UNDER THE HOOD: THE AUTOMOTIVE CHALLENGE

Inbar Raz
Argus Cyber Security, Israel

inbar.raz@argus-sec.com

ABSTRACT

In an average five-year-old car, there are about 30 different computers on board. In an average new car, there are double that number, and in some cases up to 100. That's the size of network an average SMB would have, only there's no CIO/CISO, and not even a part-time IT guy. We have no idea what's going on under the hood. To add to the complexity, there are between two and five different bus types in an average modern car. With different protocols and even different wiring, a modern car's network diagram is a CISO's nightmare.

There are many challenges in the automotive domain. From strict development regulations, through very long development cycles, to very little security by design in vehicles currently on the road – working in this domain is challenging, to say the least. But unlike almost anywhere else, this time the defence might actually have a fighting chance.

In this paper, we will share our experience in the automotive domain. We will explain the complexity of the playing field, share examples of the problems we've encountered, and talk about the challenges involved.

PART 1: THE PROBLEM

In the last few years, we've been hearing more and more about car hacking. A subject nearly unheard of until the turn of the decade, it has become a headline generator and a theme that makes it, through popular media, all the way to the homes of the users – the drivers.


ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

ANDY GREENBERG/WIRED

Figure 1: Chrysler recalls 1.4m vehicles. (Image: Wired Magazine.)

Unlike many other 'cyber' events – and I beg your pardon for using the 'C' word – car hacking has implications that extend far beyond our computers and the digital world, as clearly seen in Figure 1.

When a recall makes you take your car to the shop, losing anywhere from a few hours to an entire day, not to mention not having your car for that duration, that is something that makes an impact and can't be overlooked.

As far as perception goes, we understand that we use our cars to transport that which is most important to us – our families. Recent publications make it increasingly clear to us that hacking a car could potentially lead to some catastrophic results, but we don't always understand why that is. We are bombarded by vulnerability disclosures and pundits talking of doomsday scenarios, but no one bothers to explain why everything is the way it is.

Figure 2: Some of the suppliers for an Audi A5. (Image: Automotive News Europe.)

Cars are a complex product

Components

As consumers, we like to think about our cars as just another end product, much like we buy and think of groceries, office supplies, furniture, tools and everything else. Where there is a product, there is a manufacturer or producer, and we expect the manufacturer to be responsible for what they make.

Cars, however, differ significantly: they are made from hundreds of different hardware and software components, requiring a complex sourcing, integration and testing process. The car manufacturer – the OEM (Original Equipment Manufacturer) – is only directly responsible for a small part of them. Most of the car's components are manufactured by third parties, called Tier 1, 2 and 3 suppliers. The OEM is responsible for putting all the pieces into a final, singular product.

Figure 2 shows an example of some of the suppliers for an *Audi A5*.

Figure 3 provides an overview of the in-vehicle architecture of a car from over a decade ago.

In the architecture, there are *almost 60* different components – Electronic Control Units (ECUs) and others – and *almost 10* different network buses, using three different protocols (but we'll get to that soon).

Imagine, for a moment, that this were the network architecture of an office. With almost 60 endpoints and servers, and close to ten different network segments, this network architecture

