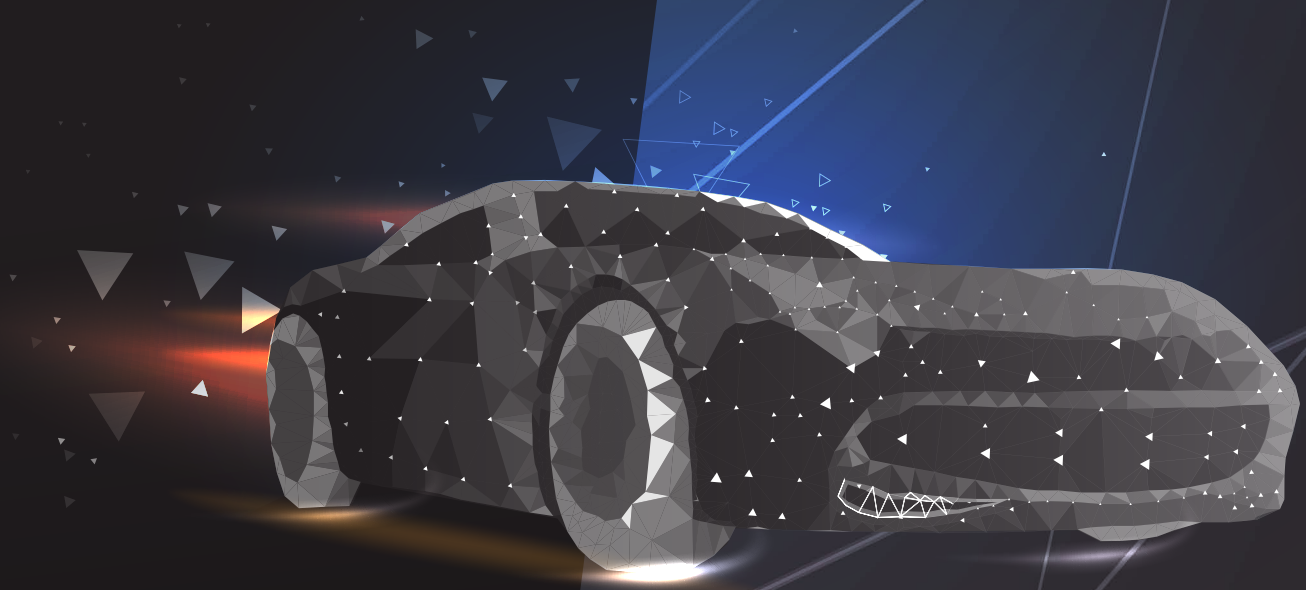
UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYBERSECURITY REPORT

2019

RESEARCH INTO
SMART MOBILITY
CYBER ATTACK
TRENDS



Upstream.auto
Securing Smart Mobility

TABLE OF CONTENTS

THE STATE OF AUTOMOTIVE CYBER-ATTACKS

Automotive cyber threats have become a popular topic in recent years. Despite much research on the various threats and risks on modern vehicles and many articles mentioning specific automotive attacks, the overall state of actual attacks and the threats demonstrated in reality still remain unclear. How many attacks have really occurred over the past decade? Are all the attacks on Smart Mobility orchestrated by White hat security researchers? What are the actual attack vectors as well as the damage done?

Visibility into these attacks should be the number one priority for anyone with skin in the game from auto makers to the consumers themselves.

Our research team has taken up the challenge of systematically classifying and analyzing multi-year data and summarizing the facts and figures into a first-of-its-kind report that covers everything from the types of attacks the industry has experienced, the popularity of the attack vectors, the most targeted sectors, and the impact the incidents have had on various stakeholders. Based on the trends emerging from the last eight years of documented attacks, we offer our predictions for 2019 and explain what sort of solutions are being employed to help minimize risks. This report's main goal is to try to answer the many questions surrounding cyber-attacks on the Smart Mobility ecosystem and provide a clear picture of the state of the overall industry.

As the term *connected automotive industry* covers more than just connected cars, this report takes a broader look across the whole connected ecosystem of transportation and Smart Mobility. This includes all connected digital transportation, from public to private, including but not limited to vehicles, car sharing, car rentals, trains, and even connected bicycles.

The aims of this report are simple. For stakeholders in the Smart Mobility world, this report will provide the essential knowledge necessary to understand the risks already targeting today's vehicles and roads. On top of this, it will allow OEMs, TSPs (Telematics Service Providers), car fleets, mobility providers and the industry as a whole to arm themselves against emerging cyber-attack trends lurking on the road ahead in 2019 and beyond.

AUTOMOTIVE GRADE IS NOT ENTERPRISE GRADE. IT'S MUCH BIGGER.

A single cyber hack can cost an automaker up to $1.1 billion today. The total cost for the industry, assuming current trends continue, could reach $24 billion by 2023, at which time Juniper Research predicts the number of connected vehicles to reach 775 million.

Our researchers looked at more than 170 documented incidents that were either published online by journalists and reporters, or by security researchers themselves between 2010 and November 2018. For each incident, our methodology was clear. We looked at the target company, the type of organization, the attack vector used, the damage done, and how the attack was achieved (whether through a physical attack, wireless, long-range or other). A full list of documented attacks can be found at www.upstream.auto/research/automotive-cybersecurity.

These cases are not a complete snapshot of all the threats and attacks that have happened during this time, as many were not published or flew beneath the public radar.

It's easy to look at the graphs, charts, and reported incidents and miss the gravity of this data. After all – under 200 incidents in a decade, and 60 in 2018 doesn't seem like a cause for concern. **Doing so would ignore the vast difference between Smart Mobility and any other industry.**

The world of IT spends a huge amount of resources on cyber-security, and there are hundreds of thousands of companies seeing an increasing amount of risk each year. This risk can be devastating to their business, damaging public image or reputation, and losing money or customer data. There is no doubt that the world of automotive is dramatically smaller. Instead of hundreds of thousands of corporations, you might see dozens of OEMs, and many thousands of fleets and businesses that sell third-party products of services. The impact however - is much greater, both in terms of risk, and ripple effect.

In the well-known Jeep Cherokee attack[1], researchers were able to remotely stop the engine of a vehicle while it drove down a busy highway. **This was one hack, on one vehicle, and yet it led to Fiat Chrysler being forced to recall 1.4 million vehicles of 7 different models**[2], which is about 50% of the cars they had sold that year in the US.[3] Furthermore, as the hack was achieved through the Harman infotainment system, it's easy to see how the risk could spread to dozens of other makes and models.

The financial impact is immense. If one individual recall costs $400[4], a recall of 1.4M vehicles would cost a business roughly $560 Million. That's before we get to brand damage, lawsuits or public image impact, known in many cases to double the size of the financial hit.[5] A single cyber incident can therefore add up to a cost of over $1.1 billion.

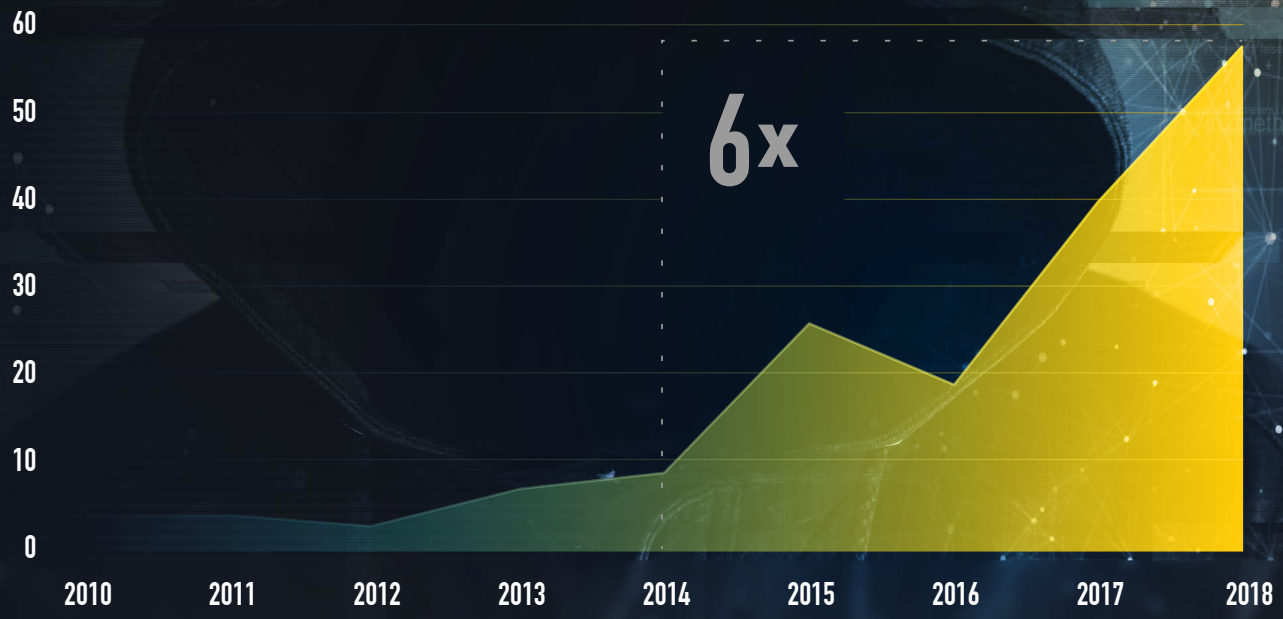
What will be the financial impact in 5 years? According to Juniper Research, 775 million consumer vehicles will be connected via telematics or by in-vehicle apps by 2023.[6] Additional research predicts that by 2020, 98% of new cars will be shipped connected.[7] Imagine an average OEM that sells around 2M cars per year today, in 5 years it will have 10M connected cars on the road. That means that a single incident will impact roughly 10M connected vehicles of one OEM. Assuming 3 major cyber incidents that requires massive recalls like in the case of the Jeep Cherokee incident, the total financial impact to the automotive industry could reach $24 billion annually by 2023.

