already acquired promising startups in this field to secure their product offerings.

Tel Aviv, Israel is the home to three major cybersecurity firms dealing specifically with automotive cyber threats: Argus, TowerSec and Arilou.[24]

Argus Cyber Security secured $4 Million in Series A funding in 2014 and $26 Million in Series B funding in 2015. It is the most high-profile startup in automotive cybersecurity space right now. Their patent-pending in-vehicle network protection is relatively straightforward on the surface: it allows sections of a vehicle to be contained. As soon as their product detects suspicious activity, it contains and blocks it without sectioning off the system being attacked, so the hacker's code simply can't access other bits of the car, explains co-founder and CEO Ofer Ben-Noon.[25] Argus has a very comprehensive suite of products that addresses most of automotive industry's cybersecurity needs, providing security for gateway devices, in-vehicle network and ECUs altogether.

TowerSec (acquired by Harman Industries in March 2016) offers two products: ECUShield and TCUShield. They are both based on Intrusion Detection and Prevention System (IDS/IPS) that monitors in-vehicle network messages and blocks out abnormal messages that could indicate an attack. Harman is a top Tier 1 supplier providing connected car solutions to

[24] Fox-Brewster, Thomas. "Meet The Former Israeli Cyber Soldiers Hoping To Stop Hackers Causing Car Crashes." Forbes. Forbes Magazine, 05 Sept. 2014. Web. 27 Apr. 2017.
[25] Ibid

Volkswagen Group, Mercedes, BMW, Fiat Chrysler Automobiles, Jaguar Land Rover, Toyota and more. They can leverage this as a huge competitive advantage by integrating the security products right into the connected car solutions and sell it as a whole package to their existing customers, meeting all their demands at once without having to shop from other competitors for a separate cybersecurity solution.

Established in 2012, Arilou Cyber Security (acquired by NNG LLC in August 2016) offers Parallel Intrusion Prevention System (PIPS) and Intrusion Detection and Prevention System (IDPS). Similar to Harman, NNG is a leading supplier in automotive technology sector. They can easily integrate the Arilou's security products into their existing product portfolio, offering their customers a comprehensive connected car solution.

Karamba Security is yet another Israeli company working in the automotive cybersecurity field. Their product Carwall is an Anomaly Detection System implemented in ECUs that monitors ECU's unique call graph based on factory settings. When a hacker tries to manipulate a process, the process will be outside of the call graph and Carwall blocks it when that happens.

> "Carwall hardens the ECU's software runtime environment to detect and prevent all attempted attacks. Carwall doesn't fix the security bugs in your code; it prevents their exploitation by permitting only operations that comply with your ECU's factory settings to run."[26]

OnBoard Security (a subsidiary of Security Innovation based in Wilmington MA) offers a product called Aerolink. Aerolink is a software library that secures DSRC communication in

[26] "Carwall — Autonomous Security for Autonomous and Connected Cars." Karamba Security. N.p., n.d. Web. 27 Feb. 2017.

connected vehicles. Aerolink has been selected to provide security and privacy for the 2017 Cadillac CTS. Renesas Electronics, a tier-one supplier that provides SOC for automotive OEMs has also included Aerolink in their R-Car V2X reference design.[27]

I have included a table on the next page summarizing some of my competitors in this market, listing their strengths and weaknesses.

[27] "Aerolink Security for Vehicles." OnBoard Security. OnBoard Security, Inc., n.d. Web. 27 Apr. 2017. <https://www.onboardsecurity.com/products/aerolink>.

| | Argus | Arilou (NNG) | Karamba | TowerSec (Harman) | Other non automotive focused cybersecurity firms |
|---|---|---|---|---|---|
| **Team Size (estimated)** | 40-45 | 10-15 | 15-20 | 25-30 | Varies from small independent firms to large multi-national corporations |
| **Financial Strength (estimated)** | Private company, $30M equity funding | Acquired by NNG for undisclosed price from shareholders, providing capital injection | Private company, $5M equity funding | Raised $3M in funding before acquired by Harman for $75M | Varies from small independent firms to large multi-national corporations |
| **Products and Services** | Gateway Security (both infotainment and aftermarket telematics), Internal Network Security, ECU Security | Gateway Security (both infotainment and aftermarket telematics), Internal Network Security, ECU Security | ECU Security | TowerSec's ECU Security and Gateway Security on top of Harman's 5+1 Cyber Security Framework | Products are mostly generic solution for IoTs and Internet security, not necessarily adapts well for automotive applications |
| **Market Focus**[1] | Broad | Broad | Specific | Broad | Very generic and not automotive focused |
| **Comprehensive Solution**[2] | Yes, Argus claims its solution suites offer the most comprehensive and modular protection from car hacking in the industry. | Yes. The suite of solutions covers most of the security needs by OEM, Tier-1s and aftermarket manufacturers. | No. The company only focuses on securing ECUs and does not security solution at other levels. | Yes. Harman is a Tier-1 supplier to connected car components and with TowerSec's technology, they offer OEM's a one-stop shop solution | No. Product offerings most likely do not address specific automotive needs. |
| **Modular Approach**[3] | Yes, Argus claims its solution suites offer the most comprehensive and modular protection from car hacking in the industry. | Yes, the suite is designed to be platform agnostic and can be easily integrated in different environments. | Yes, Carwall is listed as "Operating System Agnostic", and will run on all processors, OSes and schedulers. | Yes. ECUShield does not require host redesign, and can be installed on any onboard ECU, telematics controller or infotainment system. | No. Product offerings most likely need to be extensively modified to fit automotive environments. |
| **Presence in Automotive Industry**[4] | Strong. It is the largest independent automotive cybersecurity company. | Strong. NNG provides OEMs and tier one suppliers navigation and connected car solutions. | Could not find any information on this one. | Very Strong. Harman is a leading Tier One supplier to automakers. | No direct tie to the automotive industries, however some do have extensive reputation in the security field |