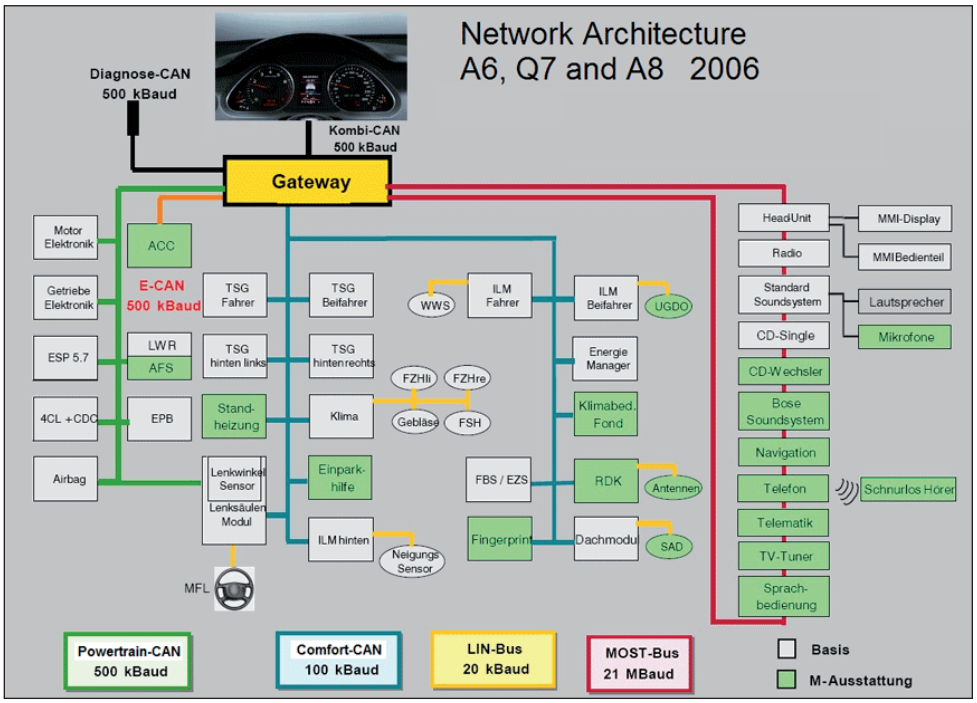

Figure 3: Overview of the in-vehicle architecture of a car from over a decade ago. (Image: EDN Network.)

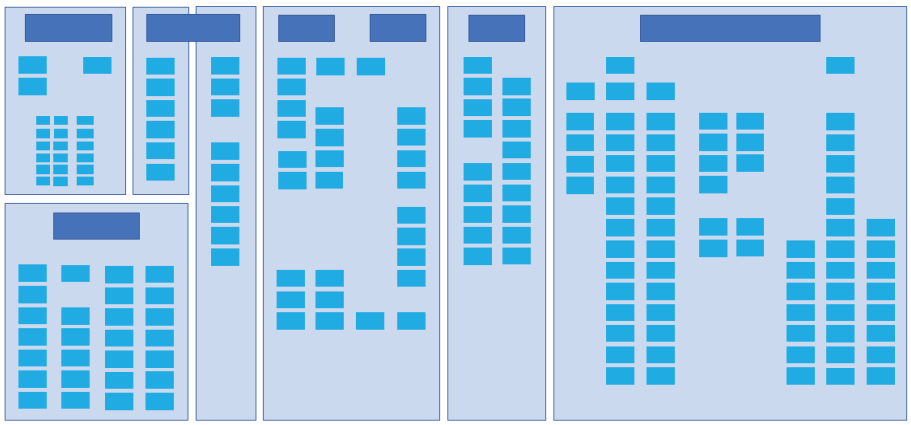

Figure 4: Architecture of a modern car. (Image: Argus Cyber Security.)

closely resembles that of a small-to-medium-sized business (SMB). It would be irresponsible for such a business not to have *someone*, even part-time, in charge of its network security, right? Someone who controls access rights, who picks the right security products for the networks, who looks at logs and alerts and responds to them. But in the vehicle, you have an Internet-enabled network that is completely unmonitored.

After establishing that a decade-old car has the complexity of an SMB, let's take a look, in Figure 4, at the newest available models.

While due to the sensitivity of the design we are unable to include network information, it is easy to see that this vehicle has close to 200 different components connected to its networks. That's more than three times the number of components that were in the vehicle from only a decade ago. Just think how complex a network this is!

Arguably, not all 197 components are of the same importance, or even complexity. On one end of the scale are components such as the Tire Pressure Monitoring System (TPMS) [1], shown in Figure 5.

These components don't do much, really. They are small sensors inside the tires that wirelessly transmit tire pressure data to a receiver that is connected to the CAN (Controller Area Network) bus of the vehicle, that's all. Even with such a limited function, TPMS components are nothing less than IoT devices, with firmware and all, directly connected to the in-vehicle network.

On the other end of the scale are the head units, or infotainment units, as shown in Figure 6.

These units are fully fledged computers running modern operating systems such as *Linux* and *Android*, running on multi-core CPUs and including multiple connectivity channels such as Wi-Fi, Bluetooth, Ethernet, USB and more. In short, a desktop PC.

Figure 5: Tire Pressure Monitoring System (Image: Shenzhen Shenyongtong Industrial Co., Ltd.)

Figure 6: Infotainment unit.

Networks

We've seen that the sheer number of connected components in a vehicle drives the complexity of the platform up. But it's not just the components.

Let's look at the different networks found in a modern vehicle, which are illustrated in Figure 7.

