Upstream

2022

GLOBAL AUTOMOTIVE CYBERSECURITY REPORT

AUTOMOTIVE CYBER THREAT LANDSCAPE IN LIGHT OF NEW REGULATIONS

TABLE OF CONTENTS

Opening letter from our CEO 4

Methodology 5

Chapter 1: Standards, Regulations, and the Connected Vehicle Ecosystem 6

- Kicking Off UNECE regulations and ISO/SAE standard 8
- UNECE WP.29 R155 CSMS and R156 SUMS in today's ecosystem 11
- Does WP.29 R155 align with in-field threats? 12
- ISO/SAE 21434 in support of UNECE WP.29 R155 & R156 17
- Threat Analysis & Risk Assessment (TARA) 18
- The evolving face of hacking 19
- Supply chain 21
- Surging demand and chip shortages 22
- The chip shortage's financial impact 23

Chapter 2: Automotive Cyber Threat Trends 24

- Incidents 25
- Who is attacking? 26
- How are CVEs prioritized? 27
- Physical access vs. Remote access 28
- Newly cataloged Common Vulnerabilities & Exposures 29
- Which industries are impacted? 31
- Expanding risks in established sectors 32
  - Insurance 32
  - Connected agriculture 32
  - Government 33
- Knowledge sharing beyond traditional hackers 33
- EV charging points 34

Chapter 3: 2021's Diverse Attack Vectors 35

- Increasingly sophisticated attacks 36
- Servers attacks 37
  - Servers, vehicles, and what's in-between 37
  - Telematics Control Unit 38
  - Ransomware attacks 38
  - Ransomware attacks beyond OEMs 39
- Mobile app attacks 39
  - Mobile apps and private information 40
  - Mobile app hack in racing 41
  - Data sharing and smart mobility 41
- Remote keyless entry system 42
- How do hackers hack into vehicles 43
- Infotainment 46

TABLE OF CONTENTS

WI-FI 47
ECUs 48
OBD Port 49
The supply chain as an attack vector 51
Autonomous Vehicles 52
V2X 54

Chapter 4: Cyber Attacks' Impacts on the Automotive Industry 57

Cyber attacks' financial and reputational impact 59
Data and privacy breaches 61
Car thefts and break-ins 61
Financial impact on insurance providers 62

Chapter 5 - What's Hiding in the Deep and Dark Web? 63

What is the deep and dark web? 64
What occurs in the deep and dark web? 65
Forums 66
Marketplaces 67
Messaging Applications 69
Looking into the future 70
The world against the dark web 71
Monitoring the deep and dark web 71

Chapter 6: Automotive Cybersecurity Solution Landscape 72

Evolving solutions 73
Securing the vehicle's full lifecycle 73
Protecting against attacks in the supply chain 73
Implementing a multi-layered cybersecurity solution 74
Developing an effective VSOC 77
Staying one step ahead of the threats with automotive-specific threat intelligence 79
Benefits to OEMs 79
Benefits to Tier-1 and 2 suppliers 79
Benefits to CISOs 80
Benefits to VSOC Analysts 80
Benefits to insurance companies 81
Benefits to shared mobility and rental car stakeholders 81
Complying with automotive cybersecurity regulations 82
Upstream's Cybersecurity and Data Management Platform 83
The Upstream Platform 83
AutoThreat® Intelligence 84
Vehicle SOC (VSOC) 84
Predictions for 2022 85

References 87

OPENING LETTER FROM OUR CEO

I am proud to present to you the 2022 Global Automotive Cybersecurity Report. Our cybersecurity experts analyzed 900+ publicly reported incidents and monitored hundreds of deep and dark web forums to compile a comprehensive report, tailor-made for actionable insights into the year ahead. You will find information about which risks were more prominent, what's on the rise, and how these impact smart mobility.

The past couple of years have been revolutionary in ways we never expected. A continuous shift in connected, autonomous, shared, and electric vehicles (CASE) has effectively turned vehicles into a mobile computing platform on wheels, enabling an improved customer and ownership experience. However, with all the apparent advantages of connectivity and software driven functionality, there are risks and threats to address, namely data privacy and cybersecurity. Over these same revolutionary years, the industry has seen an exponential rise in the magnitude, frequency, and sophistication of cyber attacks. The automotive industry is now accelerating the proactive measures necessary to secure their vehicles and ensure that drivers and passengers remain safe.

Upstream has been helping automotive ecosystem stakeholders understand and mitigate cyber risks for several years now, working with some of the leading automotive OEMs, parts suppliers, insurance providers, aviation leaders, and others to protect millions of vehicles that are already on the road today. We have been providing complete automotive-specific threat intelligence, utilizing surface, deep, and dark web sources to help automotive stakeholders identify and manage risks and vulnerabilities detected in their supply chain and assets.

To this end, we at Upstream are committed to empowering the industry to leverage the data gathered from connected vehicles and our threat intelligence analysts to help make smart mobility safe and secure. Our industry has a lot to look forward to in the years ahead, including paving the road for a better, more secure, and fascinating connected universe.

Best regards,

Yoav Levy
Co-Founder & CEO

METHODOLOGY

For years, we at Upstream Security have been monitoring and analyzing worldwide automotive cyber incidents with the purpose of learning, understanding, and helping protect the automotive ecosystem from cyber threats and misuse. Our researchers have carefully categorized the data we have collected, analyzing each incident's attack methods, attack vectors, impact, target industries, and many other aspects. As a result, we learn more about the threats and impact of cyber attacks targeting connected vehicles on the road today, using this newfound knowledge to better protect them.

This report was created by analyzing 900+ publicly reported incidents that occurred since 2010, with an increase of more than 225% in the number of incidents taking place in 2021 alone, when compared to 2018.

Upstream's AutoThreat® Intelligence team of cyber researchers and cyber analysts are constantly looking for new incidents, analyzing and indexing every incident to the AutoThreat® platform. A community version of AutoThreat® is publicly available on Upstream's website (AutoThreat Intelligence Cyber Incident Repository), for creating greater awareness and helping automotive stakeholders improve their security posture. Each incident and relevant contextual data are added to the platform to create a more action-driven repository. These include the attack's geo-location, impact, attack vector, company type, and required proximity of the attacker to its target and beyond.

Incidents studied and presented in this report were taken from various sources such as media, academic research, bug bounty programs, verified Twitter accounts of government law enforcement agencies worldwide, the Common Vulnerabilities & Exposures (CVE) database, and other publicly-available online sources.

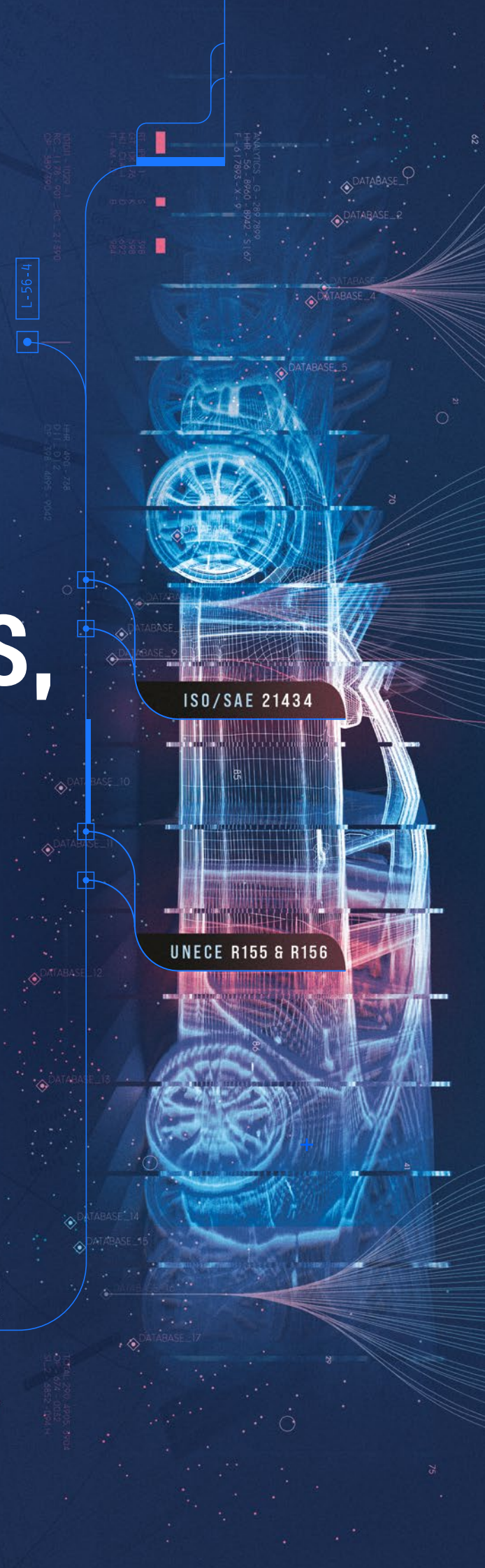
In addition to the publicly reported cyber incidents, Upstream's analysts probe the deep and dark web to monitor black-hat actors that operate behind the scenes of automotive-focused cyber attacks. This helps OEMs, Tier-1 and Tier-2 companies, insurance, and other automotive-related companies take preventive steps to protect their products, data, information, and internal assets. These incidents are discussed in a separate designated section of this report titled "Deep and Dark Web" and are not included in any charts or statistics in any other section.

The automotive industry must have a continuously updated database of security incidents at the ready. To achieve this, select details of the publicly reported incidents are available in the AutoThreat® repository. In addition, a comprehensive analysis is available to AutoThreat® intelligence customers.

While every effort was made to identify and analyze each cyber incident within the automotive ecosystem, it is possible that additional automotive cyber attacks occurred but have not been publicly reported and thus, not publicized by Upstream in this report.

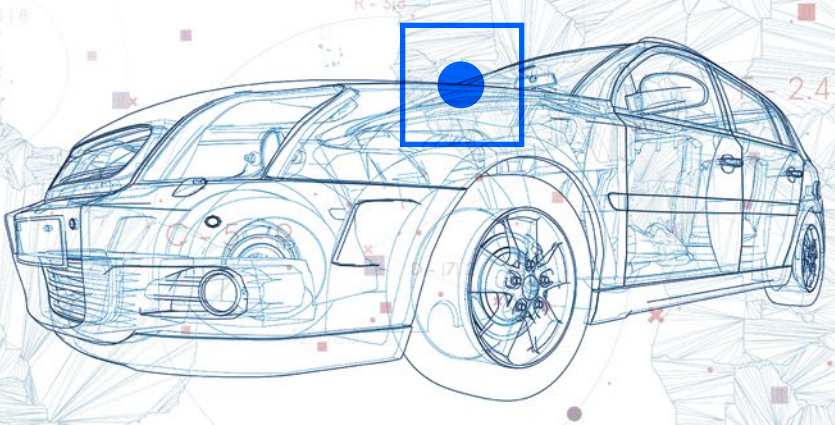
CHAPTER 1

STANDARDS, REGULATIONS, AND THE CONNECTED VEHICLE ECOSYSTEM



GLOBAL CONNECTED VEHICLES WILL JUMP 134% FROM 330 MILLION IN 2018 TO 775 MILLION IN 2023

Source: Juniper Research[1]



KICKING OFF UNECE REGULATIONS AND ISO/SAE STANDARD

Recent years have seen an alarming spike in the number of cyber attacks targeting the automotive industry.

This new prevalence of cyber attacks on vehicles comes from the sharp increase in connected vehicles on the road today and the proliferation of knowledge, as well as tools for vehicle cyber hacking, compared to just a few years ago. Increased data collection across widely connected wireless networks creates attack vectors that range from the OEM back-end servers to vehicle Electronic Control Units (ECUs) and even an infotainment unit's Bluetooth capabilities.

The need for improved driving and a better customer experience pushes OEMs to create new technologically advanced innovations that are enabled by connectivity. Unfortunately, the other side of connectivity is that this widens the attack surface for hackers to find new attack vectors and exploit every flaw leaving vehicles, networks, and back-end servers vulnerable.

To create a unified approach that will address these cyber threats, automotive OEMs, Tier-1, and Tier-2 suppliers are implementing the UNECE's WP.29 R155[2] & R156[3] regulations and also the ISO/SAE 21434 standard. These are designed to give manufacturers the flexibility to deliver innovative cybersecurity approaches while ensuring a high level of safety and security for their customers while creating uniform terminology across the industry.

UNECE WP.29's two main components:

R155 CSMS

Cybersecurity Management System

Cybersecurity management from ideation through post-production

R156 SUMS

Software Update Management System

Cybersecurity measure to ensure safe software updates throughout the vehicle lifecycle

It is worth noting that these standards and regulations reflect the fluid nature of technology adoption throughout the automotive industry. Both WP.29 R155 and ISO/SAE 21434 stay away from outlining specific solutions and exact processes, instead focusing on implementing a high standard of cybersecurity analysis.

Guidelines highlight the requirement to consider life-long cybersecurity threats and vulnerabilities, beginning with development, through production, and throughout the vehicle's post-production lifecycle.

While many countries are planning to accept this new regulation, others will adopt their own local regulations and oversight. This demands that OEMs, Tier-1, and Tier-2 suppliers comply with various regulations, depending on the intended market for their products. An example of a government that chooses not to partake in the UN regulation is the US, who has the National Highway Traffic Safety Administration (NHTSA). This organization sets local vehicle safety standards and recommends best cybersecurity practices.

In October 2021 China implemented new regulations surrounding collecting user and driver personal data. In addition, data must be stored in China. In the case that data needs to be transferred abroad, the relevant company must first undergo a regulatory evaluation for approval[4]. They defined government agencies, criteria, and various data protection steps that are not being adopted beyond their borders.

Nevertheless, we see that the WP.29 regulation and the ISO/SAE 21434 are moving the needle on the decision making of OEMs on the global level, because the adoption of WP.29 is passing a critical mass which leads to global operations changes.

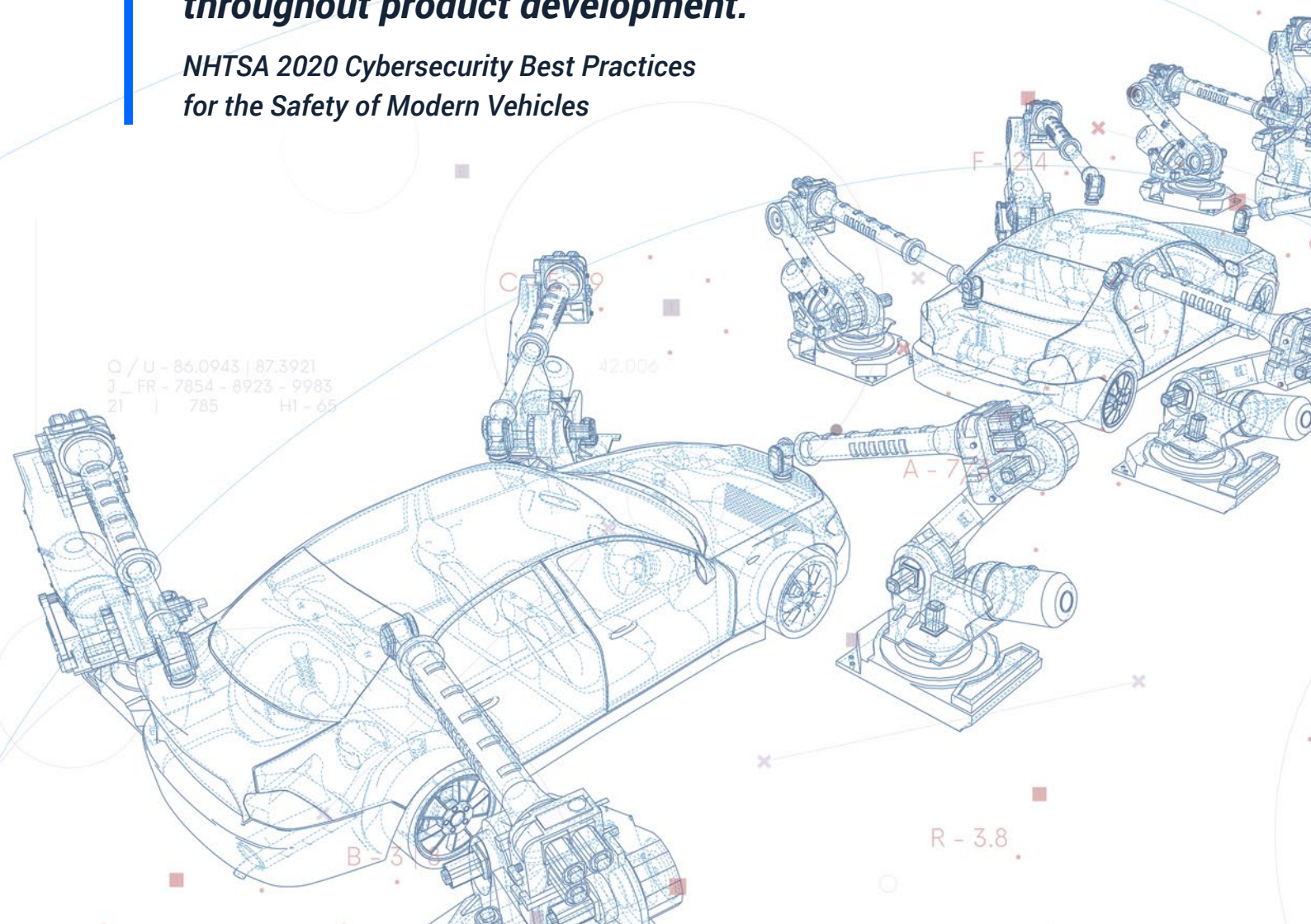
Which vehicles do WP.29 R155 & R156 impact?

Vehicle Category	*Definition*	*Applicable Regulation*
L6	Vehicle with four wheels weighing under 350kg (~770lb.) whose engine does not exceed 50 cubic cm. and whose maximum speed is designed for 45 km/h (~28mph)	R155 if equipped with level-3 functionalities and above
L7	Vehicle with four wheels weighing under 400kg (~880lb.) and whose continuous rated power does not exceed 15kW	R155 if equipped with level-3 functionalities and above
M	A vehicle with at least four wheels and meant to carry passengers	R155 & R156
N	An automobile with at least four wheels meant to carry goods	R155 & R156
O	Trailers that have at least one ECU	R155 & R156
R	Agricultural Trailer	R156
S	Interchangeable towed agricultural or forestry equipment	R156
T	Any motorized, wheeled, or tacked agricultural equipment that has two axles and is meant to travel at speeds greater than 6km/h (~3.5mph)	R156

Vehicles are regulated under R155, R156, or both of WP.29 guidelines[5] depending on category classification.

Source: UNECE

> ***"Emphasizing the importance of cybersecurity from the leadership level down to the staff level demonstrates the seriousness of effectively managing cybersecurity risks and will help the organization better prioritize cybersecurity throughout product development."***
>
> *NHTSA 2020 Cybersecurity Best Practices for the Safety of Modern Vehicles*

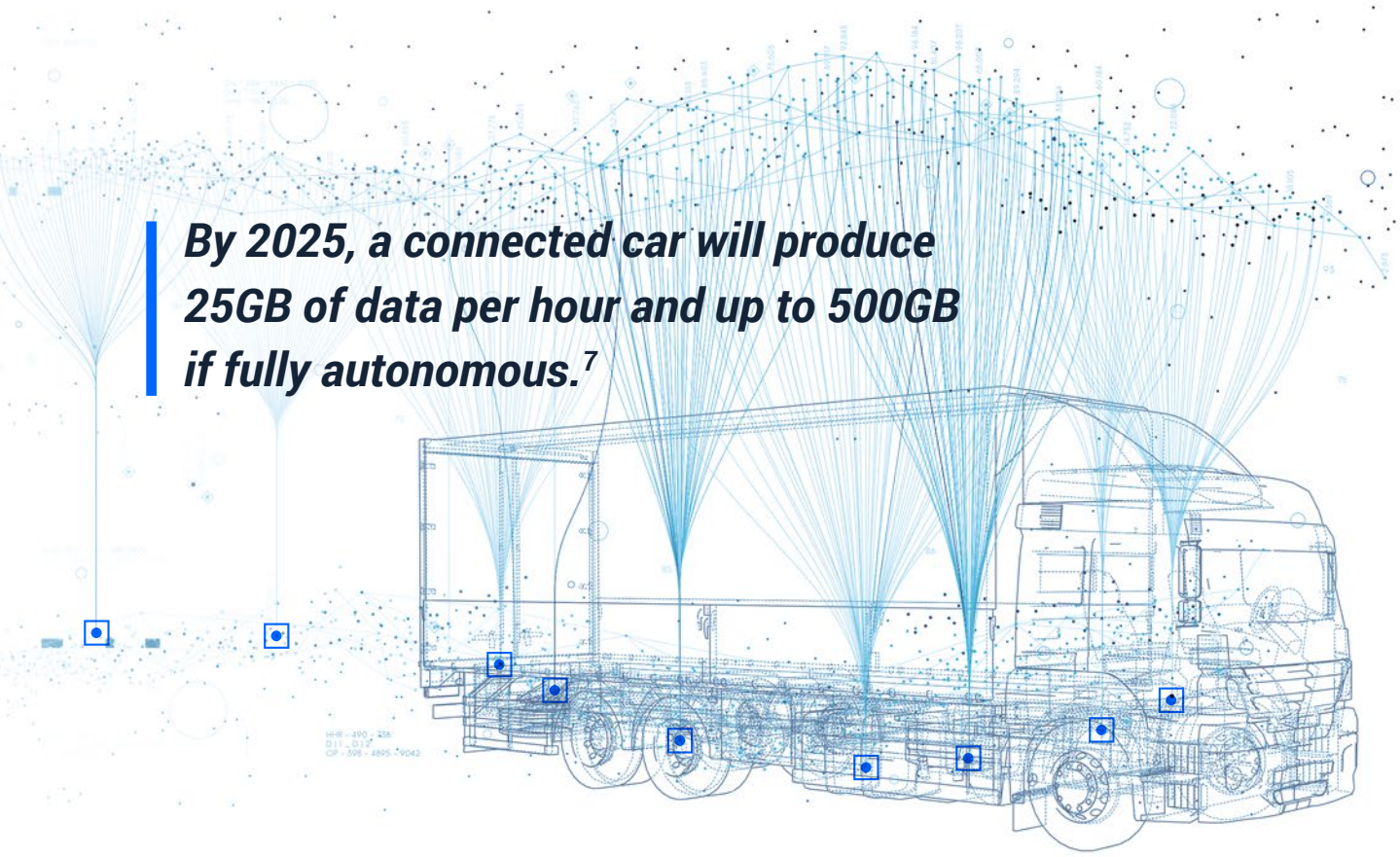


UNECE WP 29.R155 CSMS AND R156 SUMS IN TODAY'S ECOSYSTEM

The UN Economic Commission for Europe (UNECE) announced[6] in June 2020 regulations WP.29 R155 and R156.

R155 demands the creation of a Cybersecurity Management System (CSMS), which encompasses all matters covering the vehicle's lifecycle from development, to production, and post-production. This includes holding OEMs accountable in ensuring that suppliers align with the security measures mentioned in the regulation.

R156 focuses on the post-production software aspect of vehicles, including the software itself and over the air (OTA) procedures. Software that received approval during production, under the WP.29 R155 regulation, must reapply for approval if any modification is made to the vehicle that affects technical performance or the original application documentation.



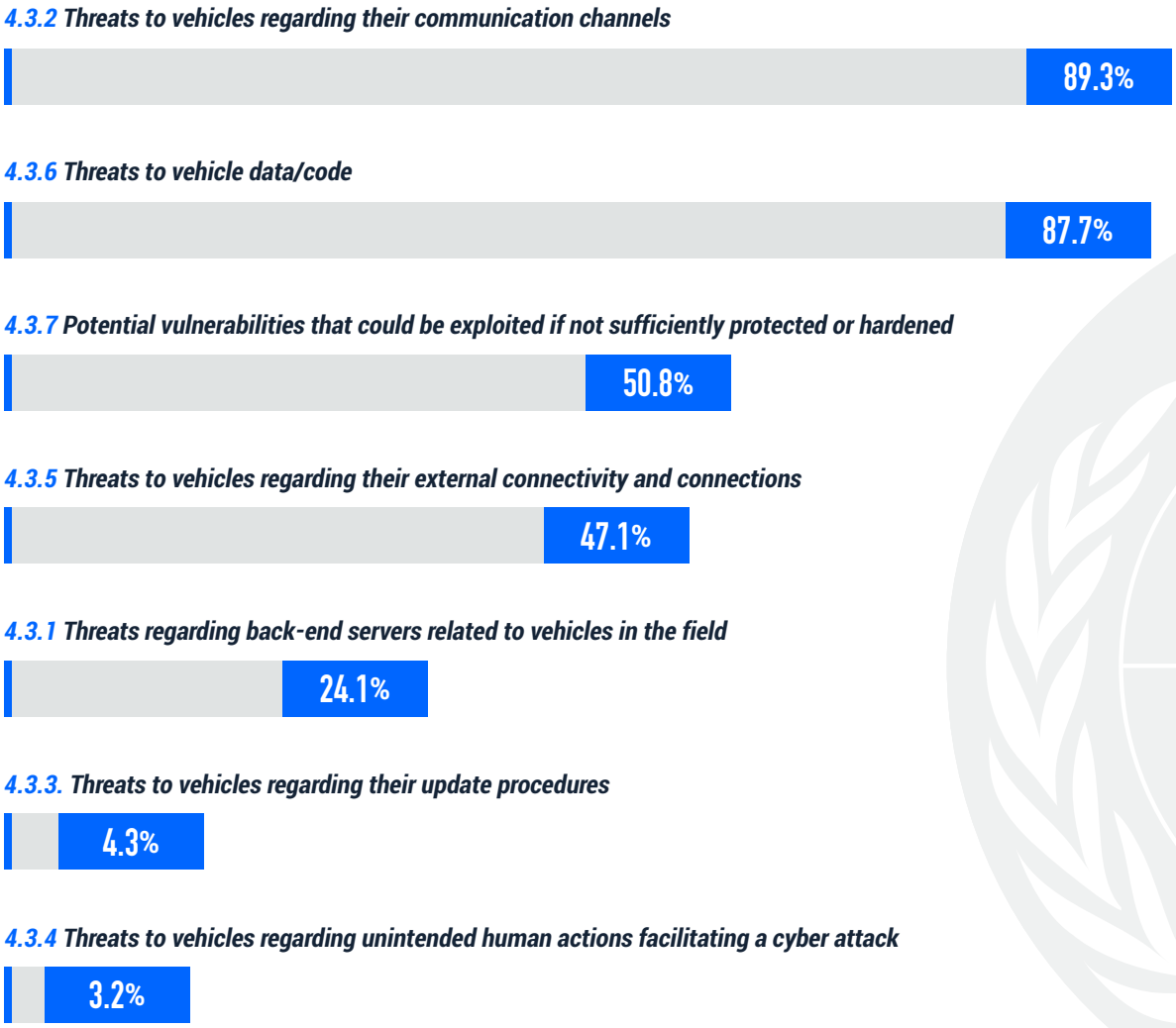
By 2025, a connected car will produce 25GB of data per hour and up to 500GB if fully autonomous.[7]

These come down to one central question that today's automotive leaders want to settle: How will companies protect the hundreds of millions of vehicles that are expected to be on the road by 2025, each expected to produce at least 25GB of data per hour, from today's known threats and unknown future threats?