Notes:

1. A company can be jack of all trades but master of none. By having a specific market focus, a company can excel in one specific product category and target their customers more effectively.
2. If a company offers a comprehensive solution, its client can have all their cybersecurity needs taken care of from the company without having to work with another company.
3. Modular approach means whether the product can be easily adapted into different environments without extensive modifications. Customizations and modifications tend to be costly and introduces bugs and hiccups.
4. The more presence a company has in the industry, the more competitive edge it possesses in customer loyalty and brand recognition.

# 4.0 The Next Step

## 4.1 Minimal Viable Product

Market analysis above shows it is the right time to enter the field of automotive cybersecurity. I have identified the market segment my startup company will focus on. Now the natural next step is to build a minimal viable product to validate the company can indeed provide a security solution for our identified customers. In our case, the minimal viable product can be a demonstration of an attack on one of our customers' fleet management telematic unit, and potentially a software solution that can be implemented on their product to mitigate the attack.

## 4.2 Team

My background is in entrepreneurship and business development, and I do not possess the technical skills to build the minimal viable product. However, I have been doing extensive research on automotive cybersecurity and trucking industry for my senior thesis paper at Hampshire College. I am currently in the process of looking for technical co-founders to join the company, working with me together to bring the MVP to our future potential customers.

## 4.3 Location

Many of our competitors are based in Israel. I suspect the most advantageous location for our company would be in Michigan. The following reasons listed by Detroit Regional Chamber confirms why Michigan is the best place for this company.

- Since 2010, Michigan announced more than $23 billion in new automotive OEM and supplier investments, more than any other state or province in North America.

- In 2014, Michigan's motor vehicle-related GDP was $36.9 billion while Indiana, Ohio and Texas' combined motor vehicle-related GDP equaled $38.9 billion.
- The state is home to 60 of North America's top 100 automotive suppliers.
- 12 assembly plants manufacture 28 cars and trucks in Michigan, producing more vehicles than any other state — more than 20 percent of all U.S. production
- More than 46,000 automotive manufacturing jobs have been added since 2009, more than any other state.
- Michigan is home to 375 automotive R&D centers, 120 of which are foreign-owned.
- The state has 15 universities and colleges with nationally ranked undergraduate engineering programs; and more than 650 automotive-focused programs at the post-secondary level.
- Over 90,000 engineers are employed in Michigan, a higher concentration than any other state.
- Michigan is No. 1 in patents granted for vehicle, navigation and relative location data processing.
- Michigan is one of seven states that have passed laws related to autonomous vehicles, while also leading the nation in connected vehicle projects (49) in 2015.[28]

## 5.0 Conclusion

The exploitation of Jeep Cherokee's demonstrated by Charlie Miller and Chris Valasek showed automakers and general public that car hacking is no longer a distant threat, but an immediate public safety concern affecting millions of new cars.[29] The time is right for entering the automotive cybersecurity market due to rapid market growth of connected automobiles. The approach to automotive security should be holistic and multi-layered. The focus of my future company will be on safeguarding the bridge between vehicle's internal network and the outside

[28] "The Auto Industry in Michigan." Detroit Regional Chamber. Detroit Regional Chamber, n.d. Web. 27 Apr. 2017. <http://www.detroitchamber.com/econdev/chamber-initiatives/michauto-universal-name/the-auto-industry-in-michigan/>.
[29] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired. N.p., 21 July 2015. Web. 14 Mar. 2017.

world, and specifically aftermarket telematic devices. The vision for the company is to become the leading industry expert on automotive security, working closely with OEMs and Tier One suppliers to ensure the safety of future connected automobiles.