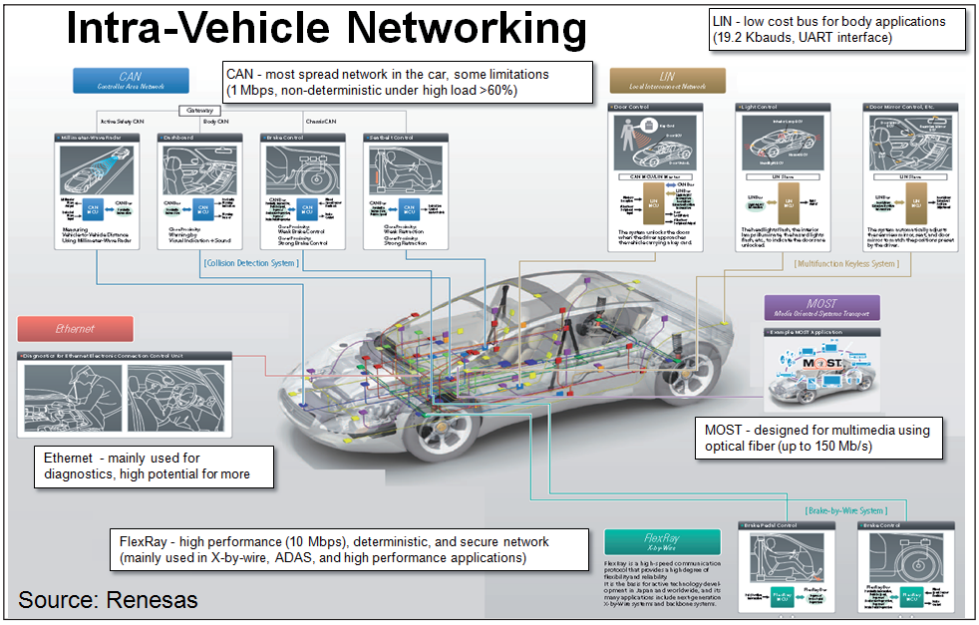

Figure 7: The networks found in a modern vehicle. (Image: Synopsys.)

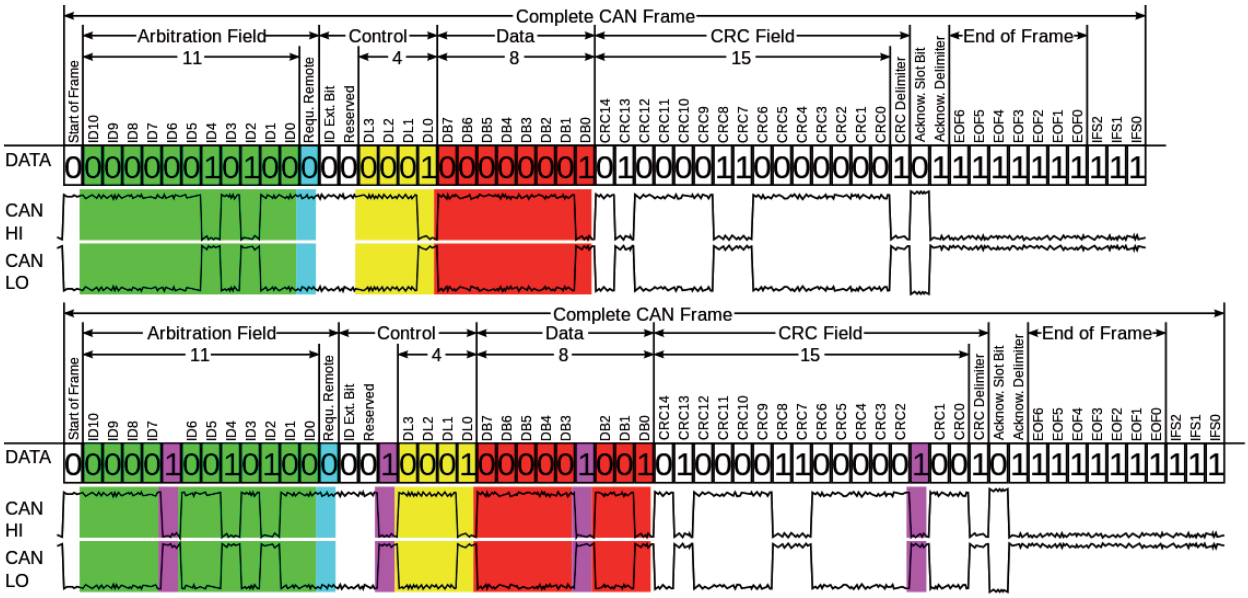

Figure 8: Overview of the CAN bus.

By far the most widely used network is the **CAN (Controller Area Network) bus** [2]. The CAN bus standard began back in 1983 when it was created by *Bosch GmbH*, coming to market in 1987. Connecting various vehicle subsystems, the CAN standard allows vehicle systems to receive input from sensors (or other systems), control actuators and other devices.

The **LIN bus** [3] standard has been introduced in recent years as a cheaper alternative to CAN bus, for use with non-critical subsystems such as air-conditioning and infotainment.