DOES WP.29 R155 ALIGN WITH IN-FIELD THREATS?

Following the UNECE's 2020 announcement, Upstream's analysts characterized each incident from the full 2020 & 2021 calendar year into the framework of the seven threat categories mentioned in Annex 5 of WP.29 R155.

2020-2021 Cyber Incidents Categorized by WP.29 R155 Threats & Vulnerabilities



Source: Upstream Security

Upstream's research team analyzed publicly reported automotive cyber incidents that occurred in 2020 & 2021, correlating them to the seven threat categories presented in Annex 5 of R155. Some incidents fall into more than one threat category.

01

Threat #4.3.1

Threats regarding back-end servers related to vehicles in the field

24.1% *Distribution of incidents across R155 threats*

The regulation focuses on three specific elements of back-end server to:

1. Back-end servers used as a means to attack a vehicle or extract data
2. Services from a back-end server being disrupted, affecting the operation of a vehicle
3. Vehicle-related data held on back-end servers being lost or compromised ("data breach")

BREACHES IN THE FIELD

In violation of the section: "Abuse of privileges by staff (insider attack)," a North American EV OEM[8] accused one of its software engineers of downloading and stealing 26,000 private files in January of 2021. In a separate incident from August 2021, a Middle-Eastern rental[9] and leasing group experienced a network problem in one of its Telematics Service Providers (TSPs) such as outlined in section 2 of 4.3.1, forcing drivers to experience operational difficulties with their vehicles.

02

Threat #4.3.2

Threats to vehicles via their communications channels

89.3% *Distribution of incidents across R155 threats*

WP.29 R155 includes eight detailed descriptions of threats related to vehicle communication channels:

1. Potential spoofing of messages or data
2. Unauthorized manipulation of vehicle code and data
3. Unreliable or untreated messages that are permitted
4. Easily accessible sensitive information
5. Potential denial-of-service (DoS) attacks
6. Privileged access for an unprivileged user
7. Viruses embedded in communication media
8. Messages containing malicious content

BREACHES IN THE FIELD

In March 2019, researchers showed[10] that a North American OEM's vehicles were vulnerable to GPS spoofing attacks. During a test drive, a staged attack caused the car to slow down and unexpectedly veer off the main road. In May 2018[11] hackers found a vulnerability in a misconfigured back-end server run by a North American IoT software applications and telematics products and services provider (TSP).
This gave hackers direct access to critical databases that track the vehicle location, user information, and even what's needed to turn off an engine remotely.
In December that same year, a mechanic found a hidden dongle installed in a European OEM's[12] instrument cluster, displacing the CAN message to show mileage manipulation. Upon removing the hardware, the odometer spiked 40,000 kilometers, revealing the true odometer count and demonstrating how easily devices can penetrate and manipulate the vehicle data.

03

Threat #4.3.3
Threats to vehicles regarding their update procedures

4.3% *Distribution of incidents across R155 threats*

The regulation lists two possible threats related to vehicle update procedures:

1. Misuse or compromise of update procedures
2. Denial of legitimate updates

BREACHES IN THE FIELD

In April 2020, hackers[13] manipulated a European OEM's infotainment software update process. A vulnerability was exploited in the parsing mechanism of the infotainment firmware update process, which enabled the attacker to bypass integrity checks, giving unobstructed access to the infotainment system that controls the traction control and contains the owners personal data. Such an access could eventually lead to exploitation of other settings, including auto headlights.

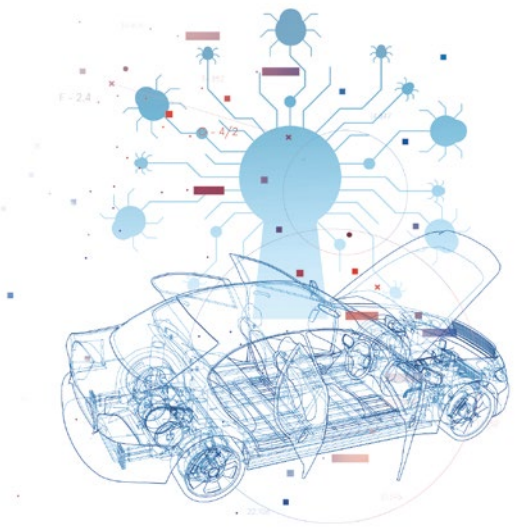
04

Threat #4.3.4
Threats to vehicles regarding unintended human actions facilitating a cyber attack

3.2% *Distribution of incidents across R155 threats*

The regulation lists two possible threats related to unintended human actions:

1. An owner, operator, or other authorized used being tricked into taking an action to unintentionally load malware or enable an attack.
2. Defined security procedures are not followed



BREACHES IN THE FIELD

The regulation outlines the danger of unintentional attacks initiated when legitimate actors take actions that could unwittingly open the door to an attack, listed as "Legitimate actors are able to take actions that would unwittingly facilitate cyber attacks."
This can occur when defined security procedures are not followed. For example: in mid-June 2021, the North American arm of a European luxury OEM experienced a breach, leaking the personal data of nearly 1,000 existing and prospective buyers[14].
The leak occurred because the data had been inadvertently stored in an unprotected manner on a cloud storage platform by a third-party vendor with access to the database. Although it was the vendor who failed to store the data in a secure location, violating the regulation, it was the OEM who was left exposed.
In another example, a major Asian OEM's confidential mobile app source code and internal tools were published online in January 2021[15]. The hackers gained access by taking advantage of a misconfigure Git server that was left with default credentials. As a result, their internal core mobile library, vehicle logistics portal, and parts of their proprietary diagnostics tool were all leaked.

05

Threat #4.3.5
Threats to vehicles regarding their external connectivity and connections

47.1% *Distribution of incidents across R155 threats*

WP.29 R155 lists three possible threats related to a vehicle's external connectivity and connections:

1. Manipulation of vehicle telematics, remote operation systems, and systems using short-range wireless communications
2. Hosted third party software, e.g. entertainment applications, used as a means to attack vehicle systems
3. Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems

BREACHES IN THE FIELD

In January 2021, a researcher hacked an infotainment unit in an Asian OEM's vehicle[16]. The hacker found a vulnerability in the in-vehicle infotainment system (IVI) whereby plugging in a USB device he was able to gain root shell access to the system.

Another example was in September 2021, when thieves used sophisticated hacking hardware to steal 25 European-made luxury cars in London[17]. Once gaining entry into the vehicle, they conducted a physical cyber attack involving connecting to the OBD port, reprogramming new keys, giving them full access to vehicle features.

06

Threat #4.3.6
Threats to vehicle data/code

87.7% *Distribution of incidents across R155 threats*

The UNECE WP 29.R155 regulation lists seven possible threats related to a vehicle's data and code:

1. Extraction of vehicle data/code
2. Manipulation of vehicle data/code
3. Erasure of data/code
4. Introduction of malware
5. Introduction of new software or overwrite existing software
6. Disruption of systems or operations
7. Manipulation of vehicle parameters

BREACHES IN THE FIELD

Vehicle software manipulation is a hazard to drivers, pedestrians, and the full OEM ecosystem. In September 2021, for example, owners of a North American EV OEM[18] in Europe were able to illegally use vehicle control system software by downloading a cracked version of the operating system, unlocking self-driving features and, potentially other sensitive telematics data. This cybersecurity breach not only opens potential vulnerabilities, it also puts the driver, passengers, and pedestrians in harm's way as the system was designed to recognize road signs commonly used in North America.

In another incident, Chinese authorities investigated an Asian OEM[19] following claims of crash-data manipulation from an accident that occurred while the driver assistance feature was activated. This is an example of data manipulation in order to falsify a vehicle's driving data (e.g., mileage, driving speed, driving directions, etc.).

07

Threat #4.3.7
Potential vulnerabilities that could be exploited if not sufficiently protected or hardened

There are six possible threats under "potential vulnerabilities":

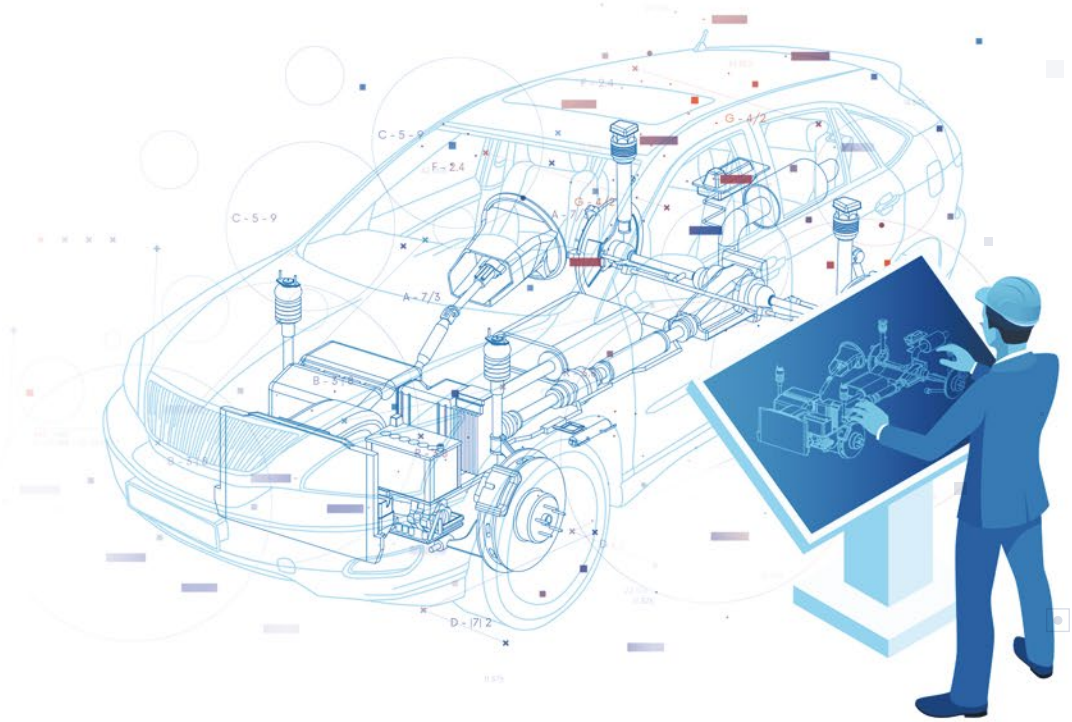
1. Cryptographic technology can be compromised or are insufficiently applied
2. Parts or supplies could be compromised to permit vehicles to be attacked
3. Software or hardware development permits vulnerabilities
4. Network design introduces vulnerabilities
5. Unintended transfer of data can occur
6. Physical manipulation of systems can enable an attack

50.8% *Distribution of incidents across R155 threats*

BREACHES IN THE FIELD

In September 2021, cybersecurity researchers from the Singapore University of Technology and Design found Bluetooth vulnerabilities in devices from various system-on-a-chip (SoC) vendors that are embedded in vehicle components[20]. Applying to part 3 of 4.3.7, this group of vulnerabilities, collectively referred to as BrakTooth (CVE-2021-28139), open the door to exploit a range of attacks, including denial-of-service (DoS) and arbitrary code execution in a vehicle. Their research revealed that BrakTooth affects over 1,400 different products across industries.

Flexibility is a crucial part of WP.29 R155 and ISO/SAE 21434, giving clear guidelines without hampering manufacturers' ability to bring new technologies to market.



ISO/SAE 21434 IN SUPPORT OF UNECE WP.29 R155 & R156

A key differentiator between WP.29 R155 / R156, ISO/SAE 21434 is that ISO/SAE gives a deep methodology on how OEMs and Tier suppliers calculate the risk score of an asset and to prioritize vulnerability urgency.

The standard provides a structured cybersecurity framework, establishing cybersecurity as an integral element of engineering throughout the lifecycle of a vehicle from the conceptual phase through decommissioning.

ISO/SAE 21434, R155, and R156 in practice

Security by design

Predict what security flaws may appear in the future after the vehicle leaves the dealership.

R155 CSMS

Continuously monitor for faults during and after production.

TARA

Assess risk and issue a risk score.

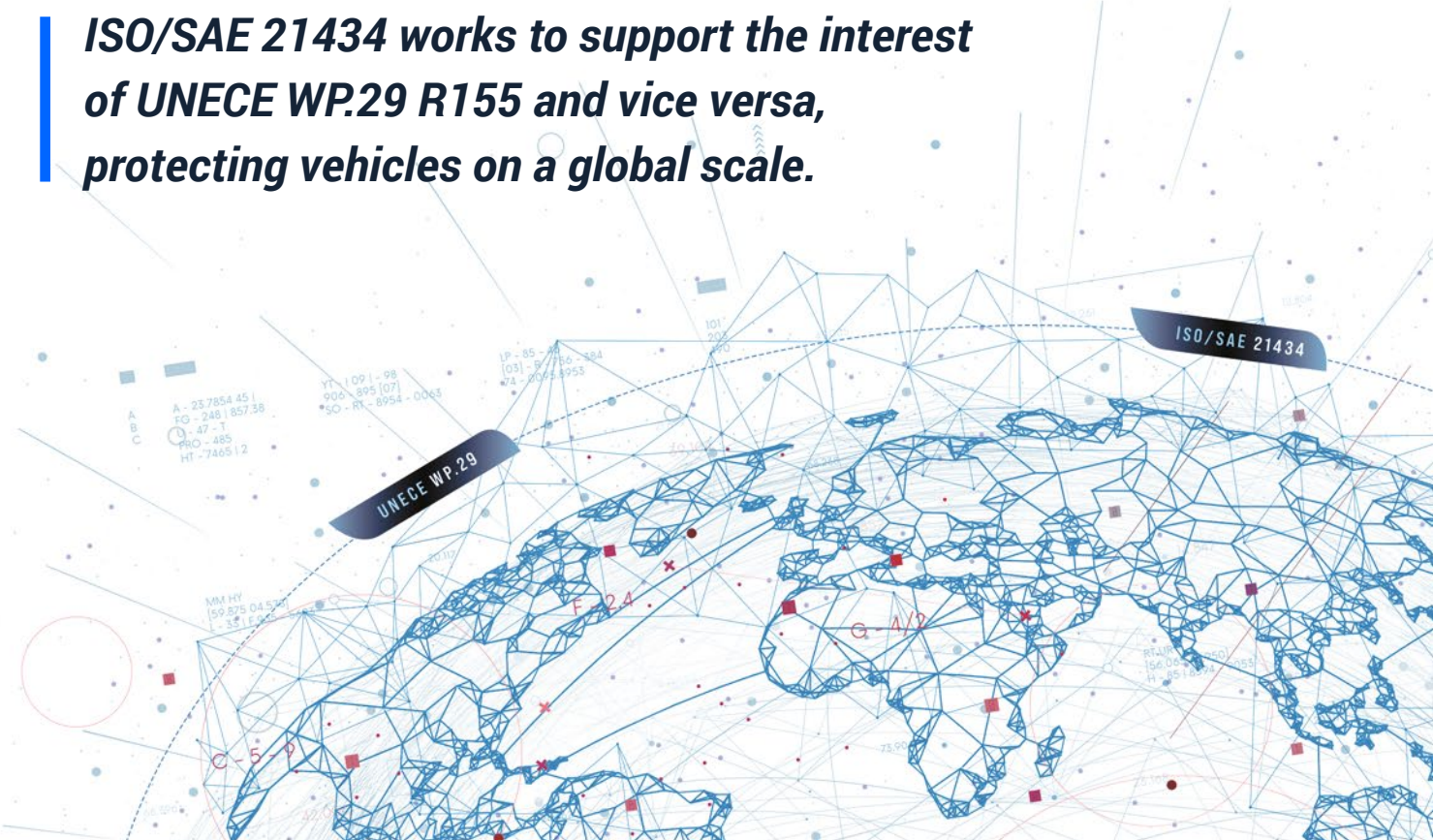
Early detection & rapid response

Rapidly respond with a fix according to R155.

R156 SUMS

Continuous updates allow OEMs to avoid recalls OTA updates in line with R156 when possible.

ISO/SAE 21434 works to support the interest of UNECE WP.29 R155 and vice versa, protecting vehicles on a global scale.



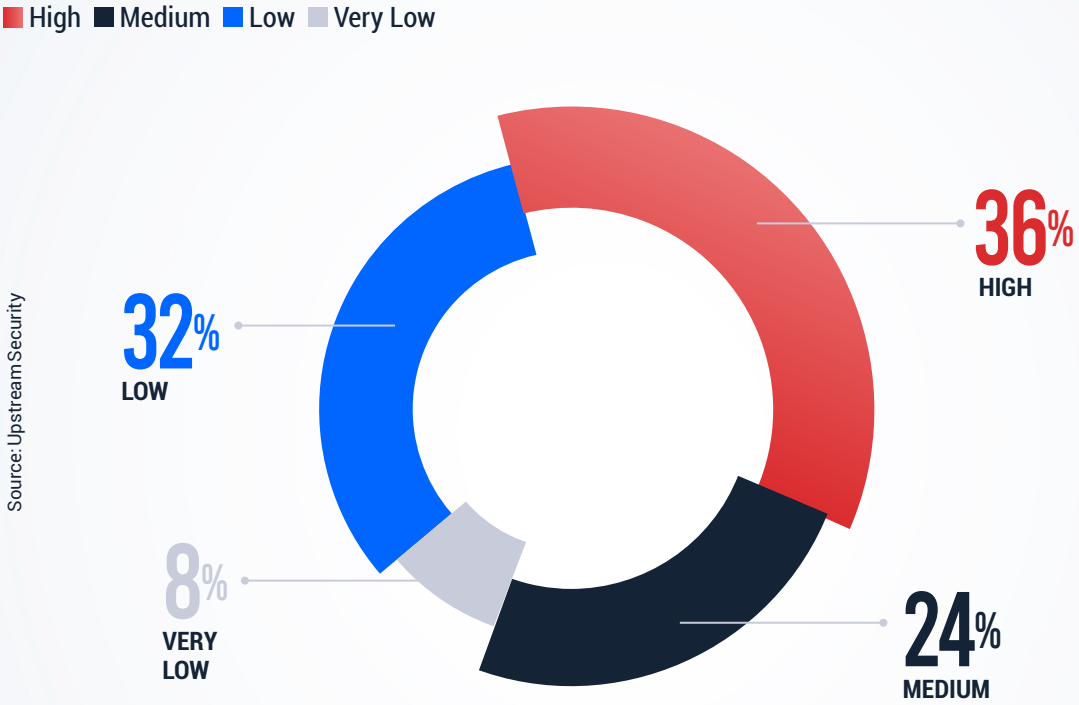
THREAT ANALYSIS & RISK ASSESSMENT (TARA)

The standard specifically requires OEMs to analyze threats and risks throughout a vehicle's lifecycle in order to determine the extent to which a road user can be impacted by automotive cyber threats and vulnerabilities. This process of "threat analysis and risk assessment" is called TARA, which is done by calculating the impact and feasibility of known and cataloged cyber threats, also known as CVEs (Common Vulnerabilities & Exposures). (See chapter 3 for more about CVEs)

The ISO/SAE standard explains that one way to determine feasibility is to use the CVE's CVSS 3.X (Common Vulnerability Scoring System) exploitability score, which has values that range between 0.12 (very low) and 3.89 (high).

When looking at the average CVSS 3.X exploitability scores of 209 automotive-related CVEs recorded that include a CVSS 3.X scoring (since 2015 when the CVSS 3.X scoring method began), more than 75% of the CVEs had CVSS exploitability scores that were graded as "medium" and "high", highlighting the high level of threat that many automotive vulnerabilities carry.

Automotive CVE Attack Feasibility Ratings and CVSS Version 3 Exploitability Scores:



Based on 221 automotive-related CVEs 2016-2021. Attack feasibility ratings according to ISO/SAE 21434.

Ultimately, what kind of risk does this pose to the owner or driver of the vehicle?

THE EVOLVING FACE OF HACKING

State hacking

The ongoing battles occurring in the cybersecurity space are said to be carried out by state-sponsored hacking groups who are increasingly targeting public systems that impact the day to day lives of its citizens. Like many hacks, it is difficult to pinpoint their locations or any official government approval to their actions, yet they focus on similar targets and impact.

2021 saw reports of cyber attacks carried out against countries' assets and civilians.

USA
Transportation firms hit by potentially foreign-sponsored cyber attacks

Discovered in November 2021, American companies including healthcare and transportation firms, were hit by cyber attacks conducted by foreign government-backed groups that have been operating as far back as September 2020. According to a cybersecurity alert published by the U.S. Department of Homeland Security (DHS), the hacking group had launched disruptive cyber attacks against a wide range of U.S. companies as the hackers managed to exploit old software vulnerabilities in products made by major software developers to break into victim computer networks[21].

HONG KONG, PHILIPPINES, AND TAIWAN
Hit by cyber attacks

An American-Japanese multinational cybersecurity software company claims that regional state-sponsored threat actors have been targeting transportation organizations and government entities related to the transportation sector since the middle of 2020. The threat actors have been around since 2011, conducting cyber attacks against organizations in government, healthcare, high-tech, and transportation sectors in Hong Kong, the Philippines, and Taiwan[22].

IRAN
Hit by what they claim are state sponsored hackers

The database of the Iranian Traffic Police was leaked and sold on the deep web. The breached database was found for sale and included complete 2021 profiles of Iranian vehicles, including motorcycles and private vehicles, as well as governmental, public and industrial vehicles[23]. In another incident, a cyber attack on Iran, which was claimed to be executed by state-sponsored hackers, disrupted operations at 4,300 gas stations[24].

ISRAEL
Transportation companies hit by a ransomware attack executed by what appears as foreign state-backed hacking group

Two major Israeli public transportation companies were hit by a ransomware attack and had their data leaked to the darknet. In addition to the stolen data, the attack had brought the companies' websites down[25].

Black-hat actors for profit

One of the classic reasons for tinkering, hacking, and manipulating cars systems is for financial gain through criminal acts. Unfortunately, the increased availability of relatively low-cost hardware, combined with more people being furloughed may have contributed to a wave of thefts.

In the first half of 2021, 124 vehicle thefts[26] occurred in Oakville, Canada alone, a city of only 211,000 residents. Sixty-six of these thefts involved a keyless entry or programming technology, and 42 of the 124 thefts took place in only four weeks. Equally concerning is the confidence in which these gangs operated, carrying out attacks in broad daylight. In under a minute, luxury vehicles can be spotted, compromised, and driven away.

As sophisticated hardware and hacking tutorials become easy to obtain, large-scale thefts are occurring in all regions around the globe, including the US, Europe, Canada, Australia, and elsewhere.

Hacking for personal gain

The desire to tinker with the inner workings of vehicles has brought us romanticized stories of bootleggers outrunning authorities and even led to NASCAR's creation. But during COVID-19 lockdowns people were at home, tampering with the system hardware or software, potentially compromising multi-vehicle networks' safety, privacy, and reliability.

Independently tampering with vehicle software or hardware can expose a vehicle's owner to unwanted repercussions. For example, installed software, found on the internet in a forum may have embedded vulnerabilities that can be exploited by hackers, allowing them to obtain data, manipulate data, and potentially carry out a cyber attack.

This has led to an increased interest by insurance companies to use vehicle telematics and technologies to better understand attacks and trends.