Outside of financial risk, it's essential to recognize that **this kind of attack is a real-life example of an existing threat towards human life**. When you consider that one hack could take the lives of not just a driver and their passengers, but also pedestrians, bystanders, and other vehicle drivers on the road – you begin to see the actual impact of one notch on a graph.

> *"In today's connected vehicles, safety and security are one and the same."*[8]
>
> *GM President Dan Ammann*

RAPID GROWTH OF CYBER-ATTACKS ON THE CONNECTED AUTOMOTIVE INDUSTRY / 2010-2018

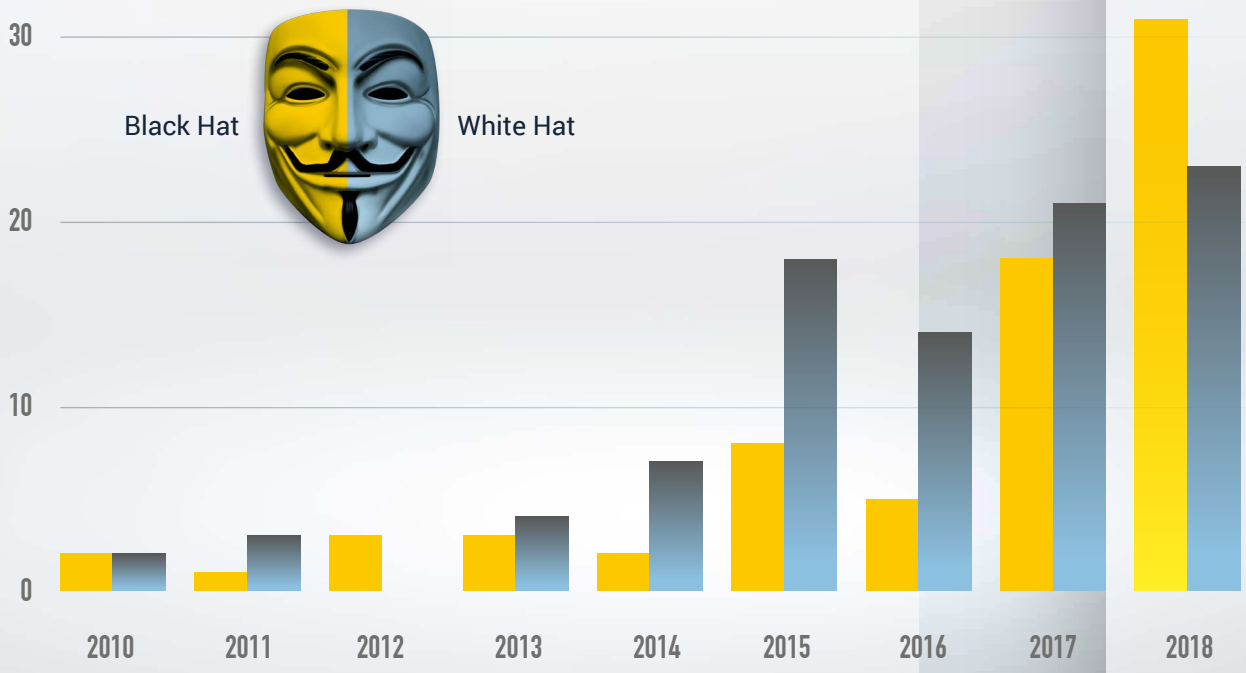
Reported automotive cyber-attacks by year



Source: Upstream Security

THE TABLES HAVE TURNED- BLACK HAT ATTACKS EXCEED WHITE HAT IN 2018

Cybercriminal attacks (Black hat) vs research-based hacks (White hat) by year



Source: Upstream Security

WHICH HAT DO YOU WEAR?

The dichotomy between Black hat and White hat attacks has long been a known distinguisher between research-based hackings to uncover and warn companies from vulnerabilities, a.k.a. White hat, and those triggered by cyber-criminals looking to cause damage or reap a ransom, a.k.a. Black hat attacks.

While White hat attacks may uncover significant vulnerabilities that should be calls for action, research-based attacks do not have malicious intent. White hat attacks can still cause financial damage or problems for a brand. However, for many companies, the warnings they receive from researchers or even technologically capable consumers are actually helpful to their security optimization and improvement. Connected car ecosystems are dynamic environments that often change and are subject to continuous updates and improvements, meaning blind spots and gaps are common.[9] The infamous Jeep Cherokee case was implemented by security researchers, as are many other high-profile cases. This could understandably lead many people to believe that the majority of attacks are White hat – and without malicious intent. However, the data paints a different picture.

IN THE SPOTLIGHT:

BLACK HAT ATTACKS

Tesla Cloud Breach Through AWS Vulnerability

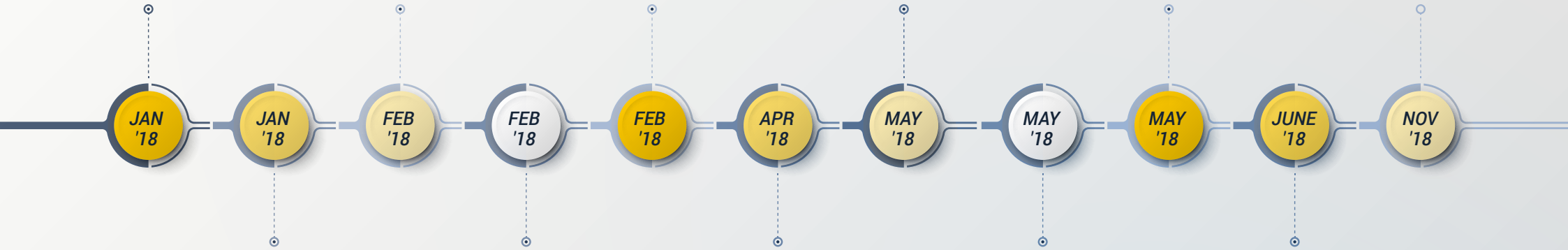
Complex hybrid data centers are increasingly causing security issues for Smart Mobility. In February 2018, hackers broke into a Tesla-owned Amazon cloud account and used it to 'mine' cryptocurrency. The breach also exposed proprietary data for the electric carmaker. The breach was possible because Tesla left credentials for an Amazon Web Services (AWS) account open to the public Internet. The scheme potentially exposed an Amazon simple storage service, also known as an S3 bucket which held Tesla telemetry, mapping, and vehicle servicing data.[11]

BLACK HAT TAKES OVER THE ATTACK LANDSCAPE

As shown in the chart above, **the Black hat attacks have not only been increasing year on year- they now exceed the White hat incidents.**

As hackers become more familiar with the components of connected vehicles, tools to attack this industry are easily found and cheap to procure. One example was seen when thieves in Winnipeg used a $5 device they bought over the internet to unlock a car using an electromagnetic pulse, stealing insurance papers that were left inside.[10] While this hack had limited damage, it is possible to imagine how effectively a device like this could be used on a fleet or even for a targeted attack on valuable documents. These kinds of attacks are real-world threats which are driven by real criminals. Once they breach a network or vehicles, the result will not be a written report.