For multimedia applications, there's the **MOST (Media Oriented Systems Transport) bus** [4], a high-speed multimedia network technology for transporting audio, video, voice and data signals via either plastic optical fibre or electrical conductor physical layers.

FlexRay [5] supports high data rates (up to 10MB/s), multiple topologies and fault tolerance. It delivers the error tolerance and time-determinism performance requirements for x-by-wire applications (i.e. drive-by-wire, steer-by-wire, brake-by-wire, etc.)

Last but not least, automotive **Ethernet** [6] networks are similar to regular Ethernet networks, with the exception of a sometimes-different physical layer. Automotive Ethernet is used for diagnostics and high-volume traffic, such as LIDAR and video cameras, and Internet traffic, when available.

Since the most important bus is still the CAN bus, it is important to understand how it works. Figure 8 gives an overview.

The arbitration field of a CAN message holds the device ID, and also the priority level – the lower the number, the higher the priority and the more 'important' you are and get to trump lower-priority messages. However, there is no authentication in this protocol – and nothing prevents any ECU from sending messages while pretending to be another ECU.

Long production cycles

A car is a product with a very long production cycle. Roughly speaking, it takes about five years from design to roll-out, even before introducing factors like new technologies or design concepts. One of the main reasons for the prolonged process, in addition to the sheer scale of the project, creating requirements for all components, procuring and integrating them, is the demanding regulatory environment that exists in the automotive world – standards like Automotive SPICE (ASPICE) [7] and ISO 26262 [8], while making a big contribution to safety and reliability, significantly prolong the development cycles.

The end result of this is that, by the time a car is rolled out, the software it is running will have already become outdated. In a world where vulnerabilities are constantly being found in all types of software, this means that the software in a brand-new car is bound to include at least a few vulnerabilities that have already been published.

While vulnerabilities are constantly disclosed and repaired, the patches, needless to say, almost never make it to the car. Patching means changing the software and that would require repeating many of the tests in order to make sure it still functions properly and no adverse effects are caused by the bug fix.

There are very few manufacturers that can implement a software patch for vehicles on the road without having to issue a recall. Therefore, issuing a recall is a loss for all parties involved – vehicle owners lose time and money while the manufacturers have to deal with the negative effects on long-term plans and resource allocation.

The attack surface

In order to properly analyse a vehicle's attack surface, we must look at *every single one* of the ways in which the vehicle connects to the outside world – radio transmissions, physical

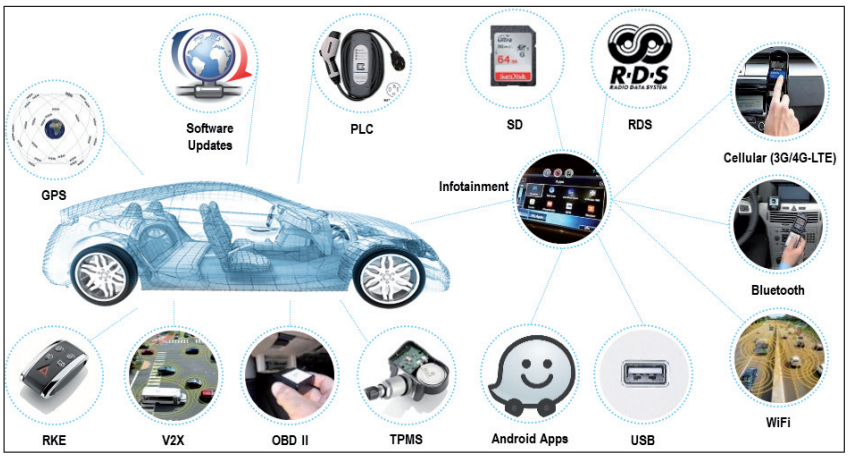

Figure 9: All the ways a vehicle connects to the outside world. (© Argus Cyber Security).

access, Internet connectivity and others are all candidates for examination and exploitation. Figure 9 provides an overview.

Every single one of these channels is an attack vector, and there is some sort of attack that can be carried out over it, whether for the purpose of Denial of Service, persistent code installation or even killing passengers. In addition to all these attacks on a deployed vehicle, there is always the looming *supply chain attack* vector where, knowingly or not, a supplier is the reason for malicious code being built into a vehicle component(s).

Industry vectors

It is no secret that the world is becoming more and more connected. The IoT revolution has brought Internet connectivity everywhere, setting a worldwide trend in consumer products in the process. Subsequently, the automotive industry jumped on the bandwagon and rushed to introduce connectivity to its products, before revisiting issues such as cybersecurity and domain separation. As a result, it is now possible to attack vehicles over the Internet and take full control over them. This has already been proven numerous times by researchers around the world.