> ***Popping the digital hood of a car to tune its performance creates opportunities for hackers to compromise personal property and safety.***

SUPPLY CHAIN

Both UNECE WP.29 R155 and ISO/SAE 21434 specifically address these risks by requiring the full automotive ecosystem to work together to secure the whole supply chain. Nearly all risks outlined in the United Nations regulation apply to multiple parties to ensure that communication systems and electronic components are secure during production, delivery, and throughout the vehicle's entire lifetime. Some guidelines are directly related to cyber threats targeting Tier-1 and Tier-2 components, to protect against malicious internal CAN messages, manipulation of functions designed to remotely operate systems like remote key fobs, immobilizers, charging piles, and prevent access by corrupted applications.

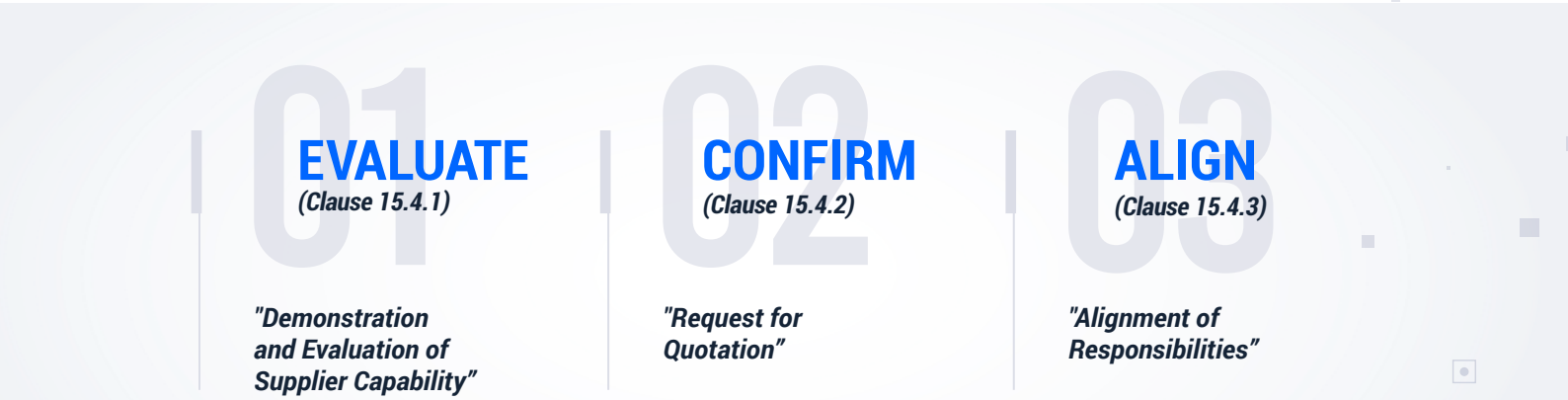
Nowadays, the UNECE WP.29 R155 CSMS regulation and the ISO/SAE 21434 standard both call for management of the automotive supply chain.

The WP.29 R155 regulation indicates that the onus of supply chain cybersecurity management lies upon the OEM. It is their responsibility to conduct due diligence into the cybersecurity practices of their supplies. Now, it is the vehicle manufacturer's responsibility to ensure that all vehicle components and parts, both hardware and software, are secure.

Furthermore, WP.29 R155 demands (in Section 5.1.1) that the OEM must "collect and verify the information required under this regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed."

The ISO/SAE 21434 standard also highlights the importance of supply chain management. Clause 15 of the standard focuses on "distributed cybersecurity activities" and discusses the cybersecurity relationship between OEMs, Tier-1, and Tier-2 suppliers.

The standard indicates that an OEM is responsible for ensuring that its suppliers are implementing methods to ensure their products and components are cyber secure and recommends the implementation of three main strategies to develop a successful supplier and OEM relationship:



ISO/SAE 21434 steps for companies, OEMs, and their suppliers to take to align on vulnerabilities and incidents.

SURGING DEMAND AND CHIP SHORTAGES

The early days of the COVID-19 pandemic saw mass-cancellations of automotive components as the industry braced for the impact of a volatile economy and stay-at-home requirements around the globe. As new vehicle orders came roaring back, there were bottlenecks and difficulties securing electronic components from manufacturers. This created an opportunity for counterfeit chips to enter the market that had major financial and potential cybersecurity implications in addition to an increase in car thefts for functioning after-market chips.

A dangerous inconvenience

The recent chip shortage, caused by multiple factors including COVID-19, supply chain bottlenecks have left a window of opportunity[27] for black-hat actors to flood the market with counterfeit parts, components, and chips.

> ***Counterfeit after-market components are a hazard to driver safety and their vehicle's security.***

While some legitimate resellers are dusting off old chips from their shelves, which can manage modern vehicle computing demands, some fraudsters create counterfeit versions of vehicle chips, making them look like they came from legitimate sources but cannot perform as needed. Even more of a hazard are the ones that work correctly but are unreliable, experiencing premature wear out and failing while in mission mode.

In the case of fraudulent components, a single device is enough for a hacker to obtain critical telematics information, such as location details, manipulate in-cabin microphones, vehicle override authority, and a host of other dangerous activities. This is in addition to their ability to gain insight into the activities of each vehicle and its owner.

THE CHIP SHORTAGE'S FINANCIAL IMPACT

The chip shortage has created parking lots full of inoperable vehicles[28] around automotive manufacturing facilities across the globe and is estimated to have cost the automotive industry $210 billion in revenue[29] in 2021.

In April 2021, A European OEM warned against a big production hit in the second quarter of 2021 due to a global chip shortage. The OEM warned that the global shortage of semiconductors affecting car production would worsen in the upcoming months[30].

In addition, an Asian OEM reported it would reduce production by 40% in August 2021, affecting most of its production lines. The OEM's reductions in North America were estimated to be between 40% to 60% that month, and the reductions meant the OEM would produce between 60,000 and 90,000 fewer vehicles[31].

Another North American OEM produced 700,000 fewer vehicles than planned due to the parts shortages[32]. At the same time, a North American OEM closed plants in the US, Canada, and Mexico for two weeks in September for the same reason. This is after they temporarily closed plants in April due to the shortage. During an earnings call, a single North American OEM worried that the shortage would impact between $1.5 and $2 billion of revenue by the end of 2021[33].

While each company manages the shortage differently, no OEM is clear from the widespread impacts or counterfeiting risks of this global chip shortage. In addition, OEMs, Tier-1s, and Tier-2 manufacturers must also contend with other cyber attacks, further hampering production (See Chapter 5 for more information).

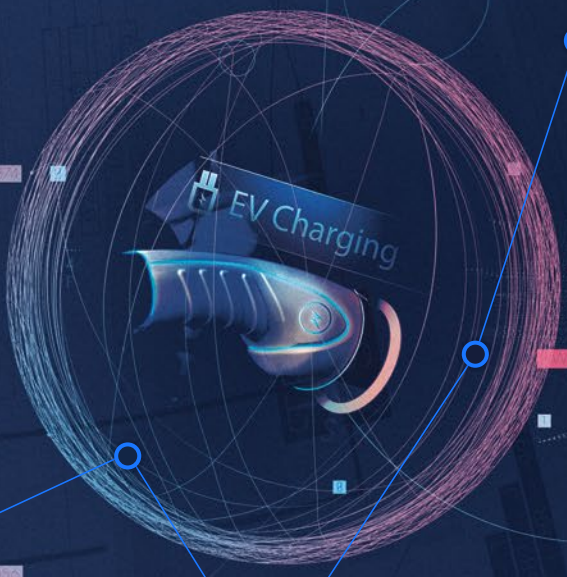
Reseller responsibilities

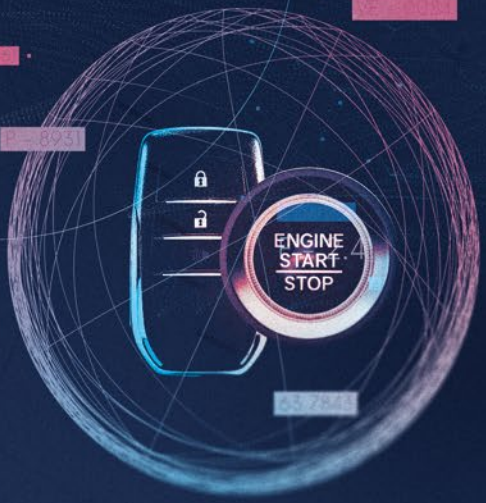
Besides for the chip shortage, scarce supply, and rising costs of new vehicles created a boom in the used-car market[34]. But with most sellers and buyers unaware of the level of computerization that vehicles have experienced in the last decade, personal data was left exposed without sellers or dealerships realizing it.

This can take the form of failing to clear saved GPS locations, not removing Bluetooth pairing information, and perhaps the most dangerous, not removing access to vehicles on various smartphone applications. An example of this is when a vehicle lessee in the USA was able to log into his vehicle's mobile application in February 2020[35] and obtain critical data on the car he returned four years earlier. He could lock, unlock, remotely start, and even track the vehicles he no longer leased, all from legitimate applications. (See more details about attack vectors in Chapter 3)

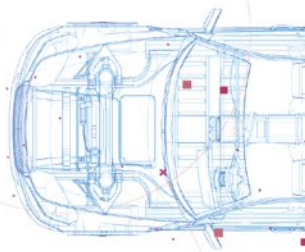
CHAPTER 2

AUTOMOTIVE CYBER THREAT TRENDS





INCIDENTS



2021 saw an increase in sophisticated attacks that brought challenges to the entire automotive ecosystem and local authorities who worked to find cybersecurity solutions against all existing and developing attack vectors and clamp down on black-hat actors.

As the UNECE, ISO, and SAE implement new standards and regulations, it remains to be seen if measures will deter black-hat actors or drive them to develop more sophisticated procedures.

Top incidents in 2021:

JANUARY

A hacker exploited a vulnerability in a major European Tier-1 infotainment system that was deployed in an Asian OEM's vehicle. This was achieved by plugging in a USB device, then executing the exploitation to gain root shell access to the system.[36]

FEBRUARY

An Asian OEM's American business arm experienced a ransomware attack by the DoppelPaymer gang, who demanded $20 million in exchange for a decryptor and not leaking stolen data.[37]

APRIL

A North American insurance agency with some 17 million vehicle policyholders, experienced a data breach that compromised drivers license ID numbers in early 2021.[38]

JUNE

Hackers exploited a feature in modern vehicles' ECUs, and managed for the first time to misuse it and remotely attack other ECUs. The hackers managed to attack and shutdown the powertrain ECU and power steering ECU in to vehicles.[42]

A data breach hit two European OEMs, impacting more than 3.3 million customers and prospective buyers in North America.[41]

MAY

Numerous vulnerabilities discovered in a European manufacturer's infotainment system, which could be exploited to take control of multiple in-cabin functions.[40]

APRIL

The doors of a North American EV manufacturer's vehicle were hacked using a drone carrying a Wi-Fi dongle, exposing the vulnerabilities these vehicles have to wireless adjacent attacks.[39]

JULY

Hacking the CAN bus of a European OEM's vehicle, a hacker was able to wirelessly transmit vehicle data to a third party device.[43]

AUGUST

An Asian EV OEM was investigated by the Chinese law enforcement due to claims that car data was tampered with following a fatal collision.[44]

Hackers exposed multiple vulnerabilities in the operating system used by major agriculture OEMs, allowing black-hat actors to remotely manipulate machinery, even taking them out of service.[45]

DECEMBER

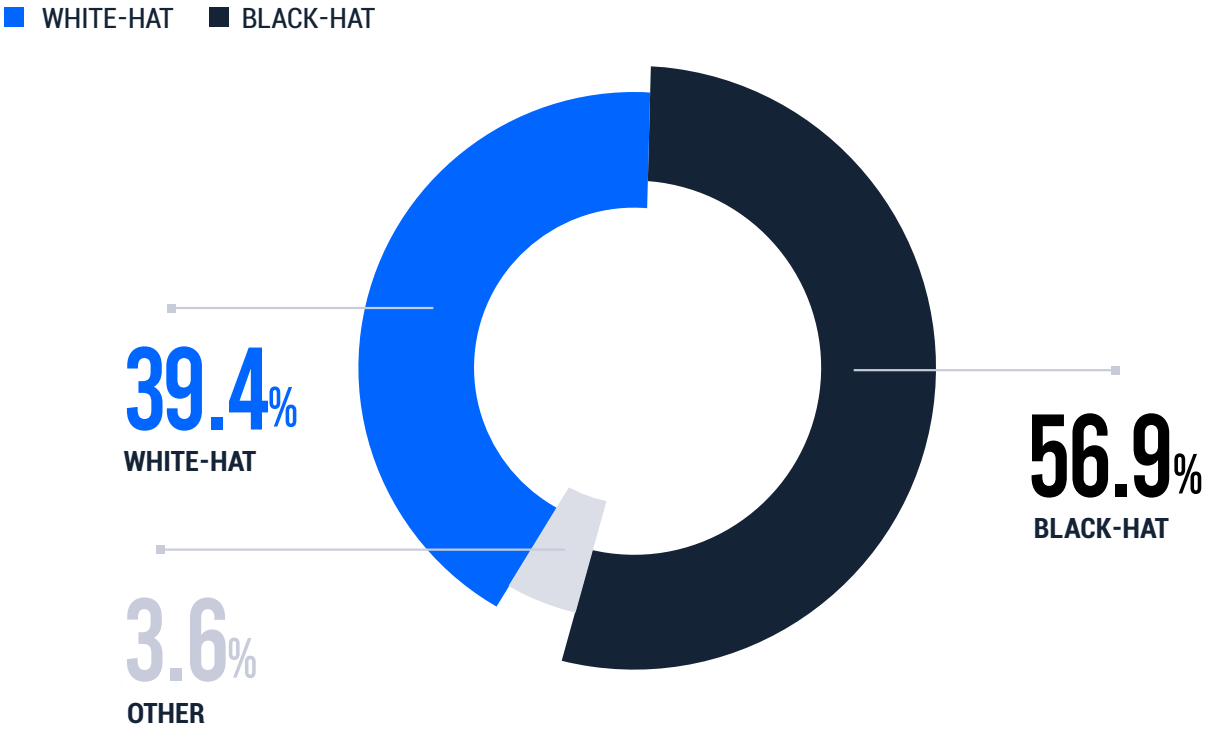
Researchers found vulnerabilities affecting devices or properties embedded in or used for connected cars, chargers, in-vehicle infotainment (IVI) systems, and digital remotes with car chargers were at risk, including vehicle-to-grid (V2G) systems in Europe.[46]

WHO IS ATTACKING?

In 2021, the majority of attacks were carried out by black-hat actors.

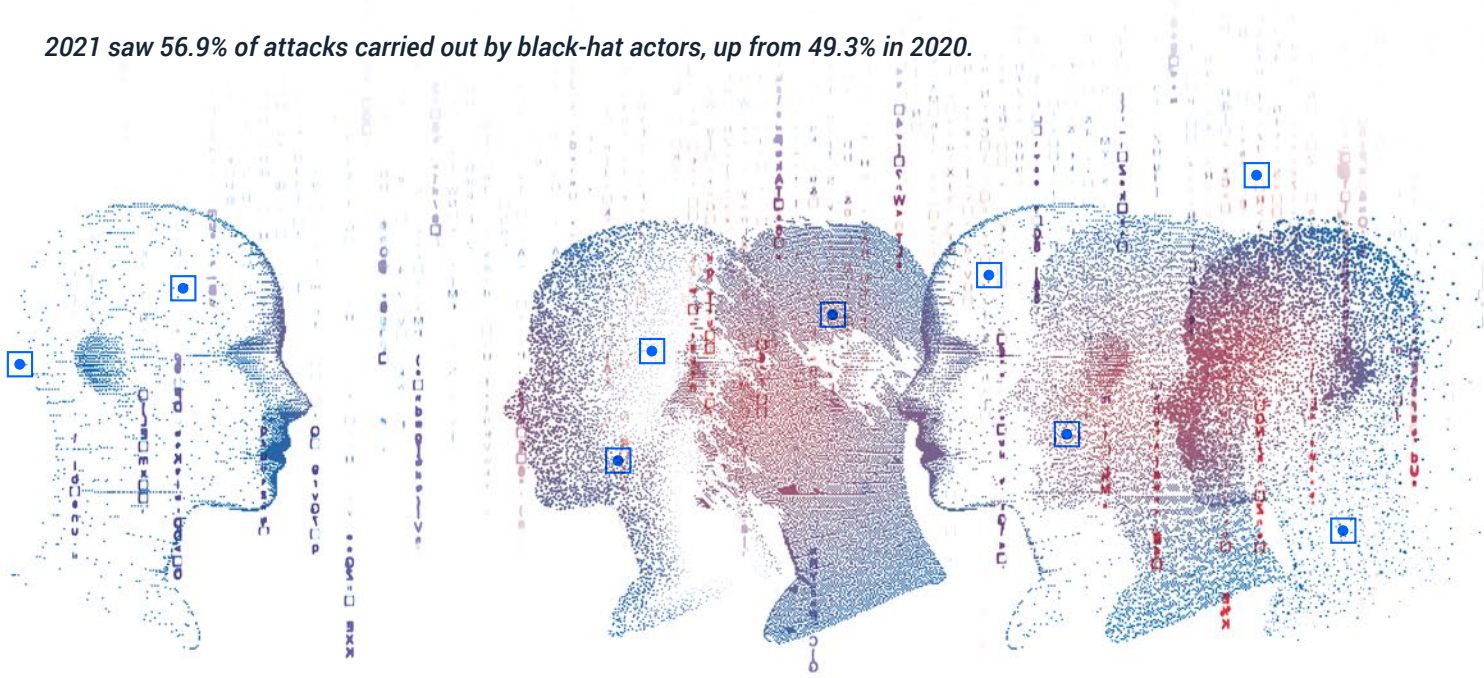
While white-hat hackers manipulate systems and discover vulnerabilities for the sake of educational research to improve vehicles' cybersecurity, black-hat hackers have an agenda that frequently aligns with criminal activity.

Black-hat actors continued to outpace white-hat hackers in 2021



Source: Upstream Security

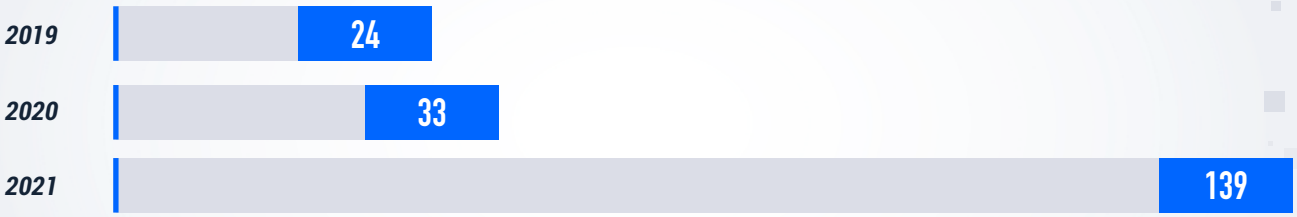
2021 saw 56.9% of attacks carried out by black-hat actors, up from 49.3% in 2020.



HOW ARE CVES PRIORITIZED?

Common Vulnerability Scoring System, CVSS, is a vulnerability scoring system designed to provide an open and standardized method for rating CVEs. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal, and environmental properties of a vulnerability[47]. The CVSS score given to each vulnerability, defines whether it is Critical, High, Medium, Low, or None[48].

Number of automotive-related CVEs found in 2019-2021:



Source: Upstream Security

To date, there have been 232 CVEs related to the automotive industry, 139 in 2021 compared to 33 in 2020

In general, CVSS scores have practical applications and as such affect security teams, developers, and researchers in companies that are part of the supply chain of a product prioritize efforts for patching these vulnerabilities, allocating resources, investing more time and human resources, and also checking whether the vulnerabilities had already been exploited.

In the automotive industry, one component can be used by multiple OEMs in different environments. As such, a vulnerability in one could not be explored evenly by various OEMs. This aspect of risk assessment is also addressed in the Risk Assessment Methods ISO/SAE 21434 standard.

Cybersecurity companies should not neglect any vulnerabilities and continuously search for any misuse or exploitation of all vulnerabilities that may affect their products, including reviewing, researching, and patching both Low and Medium scored incidents.

PHYSICAL ACCESS VS. REMOTE ACCESS

Our analysts divide cybersecurity incidents into two main categories: Physical attacks, where the hacker needs physical access to its target, and remote attacks, where the hacker can strike from a short or long distance without physically being connected to the car.

In January 2021[49], a researcher hacked an infotainment unit in an Asian OEM's vehicle. The hacker found a vulnerability in the infotainment system whereby plugging in a USB device, he was able to gain root shell access to the system.

An example of a short-range attack occurred in the UK in July 2021 when a European-made vehicle was hacked and stolen outside its owner's home[50] by an exploitation and misuse of a remote keyless entry system. The thieves used a relay attack device aimed at the house to activate the ignition and drive away in the stolen car.

While long-range attacks have primarily occurred in specific white-hat-controlled environments[51], experts fear that increased connectivity means it is only a matter of time until a black-hat actor executes this attack.

2021's short vs. long-range attacks

Source: Upstream Security

Between 2010 and 2021, 84.5% of the reported attacks were remote, while 15.5% required physical access to the target. This trend is likely to continue as the number of connected components in vehicles increases and long-range accessibility becomes more reliable via cellular networks.

Remote attacks greatly outnumbered physical attacks in 2021

Source: Upstream Security

With vehicles becoming more connected, the need for physical access to a car in order to hack it reduces significantly.

NEWLY CATALOGED COMMON VULNERABILITIES & EXPOSURES

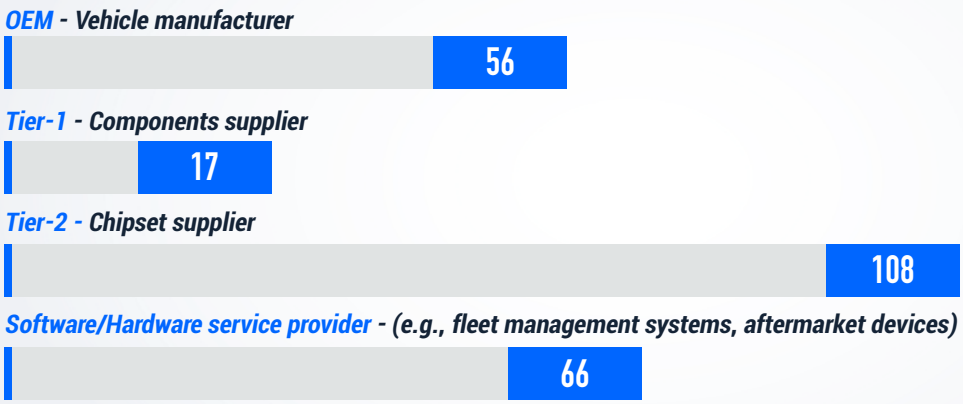
Common Vulnerabilities & Exposures (CVEs) are acknowledged and cataloged cybersecurity risks that can be quickly referenced across the automotive ecosystem. These threats are commonly found directly on OEM products; however, they may also appear throughout OEMs' supply chain companies' products.

In 2021 alone, there were 139 new CVEs related to the automotive industry. These CVEs varied from vulnerabilities discovered on a chip used in a system towards a vehicle or vulnerabilities found on vehicle systems. For example, in October 2021, a vulnerability (CVE-2021-0583)[52] was found on a Bluetooth pairing transaction in the Android Automotive operating system, allowing Bluetooth to be enabled in the vehicle without user consent. Such an action could lead to a local escalation of privilege with user execution privileges needed.

Two months earlier, in August 2021, a North American software company announced that one of its most popular products, an in-vehicle infotainment operating system, contains a high-level risk security vulnerability[53] (CVE-2021-22156). The vulnerability can be exploited remotely and allows an attacker to perform a denial of service (DoS) attack or execute malicious commands on the affected device.

OEMs who manufacture the vehicles assemble them from dozens of software and hardware modules produced by Tier-1s suppliers. These components are constructed from various individual components supplied to the Tier-1s by their Tier-2s. Each component's quality and safety are entrusted to the company that produces it. Therefore, the importance of overseeing the quality and safety of each automotive-related product, is the responsibility of each company in the supply chain. As vulnerabilities and flaws are not always addressed on time, or at all, all it takes is a flaw in one commonly used chip's design to dangerously impacting millions of vehicles.