MAJOR AUTOMOTIVE CYBER-INCIDENTS OF 2018



JAN '18 — Researchers uncover mobile malware that spoofed **Uber**'s Android app and harvested user passwords [12]

JAN '18 — Hacker arrested after fraudulently accessing **GoGet** car sharing servers, downloading customer identification information and riding for free [13]

FEB '18 — More than 100,000 sensitive customers documents are stolen from an unsecured Amazon S3 server owned by **FedEx** [14]

FEB '18 — Proprietary data belonging to **Tesla** customers is exposed as hackers break into an unsecured AWS server to 'mine' cryptocurrency [15]

FEB '18 — The data of 28,700 **Porsche** customers is accessed in cyberattacks targeting a contractor's data servers [16]

APR '18 — 14 million **Careem** taxi users experience personal data breach as cybercriminals hack into customer app accounts via backend servers [17]

MAY '18 — A vulnerability in **CalAmp** back-end telematics servers is exposed. This could enable the tracking of vehicle location, stealing of user information, and even remotely controlling critical components of multiple vehicles [18]

MAY '18 — Chinese security researchers discover 14 vulnerabilities in the onboard compute units of **BMW** cars [19]

MAY '18 — 50,000 users of **Honda** Connect App suffer a data breach after researchers discover two unsecured AWS S3 Buckets [20]

JUNE '18 — **Tesla** employee takes vengeance by changing manufacturing source code and exfiltrating sensitive data to outsiders [21]

NOV '18 — Spike in keyless entry attacks in Heaton, UK as burglars use a relay amplifier and transmitter to pick up a signal from the fobs, allowing them to steal vehicles [22]

Source: Upstream Security

EMERGING TREND:
DATA PRIVACY IN USED (CONNECTED) CARS

A new category of incidents has emerged throughout 2017-2018, triggered unintentionally by innocent users of the connected car. Driver Exchange Privacy Breaches.

There are two types of cases which fall under this category. First, previous car owners who had been connected to OEM services such as mobile apps or web portals find that they are still able to access the services, see data and in some cases even control car functions remotely.[23] Second, data and privacy breaches through car-sharing or car rental services where users have synced the infotainment systems with their own mobile devices.[24] The question is clear: **What happens to the data from a connected vehicle when the car moves on to a new owner?**

The Better Business Bureau has warned that connectivity through technology like Bluetooth is opening the door for identity theft and data privacy breaches in second-hand vehicles[25]. Going deeper, this kind of driver exchange data breach could expose a vehicles historical and current locations, access codes for a garage door, log-in information and any stored information in the vehicle infotainment center. The vulnerabilities of an accidental breach go in both directions, with a new driver at risk that a previous owner can still remotely access the vehicle, even months or years after it has been sold on.

> This new category of incidents can be just as devastating as Black hat attacks. While the individuals who find these vulnerabilities might not be intentionally malicious, in terms of data privacy, compliance and customer privacy – the consequences are the same. If drivers can access the data of a previous owner of their vehicle for example, your business may be liable under GDPR regulations. If a customer's mobile app allows them to see the payment details of the last person to rent the same vehicle, the fleet renting the car could find themselves coming under scrutiny from PCI-DSS, not to mention a potential lawsuit.

Black and White hat attacks have clear ownership behind them, but the burden of responsibility for this new category of driver exchange breaches is far less clear. Should owners take on the task of ensuring that their digital footprint is erased before they sell on their vehicle, the same way as they might for a smartphone? Or should it be OEMs and dealerships, ensuring that they disable access as well as restore factory settings before they make a sale? Even if this becomes the norm, who is responsible for deleting data from the cloud that remains accessible even after factory settings are restored on the car itself? Unfortunately, regulation has not yet caught up to provide answers to these important questions.

IN THE SPOTLIGHT:

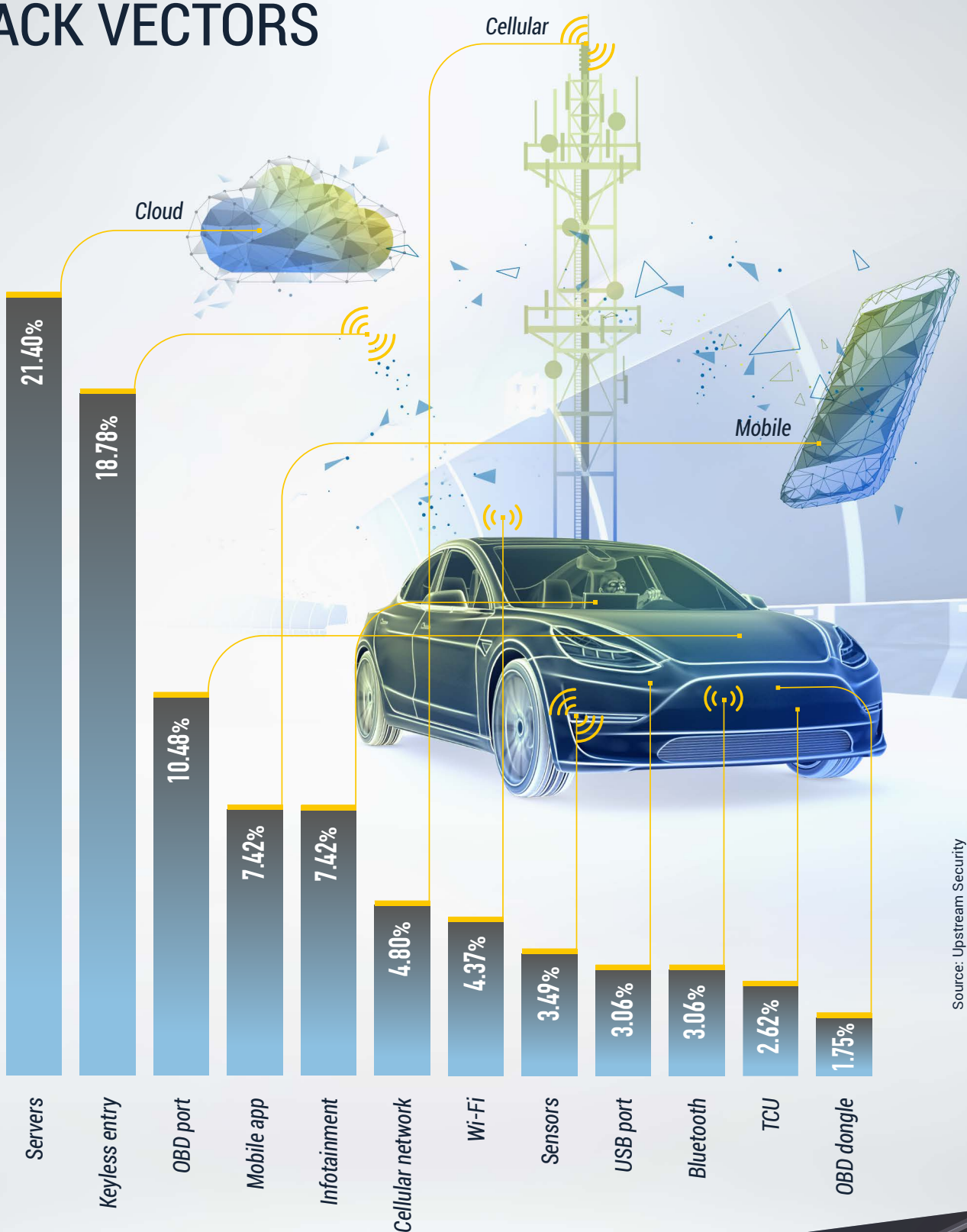
DRIVER EXCHANGE DATA BREACH PUTS PRIVACY AT RISK

In December 2017, Ashley Sehatti sold her 2015 Jetta to a Volkswagen dealership in California. After continuing to receive reports on the car's health and status, she signed onto the online portal for the Car-Net telematics system in hopes of disabling the alerts. Instead, she immediately saw she still had access to location, mileage and the status of features such as car locks and lights. According to Sehatti, "There was nothing in place to stop me from accessing the full UI." Volkswagen maintains that the seller bears the responsibility of disabling the Car-Net service, or they could continue to have access to personal data.[26]

HOW ARE THE HACKERS GETTING IN?

THE ATTACK VECTORS YOU NEED TO KNOW

TOP SMART MOBILITY ATTACK VECTORS



Source: Upstream Security

Using data driven insights into the favored entry points of criminals, we can begin to understand the true risks of the connected car, and where we should be focusing our protective cyber-security measures.

SERVER ATTACKS

21.4% of the attacks on a connected vehicle are server attacks, and the majority are Black hat - launched by criminals with malicious intent. The term 'server' covers a wide range of incidents, including Telematics command and control servers, Smart Mobility application services and breached web servers such as the website of an OEM. It also covers databases that hold vehicle, customer, code and driver data. This information could be held by a 3rd party public cloud vendor, or on a private cloud. These attacks are remote, and long-range, meaning attackers do not need to be in any kind of close proximity to the car to access data.