According to published research, what has become evident is that many 'old-world' problems, seen and mitigated in the traditional ITSec world, still find their way into modern vehicles. And that's even before we account for 'new-world' problems which haven't been discovered yet.

PART 2: WAR STORIES

In part 1 we established that a car is a complex product whose design and manufacturing processes introduce some inherent security risks – many suppliers, increasingly complicated network architectures, etc. Given our knowledge of how connectivity works, the risks we've mentioned all make sense. In this section, we will show how many of the risks mentioned have already been exploited.

Academia

Academic research of connected vehicle vulnerabilities has been going on for well over a decade. As early as 2004, Wolf, Weimerskirch and Paar published a paper entitled 'Security in Automotive Bus Systems' [9].

In 2007, a paper entitled 'Securing Vehicular Ad Hoc Networks' [10] was published by Maxim Raya and Jean-Pierre Hubaux from the School of Computer and Communication Sciences, EPFL, Switzerland. In this paper, the academics discussed the concepts of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications and their potential security implications – concepts that are still not in full deployment.

A paper entitled 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' was published in 2011 at the 20th USENIX Security Symposium by researchers at the University of California, San Diego and the University of Washington.

More recently, a paper entitled 'Who Killed My Parked Car?' [12] was published by researchers at the University of Michigan. The paper discusses possible battery drain attacks on electric vehicles.

Numerous other research papers have been published including research into specific vulnerabilities and attack exploits of remote keyless entry systems, the CAN bus network, and more.

Security industry

Without a doubt, the work that had the most significant effect on how both the automotive and security industries look at automotive cybersecurity was the research published by Dr Charlie Miller and Chris Valasek.

Figure 10: Charlie Miller and Chris Valasek. (Images: Slideshare, Miller/Valasek.)

Their two-part work, 'A Survey of Remote Automotive Attack Surfaces' [13], published in 2014, and 'Remote Exploitation of an Unaltered Passenger Vehicle' [14], published in 2015, shook the automotive and cybersecurity worlds to their cores. The findings they published eventually led *Fiat Chrysler Automobiles* to issue a recall order for no fewer than 1.4 million vehicles.

Covered in popular media by notable publications such as *Wired Magazine*, the work of Dr Valasek and Mr Miller was a wakeup call for the industry and led to a renewed focus on security for the new, highly connected vehicles both already on the road and planned for the future. From car manufacturers to security researchers, automotive cybersecurity became a burning issue.

On cue, researchers all over the world began researching various vehicles, eager to uncover vulnerabilities in multi-ton, moving computers. It didn't take long for one researcher after another to disclose, publicly and privately, vulnerabilities found in connected vehicles and vehicle components.

Research didn't only focus on security *per se* – it's not only about how vulnerabilities can allow a hacker to crash a car. One fresh angle came in the form of research performed by two Romanian researchers – Stefan Tanase and Gabriel Cîrlig – who exposed data privacy issues originating in infotainment systems [15].

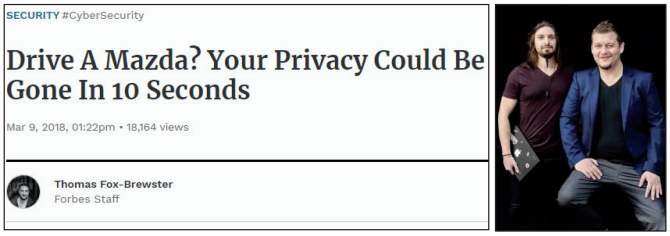

Figure 11: Stefan Tanase (right) and Gabriel Cîrlig (left) exposed data privacy issues originating in infotainment systems. (Right image: Forbes; left image: Stefan Tanase.)

When *Tesla* released its first vehicle, it was the sexiest, most advanced and most connected vehicle in the world. Naturally, it attracted a lot of attention from the security community, and sure enough, vulnerability research and disclosures started popping up.

At Defcon 23, Marc Rogers and Kevin Mahaffey gave a talk entitled 'Hacking the Tesla Model S' [16], in which they used physical access to the vehicle (together with some disassembly) to find vulnerabilities through which they were eventually able to install code that gave them remote control of the vehicle.

At Black Hat 2017, the Chinese *Keen Security Lab* presented 'Free-Fall: Tesla Hacking 2016' [17], showing how they hacked a *Tesla* remotely without any need for physical access.

Another piece of research, performed by the Norwegian company *Promon* and showcased at CeBIT 2017 [18], targeted the *Tesla* app on the driver's mobile phone and allowed the researchers to 'steal' the car.