Breakdown of publicly reported automotive-related vulnerabilities



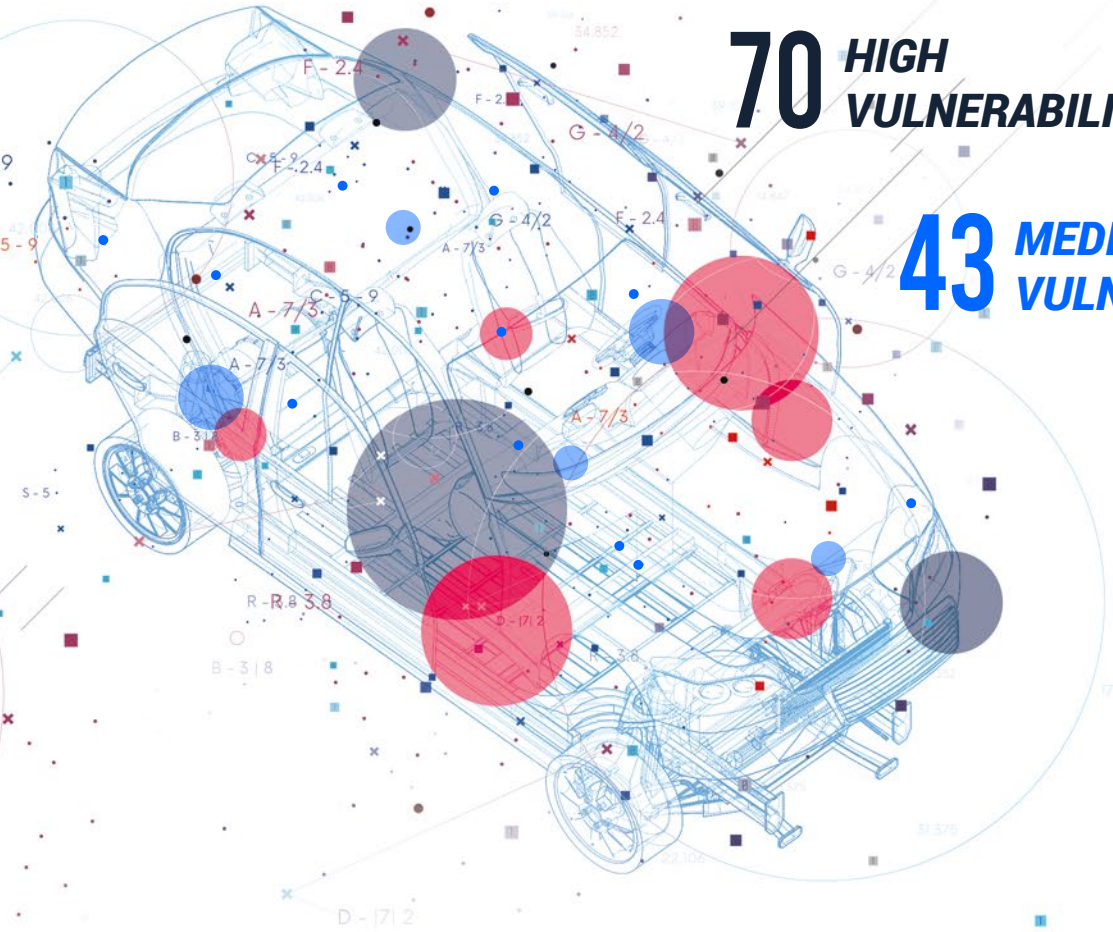
CVEs

In 2021, the CVSS-scored vulnerabilities found by Upstream's analysts had:

26 ***CRITICAL VULNERABILITIES***

70 ***HIGH VULNERABILITIES***

43 ***MEDIUM VULNERABILITIES***



Source: Upstream Security

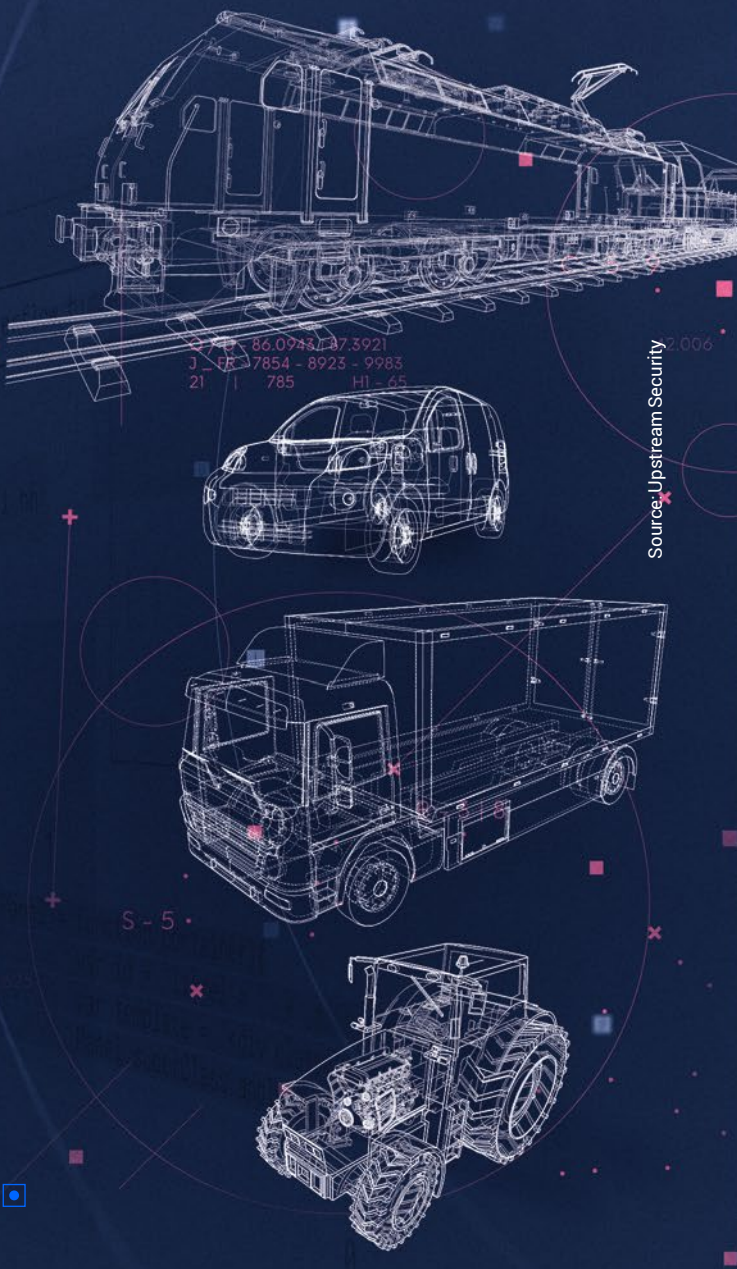
Will regulations help mitigate against cyber attacks?

With 139 new CVEs discovered in 2021, each company must address and implement proper mitigation techniques to protect their products against both existing and yet unknown vulnerabilities that may arise down the road. VSOCs (Vehicle Security Operation Center) must be maintained to enforce continuous monitoring for over a decade after vehicles roll off the assembly inline order to keep in line with the ISO/SAE 21434 standard.

WHICH INDUSTRIES ARE IMPACTED?

No segment of the connected vehicle ecosystem is clear from the threat of cyber attacks.

- *OEMs*
- *Tier-1s*
- *Tier-2s*
- *Electric Vehicles*
- *TSP / Fleet Management*
- *Trains*
- *Car Sharing*
- *Car Rental*
- *Car Dealerships*
- *Insurance*
- *Logistics & Delivery Fleets*
- *Autonomous Vehicles*
- *Ride Sharing*
- *Public Transportation*
- *Ride Hailing*
- *Government Fleets / Emergency Services*
- *Smart Cities*
- *Bike Sharing*
- *Agriculture*



Source: Upstream Security

Sectors that have expanded their digital footprints, such as the Agriculture and the Car rental sectors, have dealt with new attacks and more eminent concerns about the people they serve.

EXPANDING RISKS IN ESTABLISHED SECTORS

Insurance

The insurance industry has undergone significant changes with the increased availability of telematics data in recent years. The industry is uniquely positioned to analyze multiple data streams, including driver habits, not for everyday usage or vehicle ability but to calculate premiums and put a dollar value on each vehicle.

Cybersecurity is an essential factor in calculating these premiums, requiring companies to understand the security posture of each vehicle make and model. Unfortunately, the expertise to do these assessments is outside the core expertise of insurance underwriters and therefore they have to collaborate with automotive cybersecurity experts to specify the relevant risks.

A cyber attack on a vehicle may even impact an insurance company's IT network. Similar to OEMs, some insurance companies communicate with their insurers' vehicles as well.

Connected agriculture

Conflicts over agricultural vehicles made big headlines in 2021[54]. Farmers who were looking to self-repair their equipment turned to online forums where they began swapping codes, manipulating their tractor systems and data. As such, the industry has experienced an increase in cyber attacks against this previously unnoticed sector.

Two significant incidents in agriculture vehicles were found this year. For example, in August 2021, security researchers found multiple vulnerabilities in the operating systems of two agriculture vehicle makers and providers of farm machinery that compromised the security of the vehicles[55]. Earlier in April 2021, the group discovered two vulnerabilities that allowed access to data of all customers who had purchased tractors or equipment from these makers[56]. These vulnerabilities, found in company apps and websites, could allow hackers to find and download the personal data of all owners of the farming vehicles and equipment. This data was then made available on the deep and dark web (see more about the deep and dark web in Chapter 5).

Government

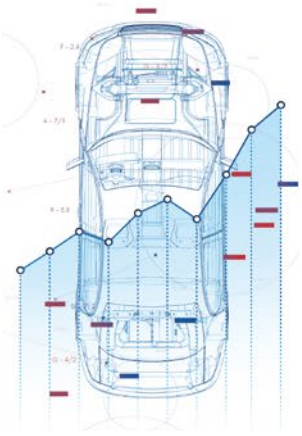
Automotive cyber attacks have also impacted governments. For example, in February 2021, the governmental transport agency for New South Wales, Australia[57] (TfNSW) was affected by a cyber attack on their file-sharing system, where hackers stole customer data[58]. In addition, in March 2021, Connecticut and seven other states' Division of Motor Vehicles (DMVs) experienced an attack[59] against their emissions software vendor. The attack affected the states' vehicle emissions testing programs leading to emissions testing suspensions in Connecticut, Massachusetts, and six other states at the beginning of April 2021.

In another incident that same month, New York City's subway and bus transit system, operated by the Metropolitan Transportation Authority (MTA), was targeted in a ransomware attack. The attack exposed vulnerabilities in the world-renowned transportation network that serves 5.5 million riders daily. The attack did not involve financial demands but instead appeared to be part of a recent series of major US infrastructure intrusions by sophisticated hackers[60].

49.3%

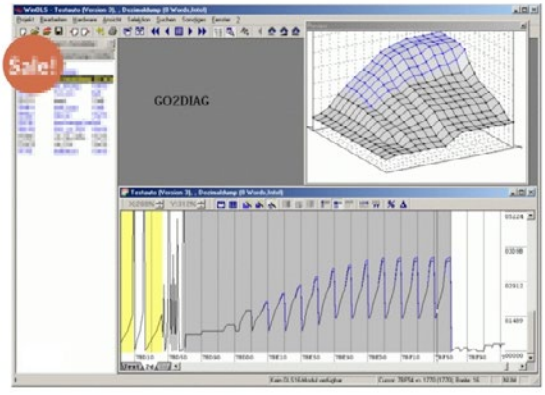
INCREASE ESTIMATED RISE IN NEW CONNECTED CARS SHIPPED FROM 2019-2023

STATISTA[61]



KNOWLEDGE SHARING BEYOND TRADITIONAL HACKERS

2021 saw individuals turn to online forums to learn how to repair vehicles without paying local dealerships. As a result, many forums and new communities allowed people to raise questions and receive help from hackers. In these cases, solutions are not approved or reviewed by OEMs. This led to individuals, who potentially do not hold extensive software or hardware knowledge, to tamper with sensitive instruments. This created new vulnerabilities, voided warranties, and created safety issues where there had been none prior.



HOME / CARS

ECU Remapping lessons Guides softwares tuned files damos ALL IN ONE

ECU Remapping lessons, Guides ,software and tuned files damos ALL IN ONE
All you need for starting remapping cars in one. Remapping software – EGR DPF OFF software (winols,ecm titanium,ecu safe) guides for winols and ecm titanium step by step (avi,pdf) super damos and tuned files pack.

See more information about citizen hacking in Chapter 5: What's Hiding in the Deep and Dark Web

EV CHARGING POINTS

While electric vehicles are vulnerable to all attacks mentioned above, they are also subjected to another realm of attacks. Thus, they can be impacted by vulnerabilities within the electric vehicles charging station (EVCS) ecosystem, and these security weaknesses can affect multiple EVCS components.

These include charging points, charge point operators (CPOs) that provide network infrastructure, and even the distribution system operators (DSO), which manage the energy distribution networks. In July 2021, researchers discovered numerous security flaws in a range of smart electric vehicle (EV) chargers[62]. The researchers could remotely switch the chargers on and off, remove the owner's access, and lock or unlock the charging cable. Furthermore, they claimed a bad actor could steal the vehicle owner's identity, stop the owner from charging their vehicle, then charge their own vehicle free of charge. One of the researchers also claimed that changing the programming on the device would allow an attacker to permanently disable the charger or use it to attack other chargers or servers. What's more, black-hat actors can infiltrate a home network in cases where the chargers are Wi-Fi connected.

The network effect could be potentially profound as charging networks use the Open Charge Point Interface (OCPI) protocol — a protocol which was designed to make charging seamless between different charging networks and operators, allowing interoperability between charging networks. However, this protocol also means that a weakness in one charging network could affect the entire power grid of charging stations, as a vulnerability in one platform could potentially create a vulnerability in another.

Ultimately, most smart EV charging points researched were vulnerable to attacks. Taking advantage of these vulnerabilities has the potential to affect millions of vehicles, enable remote control of the charging process, and act as a vector to steal information.

One weakness in one of the chargers enabled pushing attacker firmware to the charger remotely, although this specific attack vector was not researched, it could be inferred that pushing malicious firmware to chargers could be used as means to a multi-vehicle attack through the vehicle charging interface.

In December 2021[63], researchers looked into how Apache Log4j Java-based logging library vulnerabilities affected devices or properties embedded in or used for connected cars, chargers, in-vehicle-infotainment (IVI) systems, and digital remotes. Their research found that car chargers were at risk, including vehicle-to-grid (V2G) systems in Europe. The V2G system allows stored energy in car batteries to be redistributed over the grid to help balance demand concerning the production level. In addition, they found that a car's IVI system, which uses a complex OS, could also be compromised. The researchers showed that by exploiting Log4j vulnerabilities, they could execute attacks on the vehicles and their connected infrastructure. (See more on V2X chapter 3)

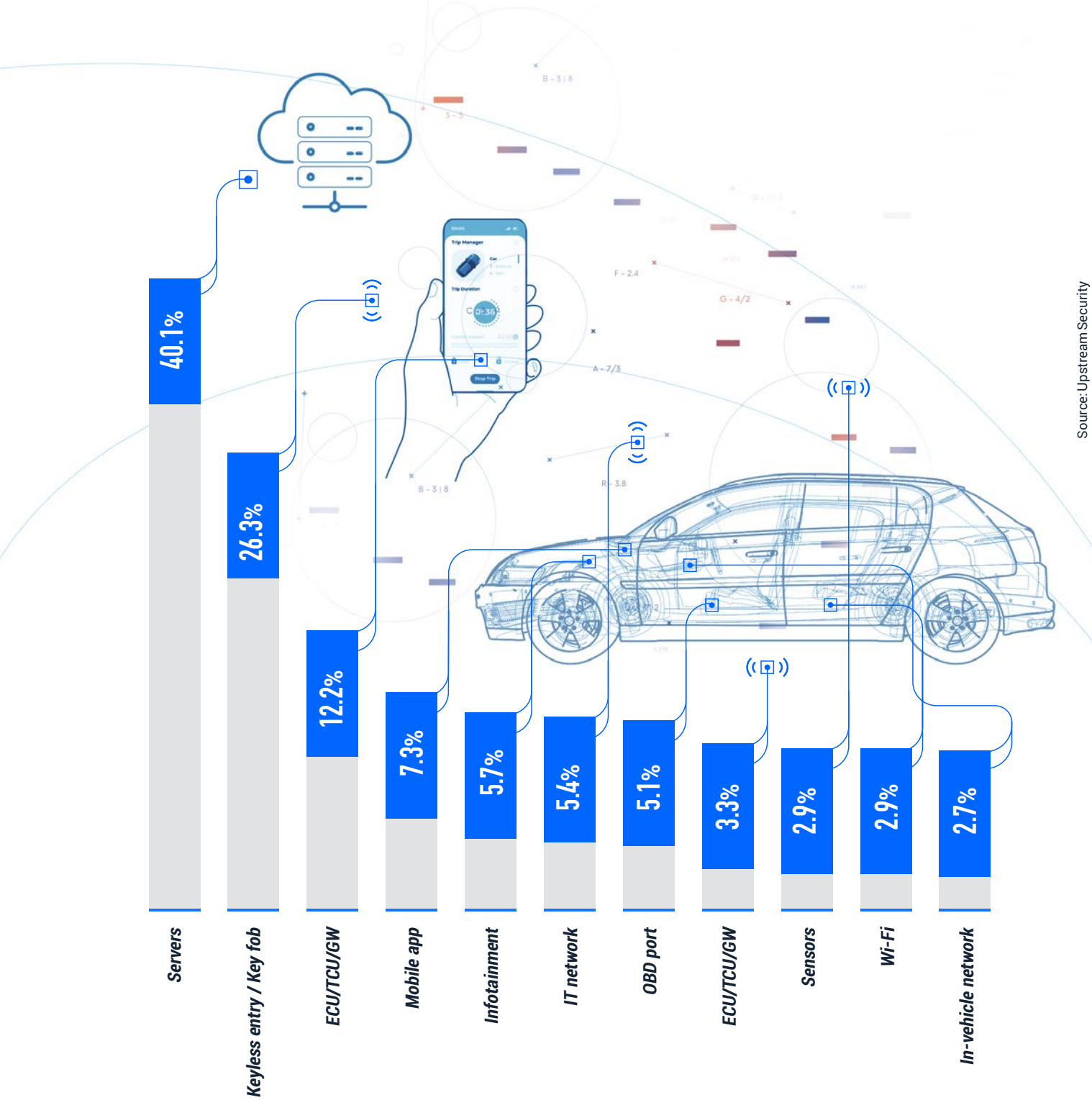
CHAPTER 3

2021's DIVERSE ATTACK VECTORS

INCREASINGLY SOPHISTICATED ATTACKS

2021 saw an increase in the use and sophistication of cyber attacks across various attack vectors. Advanced attack practices are creating a heightened awareness across the industry of how any point of connectivity is vulnerable to new threats.

Connected vehicle's most common attack vectors 2010-2021



Source: Upstream Security

SERVERS ATTACKS

Servers, vehicles, and what's in-between

Connected vehicles collect essential information throughout a vehicle's life. This involves open communication with their OEMs' telematics and application servers, which in turn communicate with the OEMs' back-end servers. Beyond OEM servers, other services that communicate with vehicles might belong to aftermarket companies, including insurance companies, fleets, management services providers, commercial fleets, car rental and leasing companies, and more.

Servers that communicate with vehicles are called telematics servers and command and control servers, and the servers that communicate with the vehicles' companion apps are application servers. Ultimately, these servers are tasked with receiving and sending data, making them vulnerable to attacks, such as injection attacks, just like many other servers. By exploiting vulnerabilities in back-end servers, for example, a black-hat actor could also attack vehicles on the road.

The significant part is that most of the OEMs' telematics back-end servers are responsible for command and control services. This means that not only can they store the vehicles' location, but they can also control vehicle functions remotely by sending commands such as "lock" and "unlock" to a car's doors, start the engine, and more. Therefore, if compromised, these servers can pose a risk to drivers and passengers.

An example of this was seen in December 2021, with the disclosure of the Log4Shell vulnerability[64] — a zero-day vulnerability in Apache Log4j Java-based logging library. The critical vulnerability would jeopardize the security of any automotive-related server using the library since the data traversing between the vehicle and server was collected, stored, and logged over a period of time in different systems or environments. This sort of communication puts vehicle data at risk of being impacted by the vulnerability.

In that study, the researchers managed to show that by exploiting the vulnerability in companies' servers, threat actors can access companies' assets. Potentially, this poses a threat to OEMs. Communicating directly with the telematics servers, and therefore with each OEMs' internal servers, opens an opportunity for a hacker to exploit the vulnerability in the back-end infrastructure and pave their way to connected vehicles in the field.

Telematics Control Unit

A Telematics Control Unit (TCU) refers to the embedded system on board a vehicle that connects it to the telematics server, enabling vehicle tracking, telemetry collection, remote commands, and additional services. In April 2020, hackers managed to reverse engineer a TCU of a vehicle and discovered that they could utilize the telematics connection to infiltrate the corporate network and gain full control of the network using admin credentials. The TCU used in the hack contained a cellular modem that provided connectivity to the device with the insertion of a SIM card, which was found in the vehicle[65]. The SIM card was configured with a private APN (a private access point name), making it more secure than a public APN. The TCU also used a VPN (Virtual Private Network) that connected the vehicle to the private services inside the corporate network (the telematics server, OTA server, etc.). Atop these security layers, HTTPS or HTTP over SSL tunnel was used. By pulling out the SIM card from the TCU and plugging it into a laptop, the hackers were able to utilize the SIM's access to the telematics private APN, which was connected to the telematics back-end using a VPN. Since the VPN had no significant segregation from the rest of the corporate network, the hackers were able to access the corporate network and servers outside the TCU back-end.

Ransomware attacks

The automotive industry has suffered from multiple ransomware attacks as OEMs, Tier-1 companies, and automobile service providers continued to be targeted by threat actors.

In 2021, ransomware attacks directly targeted OEMs, such as a February 2021 attack on an Asian OEM, when the DoppelPaymer group demanded $20 million in exchange for a decryptor. In addition, customers were unable to purchase vehicles for a number of days until the OEM was able to fix the issue[66].

Ransomware attacks were almost a third of all reported black-hat hacks in the past year. These attacks generally target companies' IT servers in an attempt to extort businesses. Still, it is essential to acknowledge that if they can access back-end IT servers, they can also control systems and facilitate attacks on vehicles. The above-mentioned attack damaged the services of all the OEM's dealerships across the United States as well as the OEM's linked apps, phone services, payment systems, and internal sites used by dealerships.

As such, one of the most critical impacts of these attacks in the past few years is the disruptions of OEM networks; damaging operations and creating bottlenecks in the vehicle production process. For example, OEMs around the globe had their plants targeted by attackers who led to disruption of these OEMs' car manufacturing processes over the last few years. Multiple OEMs from Asia and

throughout Europe[67] had their plants targeted by attackers who disrupted the OEMs' car manufacturing processes.

Ransomware attacks beyond OEMs

In September 2021, a European supplier of automotive exhaust and heat management systems confirmed that it was a victim of a cyber attack against its IT infrastructure. The impacted company declared it an "organized cyber attack"[68].

Another incident took place earlier, in February 2021, when an East European car-sharing service was hit in a ransomware attack in which the personal data of 110,000 people, including the company's customers, was leaked to an online hacker website and posted for sale on an online dark web forum. The stolen data included usernames, personal identification numbers, telephone numbers, email and home addresses, driver's license numbers, and encrypted passwords[69].

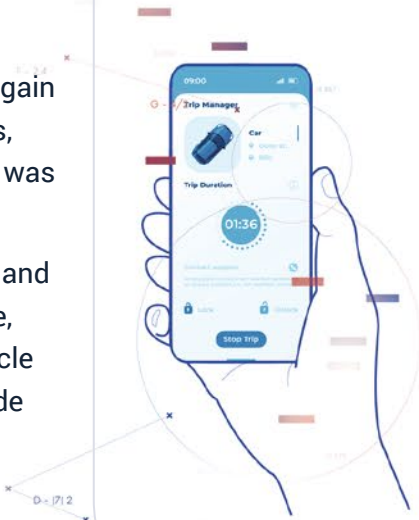
MOBILE APP ATTACKS

Greater vehicle connectivity has allowed OEMs to release remote services using vehicle companion apps that connect vehicles to smartphones, conveniently allowing owners to control features such as remote start, lock, unlock, track the location and status of the vehicle, and more[70]. These allow users to control critical functions from across the street or the globe. The flip side to this convenience is that these same apps, which help us communicate with our vehicles, also act as an additional attack surface for hackers to exploit. With the rise in popularity, the industry is seeing 7.3% of all automotive cyber-related incidents between 2010 and 2021 involve a mobile app.

7.3%

OF ALL INCIDENTS BETWEEN 2010-2021 INVOLVED A MOBILE APP

Source: Upstream Security



Mobile app attacks are not new. Back in 2016, an Asian OEM disabled their companion app after they found it was easy for hackers to exploit the app to gain unauthorized access to the car. While they could only access basic functions, turning on and tampering with cabin temperature functions while the vehicle was not in use could drain the battery or damage the car[71].

They weren't the only ones that saw how car mobile apps could be exploited and misused. In 2019, car owners who were using mobile apps to remotely locate, unlock, and start their cars, were displayed other people's accounts and vehicle information[72]. In addition, in August 2020, an owner of a North American-made vehicle opened his vehicle's smartphone app with 5 cars parked in Europe displayed. He was able to view all of the details of these cars and remotely control them as if he owned them[73].

> ***Some of the greatest conveniences that OEMs offer their customers are the most tempting for hackers.***

White-hat hackers have also discovered disturbing vulnerabilities involving mobile apps. In February 2020, a researcher showed that users could use a custom open-source mobile app to bypass the access pin and prompt required by the OEM's mobile app to remotely control a number of the OEM's vehicle functions[74].

Some applications may lack proper security standards, leading to multiple high-risk vulnerabilities in a single app. This can grant access to not only vehicle controls but potentially back-end servers as well.

Beyond attacks on vehicles, mobile app attacks can also apply to connected charging stations.

For example, in November 2021, a vulnerability in a UK domestic car charging provider's app led to exposure of full names, addresses, and charge history of thousands of consumers. More than 140,000 users were put at risk, potentially allowing black-hat actors to identify their common charging locations. Although it was believed that the issue affected only customers with home chargers, it was unclear if the risk also applied to users of the company's public charging points[75].

These vulnerabilities leave the vehicle owner's privacy and property at risk of theft. The new level of both digital and physical connectivity requires OEMs and ecosystem suppliers to consider how to protect customers, in line with new regulations, if they are going to earn public trust.