41.3%

OF BLACK HAT INCIDENTS INVOLVE BACK END SERVERS

One attack on Porsche Japan shows the gravity of this situation, and how wide the impact of a single hack can be. In February 2018, the email addresses of thousands of Porsche Japan customers were compromised after a cyber-attack on a contractor's data servers. The personal information of over 28,700 Porsche customers in Japan were exposed.[27]

In many privacy cases, it can be difficult for stakeholders to even recognize that these breaches are happening. In September 2017, after an unsecured Amazon S3 server was uncovered by researchers, the SVR car tracking service admitted that a cache containing half a million records was left publicly accessible for an unknown amount of time.[28] Email addresses, passwords, user vehicle data and IMEI numbers of GPS devices were all unprotected, as a result of weak third-party security was more than two decades out of date.

Server attacks often involve vulnerabilities and misconfigurations with TSPs (Telematics Service Providers), which could lead to fleet-wide attacks. An example involving TSP CalAmp shows how dangerous this could be when hackers were able to exploit the Viper SmartStart vehicle tracking mobile app. This app connected to the CalAmp telematics server as did the CalAmp modem installed in the car. When hackers gained access to the server and production databases of CalAmp, they could potentially access Viper controls that could allow them to remotely find a vehicle, steal user information, and even gain control of the car itself.[29]

IN THE SPOTLIGHT:

INSIDER ATTACKS

Employees with a Grudge Take Advantage of Insider Knowledge

Attacks from current or former employees can be extremely dangerous, as the hackers often have proprietary knowledge of internal systems. This was the case when 100+ cars were disabled remotely by a disgruntled employee of an Austin Texas car dealer in 2010. The attacker used his inside-information to hack into Webtech Plus, a web-based remote vehicle-immobilization system used for alerting customers to late payments.[31]

More recently, in 2018 Tesla were hit by an insider saboteur who changed the code on internal products and then exfiltrated private data to outsiders. This attack not only damaged company operations but may have caused a fire. The attacker was able to make direct code changes to the Tesla Manufacturing Operating System under false usernames and even managed to export large amounts of highly sensitive Tesla data to unknown third parties.[32]

EMERGING TREND- RANSOMWARE

TNT Express Hit by Petya and WannaCry

Server attacks are also a favorite vector for criminals using ransomware. FedEx found this out the hard way just last year. The delivery and communications of their subsidiary TNT Express was in their own words, "significantly affected" by the wave of ransomware-attacks that included Petya and WannaCry. While there were no data breaches involved in these attacks, any fleet understands the importance of business continuity and service, proving ransomware can truly hit where it hurts.[30]

REMOTE KEYLESS ENTRY

Historically, keeping your vehicle safe was as simple as holding onto your keys. With the rise in modern vehicles, keyless entry is gaining the attention of cyber-thieves, making up 18.8% of attacks. With keyless entry attacks, you can gain entry to a car without using a key for either the door or the ignition switch.

In July 2017, thieves stole a BMW worth more than $113,000, in a relay attack that extended the signal of a key fob.[33] While the owner would usually automatically unlock the car as they drew close enough, this device allowed the car to unlock and start while the owners slept at home. All the attackers did was hold the device near the front door of their house, in sight of the BMW.

There are four trends for this kind of attack that are becoming increasingly common. One is a key programming device that thieves have used to subvert the diagnostics connector and steal expensive cars. This vector is often seen in Europe, due to privacy laws dictate that the data accessible through the OBD connector cannot be encrypted.[34] Keyless Jamming is another technique where the signal used to lock car doors is blocked. Spoofing involves stealing a vehicles cryptographic key, an attack which can take literally seconds to launch and complete, as in the case of a researchers' attack on a Tesla Model S in October 2018.[35] Lastly, we are seeing a swift increase in Relay hacks like the example above, where criminals use a relay box to pick up the signal from a key fob inside a home, and transmit it to open a vehicle's door.

40%

OF BLACK HAT INCIDENTS INVOLVE REMOTE KEYLESS ENTRY

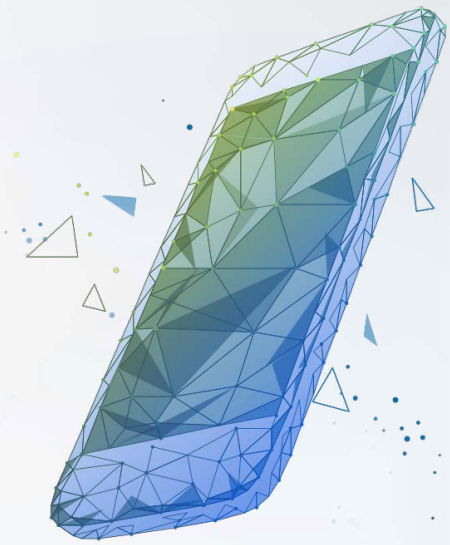
OBD PORT

OBD port attacks need the hacker to have initial physical access to the vehicle itself, which makes them more challenging. Despite this, they still make up around 10.5% of attacks, and once this physical connection has been made – it can result in car theft or the injection of malicious CAN bus messages to manipulate car system behavior. One example enabled hackers to steal luxury vehicles in the UK. The attackers used a signal jammer to prevent car doors from locking. Once they were in the vehicle, they used the OBD port to uncover information on the key. The next stage was installing a covert GPS tracking device, enabling them to track the vehicle anywhere it went. For each stolen vehicle, the thieves created false documents and then sold them on in Cyprus.[36]

MOBILE APP

OEMs often develop mobile applications that allow vehicle owners to take control of various features of their car remotely, for accessibility and ease of use. These apps, and mobile vectors in general make up 8% of attacks on connected vehicles in several ways.

First, an attacker can breach the app itself, reverse-engineer it to uncover vulnerabilities and use this to access a car. Of course, if a criminal gets hold of the mobile phone itself, it's even easier for them to steal your car or your connected vehicle data. Researchers found vulnerabilities in seven popular mobile apps that allow attackers to gain entry to vehicles.[37] In February 2016, Nissan disabled their Leaf mobile app due to cyber-security concerns of this kind.[38]



Second, some apps themselves are not as they seem, they may be in fact fake malicious mobile apps that are created to look legitimate. Attackers can use these to harvest user passwords and take over their accounts, as well as control of the vehicles. Symantec researchers found one such example masquerading as the Uber application.[39]

Lastly, Man-in-the-Middle attacks. As shown in this example[40],where Hyundai's BlueLink mobile app exposed personal data and vehicle controls to opportunistic attackers, a user's legitimate connection (in this case Wi-Fi) can be misused or altered by a third party.

INFOTAINMENT

Infotainment systems can be breached with as commonplace a tool as a simple USB flash drive. In one example from March 2018, researchers were able to run a script using the car's Linux operating system, giving them a permanent connection to Mazda's infotainment system.[41] While this attack involved a physical connection to the vehicle, Volkswagen and Audi cars have been shown to be vulnerable through remote attacks on their infotainment system, too. By connecting to the IVI system's root account, researchers were able to access conversation history, address book and even location data.[42]

DISTANCE MATTERS.

THE RISE IN LONG-RANGE ATTACKS

THE RISE IN LONG-RANGE ATTACKS

Understanding the types of attacks is essential for protecting the Smart Mobility ecosystem. One of the ways the attacks differ is by the distance they can be launched from. First, there are physical attacks which require a connection to the vehicle itself. Examples include the use of OBD ports to infect the vehicle with malware or send malicious CAN messages to the CAN bus.

Second, there are wireless short-range attacks. These can be triggered from a short distance away from the vehicles in question. They work in a variety of ways, usually through devices that amplify the wireless signal from a key fob, and/or relay the signal to disarm the security controls on the vehicle itself.[43] They can also be exploited via Wi-Fi, Bluetooth or wireless car sensors.