But *Tesla* hasn't been the only target. Two recent cases showed more or less the same vulnerabilities involving infotainment systems:

- In April 2018, the Dutch *Computest* released a report entitled 'The Connected Car – Ways to Get Unauthorized Access and Potential Implications' [19], which showed numerous vulnerabilities in infotainment systems manufactured by *Harman* and installed in *Volkswagen* and *Audi* vehicles.
- In May 2018, the Chinese *Keen Security Lab*, after completing their work on *Tesla* vehicles, directed their research at *BMW*, eventually publishing the paper 'Experimental Security Assessment of BMW Cars: A Summary Report' [20]. This research showed that infotainment systems could be used as an initial attack vector.

Part of *Argus Cyber Security*'s offering includes services such as threat assessments, risk analyses and penetration testing. In every single one of the dozens of cases where *Argus* has performed a service, vulnerabilities have been found that enabled either remote code execution or CAN bus message injection. Not a single project ended in failure.

In addition to all these documented successes, there are rumours in the industry about an in-the-wild attack that was detected, mitigated and then silenced. We have no official corroboration for this, but we've heard it more than once.

Tinkerers and after-market tools

The fact of the matter is, you don't need a team of highly skilled researchers in order to hack a car. Dongles that connect to the vehicle's OBD-2 (onboard diagnostics) port can be bought for as little as $7 and operated with a mobile phone. Such devices allow users to send diagnostic messages, query error codes and reset alerts to the vehicle. As such, even an unskilled hobbyist could, intentionally or not, inflict damage on a car.

Figure 12: Dongles that connect to the vehicle's OBD-2 port can be bought cheaply and operated with a mobile phone. (Image: Amazon.)

There are, in fact, standards and specifications that can prevent some of these attacks. For example, AutoSAR SecOC [21] (Secure Onboard Communication), but they are not in wide use by automakers. When they are, there have been common implementation errors that have led to other, sometimes extremely damaging, vulnerabilities.

PART 3: WHAT'S NEXT?

Looking back at the examples mentioned, what's evident is that you don't need to have the resources of a nation state or be a

super hacker in order to successfully hack a car. Published research shows trivial problems recurring time and again where even old, unpatched software, is repeatedly deployed. In an industry that, by and large, lacks proper update procedures, such vulnerabilities remain out there. In fact, even some script kiddies are skilled enough to hack a car.

Let's look at the driving forces behind cyber attacks and compare those of the automotive world to those of the ITSec world we're already familiar with.

Cost of operation

	Automotive	ITSec world
Find vulnerability	Trivial and up	Trivial and up
Exploit	Low-medium	Harder every day

Let's explain the table a bit. As far as finding vulnerabilities goes, both the automotive and IT security worlds have shown that there are vulnerabilities that are trivial to find. However, there are also those vulnerabilities that require considerable research and extensive knowledge to uncover.

Regarding ease of exploitation, however, things look a bit different: exploiting vulnerabilities in the ITSec world is becoming harder and harder due to the massive volume of vulnerabilities and attacks already published. Such activities, in turn, drive the industry forward as mitigation technologies are in high demand. Consequently, being able to execute code remotely on a state-of-the-art platform often requires the exploitation of not one, but rather a chain of different vulnerabilities.

In the automotive world, however, there are almost no mitigation technologies in existence, even fewer actually on the road, and as a result, exploiting vulnerabilities is significantly easier.

Return on investment

	Automotive	ITSec world
Monetization	No (except ransomware, cryptomining)	Yes
Scale	Proven, not witnessed	Yes

As criminals use cybercrime primarily to make money, especially in cases where there is little to no chance of being caught, they have no reason to stop.

Large-scale criminal gangs are effective. For the most part, they aren't interested in small-time operations. They are looking for two things: monetization (how to make money out of something) and scale (making sure the potential return is worth their investment of time and risk).

In the ITSec world, both problems are solved. Cybercrime has evolved so rapidly that, for over half a decade, there has existed such a thing as 'crime-as-a-service' – people and organizations that will perform the nitty-gritty you need in order to pull off whatever illicit operation you want. In order to monetize on, say, ransomware, you outsource the malware writing, the email database rack-up and the email distribution (or the exploit kit installation) and the malware installation.

Once you've contracted someone, or some group, to do the work, the operation becomes quite effortless and you can kick back and watch as the malware infects more and more machines and the ransom money pours into your cryptocurrency account. Both monetization and scale are solved for you.

In the automotive world, however, things look completely different. With the exception of ransomware and crypto mining – two illicit activities that seem to be platform-agnostic – there is no good way to monetize the hacking of cars, yet. When it comes to scale, the *Jeep Cherokee* research by Miller and Valasek showed us a real-world vulnerability and exploit at scale, but the problems have since been reported and fixed. Further, to the best of our knowledge, there still hasn't been any in-the-wild automotive attack on a large scale. This is why we say it has been proven as possible, although not yet seen.

True, in the UK a criminal group was found using Near-Field Communication (NFC) relay attacks to steal cars and managed to get away with about £4M worth of them. But that was a singular event and, in any case, £4M does not constitute real scale. In comparison, Miller and Valasek estimated their attack surface to include between 292,000 and 471,000 vehicles, only to later realize that they caused a recall of 1.4M vehicles – now that's *real scale*!

And here's where we see how lucky we really are. In an almost unprecedented way, since the monetization of automotive attacks at scale is still far from easy, we, the 'defence', are actually ahead of 'offence'. Our job is to maintain that advantage lest cybercrime becomes widespread and a costly arms race develops.

The fact that there are many different technologies, standards and protocols in use means that the complexity of reaching scalable attacks remains relatively high. As automakers take different approaches to design and security, and given typical consumer behaviour – not yet in the age of autonomous fleets and on-demand mobility – monetization and scale still remain difficult to achieve.

But it won't last forever. Things are already starting to change. The introduction of car connectivity, vehicle-to-infrastructure and vehicle-to-vehicle communications is forcing the industry to agree on and comply with new standards and regulation (e.g. ISO/SAE 21434 [22] and UNECE TF on OTA/CS [23]), which ultimately will simplify things for adversaries. Similarly, the introduction of autonomous vehicles will create further opportunities for monetization (fleet hijacking, for one). New concepts for ECU consolidation will create a single network node that, if compromised, will lead a number of ECUs to be compromised, not just one, like today.

What we need to do

A modern vehicle has a network that's as complicated as that of a small or medium business, so we need to treat it like one. An SMB typically has a CISO, a security policy, a sysadmin – in short, someone to monitor the operations on the network.

Wouldn't it seem odd for an SMB today not to have one? Well, the same goes for in-vehicle networks. Failure to incorporate security into the network and its components falls nothing short of negligence.

That being said, there's no need to completely reinvent the wheel. The ITSec world has faced these problems in the past and there are lessons to be learned and best security practices, tools and methodologies to follow and use. We can't just import existing tools because they don't fit, but we can rebuild them for the automotive world, informed by the experience and wisdom gained in IT.

Just like in the ITSec world, there is no one solution for the problem – no silver bullet. The solution must be multi-layered and include prevention, detection and mitigation. In *Argus*' lingo, there are three layers:

1. **Prevent**: Make it as hard as possible to attack.
2. **Understand**: Know you are being hacked, and how, in real time.
3. **Respond**: Mitigate the damage and immunize the fleet in hours.

Security by design

The term 'Security/Secure by Design' has been around for a while now, and even has its own *Wikipedia* page [24]. It basically means that, in order for something to be properly secure, you have to start incorporating security into the earliest design stages. This is especially important in the automotive industry where development cycles can take well over five years. As such, security mishaps made in electric architecture or elsewhere are costly and time consuming to fix, if they can be remedied at all. But saying that is not enough. There is something missing.

Security is a profession, and having expertise in it is a function of how dedicated you are and how long you've been around – like other professions, it takes years, even decades, of experience to become a real guru. So, you need a security person doing your security, and therefore the complete saying should be 'Security by Design, done by Security People'.

But what if you don't have that sort of manpower in your company? Simple: get it from someone else. Collaborate with a security firm or rent their services. 'Security as a Service' is a totally acceptable practice.

Legislation

Car manufacturers are aware of the cybersecurity risks, but as long as there are no legally binding regulations, it will be a business decision whether to address those risks and how to address them. One of the ways this can change is by government regulation and legislation.

In the USA, government interest in automotive cybersecurity began as early as December 2013, with a letter [25] from US Senator Edward J. Markey to the CEO of *General Motors*, stating his concern and posing questions. Since then, various attempts at legislation have been made, some more successful than others. Michigan SENATE BILL No. 927 [26], for instance, attempts to make car hacking punishable by life imprisonment. The 'Security and Privacy in Your Car Act of 2015' (SPY Car Act) [27] was the first legislation to propose mandating vehicle cybersecurity in motor vehicles manufactured or imported for sale in the United States. More recent regulatory activity includes US H.R.3388 – SELF DRIVE Act [28], which unanimously passed the US House of Representatives in 2017 and the California Department of Motor Vehicles' new requirement for autonomous vehicles to have cybersecurity protections in place before they are certified for use in the State.

Similar guidelines and legislation have been passed and are under consideration in other regions of the world as well.