Mobile apps and private information

One of the dangers lurking in car mobile apps is identity theft by black-hat actors who get their hands on real users' private data. Vulnerabilities in mobile devices and in their corresponding application servers are constantly evolving and infecting an ever-increasing number of users. These nefarious threats can completely compromise private users' information and steal all credentials stored on it.

For example, in April 2020, researchers exposed an unsecured S3 bucket of a French OEM's mobile app that exposed the activity and private information of hundreds of thousands of app users in India. These vulnerabilities could be exploited to carry out massive-scale attacks that compromise sensitive data and the safety of all road users[76].

Mobile app hack in racing

Racing teams can use mobile applications to connect with their fans and build buzz around a new vehicle before it appears on the track.

In March 2021, the smartphone application of a European Formula One motor racing team, was hacked prior to the official augmented reality launch of the company's new Formula One car. The hackers extracted data from the app, including the renders of the vehicle and its new livery. In addition, CAD models of the new vehicle were easily made available. In light of the attack, the company removed the application from both the Apple App Store and Android Google Play store but the data had already been extracted and leaked[77].

Data sharing and smart mobility

Many businesses in the automotive industry rely on the new technologies introduced by connected cars and smart mobility. Such businesses include car rental agencies, car leasing companies, and the expanding realm of car sharing companies. Mobile apps enable companies to provide data-driven modern services, allowing them to remotely track and monitor their fleets. While these technologies are very beneficial to businesses, they also entail the risks of fraud and misuse which can have a grave impact.

In March 2021, it was published that 52% of apps share your data. Smart mobility services were among the top 10 apps that share the most information with third parties. In addition, ransomware attacks on the services we use may steal the data we insert to our mobile apps and from there to their connected servers as well[78].

> ***More than 50% of all reported automotive-related cybersecurity incidents took place during the past two years alone***

Source: Upstream Security

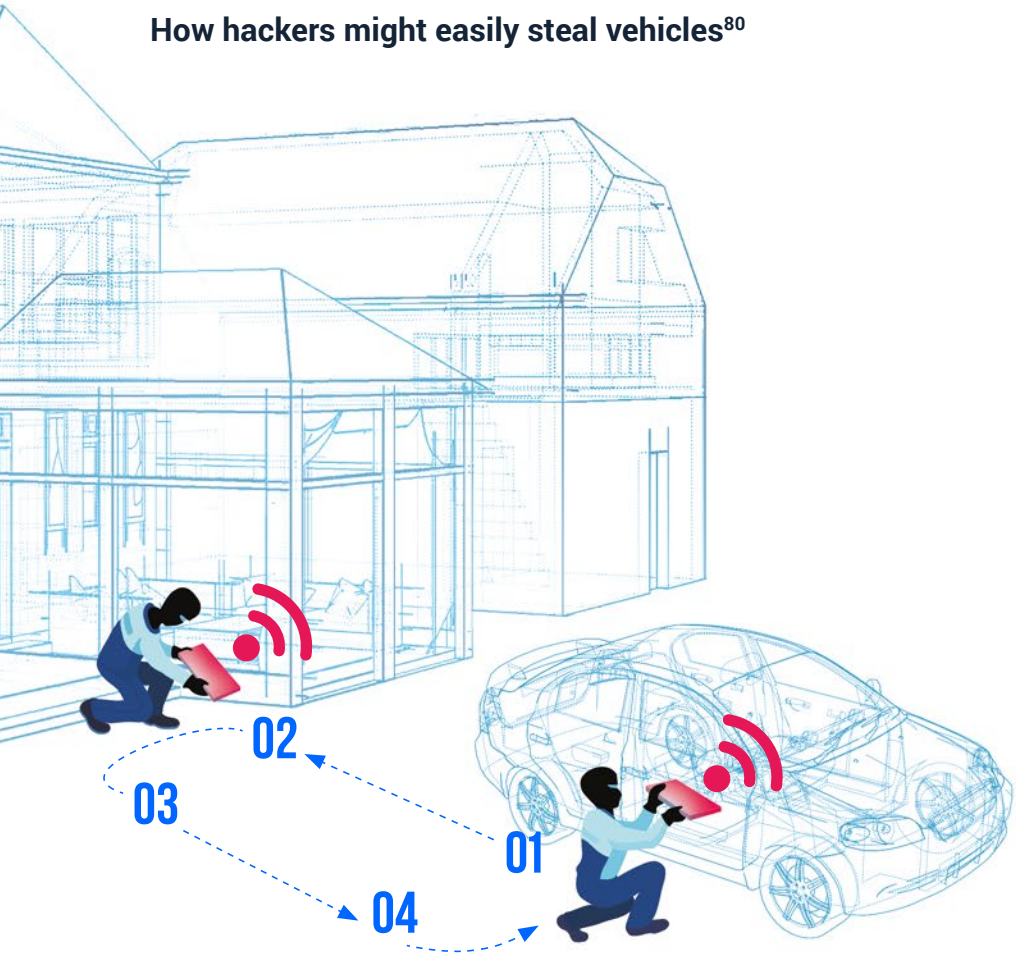
REMOTE KEYLESS ENTRY SYSTEM

Over the past decade, keyless entry and fob systems (wireless key fobs) have become a common feature, moving from a luxury to a common industry standard. This has led to a wave of wireless key fob misuse and manipulations, made easier by the presence of keyless entry hacking tutorials on popular video-sharing platforms.

> ***Keyless entry car technology now accounts for nearly 50% of all vehicle thefts.***[79]

These attacks are mostly conducted by thieves who get their hands on readily available devices online. When sold, some sellers ask purchasers not to use them for criminal activity, but no register or follow-up process exists, leaving black-hat actors free to carry out attacks unabated.

How hackers might easily steal vehicles[80]



Step 1: *One thief stands close to the vehicle, sending a signal to a second thief who is close to the car owner's house holding a hacking device.*

Step 2: *The thief who is next to the house holding a second device guessing where inside the owner's key may be.*

Step 3: *The second thief relays information from the key (inside the house) back to the thief who is standing next to the car.*

Step 4: *The first thief enters the car and uses the relayed signal to unlock the door and start the engine.*

HOW DO HACKERS HACK INTO VEHICLES

Keyless fobs contain a short-range radio transmitter. When a car's key fob is within a certain close proximity to its vehicle, it sends a coded signal by radio waves to a receiver unit in the car. This signal is then interpreted to actions such as locking or unlocking the vehicle's doors, or opening and closing the vehicle's windows.

Communication between the key fob and the vehicle is subject to exploitation by devices designed to intercept, interfere, or steal information from a fob's radio signal.

There are a few types of attacks for exploiting the communication between the key fob and the vehicle used by hackers and thieves worldwide.

01

Relay attacks

In general, relay attacks are designed similarly to the concept of the Man-in-the-Middle (MitM) attacks and replay attacks (see more on replay attacks below). These attacks involve the interception of information between a sender and a receiver at a certain time they communicate, to use the intercepted information for other means.

Hackers steal a car by intercepting the communication between the key fob and the vehicle, as a transmitter or a repeater, without manipulating or changing the content of the communication. By using equipment for carrying relay attacks, such as relay attack stations, hackers can retransmit the signals which are constantly broadcast in the communication of key fobs and their vehicles, as well as amplify or boost the radio signal of a key fob that is out of range of the car.

This type of attack has become common amongst thieves. Car thieves intercept the signal from a key fob inside a vehicle owner's house. Once locking on to the signal, another device is placed near the car, which in turn relays a message to unlock and start the vehicle's engine. Once unlocked and running, the vehicle can be driven off.

02

Replay attacks

In replay attacks, the hacker intercepts and steals the content of a message sent from the key fob or the car's remote, storing it for later use. Once the relevant message is within the hacker's possession, they can use it whenever they desire to carry out an attack, be it unlocking the car's doors, or starting the ignition.

Reprogramming key fobs

Reprogramming key fobs is a method used by hackers who utilize more sophisticated and expensive technology to reprogram a car's key fob. By creating a new key for the car to communicate with, it renders the previous key unrecognizable. The reprogramming device is legal to obtain and is mostly used by authorized mechanics and automotive service centers. The hackers connect the device to the OBD port and program themselves a new fob. Car thieves who obtain devices of these sorts can gain full control over the vehicle with little experience.

Jamming the communication between a key fob and a vehicle

Car thieves also use a method of jamming the communication between a key fob and a vehicle to hack into cars. The thieves use signal jammers which interfere with the proper communication between the key fob and the vehicle when the vehicle's owner tries to lock their car, and prevent it from succeeding, without the car owner realizing that their car had failed to lock. Once the car owner is out of sight, the thieves are able to open the unlocked doors.

2021 saw theft via manipulation of the keyless entry system increase significantly including a 93% spike in keyless entry thefts in the UK[81]. For example, In March 2021, two thieves managed to unlock a keyless car using a wireless relay device, that received the key fob's signal from inside the owner's house, remotely unlocking it before they drove away[82].

In another incident in the UK, a European-made vehicle was hacked and stolen outside its owner's home. The hackers used a relay attack device aimed at the house to activate the ignition and drive away in the stolen car[83].

In Germany, hackers compromised and stole a European-made sports car. According to the police, the thieves gained access and drove away with the vehicle by tampering with the keyless entry radio signal[84].

In September 2021, hackers in the UK were targeting expensive cars including multiple European luxury-grade vehicles, stealing them using by reprogramming their key fobs and using practically new keys[85].

In Italy during October 2021, a hacker was searching for cars[86] that had recently parked. Immediately after drivers had exited their vehicles and used their key fob to lock the vehicle, the hacker used a signal jammer to prevent the car's locking mechanism from engaging. As the owners walked away the hacker could enter the vehicle and turn on the vehicle.

Tracker, a vehicle managing and tracking service, recorded an increase in vehicle thefts during the first half of 2021 amongst keyless vehicles just as COVID-19 lockdown restrictions began to ease. An analysis report by Tracker indicated that relay attacks accounted for 92% of recorded thefts in 2020, a 27% increase over the last five years[87].

> ***Thieves only needed to be close to the key fob for the programmer to pick up and reproduce its signal.***

In November 2021, an American-made vehicle was stolen in Detroit, MI, USA when thieves hacked the car owner's key fob to get in, start the car, and drive away. This incident came along with other incidents in the same area, where upon the recovery of the stolen vehicles, owners discovered that their key fobs no longer worked, as the hackers reproduced new key fobs, rendering previous keys unrecognizable to their vehicle. According to the police, the hackers had an $8,000 programmer, meaning the thieves only needed to be close to the key fob for the programmer to pick up and reproduce its signal[88].

An internal memo from the Michigan State Police published in February 2021, showed how thieves were breaking into cars and using a device to program a new key fob, meaning the original key would no longer work. The Michigan State Police bulletin said hundreds of European and American OEMs' vehicles have been stolen by this method[89].

In August 2021, white-hat hackers uncovered that many modern Asian OEMs' vehicles can be accessed with a replay attack using cheap hardware. The hackers managed to execute a replay attack and hack into 5 different vehicles which claimed to harbor this vulnerability. The hacker found that simply recording signals from the vehicles' key fobs was enough to compromise the vehicle[90].

INFOTAINMENT

In-vehicle infotainment (IVI) systems are of the most vulnerable units in modern vehicles. They are exposed to installed software, apps, and short term communications such as mobile phones and Bluetooth devices. These computers are one of the car's gates to the outside world — the internet. Drivers frequently connect their devices, such as a smartphone, to a vehicle's infotainment system, permitting it to access private data, such as contacts, messages, and more. This connection poses risks to the vehicle, as infotainment systems are highly likely to be connected to the vehicle CAN bus.

As IVI systems are the one unit that connects the inner ECUs of the vehicle to the outside world, it can also be the path of least resistance for malicious software to enter the internal systems. For example, in May 2021, researchers published that they had discovered numerous vulnerabilities in a European OEM's infotainment system[91], which could be exploited in hacking the vehicle's internal systems. The hackers conducted a detailed study of the IVI system and found multiple security flaws that triggered attacks. In a white paper publishing their findings, the hackers found numerous attack surfaces, including the Bluetooth stack, Wi-Fi chip, USB functions, JavaScript engine, and third-party apps in the head unit – the infotainment ECU -- in use in some European-made vehicles since 2018. After finding these bugs, the researchers reached out to the OEM to report the flaws. Consequently, the OEM began patching the vulnerabilities three years after the system's initial rollout.

Furthermore, in January 2021, a vulnerability was found in a Tier-1 semiconductor manufacturer's chip, used by OEMs to power in-vehicle infotainment, navigation, and a 4G LTE modem for connectivity. The vulnerability in the hardware component can create video playback issues in the infotainment system[92].

WI-FI

In April 2021, white-hat researchers managed to hack the ECU that controls the doors of a North American EV manufacturer's vehicle with a drone carrying a Wi-Fi dongle. The hackers exploited vulnerabilities to compromise parked cars and control the infotainment systems over Wi-Fi[93] and were then able to manage network connections and run commands on the infotainment system of the vehicle. The researchers noted that it would have been possible for an attacker to unlock the doors and trunk, change seat positions, and enter both steering and acceleration mode but not manipulate the vehicle's driving capabilities.

While Wi-Fi connectivity can be used to be more productive and even entertain passengers while in transit, it creates an attack surface that, with the right knowledge, can grant hackers access to a vehicle's sensitive controller area network (CAN bus).

> ***With cars containing multiple computers, connected together in one complex network, taking advantage of one vulnerability can give access to multiple vehicle controls.***

All hackers need to do is find a minor vulnerability somewhere within one of the networks to sneak in.

In June 2021, researchers from a Middle Eastern IoT security firm disclosed a new set of critical vulnerabilities in a Wi-Fi module[94]. These vulnerabilities were enough for a black-hat actor to hijack a device's wireless communications, potentially resulting in the manipulation of automotive data. The flaws found in the module, which is in use in the automotive industry, affect all embedded and IoT devices that use the component to connect to Wi-Fi networks. They also mentioned that an attacker would need to be on the same Wi-Fi network as the specified device module or know the network's pre-shared key. The researchers stated that new firmware versions, released after January 2021, include fixes that resolve the issue.

ECUs

ECUs (Electronic Control Units) are responsible for engine, steering, braking, windows, keyless entry, and various critical systems, are subjected to interference or manipulation. Running multiple sophisticated systems simultaneously, hackers try to manipulate electronic control units to gain control over the functions they are responsible for.

In June 2021, researchers confirmed the feasibility of vulnerabilities by launching proof-of-concept attacks on two vehicles. The researchers launched disruption attacks against the two vehicles[95], exploiting the fact that ECUs often implement a time-out feature that prevents a CAN transceiver from holding the dominant state for an extended period of time. They managed to shutdown one of the vehicles' powertrain ECU and the other vehicle's power steering ECU.

The researchers worked under the assumption that many modern cars were likely vulnerable to these kinds of attacks, but an attacker would have to compromise the vehicle's network first before launching these types of attacks. They believe that once an attacker has control over a particular component in the vehicle, they could then impact the operations of another component while undetected. Furthermore, the new class of vulnerabilities stem from some architectural choices that automakers have made in recent years, as most modern car functions are controlled by one or more ECUs.

> ***Attacks can be launched remotely, without requiring hardware modifications. Bypassing several state-of-the-art defenses.***

These white-hat hackers found a way to exploit the "peripheral clock gating" feature implemented in the vehicles to reduce the amount of power the ECUs consume, which enables ECUs that aren't actively being used to shut down to conserve energy. Hackers found a way to control this function and shut down any ECU they wished. The researchers explained that while some of these shutdown attacks were shown in prior work, they required either physical access to cars or hardware modifications. The novel part of their attack was that it could be launched remotely, without requiring hardware modifications, and it also bypassed several state-of-the-art defenses.

In an August 2020 incident, a group of researchers worked with more than 10 auto manufacturers and suppliers to assess the hardware and software of more than 40 ECUs in development. Within those, they found over 300 vulnerabilities. They assigned each vulnerability with a risk score according to ISO/SAE 21434 and found that all vulnerabilities assigned with a high-risk score were a result of a fault in the software or OS of the ECU. The results highlight that the more complex an ECU is, the more vulnerabilities exist in it and the percentage of the high-risk vulnerabilities rises[96].

OBD PORT

The On Board Diagnostics (OBD) port allows mechanics to identify problems in the vehicle mainly by plugging in a dedicated diagnostic dongle, or by using a software that runs on diagnostic equipment. Ultimately, the main purpose of the OBD port is to read diagnostics data from ECUs. However, it can be used to update software or even change ECU memory. Additionally, the OBD port may be used to connect a device to upload software that can communicate with the vehicle from anywhere, e.g. a laptop that is connected to the OBD port using a connector or a ride sharing program that can remotely unlock and start a vehicle.

However, hackers can use a device connected to the OBD port to connect to the vehicle and manipulate systems through diagnostic protocols.

In an incident that occurred in September 2020, a hacker tried to prevent an Asian OEM's EV battery degradation. The hacker developed a CAN-bridge to hack the CAN message between battery management and vehicle to avoid degradation. By crafting a new message and sending it to target the battery management system, the hacker lowered the charging speed and prevented the battery from heating, a primary cause of degradation[97].

Today, there are more lines of code in the connected car than other highly sophisticated machines, including the U.S. Air Force's F-35 Joint Strike Fighter, the Boeing 787 Dreamliner, or a NASA space shuttle[98]. With each region demanding its own code to meet local regulations.

Source: EE Times

THE SUPPLY CHAIN AS AN ATTACK VECTOR

Modern vehicles contain an estimated 100 ECUs per vehicle[99]. Many of these are produced by trusted Tier-1, Tier-2, and periphery vendors.

Each one is important, yet each has the potential for hackers to penetrate internal systems, gain insights on other vehicles, access centralized servers, and even harm a driver or a passenger.

In the automotive industry, automotive OEMs and their supply chain companies and vendors may struggle to follow and manage a bill of materials for a product, be it an infotainment system or a certain ECU.

As such, a connected car could contain software vulnerabilities within a vehicle's hardware components. These supplier manufactured components find their way into a vehicle without the OEM being able to properly identify the source of a vulnerability. Even if a consumer did want details of vehicle components, tracking them would be a daunting task.

Consumers have no choice but to trust car manufacturers and regulatory bodies with issues that directly relate to their health and well-being. Often, OEMs and federal bodies do not even have access to the in-depth component data and potential threats posed by them.

In January 2021 for example, a hacker managed to hack a European Tier-1 giant's infotainment unit used in a major Asian OEM's vehicle[100]. They found a vulnerability in infotainment system. By plugging in a USB device, they could gain root shell access to the system and gain administrator access to install unauthorized software. The hacker found that the European produced infotainment vulnerability could also affect more than four additional models and commercial models produced after 2015.

In addition, in 2021 alone, more than a hundred vulnerabilities were found on Tier-2 suppliers' chips used in the automotive industry. These chips are eventually put into Tier-1 products that in turn are put into the vehicle[101]. These vulnerabilities may affect more than one OEM, as one Tier-1 supplier may supply its products to numerous OEMs and one Tier-2 supplier may serve various Tier-1 suppliers. Additionally, in August 2021, a research paper disclosed that a Tier-2 supplier has confirmed a vulnerability that allows an attacker to gain privileged control of code execution for a North American EV OEM's autopilot system[102]. The attack involves unlocking a bootloader that's usually disabled for consumers and intended for laboratory conditions. The attack is also valid for a European OEM's infotainment system, as it uses the Tier-2 supplier's hardware as well.

> ***A single vulnerability in one of the 100 ECUs is all it takes to make a car harm a company's reputation and even endanger an operator's life.***

In 2021, as supply chains became strained, companies were under increased pressure to receive the materials they needed and get products to their customers in a reasonable time frame. To keep companies focused on cybersecurity, even when under immense pressure, new guidelines and regulations were coming at a pivotal moment for OEMs, ensuring that vehicles are properly secured. By following the required procedures, our roads would be safer and OEMs would be able to ensure reliable operations from their vehicles years down the road.

AUTONOMOUS VEHICLES

Autonomous vehicles, or self-driving cars, are vehicles that operate autonomously, with or without little human oversight or intervention. By using sensors and cameras to interpret their environment in every moment, autonomous vehicles read details and analyze information from the car's surroundings to self-perform accordingly.

Autonomous vehicles function according to machine learning and artificial intelligence-based softwares that are "trained" to read signs and traffic lights on the road, weather conditions, and other risks or calculations that need to be constantly considered by a human driver and function according to them. As such, a dangerous situation can occur when an autonomous vehicle does not respond to certain inputs. This can result from a scenario where the vehicle was not "trained" to process specific data it had encountered or that it could not read the data correctly due to an exterior interference, be it a scenario of unfamiliar signage or other. Installing and constantly updating software on vehicles that they are not intended for can create risks and severe consequences.

Across the globe, roads are structured differently; signs are designed differently, headlights look different, and not every country has a standardized set of road markings. OEMs and autonomous vehicles' software companies design in-vehicle software uniquely to the regions these are to be driven in.

In September 2021, The software which enables certain American OEM's cars to drive autonomously was leaked, enabling hackers outside of the USA to hit the streets hands-free. The self-driving package was a feature for the OEM's vehicles, and certain owners in the USA were granted limited test access to the 'beta' software that enabled the feature. However, cars of that OEM outside of the US haven't been eligible for the software, as the machine learning and artificial intelligence algorithms powering the vehicles were trained on US road signs. That software has reportedly leaked to the OEM's hacker community, granting drivers outside North America the chance to use the feature. A car owner in Ukraine posted a video of his car running the beta software in his vehicle as he was driving through the streets of Kyiv. The Self-driving software could be downloaded directly to the OEM's vehicles. Using a range of sensors and powerful artificial intelligence enabled drivers to type in a location to their navigation dependent on information received from satellites, which the car would then attempt to drive to autonomously[103].

V2X

In the near future, vehicles will constantly correspond and communicate with their environment through sensors, cameras, radars, cellular IoT modules, and more. Vehicles will operate while processing input that their sensors collect from their surroundings, such as headlights, signs, weather conditions, etc. However, the profound addition will be that one vehicle would be communicating with other vehicles on the road and receiving data from other sources, such as a road's infrastructure. Vehicles will correspond with their entire environment, from pedestrians and cyclists that they may come across to navigation satellites and the traffic light in the next junction.

V2X, or Vehicle-to-Everything, is the term for the communication between a vehicle and any other entity which could affect or be affected by the vehicle. This communication system comprises the specific types of communication systems:

V2V *Vehicle-to-Vehicle*

V2I *Vehicle-to-Infrastructure*

V2N *Vehicle-to-Network*

V2P *Vehicle-to-Pedestrian*

V2D *Vehicle-to-Device*

V2G *Vehicle-to-Grid*

V2C *Vehicle-to-Cloud*

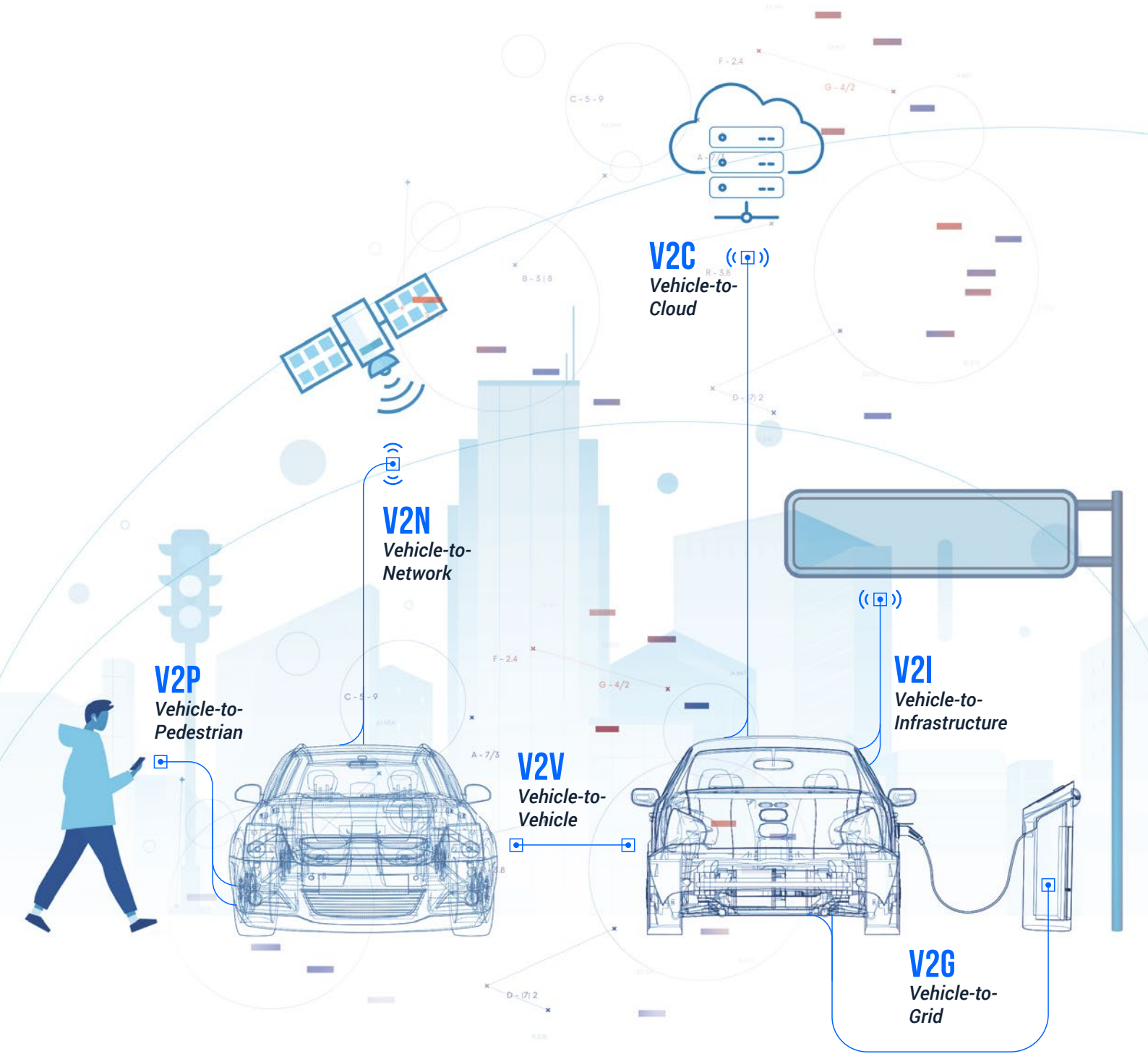
This wireless communication technology that would be deployed in tomorrow's vehicles, upon which they will be operating, is called Cellular Vehicle-to-Everything (C-V2X).