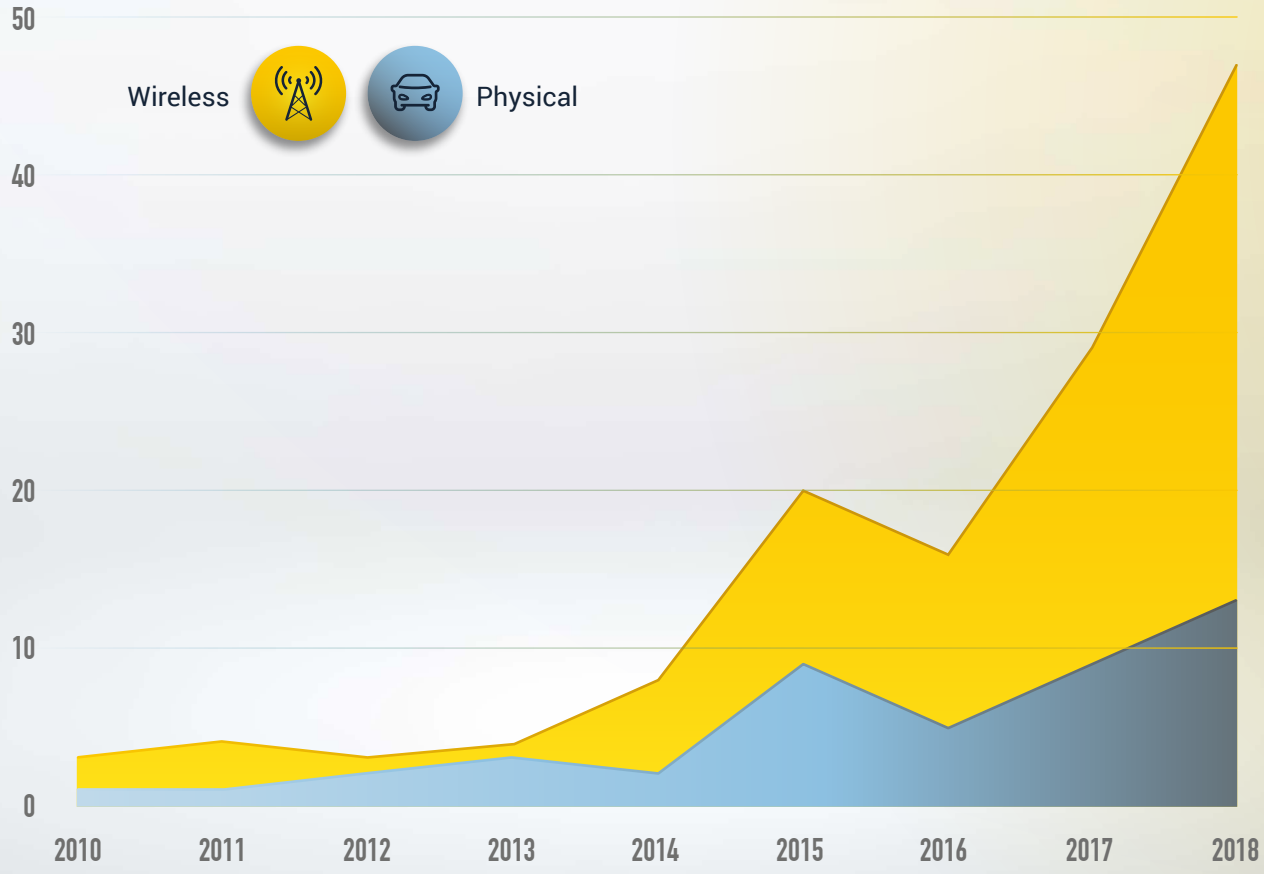
Lastly, we are seeing a rise in long-range attacks, which are also remote, but can be completed from anywhere. This could be relatively close by, such as from a few streets away, or as far away as another country. These attacks are performed via the internet or a cellular network, thus the physical location becomes irrelevant. On one occasion, researchers were able to exploit an OBD dongle remotely by SMS message. They were able to transmit commands to the CAN bus of the car, controlling physical driving components such as the brakes, windscreen wipers and headlights.[44]

91%

OF BLACK HAT ATTACKS ARE WIRELESS, NOT PHYSICAL

WIRELESS ATTACKS ARE BECOMING MORE POPULAR THAN PHYSICAL ONES.

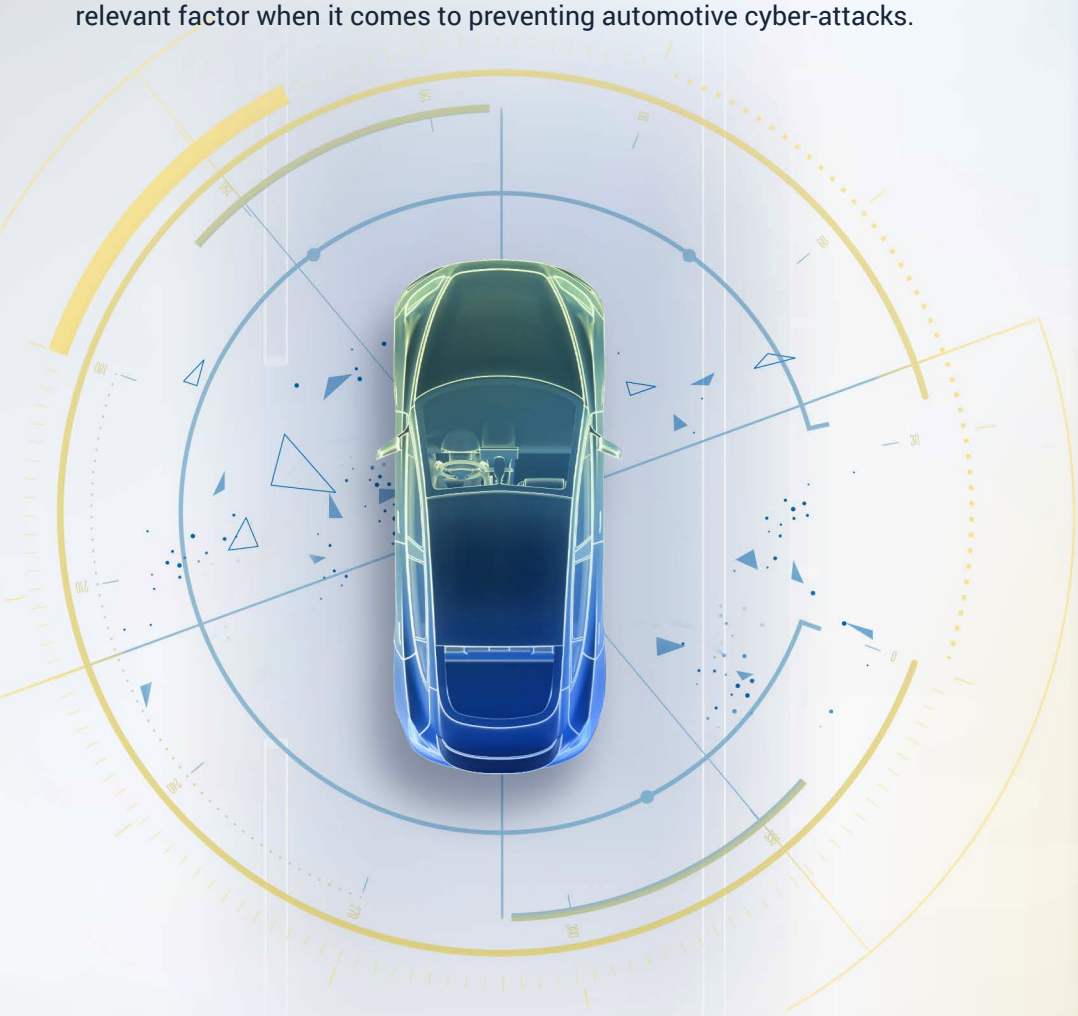
Physical vs Wireless attacks



Source: Upstream Security

REMOTE ATTACKS TAKE THE LEAD

Tracking the data, we can see that long-range remote attacks are becoming more prevalent, even overtaking the numbers of physical attacks. It is evident that the proximity of attackers or the location of your vehicles or servers is no longer a relevant factor when it comes to preventing automotive cyber-attacks.