## 6.0 References


- Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired. N.p., 21 July 2015. Web. 14 Mar. 2017.
- Strohm, Mitch. "9 Most Hackable Cars." Bankrate. N.p., 21 Mar. 2017. Web. 16 Apr. 2017.
- Fox-Brewster, Thomas. "Meet The Former Israeli Cyber Soldiers Hoping To Stop Hackers Causing Car Crashes." Forbes. Forbes Magazine, 05 Sept. 2014. Web. 27 Apr. 2017.
- Kalyani, Darshan. Fleet Telematics Systems in the US. Rep. no. OD4546. N.p.: IBISWorld, 2017. Print.
- Simonite, Tom. "Your Future Self-Driving Car Will Be Way More Hackable." MIT Technology Review. N.p., 16 Mar. 2016. Web. 10 Dec. 2016.
- Overly, Steven. "What We Know about Car Hacking, the CIA and Those WikiLeaks Claims." The Washington Post. WP Company, 08 Mar. 2017. Web. 09 Mar. 2017.
- Toews, Rob. "The Biggest Threat Facing Connected Autonomous Vehicles Is cybersecurity." *TechCrunch*. N.p., 25 Aug. 2016. Web. 10 Dec. 2016.

- "Connected Car Security and the Need to Replace CAN with Ethernet." Innovasic. N.p., 19 Aug. 2015. Web. 26 Feb. 2017.
- Bray, Hiawatha. "After Car Hack, Internet of Things Looks Riskier." The Boston Globe. BetaBoston, 3 Aug. 2015. Web. 26 Feb. 2017.
- Vanian, Jonathan. "Automobile Manufacturers Form Cybersecurity Information Sharing Hub." Automobile Manufacturers Form Cybersecurity Information Sharing Hub | Fortune.com. Fortune, 15 July 2015. Web. 30 Apr. 2017.

- Toews, Rob. "The Biggest Threat Facing Connected Autonomous Vehicles Is cybersecurity." *TechCrunch*. N.p., 25 Aug. 2016. Web. 10 Dec. 2016.
- Baunfire.com, Spark CMS by. "Frequently Asked Questions." Open Alliance. Open Alliance SIG, n.d. Web. 19 Apr. 2017.
- Yoshida, Junko. "Ethernet Backbone in Car: Hype or Reality? | EE Times." EETimes. N.p., 6 Aug. 2013. Web. 26 Feb. 2017.

- Foster, Ian D., et al. "Fast and Vulnerable: A Story of Telematic Failures." WOOT. 2015.
- Greenberg, Andy. "Hackers Hijack a Big Rig Truck's Accelerator and Brakes." Wired. Conde Nast, 02 Aug. 2016. Web. 19 Mar. 2017.
- Thomas, India. "Special Report: Connected Trucks Published by Automotive World." Automotive World. N.p., 28 Nov. 2016. Web. 26 Apr. 2017.
- "Automotive Cyber Security Market Forecast 2015–2025: The Secure Connected Car." Auto2x. N.p., n.d. Web. 26 Apr. 2017.

- Muoio, Danielle. "Blackberry Is Quietly Trying to Make a Comeback - but Not with Phones." Business Insider. Business Insider, 11 Jan. 2017. Web. 26 Apr. 2017.
- Heavy Vehicle Cyber Security Bulletin. Issue brief. Alexandria VA: National Motor Freight Traffic Association, 2016. Web. 28 Mar. 2017.

- "Exposing Log Book Tricks." TruckersReport.com Trucking Forum | #1 CDL Truck Driver Message Board. N.p., 1 Jan. 2008. Web. 19 Apr. 2017.

- OOIDA Appeals to U.S. Supreme Court on ELD Mandate Lawsuit. OOIDA. Owner-Operator Independent Drivers Association, 13 Apr. 2017. Web. 18 Apr. 2017.
- Ratings, ELD. "Omnitracs IVG." ELD Ratings. Tandem Technology, 06 Apr. 2017. Web. 19 Apr. 2017.
- Nikonov, Gleb, Melanie Serr, Alex Sukhov, and Scott Sutarik. "Best Practices for Cybersecurity Management in Telematics." (2017): n. pag. Print.
- "Carwall — Autonomous Security for Autonomous and Connected Cars." Karamba Security. N.p., n.d. Web. 27 Feb. 2017.
- "Aerolink Security for Vehicles." OnBoard Security. OnBoard Security, Inc., n.d. Web. 27 Apr. 2017. <https://www.onboardsecurity.com/products/aerolink>.
- "The Auto Industry in Michigan." Detroit Regional Chamber. Detroit Regional Chamber, n.d. Web. 27 Apr. 2017. <http://www.detroitchamber.com/econdev/chamber-initiatives/michauto-universal-name/the-auto-industry-in-michigan/>.
- Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired. N.p., 21 July 2015. Web. 14 Mar. 2017.