This C-V2X technology has been in testing in the past few years. In 2020, Ford conducted its final testing of V2I communications equipment in Hunan Province, China in 2020[104] and in 2021, the OEM was already selling cellular vehicle-to-everything (C-V2X) technology in mass production vehicles in its Mach-E[105].

Ford's SYNC+ in-vehicle infotainment system can analyze and provide drivers with timely road information and recommend appropriate driving speeds to help drivers avoid waiting at traffic lights, decreasing the chances of red light violations[106].

With the advancement of technology on the roads, and deployment of new technologies to connect our vehicles to new sources, such as road infrastructure, satellites, and electric charging grids to which hundreds and thousands of vehicles can be connected at the same time, the automotive industry will be vulnerable to new threats. This will become much more delicate and dangerous when it comes to autonomous vehicles, which are designed to operate without or with little intervention or supervision of an in-vehicle driver.

This raises the big question: Are we going to face new attack vectors in 2022?

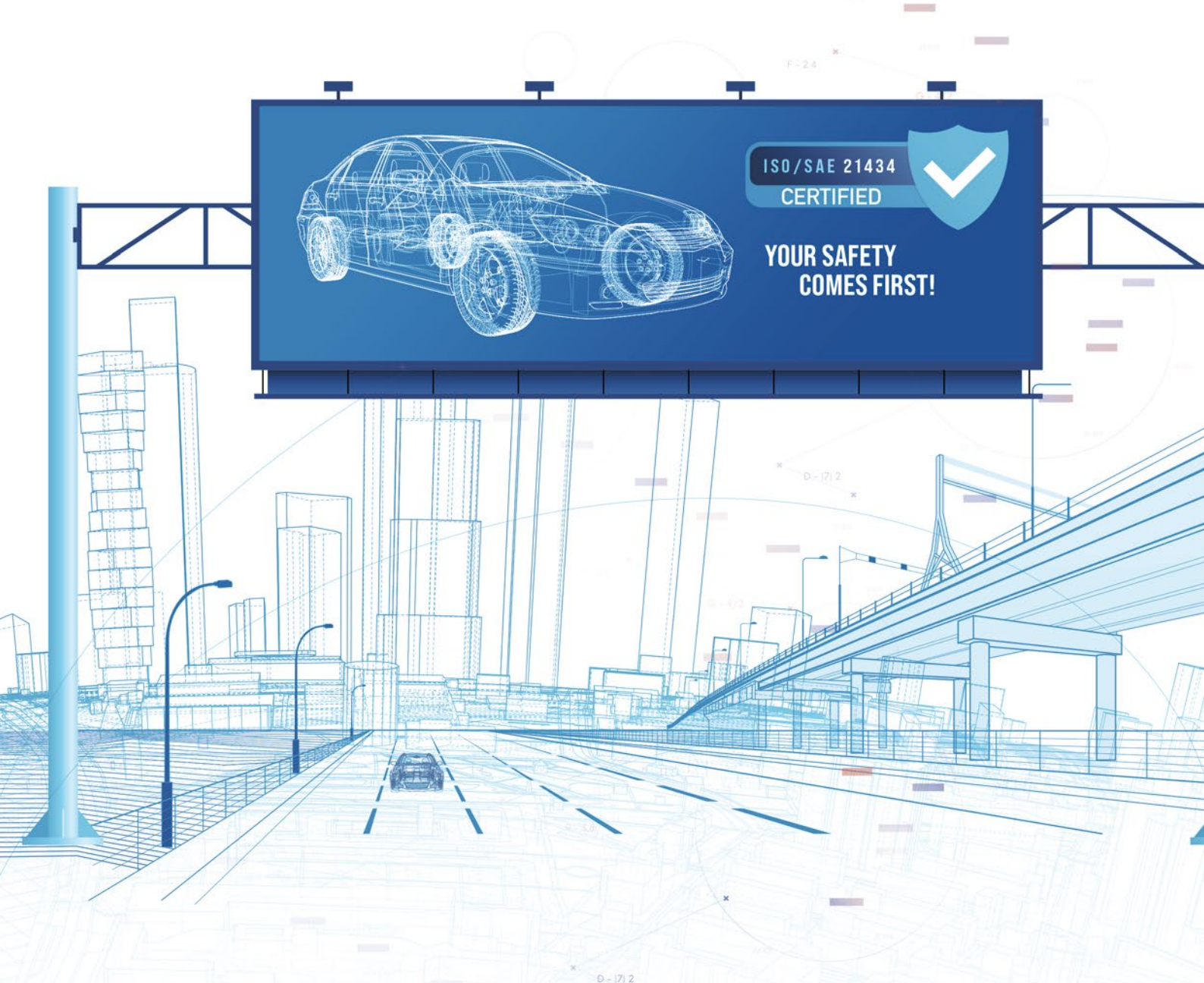


Regulations as a branding opportunity

The increasing avenues for interacting with a vehicle, whether through a mobile app, Wi-Fi, Bluetooth, keyless fob, etc., also impacts the growing ease of hackers to manipulate systems for their benefit.

As standards and regulations begin to take effect in July 2022, OEMs will face an uphill battle in securing all channels that are so prone to human error. Behaviors such as not changing default passwords, locking a car from a distance so the signal can be intercepted, or not being vigilant enough in regard to proper cybersecurity practices can have substantial financial and reputational repercussions for OEMs, Tier-1s, Tier-2s, and the whole ecosystem.

Manufacturers will have new incentives to reimagine the driver's experience both inside and outside the vehicle. This creates an opportunity for brands to establish themselves as safety-first companies, protecting passengers in case of a crash or a targeted cyber attack.

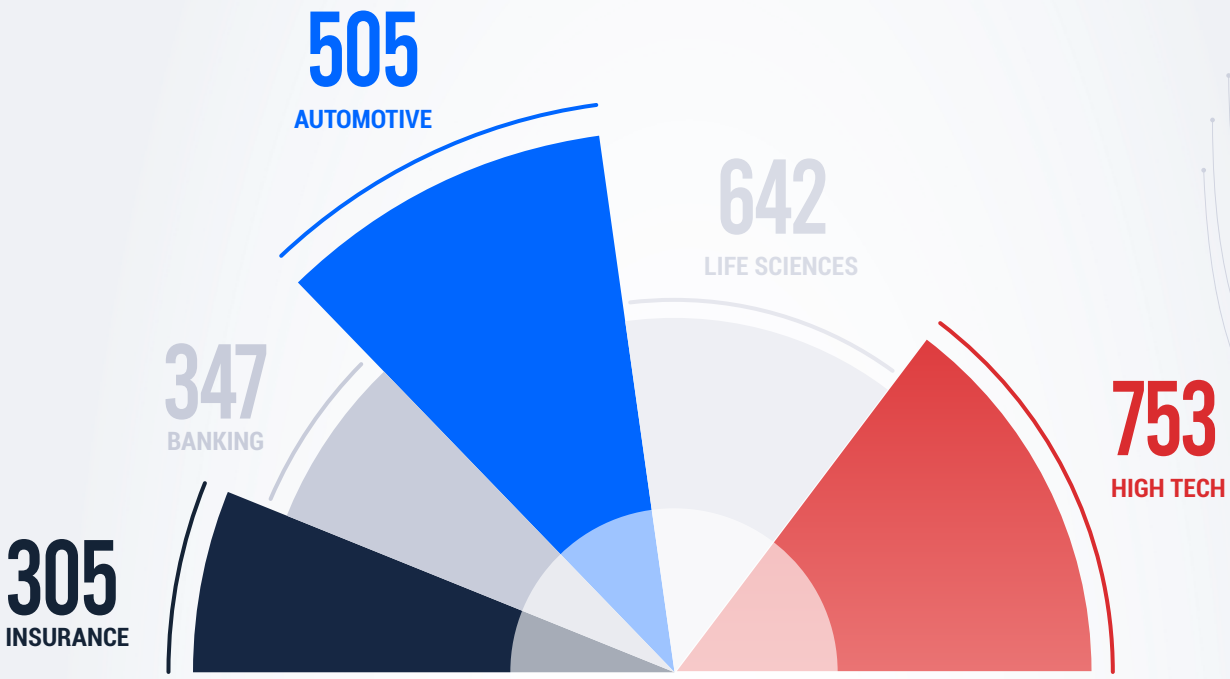


CHAPTER

4

CYBER ATTACKS' IMPACT ON THE AUTOMOTIVE INDUSTRY

Financial impact across the automotive compared to other industries

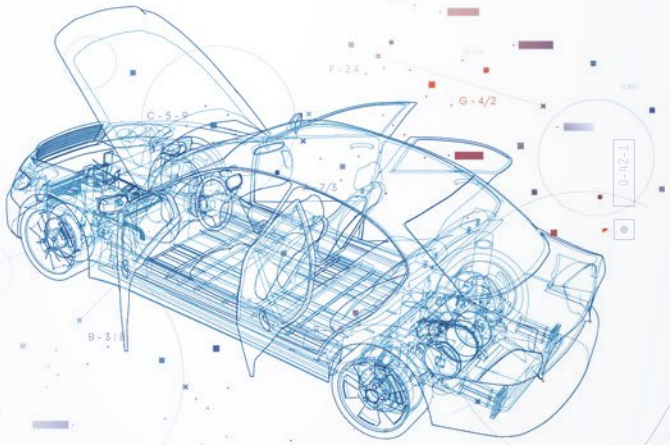


$505 BILLION

Data in $Bn

Source: businesswire

The automotive industry stands to lose over $500 billion by 2024[107] to cyber attacks, behind only High-tech and Life Sciences. What does it look like and how can it be avoided?



CYBER ATTACKS' FINANCIAL AND REPUTATIONAL IMPACT

With the projected value of the connected car market to reach $215 billion by 2027[108], attacks on the automotive industry will continue to have far-reaching impacts.

In the past number of years, an increased number of companies have fallen victim to increasingly sophisticated cyber attacks. In some cases, we can still sense the impact on the industry, as recovery from some attacks can span from days to months.

In February 2021, a European IT software and service company that provides IT and product engineering services to the automotive industry and others was hit in a ransomware attack[109], causing the company to experience technical issues with its customers.

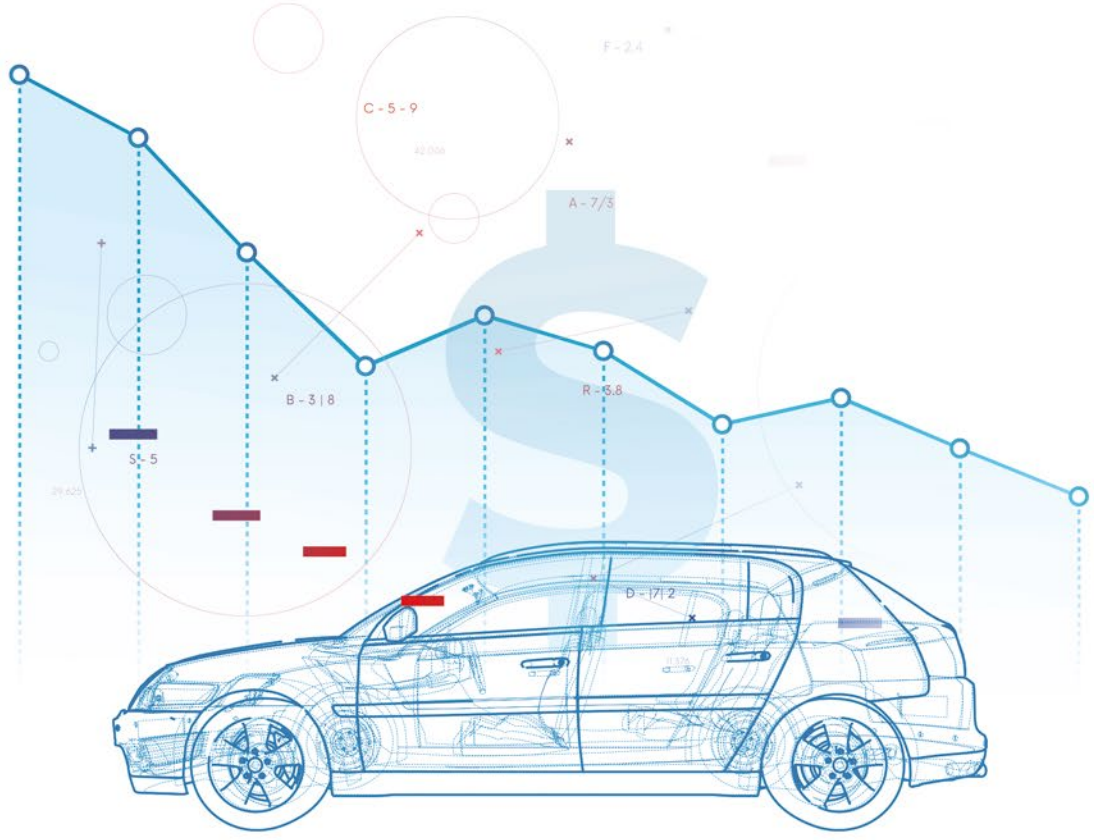
In May 2021, hackers targeted the U.S. manufacturing unit of an Asian OEM, days after the European subsidiary of the brand was also targeted[110]. The attack resulted in exposed financial and customer data being published online.

Besides for OEMs, Tier-1s, and Tier-2s, dealerships are targets for attacks as well. For example, an attack on an Asian OEM in February 2021 by the DoppelPaymer ransomware group demanded 404 Bitcoin to return access to their dealership's systems. Dealers were unable to sell any vehicles until the attack was addressed[111].

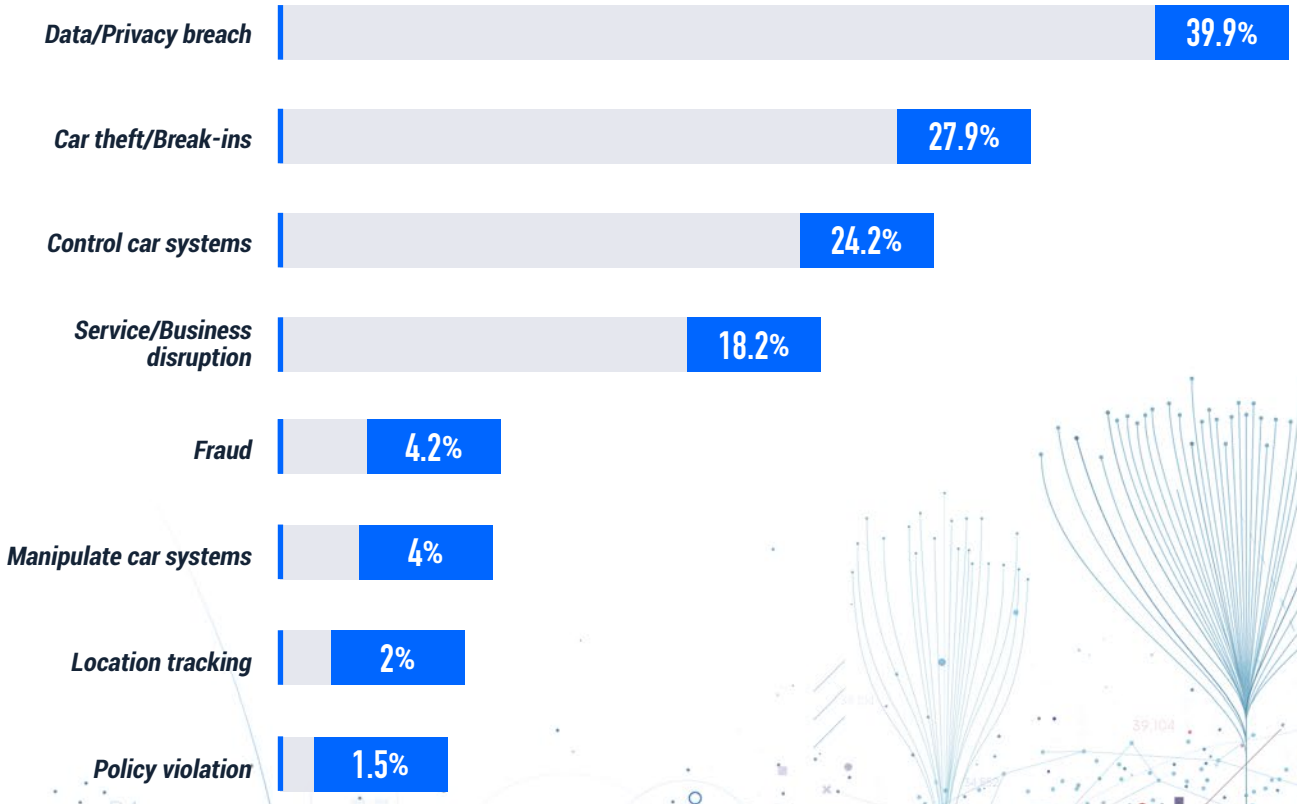
$215

BILLION VALUE OF THE CONNECTED CAR MARKET BY 2027

Source:
World Economic Forum



Impact Breakdown 2010-2021, based on 900+ automotive-related cyber incidents



Source: Upstream Security

DATA AND PRIVACY BREACHES

A company's private data is one of its most significant assets. It includes customer data, personal information, and even internal trade secrets.

For example, in August 2020 a researcher found a privacy issue in a popular GPS driving app that was caused by improper management of the API. At the time, if a user acknowledged a road obstacle by notifying other drivers via the application, their user ID, user name, and location appeared on the API. An attacker could leverage this vulnerability by picking multiple locations and periodically calling the API while crawling the users who confirmed the existence of an obstacle. Over time, an attacker could build a dictionary of user names and their IDs[112].

40%

OF REPORTED INCIDENTS IN 2021 LED TO AUTOMOTIVE DATA AND PRIVACY BREACHES

CAR THEFTS AND BREAK-INS

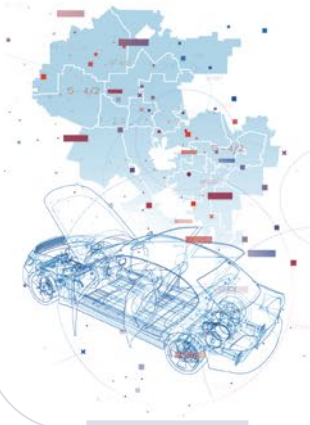
Remote keyless car thefts are becoming increasingly common as there are new technological ways of unlocking and starting vehicles. These come alongside the tools and technologies used to manipulate vehicles, which are then sold on the internet. As a result, car thefts and car break-ins have become a leading impact of cyber incidents over the past decade. Besides the anguish that the car owner experiences when their vehicle is broken into and stolen, auto insurance companies manage the damage and cover the cost for the many drivers whose cars were hacked. This phenomenon has become a severe problem in many countries as it is also shown that its impact is one of the most profound in today's automotive world. In numbers, car thefts and break-ins accounted for more than a quarter of the industry's total number of incidents.

In addition to the frequency of car thefts mentioned above, COVID-19 contributed to an increase in vehicle car thefts. In the first nine months of 2021, 17,195 cars were stolen solely in Los Angeles, USA, hitting a record of the highest annual tally of stolen vehicles in more than a decade[113].

17,195

CARS

WERE STOLEN IN LOS ANGELES, USA DURING THE FIRST 9 MONTHS OF 2021



> ***Car thefts accounted for 27.9% of all publicly reported incidents between 2010 and 2021***

For example, in September 2021, the New York Attorney General and NYPD Commissioner announced the indictment of 10 members of an auto theft and distribution operation for their alleged roles in the theft or criminal possession of 45 vehicles during a six-month period[114]. These indictments are related to the

theft and resale of more than 225 vehicles throughout New York City and the Hudson Valley. According to the police, in a 6 month period, the group scoped out and targeted cars to steal, obtained key code information for these vehicles from unlawful websites, and created keys that allowed them to breach and steal the vehicles in as little as 30 seconds.

FINANCIAL IMPACT ON INSURANCE PROVIDERS

Cyber attacks and hacking thefts have increased significantly since the beginning of the COVID-19 pandemic. Kicking off this new wave of thefts were lockdown orders that saw their people parking their vehicles for prolonged amounts of time. This allowed hackers the freedom to scope out vehicles, learn their vulnerabilities, and take advantage of gaps in their security.

In Los Angeles, USA alone, in the 18 months following the first state-wide stay-at-home order, 33,985 vehicles were stolen. This is a 40.6% jump when compared with the 24,179 vehicles that went missing during the 18 months before this order went into effect[115].

This trend continued after lockdowns were lifted, remaining as high as the mid-2020 peak, well into October 2021.

Insurance companies are left to deal with the financial aftermath of this high number of thefts, giving them incentive to better understand the vectors and vulnerabilities used to steal vehicles.

> ***40.6% increase in Los Angeles, USA vehicle thefts during the first 18 months of COVID-19***

CHAPTER

5

WHAT'S HIDING IN THE DEEP AND DARK WEB?

WHAT IS THE DEEP AND DARK WEB?

Our internet can be divided into three main surfaces. Access to each part comes with different criteria, such as demonstrating a familiarity in the realm.

The first layer of the internet is the smallest, yet the most familiar and is commonly referred to as the “clear web” or the “surface Web”. This part of the internet contains the information accessible and indexed in search engines that most people rely on daily.

The second surface of the internet is the deep web. This part of the internet contains information and data that is not indexed with search engines since they mostly require an authentication process (e.g., login to access the information). Deep web data is inaccessible to the public in many cases. For the average individual, these include social media platforms. However, for hackers these could be imageboards such as 4chan and 8chan, and even certain profiles on popular social media sites that require login credentials to access pages.

The last surface of the internet is the dark web, where malicious activities, crime, and stolen data are available. The dark web’s name suits it very well; it tries to remain out of the limelight, is fairly hidden, and requires the user to have prior knowledge of how to access desired information. Forums or pages are frequently managed by moderators and suspicion is always high due to a lack of transparency amongst users.

Most actors in the dark web use aliases or nicknames while spoofing their locations to confuse authorities, making it challenging to track black-hat actors. Some individuals gain access to the darknet with anonymous credentials through The Onion Router (Tor), IRC channels, or a P2P network.

WHAT OCCURS IN THE DEEP AND DARK WEB?

More than 95% of internet activity[116] occurs in the deep and dark web. Whether the information would be accessed using hidden or legitimate routes — most of the internet is private.

> ***People use these deep web forums to manipulate and collude to access otherwise unobtainable resources.***

There are numerous methods for engaging with content and other users within the deep and dark web. Automotive-related content appears throughout deep and dark web forums, marketplaces, messaging applications, and paste sites.

In many cases, individuals rely on deep and dark web forums to find information that OEMs keep private and do not want exposed to consumers. People use this information to pirate-fix their cars or manipulate their cars' systems. In addition, it is common to see auto parts, components, chips, softwares, and other items for sale that would be against a manufacturer's terms and agreements in a public marketplace. Much of this is done without the drivers understanding the risks to life and limb by tampering with highly advanced automotive systems.

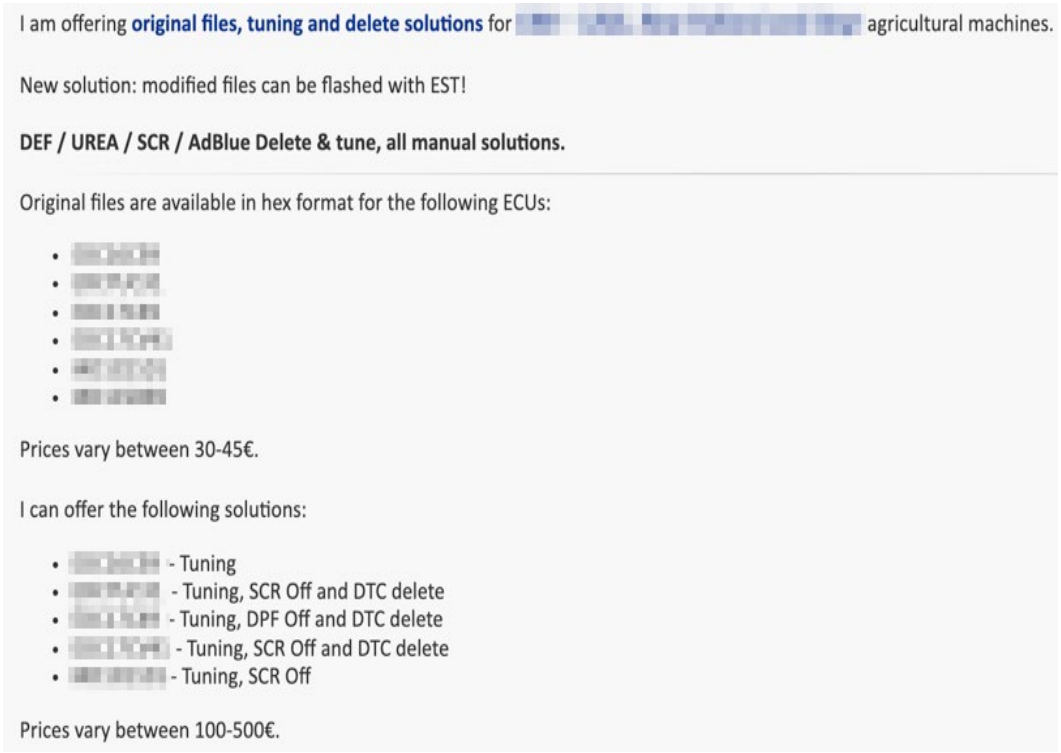
Some of these vulnerabilities can impact the automotive and insurance industries. As individuals tamper with their vehicles, it may cause the vehicle to report misinformation which appears as legitimate. In an extreme case, it may be possible to reverse engineer data and access company servers via authorization granted to vehicles.