IN THE SPOTLIGHT:

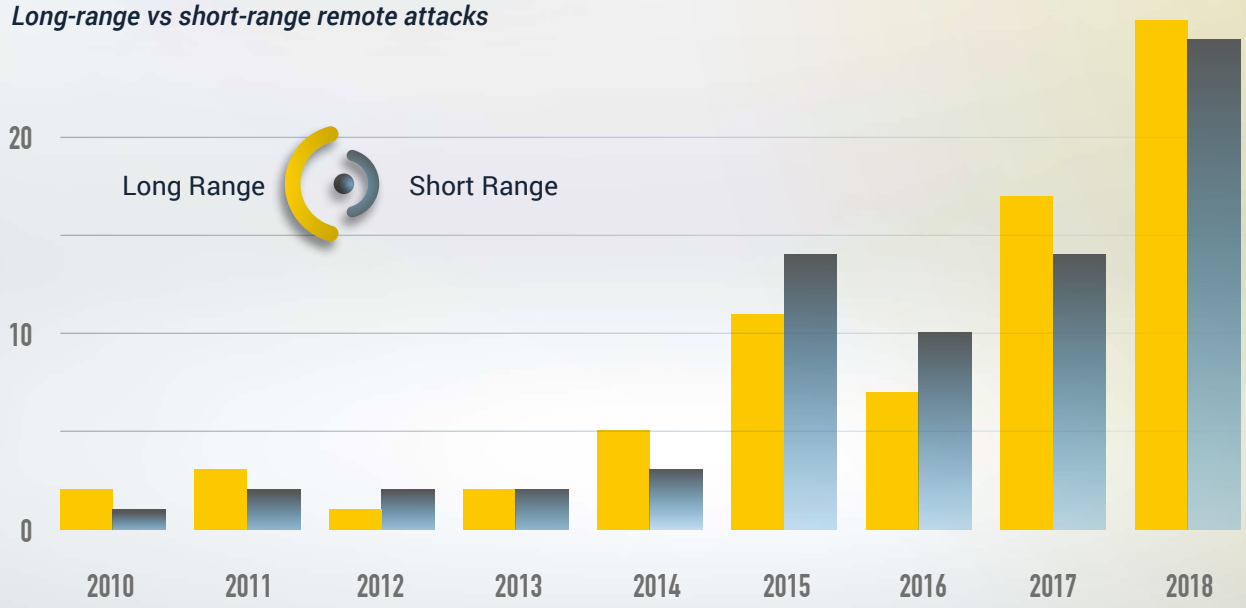
REMOTE ATTACKS

Who could forget when hackers Charlie Miller and Chris Valasek proved they were able to remotely control a Jeep Cherokee's engine while it was in motion on the highway? Using an exploit the attackers took wireless control via the cellular network back in 2015.[45]

Aside from the risk to driver and pedestrian safety, this was a public image nightmare for Fiat Chrysler. The company recalled 1.4 million vehicles for a software fix and this became one of the most infamous attacks in the Smart Mobility world.

Miller made a stark public call to action to any and every stakeholder in Smart Mobility ecosystem. "If consumers don't realize this is an issue, they should, and they should start complaining to carmakers," Miller says. "This might be the kind of software bug most likely to kill someone."

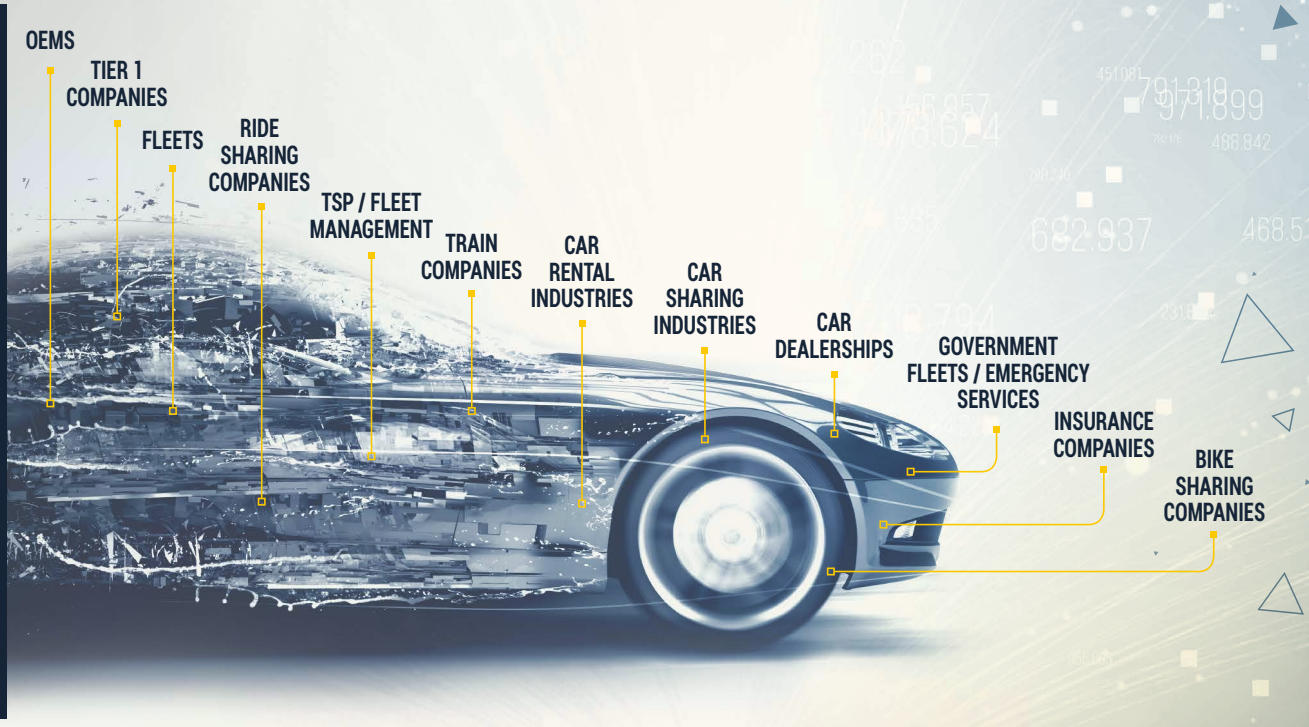
Long-range vs short-range remote attacks



Source: Upstream Security

WHO ARE THE HACKERS TARGETING?

COMPANIES IMPACTED



Analyzing eight years of data, it's clear that the entire range of companies that fall within the Smart Mobility ecosystem are at risk from cyber-security vulnerabilities. Attack headlines often show that OEMs suffer the most, with hackers both malicious and well-intentioned exploiting vulnerabilities in back-end servers and front end-vehicles alike. But this is just the beginning.

Companies operating fleets should be aware that there are many threats and vulnerabilities that will potentially impact commercial and industrial vehicles too. One attack showed how malicious commands could be sent via the OBD port within the internal network of a truck rig. This allowed hackers to change the instrument panel readout, and even disable the brakes.[46] In ride-sharing, many attacks manifest through fraud and misuse, such as the 'phantom rides' that many UK and US Uber users have found on their accounts in the past, despite never taking the trips themselves.[47]

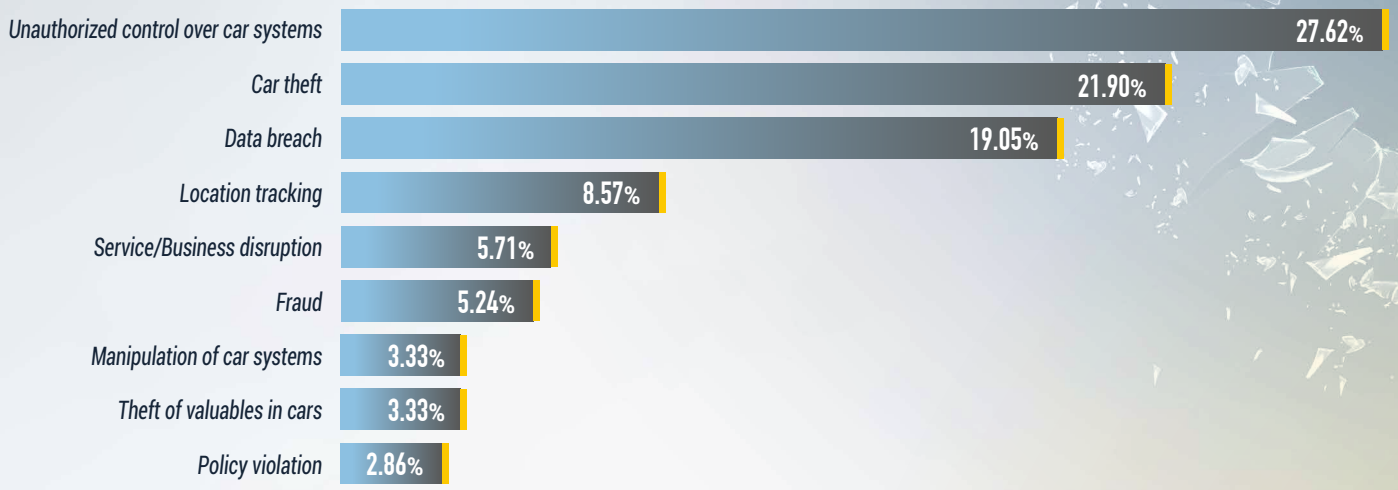
Attacks impact both private vehicles, government or commercial fleets, too. One frightening example showed how emergency service vehicles could be at risk. Through unsecured wireless mobile gateways installed in police cars, ambulances, and other emergency vehicles, locations and vital configurations are exposed to potential attackers. Bad actors would be able to take control of dash cameras, in-vehicle computers and any other devices that rely on wireless gateways.[48]

There are also huge threats to public transportation systems. One such example was the ransomware attack that ground the German train system to a halt in 2017 [49] or the attack on Copenhagen's city's bicycle sharing system. In this incident, more than 1,800 bicycles were affected, and riders were unable to use the service for two days. A logistical nightmare, the administration had to manually update every bike in the city.[50]

The Smart Mobility ecosystem is constantly evolving, and with it, the types of vehicles covered by connected or modern transportation. From TSPs, software services, dealerships and Industrial services, to electric car charging stations, emergency services, industrial robot manufacturers or used car salespeople, the list goes on, and the threats are existing and emergent.