SUMMARY

Cars are very complex products and in-vehicle networks are as complicated as those of an SMB – they should be treated as such. The good news is that there's no need to reinvent the wheel – the ITSec world has solutions for most (if not all) the problems, and all that is left to do is make proper adjustments, adapt and rebuild these solutions for today's vehicles. There is no silver bullet, no single solution or product that makes the problem go away, and just like in the ITSec world, we need multiple solutions covering the entire ecosystem in a layered way.

Cybercriminals are carefully monitoring automotive vulnerabilities, gauging risk and return and waiting for an opportunity to monetize. Once it becomes clear how and where to capitalize, automakers will likely enter a fervent arms race with the cybercriminals and the number of attacks will spike. We are enjoying an unprecedented advantage of the defence over offence, and just like the kid with his finger in the dyke, it is up to us, the security industry, to hold down the fort, maintain and extend this gap for as long as we can. When the gap is finally closed, the floodgates will open.

REFERENCES

[1] Tire pressure monitoring system. https://en.wikipedia.org/wiki/Tire-pressure_monitoring_system.

[2] CAN bus. https://en.wikipedia.org/wiki/CAN_bus.

[3] Local Interconnect Network. https://en.wikipedia.org/wiki/Local_Interconnect_Network.

[4] MOST Bus. https://en.wikipedia.org/wiki/MOST_Bus.

[5] FlexRay. https://en.wikipedia.org/wiki/FlexRay.

[6] BroadR-Reach as an example. https://en.wikipedia.org/wiki/BroadR-Reach as an example.

[7] Automotive SPICE Process Assessment / Reference Model. http://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf.

[8] ISO 26262. https://en.wikipedia.org/wiki/ISO_26262.

[9] Wolf, M.; Weimerskirch, A.; Paar, C. Security in Automotive Bus Systems. http://www.weika.eu/papers/WolfEtAl_SecureBus.pdf.

[10] Raya, M.; Hubaux, J.-P. Securing Vehicular Ad Hoc Networks. https://koala.cs.pub.ro/redmine/attachments/70/JCS275.pdf.

[11] Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive Experimental Analyses of Automotive Attack Surfaces. http://www.autosec.org/pubs/cars-usenixsec2011.pdf.

[12] Kyong-Tak Cho, K.-T.; Kim, Y.; Shin, K. G. Who Killed My Parked Car? https://arxiv.org/pdf/1801.07741.pdf.

[13] Miller, C.; Valasek, C. A Survey of Remote Automotive Attack Surfaces. https://ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf.

[14] Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. http://illmatics.com/Remote%20Car%.pdf.

[15] Fox-Brewster, T. Drive A Mazda? Your Privacy Could Be Gone In 10 Seconds. Forbes. https://www.forbes.com/sites/thomasbrewster/2018/03/09/mazda-privacy-hack-via-usb/#4e2b8504d0c3.

[16] Rogers, M.; Mahaffey, K. Hacking the Tesla Model S. Defcon 23. https://www.youtube.com/watch?v=KX_0c9R4Fng.

[17] Chinese Keen Security Lab. Free-Fall: Tesla Hacking 2016. Black Hat 2017. https://www.youtube.com/watch?v=BLNyNWCFhlM.

[18] Lysemore Hansen, T. CeBIT 2017. https://www.youtube.com/watch?v=FY_tV7SF-zQ.

[19] The Connected Car – Ways to Get Unauthorized Access and Potential Implications. Computest. https://www.computest.nl/wp-content/uploads/2018/04/connected-car-rapport.pdf.

[20] Experimental Security Assessment of BMW Cars: A Summary Report. https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf.

[21] Specification of Secure Onboard Communication. AUTOSAR CP Release 4.3.1. https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_SecureOnboardCommunication.pdf.

[22] ISO/SAE AWI 21434. International Organization for Standardization. https://www.iso.org/standard/70918.html.

[23] UN Task Force on Cyber security and OTA issues (CS/OTA). https://wiki.unece.org/pages/viewpage.action?pageId=40829521.

[24] Secure by Design. https://en.wikipedia.org/wiki/Secure_by_design.

[25] Letter from US Senator Edward J. Markey to the CEO of General Motors. https://www.markey.senate.gov/documents/2013-12-2_GM.pdf.

[26] Michigan SENATE BILL No. 927. http://legislature.mi.gov/documents/2015-2016/billintroduced/Senate/pdf/2016-SIB-0927.pdf.

[27] Security and Privacy in Your Car Act of 2015. https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf.

[28] US H.R.3388 – SELF DRIVE Act. https://www.congress.gov/bill/115th-congress/house-bill/3388.