253%

INCREASE IN INCIDENTS FOUND BY UPSTREAM IN THE DEEP AND DARK WEB IN 2021, COMPARED TO 2020.

Forums

The deep and dark web include automotive-related forums in which discussions and posts deal with chip tuning, engine tuning, infotainment cracking, reverse engineering, vehicle software cracking, key-fob modifications, immobilizer hacking, and the exchange of automotive software. There are also many general hacking forums that include automotive-related hacks.
People constantly trade information, insights, hacks, and software manipulations to their needs. ECU tuning is a common discussion in deep and dark web automotive forums. Among others are infotainment systems hacking, source codes, data breaches, car hacking tools, tutorials for unauthorized individuals, and more. Whether for the sake of saving money or under the guise of Right to Repair, thousands of questions and offers regarding self-programming vehicles occur regularly. In addition, ECU remapping lessons, guides, software, and tuned files demos are easily accessible.


I am offering **original files, tuning and delete solutions** for [redacted] agricultural machines.

New solution: modified files can be flashed with EST!

DEF / UREA / SCR / AdBlue Delete & tune, all manual solutions.

Original files are available in hex format for the following ECUs:

- [redacted]

Prices vary between 30-45€.

I can offer the following solutions:

- [redacted] - Tuning
- [redacted] - Tuning, SCR Off and DTC delete
- [redacted] - Tuning, DPF Off and DTC delete
- [redacted] - Tuning, SCR Off and DTC delete
- [redacted] - Tuning, SCR Off

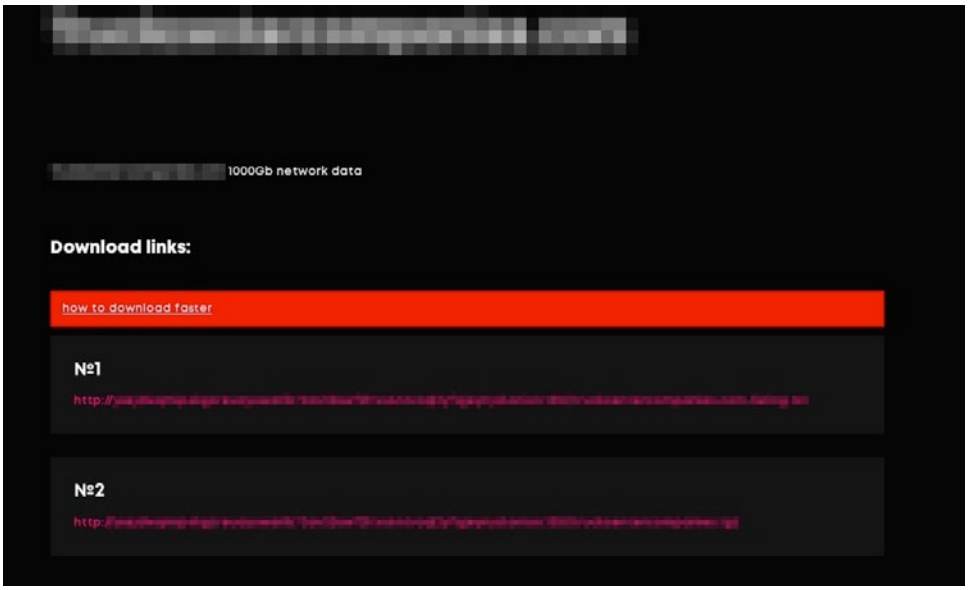
Prices vary between 100-500€.

Image taken from an automotive forum, where a member offers original files, tuning and delete solutions for agricultural machines

Various outlets, including amateur hacker forums, have become expanded battlegrounds that OEMs need to consider when protecting their vehicles today and into the future.

Marketplaces

A darknet market is a commercial website that operates via browsers such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details and credentials, forged documents, and other illicit goods as well as the sale of legal products. After discovering the location of a market, a user must register on the site after which they can browse listings. Some automotive-related dark web marketplace listings on the Empire and Genesis markets offered vehicle-related "products" and services like forged documents, credentials to access user accounts of smart mobility services (such as OEM connected car services and shared mobility services), or stolen credentials of automotive application users.

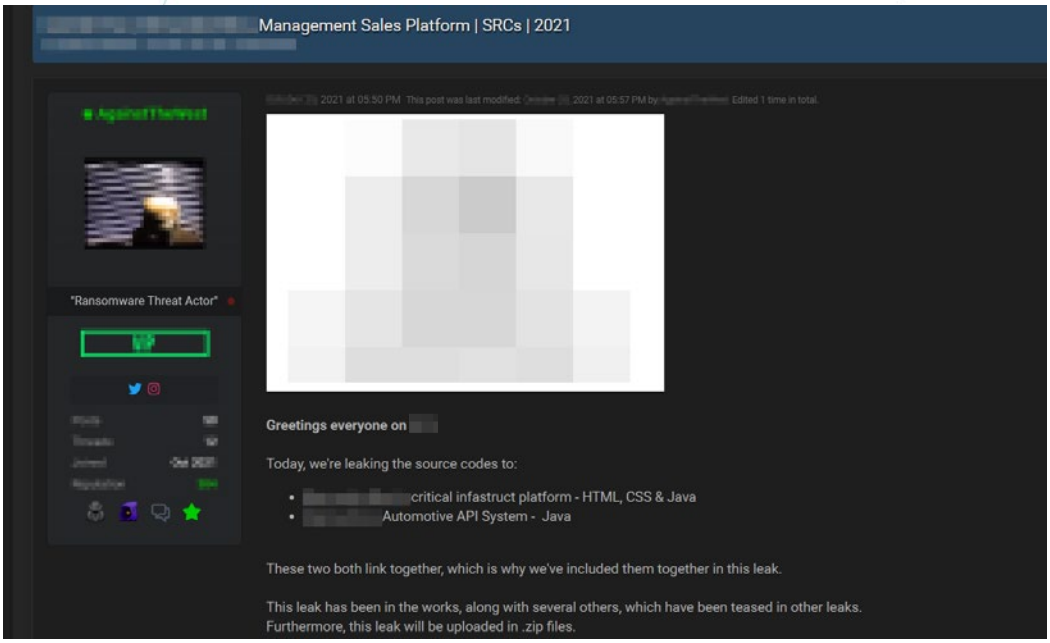


1,000 Gigabytes of a giant American freightliner dealership put for sale on the darknet

Automotive cyber threats in the deep web include, but are not limited to:

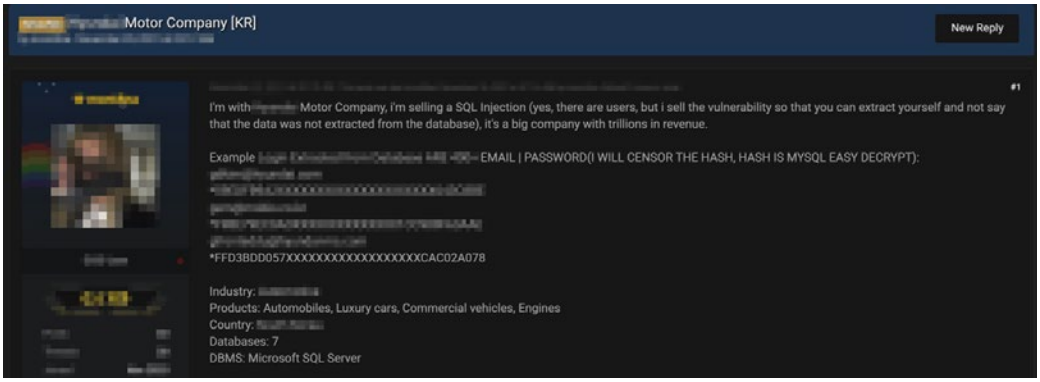
- Steps and guides related to infotainment hacking, CAN bus reverse engineering, chip tuning, and software hacks or illegal upgrades
- The sale or exposure of OEM-related information and credentials stolen in data breaches
- Discussions and sales of tools for vehicle theft or modification, including key signal grabbers, key fob programmers, GPS jammers, radar detectors, and more
- Hacks or fraud related to car-sharing or ride-sharing accounts
- Sales of fake driving licenses or automotive insurance policies

Most common deep and dark web discussions:



Source codes being leaked in a deep web forum

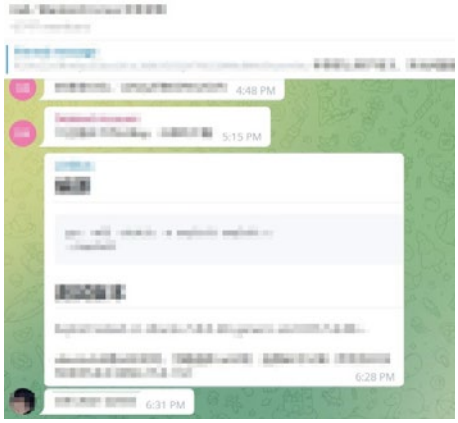
Vehicles data files are common to see, as many car owners submit requests and receive responses, making them easy to find and familiarize oneself with common messages. In addition, code grabbers, signal jammers, repeaters, and key programmers, can be purchased on the deep and dark web creating a low barrier of entry for individuals who want to hack and steal vehicles. Recent years have seen an alarming rise for these devices by Upstream's AutoThreat® Intelligence analysts, leading to a direct correlation between requests and publicly reported incidents.



Two giant Asian OEM's data leaked in the deep and dark web

Messaging Applications

The use of mobile messaging apps for illicit activity has been on the rise as more online activity moves to mobile devices. Users are actively abusing popular mobile messaging apps such as Telegram, Discord, Signal, ICQ, and WhatsApp to share automotive hacking methods and ideas and trade stolen credit cards, account credentials, exploitations of vulnerabilities, leaked source codes, and malware. These chat applications have become valuable alternatives to the secretive forums on the dark web.



Hacker claiming they managed to exploit a vulnerability affecting automotive Tier-1s' products

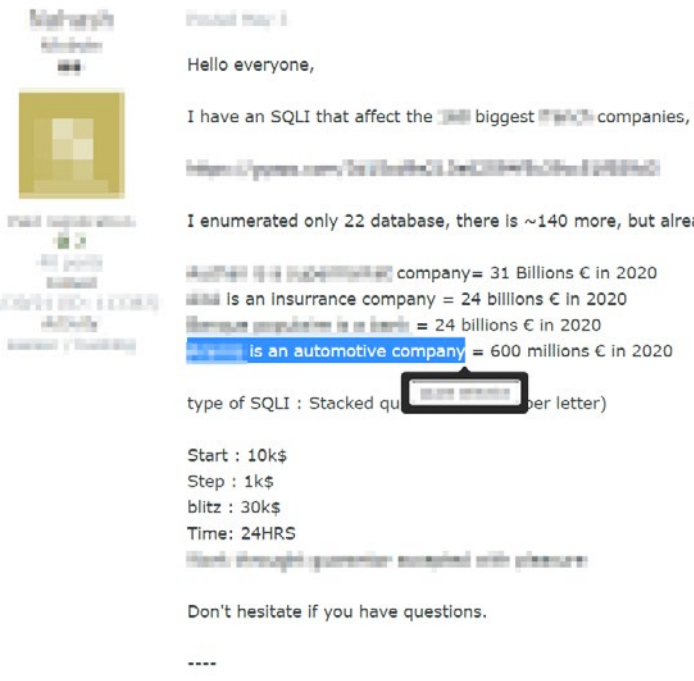
The data - personal information of clients and their transactions with the OEM

LOOKING INTO THE FUTURE

In the past year, we have seen increased data sharing in the deep and dark web. Upstream analysts are discovering increasingly higher amounts of information on unindexed deep and dark websites. Automotive-related searches showed an increase of 253% in automotive cyber-related incidents found in the deep and dark web in 2021, compared to 2020. By monitoring the deep and dark web for automotive cyber threats and incidents as part of the company's threat intelligence efforts, Upstream learns and knows automotive-related cyber trends and occupations before they are out for the world to see. This allows Upstream to identify and mitigate against new vulnerabilities before they become public knowledge. New vulnerabilities are often published in the deep and dark web before their public release; 75% of more than 12,500 CVEs were reported online before officially entering the database[117].

The rising usage in places hidden from OEMs, Tier-1s, and other supply chain companies on the internet are alarming and should be monitored continuously. As new regulations and standards come into effect, it is likely to become more difficult for OEMs and other companies to stay aware of what hackers are planning against their products.

It is crucial to monitor these forums if manufacturers intend to stay one step ahead of black-hat actors.


Hello everyone,

I have an SQLI that affect the biggest companies, they are all really, really big :

I enumerated only 22 database, there is ~140 more, but already in thoses enterprise :

company= 31 Billions € in 2020
is an insurrance company = 24 billions € in 2020
= 24 billions € in 2020
is an automotive company = 600 millions € in 2020

type of SQLI : Stacked qu er letter)

Start : 10k$
Step : 1k$
blitz : 30k$
Time: 24HRS

Don't hesitate if you have questions.

SQLI sold to automotive secondhand car group

The world against the dark web

In January 2021, DarkMarket, the world's largest illegal marketplace on the dark web, was taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (the National Crime Agency), and the USA (DEA, FBI, and IRS). Europol supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved.

Almost 500,000 users and more than 2,400 sellers with over 320,000 transactions of more than 4,650 bitcoin and 12,800 monero transfers were active in this marketplace[118].

Monitoring the deep and dark web

New automotive-related security vulnerabilities, data breaches of sensitive information, and other automotive-related cyber threats are consistently published then discussed on the deep and dark web. It is crucial that stakeholders keep an eye out and monitor these areas of the internet or risk severe gaps in their security posture. A key component in ensuring that effective cybersecurity protections are in place within an organization is knowing when and in what context an organization and its products are being mentioned, both publicly and in the shadows. The new WP.29 regulation as well as the ISO/SAE 21434 standard demand for in-depth threat intelligence; monitoring the deep and dark web as part of the threat intelligence is integral.

By continuously monitoring the deep and dark web, organizations can reduce the mitigation time between a discovered vulnerability or security breach and the time this information reaches the masses. It can also minimize the window of opportunity that criminals have to make copies of the breached data to sell, and warns about the potential exploitation of automotive partners, employees, key executives, and customers. By tracking and monitoring relevant forums, topics, and marketplaces in the deep and dark web, vital players in the automotive ecosystem can take actions to implement necessary cybersecurity measures to prevent the next cyber incident.

CHAPTER

6

AUTOMOTIVE CYBERSECURITY SOLUTION LANDSCAPE

EVOLVING SOLUTIONS

The lure of an elevated owner experience alongside new revenue streams is leaving the days of non-connected vehicles in the rearview mirror, however we are seeing hackers take advantage of vulnerabilities before OEMs can develop relevant security measures.

With new standards and regulations, the industry's push for greater cybersecurity around their vehicles will continue to be a top priority for OEMs, Tier-1s, and Tier-2s who wish to stay competitive in today's landscape.

Regardless, automotive security vulnerabilities and cyber threats remain ever present. As a result, companies are constantly searching for new ways to address vulnerabilities and threats to protect both assets and consumers.

As cyber attacks continue to target vehicles, a holistic approach that incorporates security by design, VSOC implementation, and an impactful multi-layer security approach is necessary to secure connected vehicles into the future.

Securing the vehicle's full lifecycle

One of the primary requirements of the current cybersecurity standards and regulations is that each vehicle must be secured throughout its entire lifecycle, namely during development, production, and post-production phases. A typical passenger vehicle can have a lifespan of approximately 12 years while commercial trucks have a 20 year lifespan, and agricultural vehicles have a lifespan of upwards of 30 years. This means OEMs must think of how to secure a product that is potentially operating on decades-old technology.

2022 will be the first year that this will be regulated and standardized through WP.29 R155 and ISO/SAE 21434. As a result, OEMs and other key stakeholders must consider using a multi-layered approach if they intend to protect against today's and tomorrow's most advanced cyber attacks.

Protecting against attacks in the supply chain

Until now, Tier-1 and Tier-2 suppliers were not always under scrutiny by OEMs to disclose their cybersecurity practices. This ran the risk of carrying security vulnerabilities from third-party vendors directly into an OEMs vehicle on a large scale, compounding the fear of production interruptions beyond supply chain bottlenecks. In addition, lax cybersecurity procedures are allowing counterfeit components to enter legitimate facilities, threatening safety by reducing wear ratings, overriding safety limits, and more.

To secure the supply chain, both WP.29 R155 & R156 and ISO/SAE 21434 require that OEMs take active responsibility to ensure that suppliers are properly following appropriate guidelines.

With the new standards and regulations (discussed in Chapter 1), OEMs will be required to implement proactive practices to ensure component security. Tighter checks are designed to protect the ecosystem from the hazards of unwanted parts finding their way into their machines. For example, WP.29 R155 requires the OEM to assess, treat, and maintain the status of each risk throughout all stages of vehicle production. They must also create processes to address and mitigate against future attacks together with their Tier-1 and Tier-2 suppliers.

ISO/SAE 21434 gives guidance on how to carry out the WP.29 R155 requirement together with suppliers. Amongst other parts of the standards, there are two key elements that OEMs must address:

01

Cyber Record of Capability

OEMs are required to check with suppliers regarding their cyber history. It is the responsibility of the OEM to ensure that the supplier is conducting ongoing risk vulnerability and management for all relevant components.

02

Define shared responsibilities

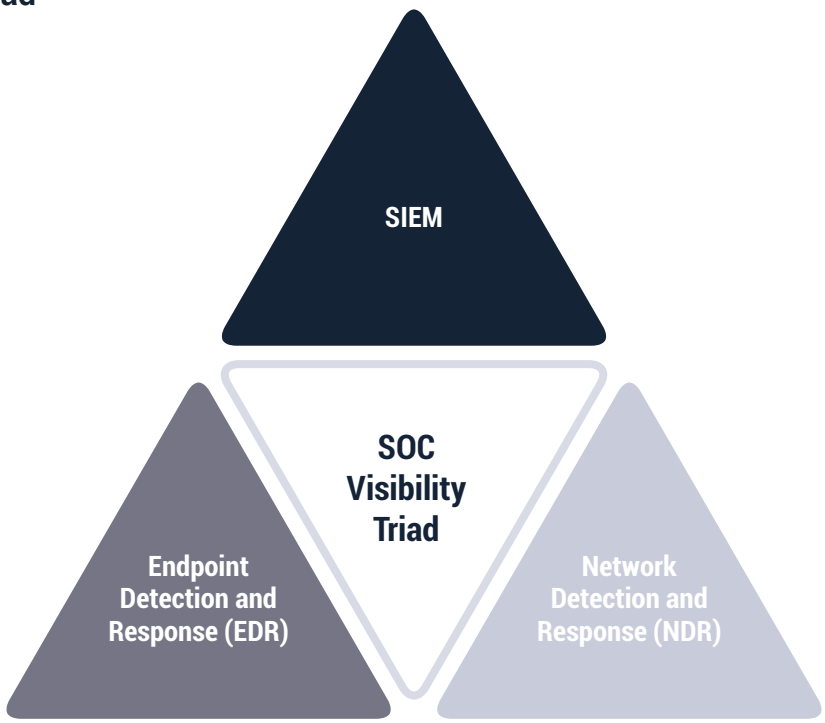
To ensure that nothing is missed due to a lack of clear delegation of responsibilities, cybersecurity responsibilities are shared. This can be done using various CIAD (Cybersecurity Interface Agreement for Development methods), such as RASIC (Responsible-Approving-Supporting-Informed-Consulting).

Regardless of the methodology that OEMs and suppliers agree upon, it ultimately is the responsibility of the OEM to ensure that practices meet or exceed WP.29 R155 & R156 and ISO/SAE 21434 requirements.

Implementing a multi-layered cybersecurity solution

Multi-layered security is already recognized as a standard in IT and enterprise security. New vulnerabilities continuously arise, pushing businesses to implement improved security. These include end-point solutions, network security solutions, cloud security, internal segmentation technology, and more. As highlighted by Gartner, traditional enterprise SOCs (Security Operation Centers) leverage endpoint and network detection and response tools together with SIEM solutions to manage more general IT-related cybersecurity events.

SOC visibility triad



Visual representation of a multi-layered SOC approach, based on Gartner enterprise SOC visibility triad

Applying a SOC approach to vehicles (VSOC) creates a more secure layering between OEMs, Tier-1s, Telematics Service Providers (TSPs), and other stakeholders in the ecosystem, minimizing threats and preventing attacks. These include taking into consideration:

In-vehicle security

Secures internal components, preventing both short and long-distance remote attacks.

IT network security

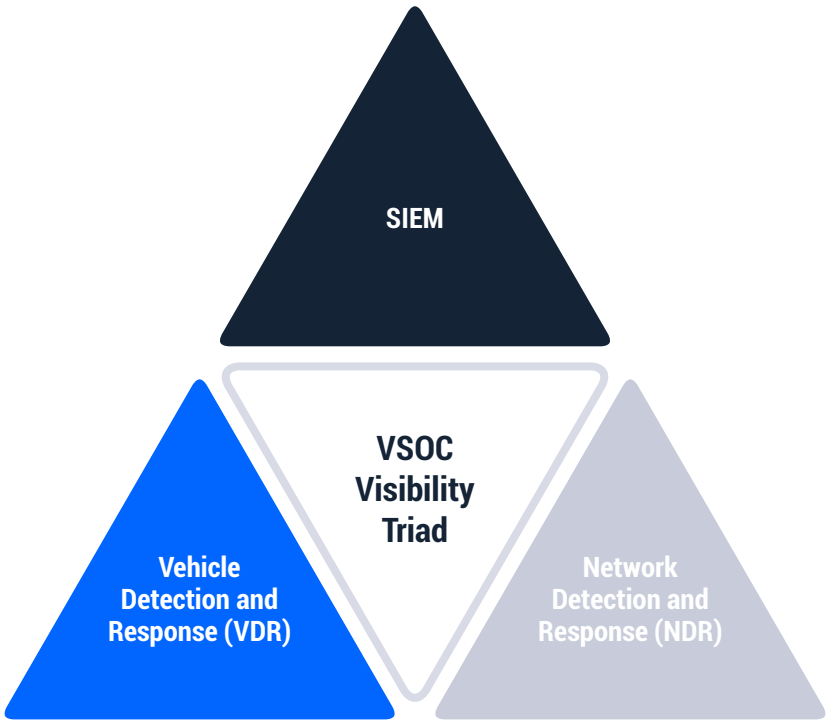
Defends an organization's servers and IT backend infrastructure.

Automotive cloud security

Cloud security offers a birdseye view of what's going on across vehicles, networks, and other connected services, including piecing together seemingly unrelated events to identify a multi-vehicle attack.

Each layer within the automotive infrastructure has its unique challenges, requiring specialized protection methods at each point. A multi-layered approach, including a SIEM and a vehicle-focused purpose-built VSOC, can create a potent team to address these challenges. Upstream's technology allows VSOCs to contextualize and understand what is happening to an individual vehicle in its environment, even drilling down to understand if specific incidents are occuring only in a specific region or globally.

The Upstream Platform is built to harmoniously work within existing IT frameworks to deliver a focused Vehicle Detection and Response (VDR) product, identifying attacks that are unique to the needs of connected vehicles.



An impactful multi-layered approach requires a cybersecurity model that is purpose-built to address the unique needs of today's connected vehicles.

DEVELOPING AN EFFECTIVE VSOC

Security Operations Centers (SOCs) are already a key part of cybersecurity teams but unlike modern computers, vehicles are constantly in motion, experiencing new environments and interacting with new inputs thousands of times a minute. The sophistication of cyber attacks that take advantage of vehicles' unique experiences demands that OEMs develop an integrated vehicle-focused SOC (VSOC).

Sometimes referred to as a "vehicle SOC", "mobility SOC", or "automotive SOC", VSOCs enable cybersecurity for the post-production phase. It is critical in ensuring the security of connected vehicles and the smart mobility ecosystem, allowing companies to monitor their entire infrastructure and vehicles in real-time, and respond in a timely manner to detected threats.