WHAT'S THE WORST THAT COULD HAPPEN?

THE TOP IMPACTS OF CYBER-ATTACKS ON AUTOMOTIVE



Source: Upstream Security

This chart shows the impact of automotive hacks, from the most common – targeting the physical systems of a vehicle, to car theft, data breaches and fraud. These vary in size and consequence but can have unintended effects to your business bottom line, such as an example where a hacker breached a car-sharing company database and used existing member credentials to ride for free.[51]

The most important impact however, is control over car systems. This involves the impact of attacks that control physical elements in the car. Currently, as many as 27.6% of incidents involve vehicle control systems. Vulnerabilities or breaches to these systems have the potential to cause the most frightening attacks. We can separate them into categories. While some introduce low physical risk, such as the unlock function, mainly responsible for theft or damage to the vehicle– others are categorized as critical safety and can have a real and devastating impact on human lives. Think about features such as the brakes, airbags or the acceleration of a vehicle. An attack timed to cause the most damage, for example while the car is in motion, could be catastrophic, and in certain cases has even been shown to be fatal.

The danger of breaches to critical components can be seen in many real-life security attacks. In September 2016, hackers took control of a Tesla Model S from 12 miles away.[52] By tricking drivers into signing in to a malicious Wi-Fi connection, they were able to interfere with the car's door locks and brakes. Earlier, in October 2015, researchers showed how they could disable a car's airbags by exploiting a zero-day vulnerability.[53] This was done through third-party diagnostics software often used by car mechanics. Once malware infected the mechanics servers, the in-vehicle systems could be switched on or off without the driver's knowledge.

It's clear that the risks of cyber-attacks on Smart Mobility are far greater than IT network security. While other businesses or verticals might worry about network cyber-risks, affecting their servers and data, the consequences are far less severe. Worst case scenarios are loss to business earnings, theft, data privacy or property damage – while what's at stake in automotive cyber-attacks is nothing less than human lives.

27.6%

OF INCIDENTS INVOLVE UNAUTHORIZED CONTROL OVER CAR SYSTEMS

IN THE SPOTLIGHT

AUTONOMOUS CARS

Hackers manipulate LIDAR through spoofing and saturation attacks

Autonomous cars have a unique vulnerability, and it lies in the LIDAR and radar systems. A hacker can manipulate the car's physical controls without gaining control over its actual systems. This is done through LIDAR and other vision sensors. Hackers can misguide the sensors to identify obstacles or signals such as stop signs. This then triggers behavior in the vehicle itself, manipulating what happens on the road.

Researchers from the Korea Advanced Institute of Science and Technology have proven how dangerous this can be, demonstrating two kinds of attacks against LIDAR: a spoofing attack, and a saturation attack. While the saturation attack illuminates the LIDAR with a light that is the same wavelength erasing the existing objects in its sensors, the spoofing attack provides an optical illusion by generating a point cloud, making the illusion look far closer than the actual device.[54]

FRAUD

The business impact of cyber-security hacks on Smart Mobility

In June 2017, GoGet – an Australian car sharing company detected and reported unauthorized access on their computer servers. It took until January 2018 for a man to be arrested in connection with the breach. He had fraudulently accessed the company's booking system and been able to download a customer identification database. Using this data, he was able to ride for free more than 30 times.[55]

In November 2017, Uber users in Singapore reported 'phantom rides' on their account, some costing customers as much as $4,000 in fraudulent charges to the credit or debit cards associated with their account. In one case, the fraudulent rides were taken over a two-week period or more, and as Uber was unaware, customers had to alert the company to the scam themselves when their own bank statements were reviewed.[56]

These cases show the importance of visibility into backend servers and customer data systems to prevent fraud that can have a damaging impact into business bottom line and public image.

DEFENSE IN DEPTH

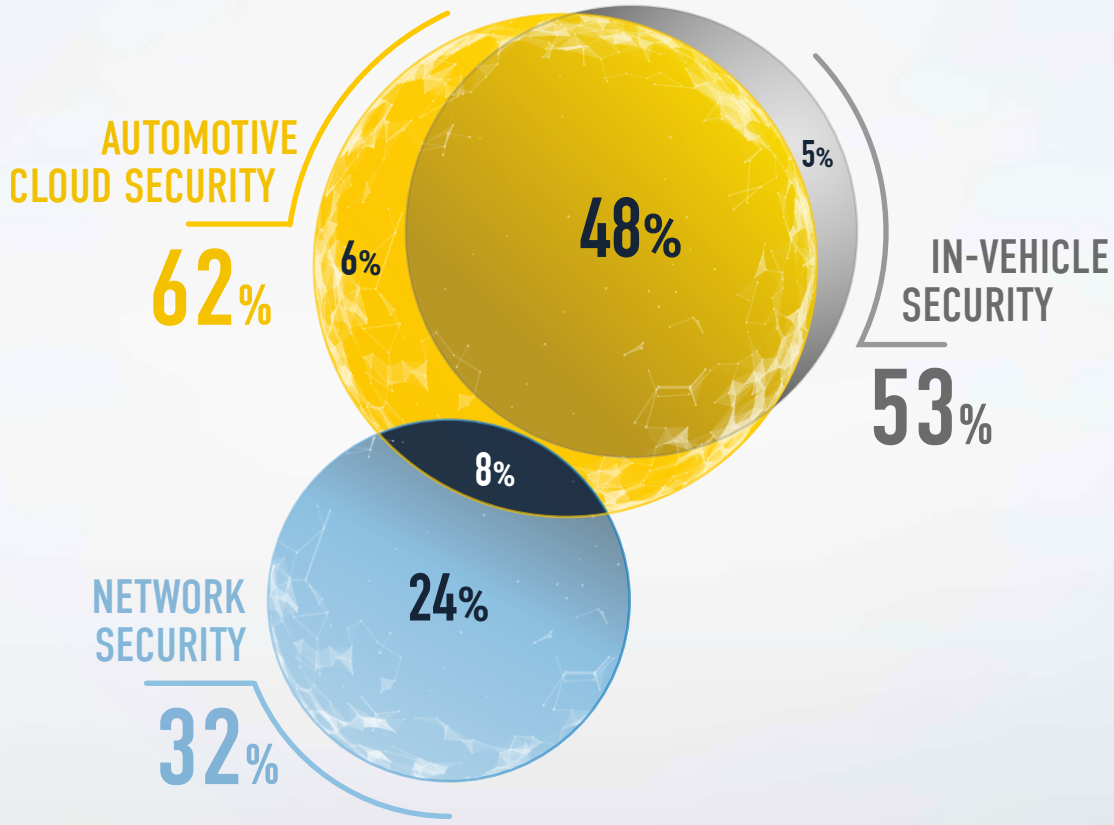
WHAT OEMS AND FLEETS ARE DOING TO PROTECT THEMSELVES

The need for multi-layered security is well established in IT security. The amount of attack vectors that a network is vulnerable to is growing all the time, and businesses are increasingly investing in improved perimeter security, anti-virus solutions, cloud-security, internal segmentation technology and more.

Smart Mobility is no different. Fleets, OEMs and TSPs as well as any other stakeholder in the automotive space are already defending themselves against multiple vectors. There are a number of choices for automotive security, all of which protect different types of attacks. In-vehicle security protects the individual components of the vehicle and can ward off close-proximity attacks as well as some remote attacks. Network security keeps a stronghold at your IT network and backend. Automotive cloud security is used to detect and resolve cyber-attacks or misuse of the Smart Mobility services, single and multi-vehicle attacks as well as attacks on telematics and mobility services in hybrid or cloud-based environments.

However, as is clear from the chart below, there is more data that Smart Mobility stakeholders need to be aware of.

PROTECTION COVERAGE OF AUTOMOTIVE CLOUD, IN-VEHICLE AND IT NETWORK CYBERSECURITY



Source: Upstream Security

From the data above, companies can see how important it is to have all three of these security types, as even the most effective – automotive cloud security, works better with complementary solutions. Clearly, the best approach is defense in depth, with multi-layer security. Each layer of your infrastructure has its own unique threats, and therefore its own unique protection methods.

When building a security framework one should account for the various attack vectors as well as the time to implement each of the solutions. While In-Vehicle Security is deployed physically inside the cars themselves and thus most likely takes the longest time to implement, Automotive Cloud Security is deployed in the Cloud environment – sitting centrally where all the data is being sent, and therefore requires the least amount of time for implementation. The data shows that Automotive Cloud Security and Network Security could be the most important protection in the Smart Mobility space, as they defend against the largest number of risks, and take the least amount of time and money to implement.

PREDICTIONS FOR 2019

WITH EVERY NEW SERVICE - A NEW ATTACK VECTOR

Remote attacks through Smart Mobility services will increase substantially, with back-end servers, telematics servers and mobile apps continuing to face attacks such as ransomware and unauthorized access. As different systems continue to work together, introducing new features and selling points for consumers, the infrastructure is becoming more complex. Each new service connected to a vehicle is a new potential entry point for hackers. The control that a company will have over a third party service varies from example to example, but the common denominator is further complexity in visibility and control.

VEHICLE EXCHANGE WILL LEAD TO DATA PRIVACY BREACHES

We will continue to see vehicle exchange causing problems for data privacy. This could be through car sharing and rentals or pre-owned vehicles. The most important services to consider are cloud-based services where data is held in an omni-channel way, and infotainment services that could store personal information of a previous user.

AUTONOMOUS SENSOR HACKING WILL CONTINUE TO GROW AND IMPROVE

As the potential and application of autonomous vehicles continues to climb, researchers will focus their attention on the security vulnerabilities behind the technology. This includes LIDAR, sensors and other radar functionality that allows the vehicles to 'see' the world around them.

SMART MOBILITY FRAUD AND MISUSE

One trend to look out for in 2019 is a growing amount of fraud and misuse by both consumers and mobility services' drivers. The complex automotive environment makes it difficult for businesses to stay on top of every transaction. Hacking incidents will include fleet drivers hiding violations of company policy or altering mileage or misuse, while consumers may steal the identity of other users to ride for free on ride hailing or car sharing services.

REMOTE KEYLESS ENTRY CAR THEFT HACKS

Keyless cars are an expensive purchase, giving them high resale value and making them an obvious target for thieves. We predict that these attacks, whether relay attacks, spoofing, key jamming or diagnostics hacking will continue to climb, increasing theft of valuable property or documents from inside the vehicles, as well as the cars themselves.

WILL 2019 BE THE YEAR WE SEE A SERVICE-WIDE HACK?

As connected cars becomes increasingly complex, and attackers of the Smart Mobility ecosystem learn how to manipulate the latest technology, could this be the year that we see an attack on an entire fleet of cars?

REFERENCES

1. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
2. http://fortune.com/2015/07/24/jeep-cherokee-recall/
3. https://www.statista.com/statistics/204354/us-light-vehicle-sales-in-september-2011-by-company/
4. https://www.cnet.com/roadshow/news/automotive-recalls-cost-22-billion-in-2016/
5. https://topclassactions.com/lawsuit-settlements/lawsuit-news/89165-fiat-chrysler-sued-in-hacking-class-action-lawsuit/
6. https://www.juniperresearch.com/press/press-releases/in-vehicle-commerce-opportunities
7. https://www.statista.com/statistics/275849/number-of-vehicles-connected-to-the-internet/
8. https://www.youtube.com/watch?v=Z5bQdW3m5qQ&feature=youtu.be#.W8W8jmgzZHZ
9. http://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/
10. https://www.cbc.ca/news/canada/manitoba/new-5-device-easily-unlocks-car-doors-for-thieves-in-winnipeg-1.2288826?cmp=rss
11. http://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/
12. https://gizmodo.com/rare-malware-targeting-ubers-android-app-uncovered-1821753862
13. https://www.tripwire.com/state-of-security/latest-security-news/man-arrested-allegedly-hacking-car-sharing-service-using-vehicles-free/
14. https://mashable.com/2018/02/15/fedex-unsecured-server-data-exposed/
15. http://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/
16. https://www.japantimes.co.jp/news/2018/02/27/business/corporate-business/hackers-steal-email-addresses-thousands-porsche-japan--customers/#.W8W8jmgzZHZ
17. http://www.arabnews.com/node/1289791/business-economy
18. https://www.zdnet.com/article/flaw-connected-alarm-system-exposed-vehicles-remote-hacking/
19. https://thehackernews.com/2018/05/bmw-smart-car-hacking.html?m=1
20. https://kromtech.com/blog/security-center/honda-leaked-personal-information-from-its-honda-connect-app
21. https://www.scmagazine.com/home/security-news/insider-threats/tesla-hit-by-insider-saboteur-who-changed-code-exfiltrated-data/
22. https://www.thisislancashire.co.uk/news/17213893.keyless-car-thefts-spike-in-heaton/
23. https://money.cnn.com/2017/02/17/technology/used-car-hack-safety-location/index.html
24. https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf
25. http://www.wmcactionnews5.com/story/39022826/used-cars-increase-identity-theft-chances-bbb-finds/
26. https://www.theverge.com/2018/5/4/17303644/volkswagen-car-net-security-location-access
27. https://www.japantimes.co.jp/news/2018/02/27/business/corporate-business/hackers-steal-email-addresses-thousands-porsche--japan-customers/
28. https://thehackernews.com/2017/09/hacker-track-car.html?m=1 https://www.zdnet.com/article/flaw-connected-alarm-system-exposed--vehicles-remote-hacking/
29. https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/fedex-delivery-unit-hit-by-worldwide--cyberattack/?noredirect=on&utm_term=.dcfe0f842674
30. https://www.wired.com/2010/03/hacker-bricks-cars/
31. https://www.scmagazine.com/tesla-hit-by-insider-saboteur-who-changed-code-exfiltrated-data/article/774472/

REFERENCES

32. https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=11847669
33. https://www.extremetech.com/extreme/132526-hack-the-diagnostics-connector-steal-yourself-a-bmw-in-3-minutes
34. https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/
35. https://www.telegraph.co.uk/news/uknews/crime/9369783/Thieves-placed-bugs-and-hacked-onboard-computers-of-luxury-cars.html
36. https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/
37. https://www.autoblog.com/2016/02/25/nissanconnect-ev-leaf-app-hacking-followup/?guccounter=1
38. https://gizmodo.com/rare-malware-targeting-ubers-android-app-uncovered-1821753862
39. https://threatpost.com/hyundai-patches-leaky-blue-link-mobile-app/125182/
40. https://www.forbes.com/sites/thomasbrewster/2018/03/09/mazda-privacy-hack-via-usb/#64e12fc54d0c
41. https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/
42. http://www.latimes.com/business/la-fi-hy-mystery-car-stealing-device-20161207-story.html
43. https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/
44. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
45. https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf
46. https://mashable.com/2017/11/21/uber-ride-singapore-phantom/#EUziTpCHEiq1
47. https://motherboard.vice.com/en_us/article/æ387k/uber-users-say-theyre-being-charged-for-trips-they-didnt-take
48. https://arstechnica.com/information-technology/2018/08/in-vehicle-wireless-devices-are-endangering-emergency-first-responders/
49. http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/
50. https://www.hackread.com/copenhagen-citys-bicycle-sharing-system-hacked/
51. https://www.tripwire.com/state-of-security/latest-security-news/man-arrested-allegedly-hacking-car-sharing-service-using-vehicles-free/
52. https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes
53. https://thehackernews.com/2015/10/hacking-car-airbag.html?m=1
54. https://eprint.iacr.org/2017/613.pdf
55. https://www.tripwire.com/state-of-security/latest-security-news/man-arrested-allegedly-hacking-car-sharing-service-using-vehicles-free/
56. https://mashable.com/2017/11/21/uber-ride-singapore-phantom/?europe=true#sC9qRSxdkiqa

ABOUT UPSTREAM SECURITY

Upstream improves the safety and security of connected vehicles and services built for them. It does this by monitoring business critical events and identifying cyber threats in real-time via a centralized cloud-based analysis of multiple automotive data feeds, including telematics and mobile applications. The solution is 100% agent-less and does not require any hardware or software inside the vehicles. Upstream's solution is already used by millions of vehicles worldwide, providing an effective and innovative method of detecting threat anomalies and mission critical events using a combination of machine learning, cybersecurity engines, and service policy enforcement. The result enables Smart Mobility services to run safely and smoothly while providing the customer with real-time alerts tailored to their needs.

For more information

VISIT US AT:
www.upstream.auto

CONTACT US:
hello@upstream.auto

FIND US:

Upstream.auto
Securing Smart Mobility