When conducted properly, an effective VSOC:

- Has a clear framework detailing the VSOC's capabilities, components, and operating model
- Defines the strategy and scope including the vision, mission, and charter of the VSOC
- Outlines governance and steering policies, standards, procedures, and processes
- Predicts threats before they emerge by leveraging purple teams, threat models, and threat intelligence fusion
- Detects threats and anomalies in near or real-time
- Conducts proactive threat hunting and tradecraft analysis
- Performs alert triage and investigation
- Builds and maintains end-to-end playbooks to structure and automate response activities
- Ingests data from various automotive-related feeds

First steps to building a VSOC

Transparency is at the heart of any effective VSOC.

Using a Build-Operate-Transfer (BOT) model is intended to be transferable between Upstream's experts and a client and/or partner. The most common two reasons are:

01

An OEM does not have enough manpower and/or the right skills to fully take on the responsibility at the time of development.

02

A company's internal team would like to work in tandem, ensuring they have all the necessary capabilities in place, before bringing all tasks in-house.

As a first step to building a VSOC, a company should use a framework to understand the different components and capabilities needed for an effective department. The structure, development, and operation of the new VSOC can then be done in-house or with an external party who can pass it off to an in-house team at a later date.

Upstream Security provides several advantages, including a data management and cybersecurity platform, purpose-built for connected vehicles, and offers a VSOC with immediately-available detection capabilities. Automated processes demand minimal intervention from teams along with customizable parameters to manage triggered alerts.

Whichever approach you take, securing modern vehicles is vital in securing consumer trust and growing capabilities throughout the full ecosystem.

STAYING ONE STEP AHEAD OF THE THREATS WITH AUTOMOTIVE-SPECIFIC THREAT INTELLIGENCE

A multi-layered approach must also include a layer of proactivity, including the monitoring of threat intelligence from various sources to bolster threat detection abilities.

An industry-specific and purpose-built threat feed that is continuously updated with new threats, based on surface, deep, and dark web incidents enables OEMs to remain within compliance guidelines while mitigating against vulnerabilities in their products.

The introduction of automotive cyber threat intelligence gives each ecosystem player new possibilities.

Benefits to OEMs

- Gain early detection of cyber threats against OEM assets
- Comply with automotive regulations and standards demanding in-depth threat intelligence
- Manage reputational risk before threats, vulnerabilities, or hacks go public
- Avoid future warranty issues by discovering warranty and policy violations early
- Build trust with customers due to increased awareness of cyber threats
- Monitor and manage direct threats to the automotive supply chain
- Gain insights into the current threat posture and benchmark it against peers or competitors in the automotive industry

Benefits to Tier-1 and Tier-2 suppliers

- Gain OEM and purchaser trust through more in-depth component threat monitoring
- Avoid future warranty issues by discovering warranty and policy violations early
- Monitor popular component-hacking forums and chats to track and remedy component vulnerabilities
- Comply with regulatory demands by engaging with and monitoring vulnerabilities via threat feeds

Benefits to CISOs

- Monitor for leaked organizational email addresses to detect potential credential breaches that can expose an organization
- Develop steps to improve IT and OT security and implement the right cybersecurity measures within cloud services and corporate networks
- Monitor and analyze attacks on other organizations to develop defense methods against similar threats to their own assets and applications
- Gain a more thorough understanding of the cyber threat landscape to better report cyber risks and thus prioritize action and allocate resources and budget
- Discover actors in the dark web actively selling access to corporate networks
- Discover insider threats to an organization
- Monitor data dumps that could contain specific IP addresses
- Monitor for leaked intellectual properties (such as products' bill of materials)

Benefits to VSOC Analysts

- Monitor forums' chat exchanges to gain the advanced notice of new and emerging threats
- Identify new fraud MOs (modus operandi), trends, and threat actors
- Recognize and monitor commonly pirated features and illegal modifications
- Detect, warn, and offer next steps with regards to data breaches involving private automotive customer information
- Find new threats that could disrupt the organization's network, resources, or business
- Remain aware of new vulnerabilities or exploits being sold in underground marketplaces
- Monitor vehicle-related software security to issue necessary OTA updates
- Prevent future connected vehicle cyber attacks by disabling compromised accounts or notifying their owners
- Track automotive-related zero-day vulnerabilities and exploit kits

Benefits to insurance companies

- Enable actuaries to effectively measure risk and evaluate policy costs by identifying primary causes, locations, and methods of automotive breaches and hacks
- Detect popular methods of insurance fraud, such as the manipulation of connected vehicle dashcams
- Identify and prevent warranty and/or insurance policy violations, such as odometer manipulation
- Ability to understand geographical risk areas in local markets and assets subsets

Benefits to shared mobility and rental car stakeholders

- Identify fraud related to identity theft
- Detect the sale of fraudulent car sharing/ride-hailing user and driver accounts
- Spot malicious vendors selling car sharing/ride-hailing or rental user data
- Monitor hacking forums for methods of stealing or manipulating shared mobility assets

As companies continue pushing toward greater connectivity in their vehicles, telematics and other data are becoming increasingly valuable targets for black-hat hackers. Only automotive-specific threat intelligence products can understand a vehicle's context to identify anomalies and prevent the desensitization of cybersecurity teams by removing false alarms.

It is vital that all CISOs address the growing threat of automotive hacking with a unique approach that fits their needs.

COMPLYING WITH AUTOMOTIVE CYBERSECURITY REGULATIONS

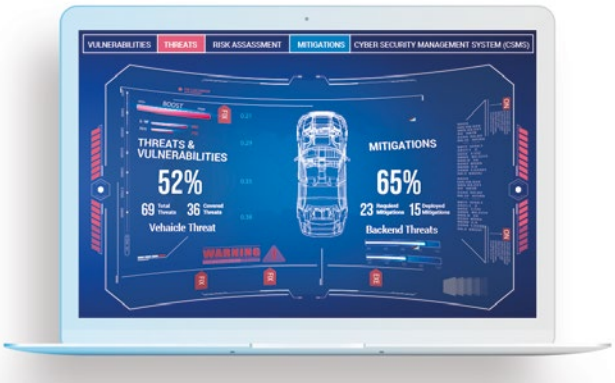
As mentioned in Chapter 1, the upcoming implementation of new automotive cybersecurity standards and regulations will be a challenge for the full cybersecurity ecosystem. OEMs that do not comply will be at risk of losing vital business and consumer trust. Tier-1s, Tier-2s, and other ecosystem players risk losing vital business to other companies who are compliant.

The concern is twofold. One, some companies find that regulations don't smoothly fit within the framework of their business, requiring them to go through great lengths in order to remain in operation. The other is the hesitancy to let a third party install any piece of hardware or software into their technologies.

Agentless technologies have the ability to allow companies to continue functioning as-is (depending on multiple factors) while still complying with both WP.29 R155/R156 and ISO/SAE 21434.

Preliminary steps toward effective compliance include

Performing an organizational gap analysis to better understand the weak spots based on risk assessments, and correlating mitigation demands in the WP.29 R155 automotive cybersecurity regulation. Upstream's gap analysis assessment tool enables OEMs to see where they stand with regard to regulatory compliance and offers a quick overview of areas that may need more attention.



Upstream's WP.29 Gap Analysis Assessment tool

It is vital to complete an effective risk assessment where automotive stakeholders can perform a threat analysis and risk assessment (TARA) as described in the ISO/SAE 21434 standard in sections 8.3-8.9. Upstream offers a tool that allows organizations to analyze the threats to their assets, calculate the total cybersecurity risk based on the formulas and matrices provided by the standard, and generate PDF reports to document the process and analysis.

Upstream's ISO/SAE 21434 Threat Analysis and Risk Assessment (TARA) tool

Building an effective cybersecurity management system requires an OEM to complete three main steps: learn, assess, and comply. Upstream's online and in-person trainings, customized tools, and cybersecurity products, like The Upstream Platform and AutoThreat® Intelligence, help OEMs, Tier-1 and Tier-2 manufacturers as well as other automotive stakeholders through all three steps in the process, leading them to compliance and to a safer and more secure vehicle.

UPSTREAM'S CYBERSECURITY AND DATA MANAGEMENT PLATFORM

Upstream Security provides a cloud-based data management platform purpose-built for connected vehicles, delivering unparalleled automotive cybersecurity detection and response and data-driven applications.

The Upstream Platform unlocks the value of vehicle data, empowering customers to build connected vehicle applications by transforming highly distributed vehicle data into centralized, structured, contextualized data lakes. Coupled with AutoThreat® Intelligence, the first automotive cybersecurity threat intelligence solution, Upstream provides industry-leading cyber threat protection and actionable insights, seamlessly integrated into the customer's environment and vehicle security operations centers (VSOC).

Upstream's customers include some of the world's leading automotive OEMs, suppliers, and others, protecting millions of vehicles.

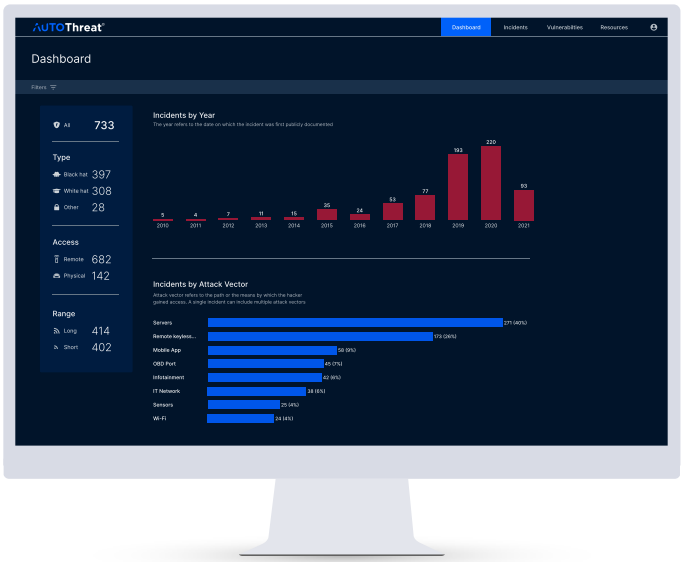
In the past year, the strong combination of the Upstream Platform and AutoThreat® Intelligence has become critical in securing the automotive industry.

The data gathered and analyzed by the AutoThreat® Intelligence analysis team was used to create detectors and solutions for vulnerabilities and flaws seen in the field. This puts Upstream in front of future threats that are yet to be known to the industry today.

The Upstream Platform

The Upstream Platform is a cybersecurity and data management platform for connected vehicles. The platform utilizes data normalization and cleansing, digital twin profiling, mobility intelligence, and AI-powered detection to identify anomalies in the connected vehicle ecosystem. This allows The Upstream Platform to offer unparalleled cybersecurity detection and response as well as data-driven actionable insights through mobility-specific applications.

- Cloud-based and Agentless
- Purpose-built for Connected Vehicles
- Powered by data
- Holistic V-XDR
- Mobility digital twins
- Mobility-specific built-in detectors
- Adaptable applications
- Actionable insights



AutoThreat® Intelligence

Upstream's AutoThreat® Intelligence is the automotive industry's leading cyber threat intelligence and risk assessment solution. Purpose-built to collect, analyze, and leverage automotive threat intelligence to empower unparalleled cybersecurity.

- Automotive-specific
- Comprehensive incident repository
- Supply chain insight
- Tailor-made threat modeling
- Deep and dark web monitoring
- Standalone or API
- Customized reporting
- User friendly

Vehicle SOC (VSOC)

Operating at the core of any VSOC, the Upstream Platform offers unparalleled automotive cybersecurity capabilities by detecting known and unknown cyber threats and improves operational efficiencies by providing automated workflows adaptable to the changing cyber threat landscape.

A VSOC powered by Upstream enables:

- Easy deployment
- Automotive-specific threat detection
- Effective cyber risk management
- Timely response and mitigation
- Industry enriched know-how
- Seamless integrations
- Regulatory compliance

PREDICTIONS FOR 2022

Based on the analysis of recent trends and emerging technologies, Upstream's team discussed predictions for 2022. While there are concerns for increased attacks by black-hat actors and white-hat hackers, there is great opportunity for OEMs and suppliers to secure vulnerabilities while pushing their technological offerings forward.

What Upstream predicts in 2022:

01

Attacks will increasingly target OEM servers and infrastructure

Increasing storage of vehicle data will make any OEM server more and more appealing. This will catch the attention of hackers who will look to test their ability against a major ecosystem player.

02

Black-hat attacks will continue to overshadow white-hat hacking

In line with previous years, attacks for personal gain will outpace research-driven hackers. With the implementation of UNECE WP.29's R155 & R156 and ISO/SAE 21434, OEMs, Tier-1s, and Tier-2s have more to lose than ever before.

03

Regulation implementation will also redefine automotive data

Regulation will force the ecosystem to better examine their data, allowing OEMs, Tier-1s, and Tier-2s to better understand the performance, context, and overall quality of their data. We predict this will lead to great innovative leaps in the next generation of vehicles, but will also act as a barrier for foreign manufacturers looking to sell vehicles in China, as mentioned in Chapter 1.

04

Keyless car thefts will continue to rise due to ease of obtaining sophisticated technology

The value of new cars keeps them as key targets for criminals. The ease of obtaining hacking hardware and tutorials means we can expect to see more cars stolen in record time.

05

Vulnerabilities will rise due to fraudsters flooding the market with counterfeit chips

The chip shortage's predicted end date keeps getting pushed back, presenting more opportunities for counterfeiters to flood the market with fake chips that contain yet to be known corruptions.

PREDICTIONS FOR 2022

06

A greater emphasis by OEMs on Software Defined Vehicles

A majority of components will be primarily enabled through software. This will pose even more cybesecurity challenges in the near future as monitoring proper functionality will require more advanced monitoring and detection capabilities.

07

EV charging stations will become a growing battleground for attacks

Hackers in 2021 made known that charging stations are valuable targets. By exploiting the grid's network through physical stations, black-hat actors will be able to steal data and even disrupt entire fleets.

08

Greater PII will be collected by industry stakeholders

In Europe we see more and more subscription models for vehicles. This will increase the need to maintain a digital user fingerprint for multimodal mobility. It will introduce the user ID as an additional attack vector.

09

V2X will become a new avenue for hacking

Going forward, hackers will begin tampering with software, image processing, and other V2X communication capabilities to influence the on-board computers which help a vehicle safely engage with its surroundings.

10

Smart cities will begin adopting emerging technologies

Smart cities will begin adopting both existing and emerging technologies that impact traffic management and enable greater ease of communication between infrastructure and vehicles.

REFERENCES

1. https://www.juniperresearch.com/whitepapers/connected-cars-how-5g-connected-commerce-blockchain-will-disrupt-the-ecosystem
2. https://unece.org/sites/default/files/2021-03/R155e.pdf
3. https://unece.org/sites/default/files/2021-03/R156e.pdf
4. https://www.jdsupra.com/legalnews/china-issued-the-auto-data-regulation-4766436/
5. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
6. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
7. https://www.wevolver.com/article/high-speed-data-and-connected-cars
8. https://upstream.auto/research/automotive-cybersecurity/?id=8000
9. https://upstream.auto/research/automotive-cybersecurity/?id=8770
10. https://upstream.auto/research/automotive-cybersecurity/?id=2020
11. https://upstream.auto/research/automotive-cybersecurity/?id=1170
12. https://upstream.auto/research/automotive-cybersecurity/?id=4590
13. https://upstream.auto/research/automotive-cybersecurity/?id=5480
14. https://upstream.auto/research/automotive-cybersecurity/?id=8600
15. https://upstream.auto/research/automotive-cybersecurity/?id=7920
16. https://upstream.auto/research/automotive-cybersecurity/?id=8010
17. https://upstream.auto/research/automotive-cybersecurity/?id=9020
18. https://upstream.auto/research/automotive-cybersecurity/?id=8910
19. https://upstream.auto/research/automotive-cybersecurity/?id=8840
20. https://upstream.auto/research/automotive-cybersecurity/?id=8900
21. https://upstream.auto/research/automotive-cybersecurity/?id=9660
22. https://upstream.auto/research/automotive-cybersecurity/?id=9940
23. https://upstream.auto/research/automotive-cybersecurity/?id=9210
24. https://upstream.auto/research/automotive-cybersecurity/?id=9610
25. https://upstream.auto/research/automotive-cybersecurity/?id=9710
26. https://upstream.auto/research/automotive-cybersecurity/?id=8740
27. https://www.marketplace.org/shows/marketplace-tech/no-chips-fake-chips-the-computer-chip-issues-are-still-with-us/,
28. https://arstechnica.com/gadgets/2021/06/chip-shortages-lead-to-more-counterfeit-chips-and-devices/
    https://www.wsj.com/articles/chip-shortage-has-spawned-a-surplus-of-fraudsters-and-fake-parts-1162625500
    https://www.thedrive.com/news/41738/ford-still-has-over-60000-incomplete-vehicles-waiting-for-chips
29. https://www.cnbc.com/2021/09/23/chip-shortage-expected-to-cost-auto-industry-210-billion-in-2021.html
30. https://www.reuters.com/business/autos-transportation/volkswagen-warns-worsening-output-hit-chip-shortage-ft-2021-04-24/
31. https://www.theverge.com/2021/8/19/22632330/toyota-production-japan-north-america-chip-shortage-ford-tesla-gm-vw
32. https://www.theverge.com/2021/8/10/22619190/ford-mustang-mach-e-chip-shortage-delay-6-weeks-250kwh
33. https://www.theverge.com/2021/9/2/22654357/gm-factory-shutdown-chip-shortage-truck-suv
34. https://publish.manheim.com/content/dam/consulting/ManCons-qtrly-call-202107.pdf
35. https://upstream.auto/research/automotive-cybersecurity/?id=4920
36. https://upstream.auto/research/automotive-cybersecurity/?id=8010
37. https://upstream.auto/research/automotive-cybersecurity/?id=8150
38. https://upstream.auto/research/automotive-cybersecurity/?id=8440
39. https://upstream.auto/research/automotive-cybersecurity/?id=8450
40. https://upstream.auto/research/automotive-cybersecurity/?id=8480
41. https://upstream.auto/research/automotive-cybersecurity/?id=8560
42. https://upstream.auto/research/automotive-cybersecurity/?id=9800
43. https://upstream.auto/research/automotive-cybersecurity/?id=8750
44. https://upstream.auto/research/automotive-cybersecurity/?id=8840
45. https://upstream.auto/research/automotive-cybersecurity/?id=8760
46. https://upstream.auto/research/automotive-cybersecurity/?id=9980
47. https://www.cvedetails.com/cvss-score-distribution.php
48. https://blog.malwarebytes.com/malwarebytes-news/2020/05/how-cvss-works-characterizing-and-scoring-vulnerabilities/

REFERENCES

49. https://upstream.auto/research/automotive-cybersecurity/?id=8010
50. https://upstream.auto/research/automotive-cybersecurity/?id=8630
51. https://upstream.auto/resources/remotely-hacking-into-a-brand-new-car/
52. https://upstream.auto/research/automotive-cybersecurity/?id=9140
53. https://upstream.auto/research/automotive-cybersecurity/?id=8880
54. https://www.agriculture.com/news/machinery/biden-backs-right-to-repair-from-tractors-to-tech
55. https://upstream.auto/research/automotive-cybersecurity/?id=8760
56. https://upstream.auto/research/automotive-cybersecurity/?id=8420
57. https://upstream.auto/research/automotive-cybersecurity/?id=8160
58. https://www.transport.nsw.gov.au/news-and-events/articles/transport-for-nsw-impacted-by-worldwide-accellion-data-breach
59. https://upstream.auto/research/automotive-cybersecurity/?id=8400
60. https://upstream.auto/research/automotive-cybersecurity/?id=8520, https://new.mta.info/agency/new-york-city-transit/subway-bus-ridership-2019
61. https://www.statista.com/statistics/743400/estimated-connected-car-shipments-globally/
62. https://upstream.auto/research/automotive-cybersecurity/?id=8780
63. https://upstream.auto/research/automotive-cybersecurity/?id=9980
64. https://upstream.auto/research/automotive-cybersecurity/?id=9880
65. https://upstream.auto/research/automotive-cybersecurity/?id=5520
66. https://upstream.auto/research/automotive-cybersecurity/?id=8150
67. https://upstream.auto/research/automotive-cybersecurity/?id=710
    https://upstream.auto/research/automotive-cybersecurity/?id=790, https://upstream.auto/research/automotive-cybersecurity/?id=9180
68. https://upstream.auto/research/automotive-cybersecurity/?id=9200
69. https://upstream.auto/research/automotive-cybersecurity/?id=8140
70. https://upstream.auto/research/automotive-cybersecurity/?id=5290
71. https://upstream.auto/research/automotive-cybersecurity/?id=440
72. https://upstream.auto/research/automotive-cybersecurity/?id=4130
73. https://upstream.auto/research/automotive-cybersecurity/?id=6930
74. https://upstream.auto/research/automotive-cybersecurity/?id=5110
75. https://upstream.auto/research/automotive-cybersecurity/?id=9510
76. https://upstream.auto/research/automotive-cybersecurity/?id=5470
77. https://upstream.auto/research/automotive-cybersecurity/?id=8230
78. https://www.komando.com/security-privacy/apps-share-your-data/782539/
79. https://www.dailymail.co.uk/news/article-9812339/Keyless-technology-drives-rise-vehicle-theft-accounts-50-cent-stolen-cars.html
80. https://www.driving.co.uk/news/motion-sensor-fobs-short-term-fix-keyless-car-thefts-say-security-experts/
81. https://upstream.auto/research/automotive-cybersecurity/?id=8220
82. https://upstream.auto/research/automotive-cybersecurity/?id=8310
83. https://upstream.auto/research/automotive-cybersecurity/?id=8630
84. https://upstream.auto/research/automotive-cybersecurity/?id=9150
85. https://upstream.auto/research/automotive-cybersecurity/?id=9020
86. https://upstream.auto/research/automotive-cybersecurity/?id=9160
87. https://upstream.auto/research/automotive-cybersecurity/?id=8870, https://upstream.auto/research/automotive-cybersecurity/?id=8220
88. https://upstream.auto/research/automotive-cybersecurity/?id=10020
89. https://upstream.auto/research/automotive-cybersecurity/?id=10030
90. https://upstream.auto/research/automotive-cybersecurity/?id=8850
91. https://upstream.auto/research/automotive-cybersecurity/?id=8530
92. https://upstream.auto/research/automotive-cybersecurity/?id=8090
93. https://upstream.auto/research/automotive-cybersecurity/?id=8450
94. https://upstream.auto/research/automotive-cybersecurity/?id=8530
95. https://upstream.auto/research/automotive-cybersecurity/?id=9800
96. https://upstream.auto/research/automotive-cybersecurity/?id=6950
97. https://upstream.auto/research/automotive-cybersecurity/?id=7360

REFERENCES

98. https://www.eetimes.com/automotive-software-cybersecurity/#
99. https://www.aptiv.com/en/insights/article/what-is-an-electronic-control-unit
100. https://upstream.auto/research/automotive-cybersecurity/?id=8010
101. https://upstream.auto/research/automotive-cybersecurity/?id=9330
https://upstream.auto/research/automotive-cybersecurity/?id=9340
https://upstream.auto/research/automotive-cybersecurity/?id=9350
https://upstream.auto/research/automotive-cybersecurity/?id=9370
https://upstream.auto/research/automotive-cybersecurity/?id=9380
https://upstream.auto/research/automotive-cybersecurity/?id=9600
102. https://upstream.auto/research/automotive-cybersecurity/?id=9080
103. https://upstream.auto/research/automotive-cybersecurity/?id=8910
104. https://www.just-auto.com/news/ford-tests-c-v2x-technology-in-china-ahead-of-2021-production/
105. https://m.futurecar.com/5092/Ford-Motor-Co-Delivers-the-First-Electric-Mach-Es-to-Customers-in-China
106. https://www.just-auto.com/news/ford-tests-c-v2x-technology-in-china-ahead-of-2021-production/
107. https://www.businesswire.com/news/home/20190117005195/en/
108. https://www.weforum.org/agenda/2021/07/why-the-future-for-cars-is-connected/
109. https://upstream.auto/research/automotive-cybersecurity/?id=8170
110. https://upstream.auto/research/automotive-cybersecurity/?id=8490
111. https://upstream.auto/research/automotive-cybersecurity/?id=8150
112. https://upstream.auto/research/automotive-cybersecurity/?id=7500
113. https://xtown.la/2021/10/20/car-thefts-soar-again/
114. https://upstream.auto/research/automotive-cybersecurity/?id=8950
115. https://upstream.auto/research/automotive-cybersecurity/?id=9650
116. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
117. https://www.zdnet.com/article/the-dark-web-is-now-a-hotbed-of-zero-day-vulnerabilities/
118. https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

ABOUT UPSTREAM

Upstream Security offers a cloud-based automotive cybersecurity and data analytics platform purpose-built for connected vehicles and smart mobility services. Upstream's platform fuses machine learning, data normalization, and digital twin profiling technologies to detect anomalies in real-time using existing automotive data feeds. Coupled with AutoThreat® Intelligence, the first automotive cybersecurity threat intelligence feed, Upstream provides unparalleled cybersecurity and data-driven insights, seamlessly integrated into the customer's environment.

Upstream is privately funded by Alliance Ventures (Renault, Nissan, Mitsubishi), Volvo Group, BMW, Hyundai, MSI Insurance, Nationwide Insurance, Salesforce Ventures, CRV, Glilot Capital Partners, and Maniv Mobility.

For more information

VISIT US AT:
www.upstream.auto

CONTACT US:
hello@upstream.auto

FOLLOW US: