Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN R155 Attack Vectors and Beyond

Numaan Huq, Rainer Vosseler, Yurika Baba

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

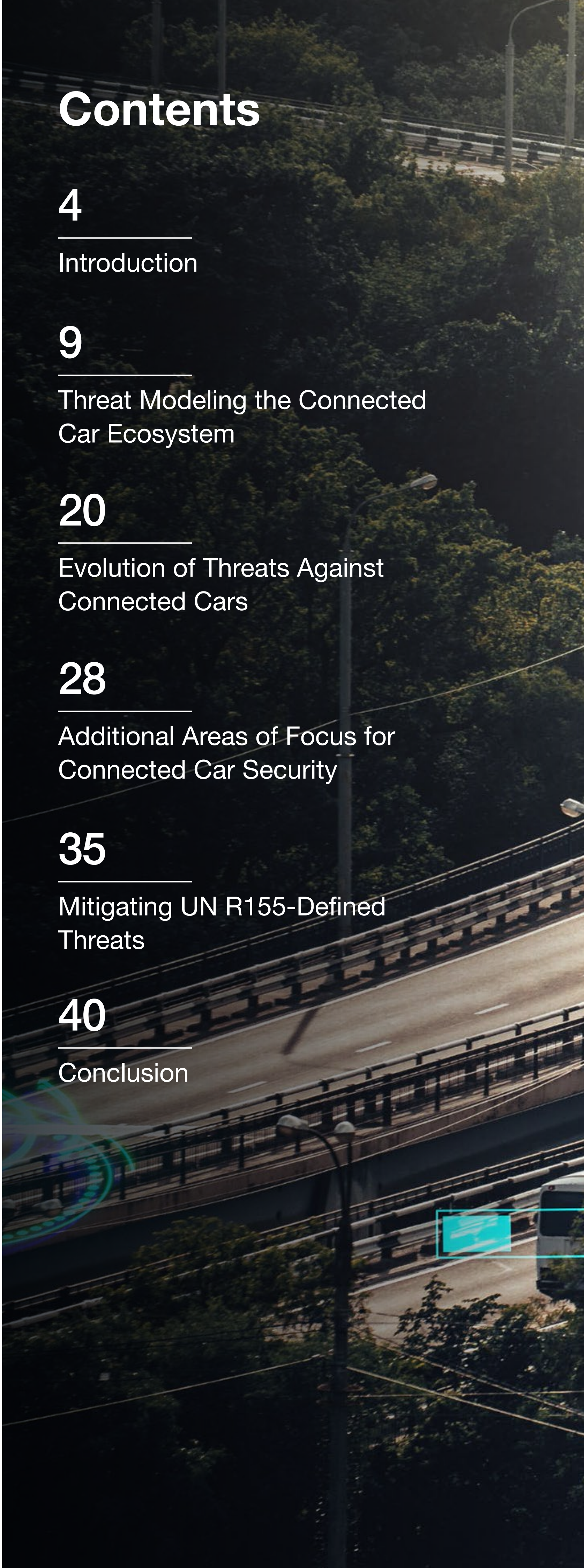
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Published by
Trend Micro Research

Written by
**Numaan Huq,
Rainer Vosseler,
Yurika Baba**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963 – 2017)



Contents

The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), is a worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee.[1] They published the “Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management systems.”[2] This document, which is known as UN Regulation No. 155, contains seven high-level and 30 sub-level descriptions of vulnerabilities and threats, including 69 attack vectors directly affecting vehicle cybersecurity.

For this research paper, we calculated the severity levels of the attack vectors listed in UN Regulation No. 155, using the industry standard DREAD threat model. We also studied the connected car ecosystem and predicted how it will evolve with the rollout of high-speed 5G networks. We then recalculated the DREAD threat model to show how threat severity will evolve over the next five to 10 years. Finally, we highlighted focus areas and cyberattack vectors not included in the regulation, but which will likely necessitate defenses against in the future. All this was done to help stakeholders better determine how to prioritize, plan, and act against these attack vectors.

Introduction

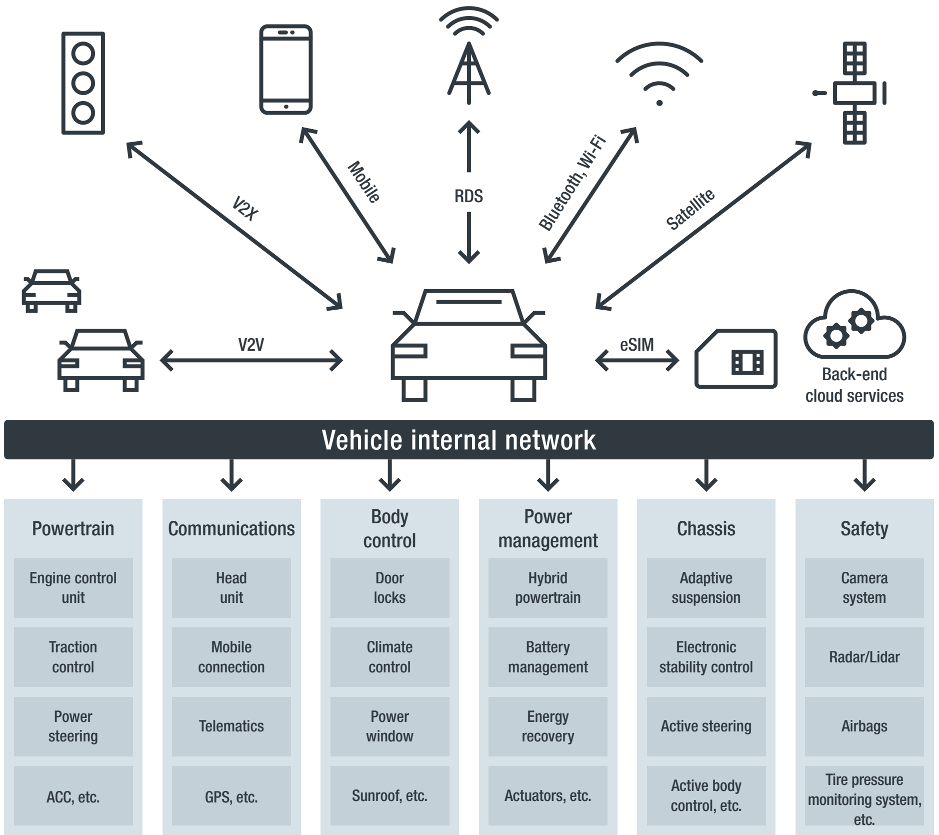
The regulatory frameworks developed by the World Forum WP.29 allows for the market introduction of innovative vehicle technologies while improving global vehicle safety.[3] In the 181st session of the World Forum for the Harmonization of Vehicle Regulations, the ECE/TRANS/WP.29/2020/79 "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management systems" was adopted, and became binding on January 22, 2021.[4] This proposal was formally published as UN regulation No. 155 (also called UN R155), "Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management systems," on March 2021.[5]

Annex 5 of the UN Regulation No. 155 contains seven high-level and 30 sub-level descriptions of vulnerabilities and threats that include 69 attack vectors directly affecting vehicle cybersecurity. These attack vectors include threats against back-end servers, vehicle communication channels, external connectivity and connections, and software update procedures. Car manufacturers, suppliers, government organizations (at both the local and federal levels), third-party service providers, and all other stakeholders' cooperation and efforts are necessary for the successful implementation of the regulation.

One of the first courses of action for stakeholders with regard to this regulation will be to sort these attack vectors according to their expected threat severity levels. This paper does that by using the industry standard DREAD threat model. We calculated the severity levels of the attack vectors listed in UN Regulation No. 155. We also studied the connected car ecosystem as it exists today, and predicted how the ecosystem will evolve with the global rollout of high-speed 5G networks. Applying these predictions, we recalculated the DREAD threat model to show how threat severity will shift in the next five to 10 years. Finally, we highlighted focus areas and cyberattack vectors that we deemed missing from the WP.29 document, but which will also require protection against future cyberattacks.

The Connected Car Ecosystem

As rapid scientific and technological innovations shape our world, autonomous vehicles are expected to be on the road as everyday transportation within the next decade or two. Semi-autonomous vehicles that communicate with cloud services, other vehicles, and road infrastructure to improve vehicle safety, assist with driving decisions, and provide access to cloud services will also become commonplace. As 5G networks rollout globally, connected cars will heavily utilize the low-latency, high-bandwidth, and network slicing features of 5G. The 5G network backbone, together with advances in Artificial Intelligence (AI) and Machine Learning (ML) applications that process both onboard and in-cloud data, will bring fully autonomous vehicles one step closer to reality. With all of this to look forward to in the near future, it is important to first define what connected cars are.



Powertrain	Communications	Body control	Power management	Chassis	Safety
Engine control unit	Head unit	Door locks	Hybrid powertrain	Adaptive suspension	Camera system
Traction control	Mobile connection	Climate control	Battery management	Electronic stability control	Radar/Lidar
Power steering	Telematics	Power window	Energy recovery	Active steering	Airbags
ACC, etc.	GPS, etc.	Sunroof, etc.	Actuators, etc.	Active body control, etc.	Tire pressure monitoring system, etc.

Figure 1. Technologies and functionalities that form the internal network of a connected car

Today's cars already come with an incredible amount of connected technologies. New car models typically run more than 100 million lines of code. Even the most basic cars have at least 30 Electronic Control Units (ECU), while luxury vehicles can have more than 100 ECUs connected across a labyrinth of different digital buses, such as Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), and Ethernet, each operating at different speeds, carrying different types of data, and enabling connections across different parts of the car.[6]

The modern car already receives satellite data for playing radio stations and getting GPS coordinates. In the future, cars will have cellular-satellite connectivity for data, which is especially useful when driving through regions with poor cellular coverage. Most new car models have a built-in eSIM, which is used to transmit telematics data, communicate with back-end cloud servers, create Wi-Fi hotspots, get real-time traffic information, transmit location for E911, and other functions. With the introduction of Apple CarPlay and Android Auto, mobile phone connectivity in cars has transformed from making phone calls and having address book access to a full-on system that gives users access to applications, maps, music, calls, messaging, etc. Radio Data System (RDS) is used to embed small amounts of data in FM broadcasts. Using RDS-TMC (Traffic Messaging Channel), cars can also receive real-time traffic alerts, which are displayed in the head unit (the car's infotainment hub). In-car Bluetooth and Wi-Fi connectivity are already common — drivers' mobile phones connect via Bluetooth to the head unit for playing music, making hands-free phone calls, share the phone's address book, etc. Cars like Tesla can connect to the home Wi-Fi to download over-the-air (OTA) software updates.[7] Vehicle-to-everything (V2X) communications includes vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-network, vehicle-to-pedestrian, vehicle-to-device, and vehicle-to-grid communications. In the future, autonomous vehicles will rely heavily on V2X to safely navigate the roads.

Figure 2 shows what we envision a cloud-connected vehicular architecture to look like. The head unit supports running applications. A software middleware layer abstracts the electrical and electronics (E/E) architecture of the car and makes it easier for developers to build architecture-agnostic car-based apps. The middleware programmatically speaks with the gateway ECU and provides application programming interface (API) access to apps that need to send messages to the individual ECUs. The bus switch will route the frames to the target ECUs. The apps talk to the OEM cloud (car manufacturer cloud) or third-party cloud services (e.g., Netflix) via a tethered cellular connection from the mobile phone or using the built-in eSIM. Depending on the E/E architecture of the car, the gateway ECU can also communicate directly with cloud services. As cars become smarter and better connected, we will see car-specific apps being developed and T1, T2, and OEM versions of apps will emerge. OEM apps will probably not need middleware to access the gateway ECU, or might even be able to communicate with the bus switch directly.

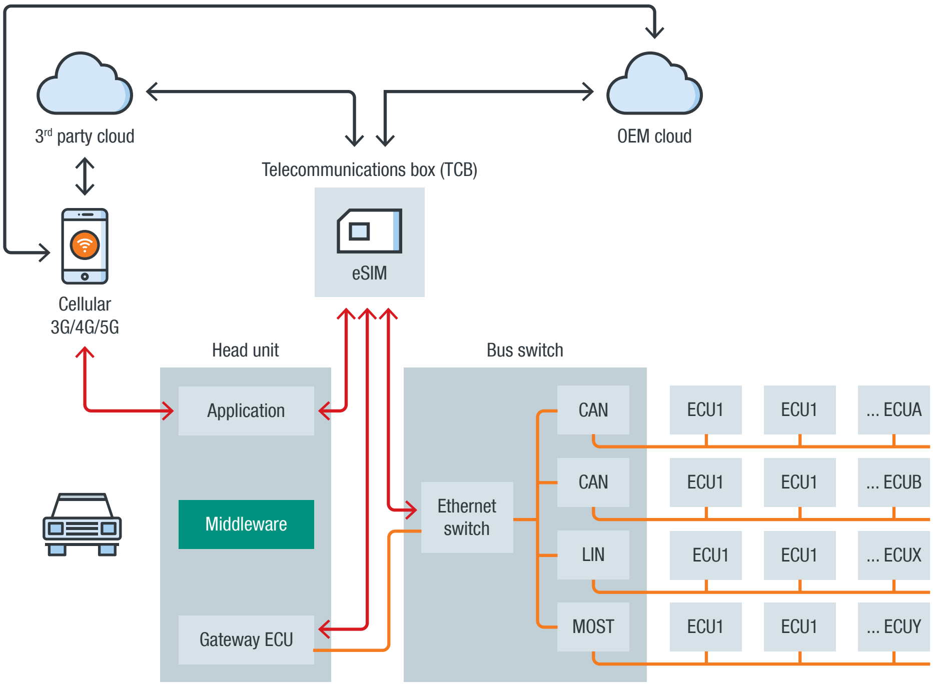


Figure 2. The cloud-connected ecosystem of a connected car

The advent of 5G standalone (SA), which no longer relies on existing LTE infrastructure, will play a big part in the connected car ecosystem. Thus, it is realistic to expect the E/E architecture to evolve and take advantage of next-generation 5G networks. Key 5G technologies that will be important to connected cars include software-defined networking (SDN); Network slicing to separate applications and quality of service (QoS); beamforming for fast communications; 5G machine learning (ML) and artificial intelligence (AI) applications; multi-user multiple input multiple output; high availability (99.999%) and low latency (1 millisecond); support for a high density of connected devices and ultra-high speeds; and low-power consumption.

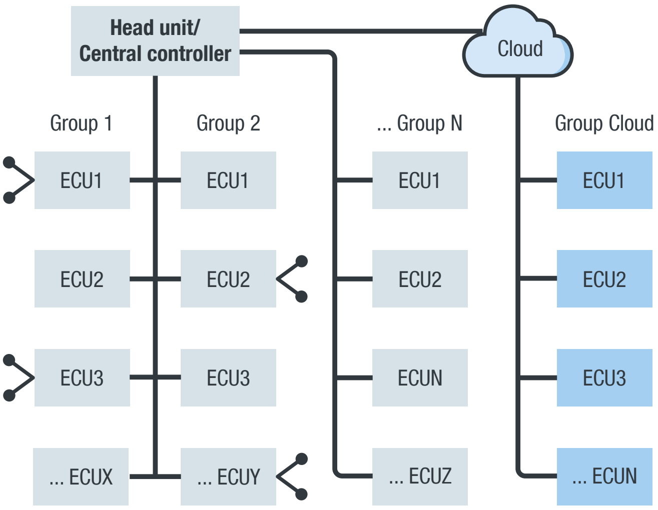


Figure 3. Cloud-based car E/E architecture

Connected cars will need very low latency vs. big bandwidth fast data rates. Network slicing and SDN can help separate the high data rate applications in the car from the ultra-low latency applications. This means that in the future, OEMs will be able to move certain ECU functions of the car to the cloud. Moving ECUs to the cloud has advantages, such as having a simplified E/E architecture with fewer ECUs to manage inside the car and massively expanded processing power using cloud computing. It could also allow expanded road situational awareness beyond that of local limits of around a 500-meter radius; the ability to flexibly add new and innovative applications using incremental OTA updates; improve fuel, battery, and emissions efficiency; expand and flexibly control road load capacity from an intelligent transportation system's (ITS) point-of-view; easy integration with third-party service providers such as revenue-generating services like Uber, which operates the car in autonomous mode; and access to distributed cloud servers plus a full-coverage low-latency network, which means attackable surfaces are more resistant to malicious attacks — it will be extremely difficult for attackers to compromise the distributed backend servers and knock offline all the 5G network nodes surrounding the vehicles.

Threat Modeling the Connected Car Ecosystem

Threat modeling is a useful and established technique software developers use to assess the security risks in their code. Other than software, threat modeling can also be applied to systems, and therefore can also be used to assess the security of industrial control systems (ICS). Threat modeling is a systematic way of classifying, identifying, and quantifying the risk presented by each threat that is being evaluated.[8] In this section, we analyze the 69 attack vectors listed in Annex 5, Table A1 of the UN Regulation No. 155 document[9] using the industry standard DREAD threat model.

Methodology: The DREAD Threat Model

Threat modeling allows us to apply a structured approach to security and address first the top threats that can have the greatest potential impact on the application.[10] One type of threat modeling is qualitative risk analysis, which is opinion based; this means it uses rating values to evaluate the risk level. The DREAD threat model can be used to perform qualitative risk analysis.[11] Using the DREAD threat model, we arrived at the risk rating for the given threats by answering the following questions:

- **D**amage potential: How great is the damage to the assets?
- **R**eproducibility: How easy is it to reproduce the attack?
- **E**xploitability: How easy is it to launch an attack?
- **A**ffected users: As a rough percentage, how many users are affected?
- **D**iscoverability: How easy is it to find an exploitable weakness?

We use the following risk rating table shown in Table 1 for our risk analysis:

	High (3)	Medium (2)	Low (1)
D	The attacker subverts the system and can inflict serious damage.	The attacker subverts the system and can inflict moderate damage.	The attacker subverts the system and can inflict minor damage
R	The attack can be reproduced every time.	The attack can be reproduced, but only within set limitations.	The attack is very difficult to reproduce, even with full knowledge of the security hole.
E	The attack requires little or no knowledge of the system in order to exploit it.	The attack requires a skilled operator with fundamental knowledge of the system in order to exploit it.	The attack requires an extremely skilled operator with in-depth knowledge of the system in order to exploit it.
A	Majority of the everyday users will be affected by the attack.	A good portion of everyday users will be affected by the attack.	A very small percentage of everyday users will be affected by the attack.
D	Published information readily explains the attack. Vulnerabilities are found in the most commonly used applications & systems.	Vulnerabilities are not common and only found in certain applications & systems. It requires skills to discover exploitable weaknesses.	Extremely difficult to discover vulnerabilities, and they are very difficult to weaponize. Extremely difficult to attack the applications & systems.

Table 1. The DREAD threat model

After answering the DREAD questions for a given threat, the risk rating is calculated by adding the rating values. The overall risk is rated as:

- **High** if the score is between 12 and 15
- **Medium** if the score is between 8 and 11
- **Low** if the score is between 5 and 7

Annex 5, Table A1 of the UN Regulation No. 155 document lists 69 attack vectors directly affecting vehicle cybersecurity.[12] We analyzed these 69 attack vectors and threat modeled them using DREAD so stakeholders (OEMs, suppliers, government and regulatory organizations, and third-party service providers, etc.) can determine the order in which to prioritize threats. We assigned scores for realistic extreme scenarios to the attack vectors and calculated their risk ratings.

Note that we maintained the same section numbers used in the UN Regulation No. 155 or ECE/TRANS/WP.29/2020/79 document regardless of the sequence. The numbering follows the sequence in the UN Regulation No. 155 document.

Threats Regarding Back-End Servers Related to Vehicles in the Field

Top-level threat	Threat Example	D	R	E	A	D	Rating
1. Back-end servers used as a means to attack a vehicle or extract data	1.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	1.2 Unauthorized internet access to the server	3	2	2	2	2	Medium
	1.3 Unauthorized physical access to the server	3	3	2	2	2	High
2. Services from back-end server being disrupted, affecting the operation of a vehicle	2.1 Attack on back-end server stops it functioning	3	2	2	2	2	Medium
3. Vehicle related data held on back-end server being lost or compromised (data breach)	3.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	3.2 Loss of information in the cloud	3	2	2	2	2	Medium
	3.3 Unauthorized internet access to the server	3	2	2	2	2	Medium
	3.4 Unauthorized physical access to the server	3	3	2	2	2	High
	3.5 Information breach by unintended sharing of data	3	1	2	2	3	Medium

Table 2. Threat rating for threats in back-end servers related to vehicles in the field

These are our observations from the threat modeling we had done on the section describing "Threats regarding back-end servers related to vehicles in the field," Section 4.3.1 in Table A1:

- When attackers have privileged access or actual physical access to the back-end servers, it would be extremely difficult to defend these systems — essentially a checkmate for defenses.
- Not all servers will be vulnerable, because of varying levels of system patching. It is also rare (but not improbable) for sensitive backend servers to be exposed and discoverable online.
- Even if there is data loss in the cloud, exploiting the data supply can be tricky. Damage potential, therefore, depends on the data stolen and its likelihood of misuse.
- Even if a backend server is compromised, a total fleet-wide cyberattack would be highly unlikely, but again, not impossible.

Threats to Vehicles Regarding Their Communication Channels

Top-level threat	Threat Example	D	R	E	A	D	Rating
4. Spoofing of messages or data received by the vehicle	4.1 Spoofing of messages by impersonation (e.g. 802.11p V2X or GNSS messages)	3	1	1	1	1	Low
	4.2 Sybil attack (vehicle pretends to have more than one identity)	3	2	1	1	1	Medium
5. Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1 Communications channels permit code injection (e.g. tampered software binary injected in the communication stream)	3	1	1	1	1	Low
	5.2 Communications channels permit the manipulation of vehicle held data/code	3	1	1	1	1	Low
	5.3 Communications channels permit overwrite of vehicle held data/code	3	1	1	1	1	Low
	5.4 Communications channels permit erasure of vehicle held data/code	3	1	1	1	1	Low
	5.5 Communications channels permit introduction of data/code to the vehicle	3	1	1	1	1	Low
6. Communication channels permit untrusted/ unreliable messages to be accepted or are	6.1 Accepting information from an unreliable or untrusted source	3	1	1	2	2	Medium
	6.2 Man in the middle attack/ session hijacking	3	1	1	1	2	Medium
	6.3 Replay attack (to downgrade ECU firmware or gateway firmware inside the car)	3	1	1	1	1	Low
7. Information can be readily disclosed	7.1 Interception of information/ interfering radiations/monitoring communications	1	2	2	1	2	Medium
	7.2 Gaining unauthorized access to files or data	1	2	2	2	2	Medium
8. Denial of Service attacks via communication channels to disrupt vehicle functions	8.1 Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	3	2	2	3	2	High
	8.2 Black hole attack (block messages between vehicles to disrupt communications)	2	2	1	1	1	Low

Top-level threat	Threat Example	D	R	E	A	D	Rating
9. An unprivileged user is able to gain privileged access to vehicle systems	9.1 An unprivileged user is able to gain privileged access, for example root access	3	1	1	1	1	Low
10. Viruses embedded in communication media are able to infect vehicle systems	10.1 Virus embedded in communication media infects vehicle systems	3	1	1	1	1	Low
11. Messages received by the vehicle) or transmitted within it, contain malicious content	11.1 Malicious internal (e.g. CAN) messages transmitted on car bus	3	1	1	1	1	Low
	11.2 Malicious V2X messages (e.g. I2V or V2V messages)	3	2	2	1	2	Medium
	11.3 Malicious diagnostic messages	3	1	1	1	1	Low
	11.4 Malicious proprietary messages (e.g. those sent from OEM or T1/T2 suppliers)	3	2	2	2	2	Medium

Table 3. Threat rating for threats regarding communication channels

These are our observations from the threat modeling section “Threats to vehicles regarding their communication channels,” listed in Table A1, Section 4.3.2:

- Sybil attacks (wherein a vehicle pretends to have more than one identity so that other vehicles in the network would be unable to verify if the received data originates from one or multiple vehicles) on the road have a limited threat radius.

- Spoofing of messages by impersonation (e.g. 802.11P, V2X, or GNSS messages) will need to be a highly targeted attack to succeed.

- Highly skilled hackers are needed to attack communication channels and it is very difficult to attack fleets. Published case studies on remote attacks against Jeep, Tesla, and Mercedes demonstrated that this is a difficult attack to achieve.[13]

- Hacked or compromised Wi-Fi routers or femtocells can be used for Man-in-the-Middle (MiTM) attacks.

- Intercepting information, interfering with radiations, monitoring communications, and gaining unauthorized access to files or data are all typically passive attacks that don’t affect road safety.

- Denial of service (DoS) or distributed denial of service (DDoS) attacks can cause widespread uncontrolled damage in the connected car ecosystem.

- Blackhole attacks, which block messages between vehicles to disrupt communications, become especially disruptive in L5 autonomous vehicles where drivers are not in control.

- Malware attacks (using viruses, worms, bots, etc.) will need middleware that interfaces with vehicle systems to become a real threat. Malware attacks would be very difficult to execute without middleware.[14]

- Compromised ITS infrastructure can be leveraged for spreading malicious infrastructure-to-Vehicle (I2V) or V2X messages; it's basically a data supply chain attack against the ecosystem. This can be critical, since the data supply chain essentially equates to the data lifecycle which involves the generation and procurement of data for an organization.[15]

Threats to Vehicles Regarding Their Update Procedures

Top-level threat	Threat Example	D	R	E	A	D	Rating
12. Misuse or compromise of update procedures	12.1 Compromise of over the air software update procedures	3	2	2	3	1	Medium
	12.2 Compromise of local/ physical software update procedures	3	3	2	2	2	High
	12.3 The software is manipulated before the update process (and is therefore corrupted), although the update process is intact	3	2	2	3	1	Medium
	12.4 Compromise cryptographic keys of software provider to do invalid update	3	2	2	3	1	Medium
13. It is possible to deny legitimate updates	13.1 Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	1	2	3	3	3	High

Table 4. Threat rating for threats regarding vehicle update procedures

These are our observations from the threat modeling section "Threats to vehicles regarding their update procedures," Section 4.3.3 in Table A1:

- Compromising the OTA software update procedure is a data supply chain attack.

- Compromising the local and/or physical software update procedure could be the work of a rogue dealership/garage, or an insider working at the dealership/garage.

- Fortunately, not much harm would be done if vehicles cannot be updated. Typically, the new firmware will not be loaded into memory and have its update process started, until the full download is completed and the hash value is calculated and confirmed.

Threats to Vehicles Regarding Unintended Human Actions Facilitating a Cyberattack

Top-level threat	Threat Example	D	R	E	A	D	Rating
15. Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1 Innocent victims being tricked into taking an action to unintentionally load malware or enable an attack	2	2	1	1	1	Low
	15.2 Defined security procedures are not followed	3	2	2	1	1	Medium

Table 5. Threat rating for threats regarding unintended human actions

These are our observations from the threat modeling section “Threats to vehicles regarding unintended human actions facilitating a cyberattack,” Section 4.3.4 in Table A1:

- Innocent victims getting tricked into unintentionally loading malware is a classic phishing attack. Compromising the head unit is easier than overwriting firmware or installing malware.
- Any negligence in following the correct manufacturer-defined security procedures for operations or vehicle servicing can lead to exploitation and the vehicle getting compromised.

Threats to Vehicles Regarding Their External Connectivity and Connections

Top-level threat	Threat Example	D	R	E	A	D	Rating
16. Manipulation of the connectivity of vehicle functions enables a cyber-attack	16.1 Manipulation of functions designed to remotely operate systems, such as remote key, immobilizer, and charging pile	3	2	3	2	3	High
	16.2 Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	2	2	2	1	2	Medium
	16.3 Interference with short range wireless systems or sensors	2	3	3	1	3	High
17. Manipulation of the connectivity of vehicle functions enables a cyber-attack	17.1 Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	3	2	1	2	1	Medium

Top-level threat	Threat Example	D	R	E	A	D	Rating
18. Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1 External interfaces such as USB or other ports used as a point of attack	3	2	1	1	2	Medium
	18.2 Media infected with a virus connected to a vehicle system	3	1	1	1	1	Low
	18.3 Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	3	2	1	1	2	Medium

Table 6. Threat rating for threats regarding vehicle external connectivity and connections

Our observations from the threat modeling section “Threats to vehicles regarding their external connectivity and connections,” Section 4.3.5 in Table A1:

- Car thieves are already doing signal capture-relay-replay attacks against wireless car key fobs.
- Electronic jamming of radio frequency (RF) is an easily executed, low-skill attack vector.
- To attack the USB and OBD ports, attackers will need physical access to the vehicle interior.
- Manipulating vehicle telematics is a bigger problem for commercial vehicles versus passenger cars, especially if the forged telematics can be used to hijack a commercial vehicle and steal goods or change the temperature settings and spoil any fresh goods being transported

Threats to Vehicle Data/Code

Top-level threat	Threat Example	D	R	E	A	D	Rating
19. Extraction of vehicle data/ code	19.1 Extraction of copyright or proprietary software from vehicle system	3	1	1	2	1	Medium
	19.2 Unauthorized access of the owner’s privacy information such as personal identity, payment information, address book, location, vehicle electronic ID, etc.	3	1	2	1	2	Medium
	19.3 Extraction of cryptographic keys	3	1	1	2	1	Medium

Top-level threat	Threat Example	D	R	E	A	D	Rating
20. Manipulation of vehicle data/code	20.1 Illegal/unauthorized changes to vehicle's electronic ID	2	2	2	2	2	Medium
	20.2 Identity fraud	2	2	2	2	2	Medium
	20.3 Action to circumvent monitoring systems (e.g. hacking/ tampering/blocking of messages such as ODR Tracker data, or number of runs)	2	1	1	1	1	Low
	20.4 Data manipulation to falsify vehicle's driving data	2	2	2	2	2	Medium
	20.5 Unauthorized changes to system diagnostic data	2	1	1	1	1	Low
21. Erasure of data/code	21.1 Unauthorized deletion/ manipulation of system even logs	2	2	3	2	3	High
22. Introduction of malware	22.1 Introduce malicious software or malicious software activity	3	2	3	3	3	High
23. Introduction of new software or overwrite existing software	23.1 Fabrication of software of the vehicle control system or information system	3	2	2	3	2	High
24. Disruption of systems or operations	24.1 Denial of service, e.g. flooding internal network with CAN messages, or by provoking faults on an ECU via a high rate of messaging	3	1	1	1	1	Low
25. Manipulation of vehicle parameters	25.1 Unauthorized access of falsify the configuration parameters of vehicle's key functions such as brake data, airbag deployed threshold, etc.	3	3	2	1	3	High
	25.2 Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.	3	3	2	1	3	High

Table 7. Threat rating for threats related to the vehicle data/code.

Our observations from the threat modeling section “Threats to vehicles data/code,” Section 4.3.6 in Table A1:

- Past case studies of hacking Jeep, Tesla, and Mercedes have demonstrated that the extraction of firmware from the vehicle is extremely difficult and requires a highly skilled operator.
- The most likely way of stealing Personally Identifiable Information (PII) is to either compromise the vehicle's head unit OS using a chain of exploits or compromise the OEM/third-party cloud services.

- The extraction of cryptographic keys requires reverse-engineering the extracted ECU firmware.
- Manipulating vehicle data/code needs a reliable attack method, which would most likely involve cloud services.
- Many of the attacks, like erasing data/code, introducing new software, or overwriting software, is more effective as a server-side attack i.e., doing a fleetwide attack versus attacking individual vehicles
- Manipulating vehicle parameters can have serious consequences for vehicle safety and can most likely be achieved using commercial OBD-II tools

Potential Vulnerabilities That Could Be Exploited if Not Sufficiently Protected or Hardened

Top-level threat	Threat Example	D	R	E	A	D	Rating
26. Cryptographic technologies can be compromised or are insufficiently applied	26.1 Combination of short encryption keys and long period of validity enables attacker to break encryption	3	2	1	1	1	Medium
	26.2 Insufficient use of cryptographic algorithms to protect sensitive systems	3	2	1	1	1	Medium
	26.3 Using already or soon to be deprecated cryptographic algorithms	3	2	1	1	1	Medium
27. Part or supplies could be compromised to permit vehicles to be attacked	27.1 Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack	3	3	2	1	2	Medium
28. Software or hardware development permits vulnerabilities	28.1 Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities.	3	2	2	1	2	Medium
	28.2 Using remainders from development can permit access to ECUs or permit attackers to gain higher privilege	3	3	2	2	2	High
29. Network design introduces vulnerabilities	29.1 Superfluous internet ports left open, providing access to network systems	3	2	1	3	1	Medium
	29.2 Circumvent network separation to gain control	3	2	2	1	1	Medium

Top-level threat	Threat Example	D	R	E	A	D	Rating
31. Unintended transfer of data can occur	31.1 Information breach. Personal data may be leaked when the car changes user	2	2	2	1	3	Medium
32. Physical manipulation of systems can enable an attack	32.1 Manipulation of electronic hardware	3	2	3	1	2	Medium
	32.1 Replacement of authorized electronic hardware	3	2	3	1	2	Medium
	32.1 Manipulation of the information collected by a sensor	3	2	3	1	2	Medium

Table 8. Threat rating for potential vulnerabilities that could be exploited if not sufficiently protected

Our observations from the threat modeling section Potential vulnerabilities that could be exploited if not sufficiently protected or hardened (Table A1 Section 4.3.7):

- Compromised cryptographic keys are a significant threat when they can be used to load malicious firmware into compromised ECUs.
- After-market tuning tools are pretty common, especially rigs for ECU flashing for unlocking features.
- Not changing the admin password would be gross security negligence on the part of the OEMs.
- Cars will need a data reset option to protect the owner's data similar to mobile phones. This is especially useful when transferring vehicle ownership or if the vehicle gets stolen.
- Multiple case studies published over the years against brands like Jeep, Tesla, Mercedes, Lexus, etc., discuss using exploit chains to compromise the head unit. This is different from compromising the vehicle ECUs and is typically the preceding step to compromising the ECUs.

Evolution of Threats Against Connected Cars

The DREAD threat modeling exercise was done by applying current technologies; hacker tools, techniques, and procedures (TTPs); and learnings from published research in the car hacking domain. The goal of our threat modeling exercise was to help stakeholders prioritize which attack scenarios to address first and develop protective countermeasures for. In the next decade, especially with the global rollout of 5G networks, the available technology stack and hacker TTPs are going to significantly change, thus threat profiles will also change. To visualize this, we made predictions about the evolution of the connected car ecosystem and then studied how the DREAD threat modeling changes. Based on past studies,[16] we predict the following will happen in the next decade:

1. V2X communications will become mainstream and will be used by L3 to L5 autonomous vehicles.
2. The data supply chain will become a critical component in the operations and safety of connected cars and will be powered by fast and reliable networks.
3. The numbers of L3 and L4 autonomous vehicles on the road will dramatically increase. We also expect to see L5 vehicles on the road within a decade.
4. With reliable 5G networks, some ECU functions from the vehicle's E/E systems will be migrated to the cloud for efficiency and simplification of the onboard E/E architecture.
5. The head unit will support a large third-party app ecosystem (similar to mobile phones), and will provide middleware access to the vehicle's E/E systems.
6. Middleware access for apps to the vehicle's E/E systems will enable connected cars to offer innovative add-on features such as autonomous ride-sharing and coordinated grocery pickups.
7. ML and AI applications hosted in cloud servers will be used extensively for traffic shaping and roadway capacity predictions.
8. Using the growing library of third-party apps, the connected car will become fully integrated with users' digital lives such as banking, office applications, and entertainment.
9. As the "all-digital, feature-rich" connected car becomes a reality, criminals will invent innovative ways to monetize the connected car's physical and digital resources

Given these broad evolutions in the connected car space, we attempted to predict how the DREAD threat modeling that we did will change. We need to keep in mind that the available TTPs will also evolve. Hacking techniques that, at present, require highly skilled hackers (with in-depth specialized knowledge), may be achieved using simple plug-and-play dongles purchased from a dark web marketplace or even done wirelessly over the internet.

The goal for the updated threat modeling is to discover shifts in the threat profile and help stakeholders develop long-term plans for addressing these threats. The risk evaluation process we followed is listed here:

- We went over all the threat vectors listed in UN Regulation No. 155 to determine which ones will be affected by our nine predictions.
- Threat vectors like 15.2 (Defined security procedures are not followed), 27.1 (Hardware or software engineered to enable an attack fails to meet design criteria to stop an attack), and 32.1 (Manipulation/replacement of hardware/information) are deliberately ambiguous, meaning the nature of the threat does not fundamentally evolve when we apply our predictions. We have thus excluded these threats from our follow-up threat modeling.
- We focused mainly on the Low and Medium threats, and attempted to determine if the risk rating will change or remains static, and explain why.
- We applied the DREAD modeling to our selected threat vectors to determine their new risk ratings.
- Threat vectors that already scored High in our risk assessment were skipped over as we didn't expect the risk rating to decrease.
- Attack vectors 1.1 to 1.3, 2.1, and 3.1 to 3.5 were skipped over because the nine predictions we made on the evolution of the connected cars do not directly affect those attack vectors.

Threat Examples	D	R	E	A	D	New	Old	Notes
4.1 Spoofing of messages by impersonation (e.g. 802.11p V2X or GNSS messages)	3	2	2	2	2	Medium	Low	Custom hardware sold in deepweb markets used in attacks. Attacking V2X protocol
4.2 Sybil attack (vehicle pretends to have more than one identity)	3	2	2	2	2	Medium	Medium	Custom hardware sold in deepweb markets used in attacks. Attacking V2X protocol
5.1 Communications channels permit code injection (e.g. tampered software binary injected in the communication stream)	3	2	2	2	1	Medium	Low	Criminals use sold-as-ready kit/service to execute these attacks. Attacking bus protocols

Threat Examples	D	R	E	A	D	New	Old	Notes
5.2 Communications channels permit the manipulation of vehicle held data/code	3	2	2	2	1	Medium	Low	Criminals use sold-as-ready kit/service to execute these attacks. Attacking bus protocols
5.3 Communications channels permit overwrite of vehicle held data/code	3	2	2	2	1	Medium	Low	Criminals use sold-as-ready kit/service to execute these attacks. Attacking bus protocols
5.4 Communications channels permit erasure of vehicle held data/code	3	2	2	2	1	Medium	Low	Criminals use sold-as-ready kit/service to execute these attacks. Attacking bus protocols
5.5 Communications channels permit introduction of data/code to the vehicle	3	2	2	2	1	Medium	Low	Criminals use sold-as-ready kit/service to execute these attacks. Attacking bus protocols
6.1 Accepting information from an unreliable or untrusted source	3	2	3	2	2	High	Medium	This is easier to pull off with kits/service as they're not meddling with complex internals
6.2 Man in the middle attack/session hijacking	3	2	3	2	2	High	Medium	Can be done with routers or femtocells and a dedicated sold-as-ready kit/service
6.3 Replay attack (to downgrade ECU firmware or gateway firmware inside the car)	3	2	3	1	2	Medium	Low	Drawing parallel to replay attacks used to mimic fobs and unlock, start, and steal cars
7.1 Interception of information/interfering radiations/monitoring communications	1	2	2	2	2	Medium	Medium	This is a passive attack which doesn't affect road safety
7.2 Gaining unauthorized access to files or data	1	2	2	2	2	Medium	Medium	This is a passive attack which doesn't affect road safety
8.2 Black hole attack (block messages between vehicles to disrupt communications)	3	2	3	2	2	High	Low	Attack become disruptive with more L3-L5 vehicles on the road and mass V2X adoption
9.1 An unprivileged user is able to gain privileged access, for example root access	3	2	3	2	2	High	Low	Middleware will make it easy to access car's E/E systems as well get root privileges
10.1 Virus embedded in communication media infects vehicle systems	3	2	3	2	2	High	Low	Middleware exploits will make virus infection easy and give access to E/E systems
11.1 Malicious internal (e.g. CAN) messages transmitted on car bus	3	2	3	2	2	High	Low	Virus infection via middleware exploit access E/E systems & injects malicious messages

Threat Examples	D	R	E	A	D	New	Old	Notes
11.2 Malicious V2X messages (e.g. I2V or V2V messages)	3	2	3	2	2	High	Medium	Uses sold-as-ready kit/service to execute these attacks. Transmits fake V2X messages
11.3 Malicious diagnostic messages	3	2	3	2	2	High	Low	Virus infection via middleware exploit access E/E systems & injects malicious messages
11.4 Malicious proprietary messages (e.g. those sent from OEM or T1/T2 suppliers)	3	2	3	2	2	High	Medium	Uses sold-as-ready kit/service to execute these attacks. Transmits fake V2X messages
12.1 Compromise of over the air software update procedures	3	2	2	2	2	Medium	Medium	Depending on the OTA update source (3rd party or OEM or T1) the risks fluctuate
12.3 The software is manipulated before the update process (and is therefore corrupted), although the update process is intact	3	2	2	3	1	Medium	Medium	Hacking the data supply chain is a difficult task. This attack would assume a major OEM or T1 supplier got compromised, in which case the entire connected car fleet is at risk
12.4 Compromise cryptographic keys of software provider to do invalid update	3	2	2	3	1	Medium	Medium	Hacking the data supply chain is a difficult task
15.1 Innocent victims (e.g. owner, operator, or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack	3	2	3	2	2	High	Low	Phishing attacks that exploit head unit middleware to access the E/E systems will be extremely dangerous
16.2 Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	2	2	2	1	2	Medium	Medium	This attack is more dangerous for commercial vehicles than passenger cars, and the risk remains unchanged because telematics won't change vehicle safety
17.1 Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	3	2	3	2	3	High	Medium	Corrupted applications or unsecure applications used to exploit head unit middleware and get access the vehicle's E/E system
18.1 External interfaces such as USB or other ports used as a point of attack	3	2	3	1	2	Medium	Medium	Attackers need physical access to the ports inside the car to attack successfully

Threat Examples	D	R	E	A	D	New	Old	Notes
18.2 Media infected with a virus connected to a vehicle system	3	2	3	1	2	Medium	Low	Attackers need physical access to the inside of the car to attack successfully
18.3 Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	3	2	3	1	2	Medium	Medium	Attackers need physical access to the inside of the car to attack successfully
19.1 Extraction of copyright or proprietary software from vehicle system	3	1	1	2	1	Medium	Medium	Extracting the firmware is still possibly difficult, but unnecessary if there is middleware
19.2 Unauthorized access of the owner's privacy information such as personal identity, payment information, address book, location, vehicle electronic ID, etc.	2	2	2	2	2	Medium	Medium	Exploiting the middleware in the head unit will make this a fairly easy attack to execute, the other way would be to compromise OEM or T1/T2 cloud services
19.3 Extraction of cryptographic keys	3	1	1	2	1	Medium	Medium	This requires reverse engineering the extracted ECU's firmware or middleware stack
20.1 Illegal/unauthorized changes to vehicle's electronic ID	3	2	2	2	2	High	Medium	Attacks will facilitate serious crimes being committed using hacked autonomous vehicles
20.2 Identity fraud	2	2	2	2	2	Medium	Medium	Stealing a vehicle's identity and using it to access paid services
20.3 Action to circumvent monitoring systems (e.g. hacking/tampering/ blocking of messages such as ODR Tracker data, or number of runs)	2	2	2	1	2	Medium	Low	Need to access the ECU via the head unit middleware to execute this type of attacks. This attack targets manipulating data and doesn't really increase road risks
20.4 Data manipulation to falsify vehicle's driving data	2	2	2	1	2	Medium	Medium	Need to access the ECU via the head unit middleware to execute this type of attacks.
20.5 Unauthorized changes to system diagnostic data	2	2	2	1	2	Medium	Low	Need to access the ECU via the head unit middleware to execute this type of attacks.
24.1 Denial of service, e.g. flooding internal network with CAN messages, or by provoking faults on an ECU via a high rate of messaging	3	2	3	2	2	High	Low	Exploiting vulnerabilities in the head unit's middleware stack to access the vehicle's E/E systems and flood data buses with malicious or useless messages

Threat Examples	D	R	E	A	D	New	Old	Notes
26.1 Combination of short encryption keys and long period of validity enables attacker to break encryption	3	2	2	2	1	Medium	Medium	This requires reverse engineering the extracted ECU's firmware or middleware stack. Extent of victim depends on how many car models have this flaw and OTA schedules
26.2 Insufficient use of cryptographic algorithms to protect sensitive systems	3	2	2	2	1	Medium	Medium	This requires reverse engineering the extracted ECU's firmware or middleware stack
26.3 Using already or soon to be deprecated cryptographic algorithms	3	2	2	2	1	Medium	Medium	This requires reverse engineering the extracted ECU's firmware or middleware stack
28.1 Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities.	3	2	2	3	2	High	Medium	Software bugs are the main cause of vulnerabilities. With increased use of software in smart cars, this increases the risk of complex chains of vulnerabilities being exploited
29.1 Superfluous internet ports left open, providing access to network systems	3	2	2	3	2	High	Medium	Third-party cloud services could be targeted as means to access the car's network
29.2 Circumvent network separation to gain control	3	2	2	1	2	Medium	Medium	Very narrow attacking scope. Easier to exploit vulnerability in middleware to subvert
31.1 Information breach. Personal data may be leaked when the car changes user	2	2	2	2	2	Medium	Medium	Second-hand cars will need a data reset option like mobile phones to prevent this

Table 9. Reevaluated risk ratings after applying our predictions on the evolution of connected cars

By applying our connected car evolution predictions to the WP.29 attack vectors and then evaluating them through threat modeling, we observed the following changes:

- Affected users increase as V2X and connected car technology usage become mainstream.
- The reproducibility of the attacks improves with new developments in off-the-shelf technology.
- The exploitability, or the minimum skills needed by an attacker, decreases. For example, car thieves can now easily perform signal capture-relay-replay attacks against wireless car key fobs using off-the-shelf technology purchased from dark web marketplaces. The signal replay attack has transformed from requiring expert level skills to anyone with basic technical know-how can now execute this.
- Discoverability of vulnerabilities and weaknesses becomes easier as many of the attacks have gone from theoretical to mainstream and then were weaponized and made available for purchase

Overall Summary

In a nutshell, immediate focus should be placed on backend and data security. While in the future, risk at the communication channel will dramatically increase. We see this happening because vehicles are bound to be better connected via APIs both internally and externally. That being said, our recommendations are to design security with an understanding of the backends, APIs, and prioritizing data security from the beginning.

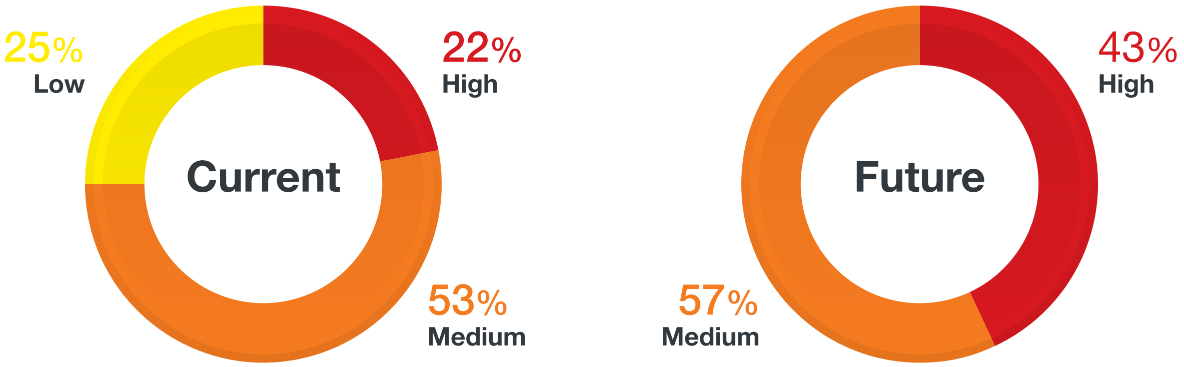


Figure 4. A comparison between current and future percentages of risks that fall under each of the three classification levels (low, medium, high).

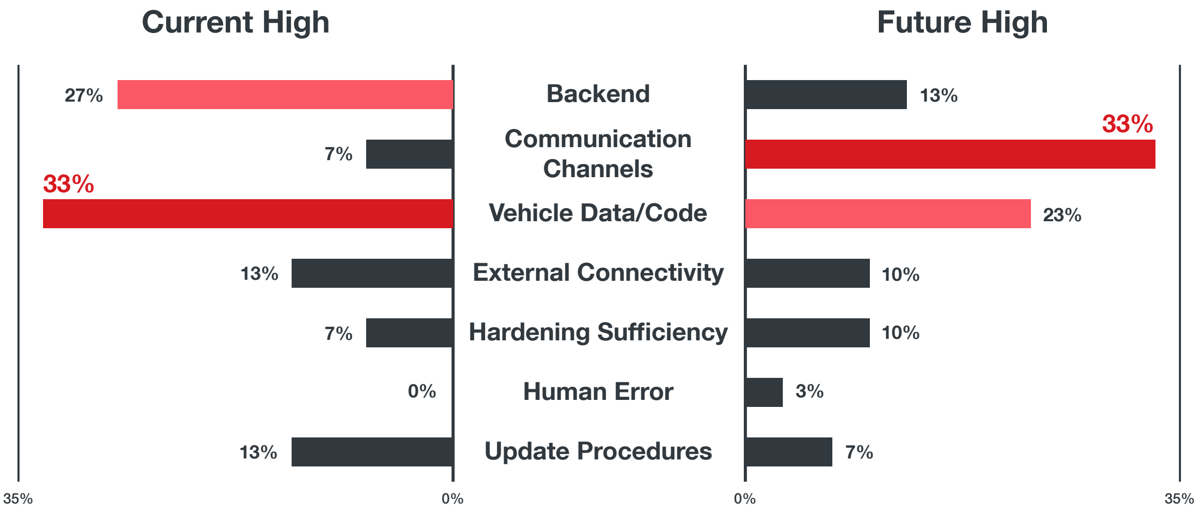


Figure 5. The current and predicted percentage of attack vectors turning into high risk threats in each subsection

The WP.29 UN-R155 document contains seven high-level and 30 sub-level descriptions of vulnerabilities and threats that include 69 attack vectors. In our opinion, the following are the top five attack vectors that need to be given the highest priority:

- Back-end servers used as a means to attack a vehicle or extract data, 1.1 to 1.3 of section 4.3.1.
- Denial of service attacks via communication channels to disrupt vehicle functions, 8.1 to 8.2 of section 4.3.2.
- Hosted third-party software, such as entertainment applications, used as a means to attack vehicle systems, 16.1 to 16.3 of section 4.3.5.
- The extraction of vehicle data/code, 19.1 to 19.3 of section 4.3.6.
- Software or hardware development, which permits vulnerabilities, 28.1 to 28.2 of section 4.3.7.

Additional Areas of Focus for Connected Car Security

We studied the list of attack vectors in the UN Regulation No. 155 document and cross-referenced them with the predictions we published in our research papers on intelligent transport systems (ITS)[17] and connected cars[18] to determine if there are additional attack vectors and/or focus areas that we can add or emphasize. It is important to note that the regulation primarily targets connected car safety and security, while our past researches explored the entire ITS ecosystem where connected cars are one piece of a bigger puzzle. In our past researches, we did cyberattack assessments that are outside the scope of the regulation, but still heavily influence the overall safety and security of connected cars. In a nutshell, there is more than one way of attacking connected cars — which is the ultimate goal for malicious hackers. We discuss here focus areas and attack vectors that stakeholders — OEMs, suppliers, government agencies, third-party service providers, and the general public should be aware of.

Attack Vehicle Image Processing

Onboard image processing to determine the vehicle position, current road conditions, speed limits, traffic signs, and other visual data is a critical application in both semi- and fully autonomous vehicles. Manufacturers like Tesla are only using the onboard camera network in their cars, versus using other obstacle discovery technologies such as LIDAR, to autonomously navigate the roads.[19, 20] On-board or cloud-based image processors crunch through vast quantities of visual data in milliseconds to make split-second driving decisions on the road. There are published researches that demonstrate how researchers were able to fool the vehicle's cameras into misinterpreting roadway signs by adding small anomalies or stickers to road signs.[21, 22]

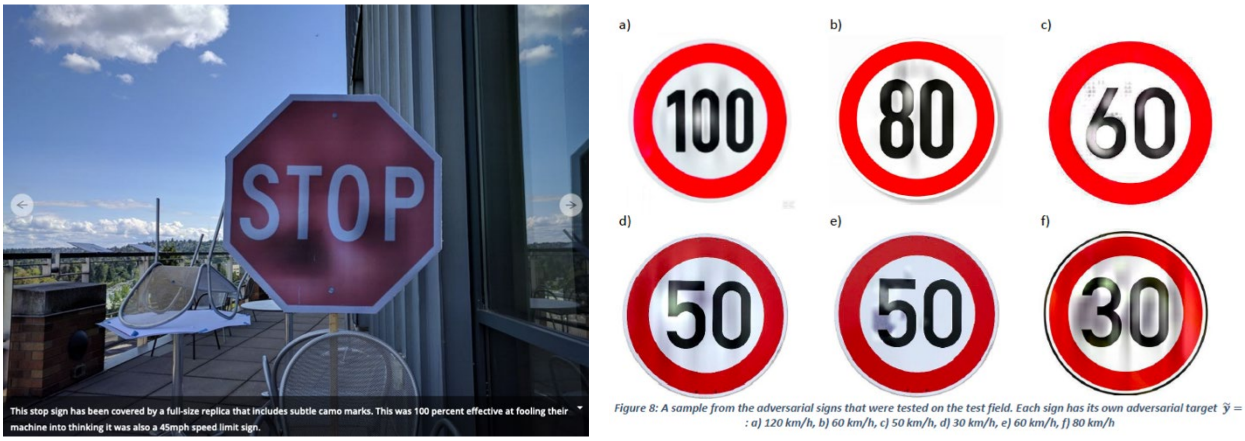

STOP
a)
100
b)
80
c)
60
d)
50
e)
50
f)
30
This stop sign has been covered by a full-size replica that includes subtle camo marks. This was 100 percent effective at fooling their machine into thinking it was also a 45mph speed limit sign.
Figure 8: A sample from the adversarial signs that were tested on the test field. Each sign has its own adversarial target $\tilde{y}$ = : a) 120 km/h, b) 60 km/h, c) 50 km/h, d) 30 km/h, e) 60 km/h, f) 80 km/h

Figure 6. Researchers successfully affecting the reading of roadway signs

Left image source: Hacking street signs with stickers could confuse self-driving cars from Ars Technica[23]

Right image source: Fooling a Real Car with Adversarial Traffic Signs by Nir Morgulis, Alexander Kreines, Shachar Mendelowitz, and Yuval Weisglass[24]

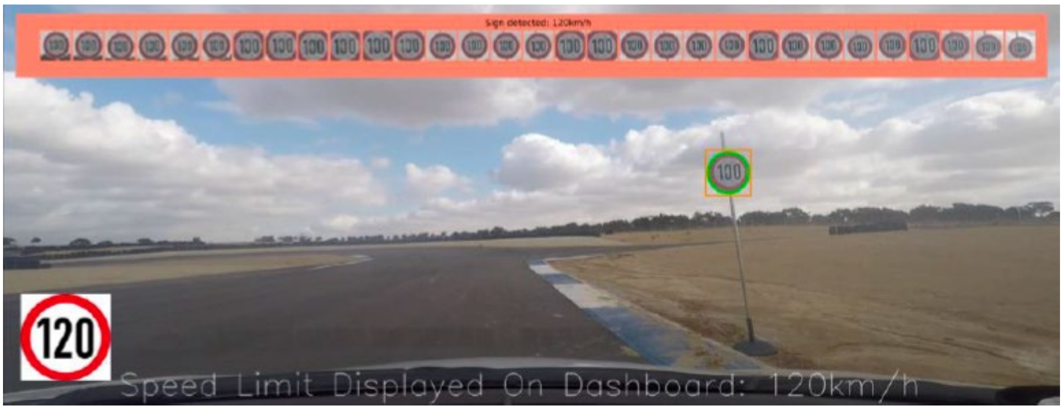


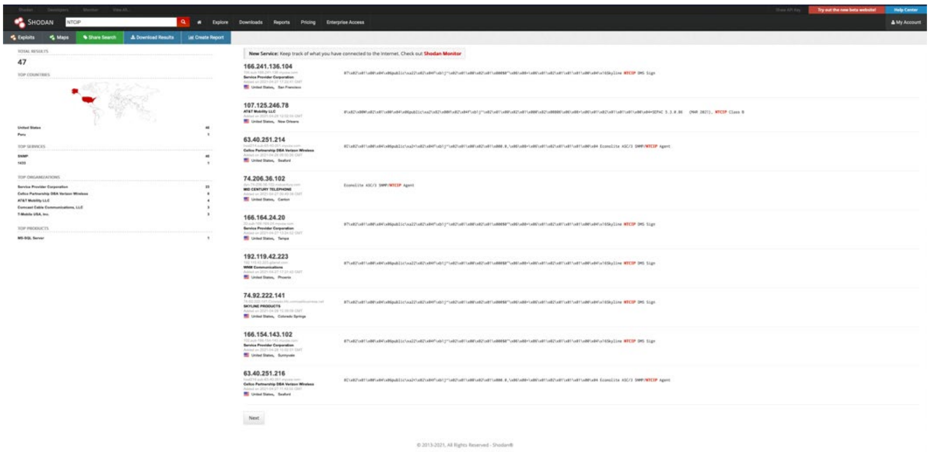
Figure 7. Researchers affecting the reading of road signs as seen from the dashboard

Image source: Fooling a Real Car with Adversarial Traffic Signs, by Nir Morgulis, Alexander Kreines, Shachar Mendelowitz, and Yuval Weisglass[25]

This is a very low-tech and easily executable attack against the vehicle's onboard image processing algorithms — and one that can have catastrophic consequences for road safety. Vehicle image processing algorithms will need a heuristic approach to interpreting road signs to avoid such visual attacks and/or a large onboard library of images to cross-reference against. But even those solutions have limitations as vehicles travel all over the country and internationally, and are met with unforeseen road conditions. A better approach would be to use cloud-based image processing. This solution would help when onboard processors fail to interpret road signs inside of a minimum confidence level. The cloud-based approach gives vehicles access to greater processing power as well as a massive library of images to cross-reference against. It is also not limited by the fixed processing hardware inside vehicles. Heavily cross-referenced images can be pushed OTA to all vehicles to bolster their onboard processing. However, this scenario assumes the existence of a nationwide low-latency high-speed 5G network. Therefore, until that becomes a reality, vehicles will be susceptible to image processing attacks.

Compromised Roadway Infrastructure Leveraged

Road-plying vehicles rely blindly on roadway infrastructure, such as traffic signals, messaging boards, pedestrian signals, dynamic road barriers to manage the traffic flow. Based on our many years of driving experience, we inherently trust that these road infrastructures will work correctly. Most roadway infrastructure today are network-connected to facilitate centralized management and control. This is achieved either via a direct network connection to central control or via cellular 3G/4G/LTE modems. Roadway operators occasionally mistakenly leave these devices exposed online, which are easily discoverable via internet scanning services such as Shodan.[26] We discovered roadway infrastructure that supports the National Transportation Communications for Intelligent Transportation System Protocol (NTCIP) and found exposed traffic signal controllers manufactured by Econolite (brand ASC/3). NTCIP-supported devices are a mixed bag consisting of traffic signals, dynamic message signs, environmental sensors, CCTV, vehicle count stations, freeway ramp meters, video switches, transportation sensor systems, field master stations for traffic signals, transit priority at traffic signals, and street lights.[27]



TOTAL RESULTS
47

TOP COUNTRIES

United States	46
Peru	1

TOP SERVICES

SNMP	46
1433	1

TOP ORGANIZATIONS

Service Provider Corporation	23
Cellco Partnership DBA Verizon Wireless	8
AT&T Mobility LLC	4
Comcast Cable Communications, LLC	3
T-Mobile USA, Inc.	3

TOP PRODUCTS

MS-SQL Server	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

166.241.136.104
Service Provider Corporation
United States, San Francisco
... Skyline NTCIP DMS Sign

107.125.246.78
AT&T Mobility LLC
United States, New Orleans
... NTCIP Class B

63.40.251.214
Cellco Partnership DBA Verizon Wireless
United States, Seaford
... Econolite ASC/3 SNMP/NTCIP Agent

74.206.36.102
MID CENTURY TELEPHONE
United States, Canton
Econolite ASC/3 SNMP/NTCIP Agent

166.164.24.20
Service Provider Corporation
United States, Tampa
... Skyline NTCIP DMS Sign

192.119.42.223
WNM Communications
United States, Phoenix
... Skyline NTCIP DMS Sign

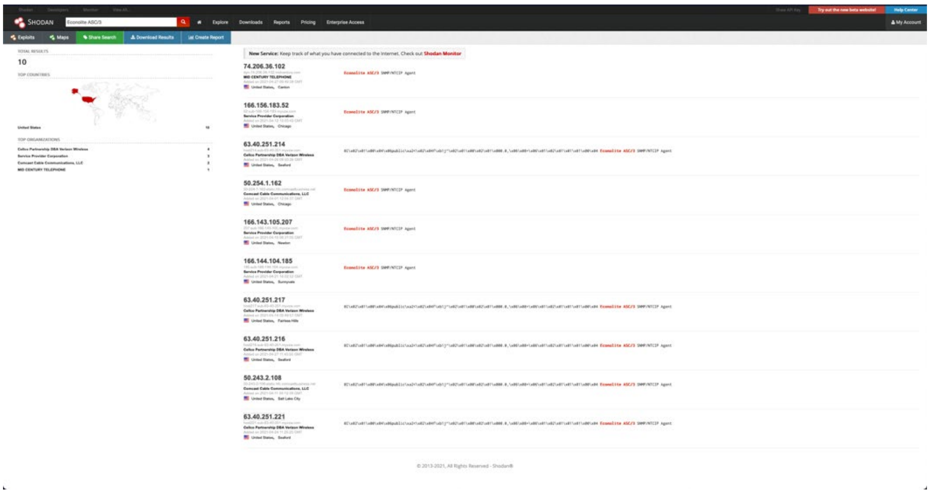
74.92.222.141
SKYLINE PRODUCTS
United States, Colorado Springs
... Skyline NTCIP DMS Sign

166.154.143.102
Service Provider Corporation
United States, Sunnyvale
... Skyline NTCIP DMS Sign

63.40.251.216
Cellco Partnership DBA Verizon Wireless
United States, Seaford
... Econolite ASC/3 SNMP/NTCIP Agent

© 2013-2021, All Rights Reserved - Shodan®

Figure 8. A list of exposed NTCIP devices in Shodan



SHODAN | Econolite ASC/3 | Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

10

TOP COUNTRIES

United States	10

TOP ORGANIZATIONS

Cellco Partnership DBA Verizon Wireless	4
Service Provider Corporation	3
Comcast Cable Communications, LLC	2
MID CENTURY TELEPHONE	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

```
74.206.36.102
MID CENTURY TELEPHONE
United States, Canton                          Econolite ASC/3 SNMP/NTCIP Agent

166.156.183.52
Service Provider Corporation
United States, Chicago                         Econolite ASC/3 SNMP/NTCIP Agent

63.40.251.214
Cellco Partnership DBA Verizon Wireless
United States, Seaford                         [illegible] Econolite ASC/3 SNMP/NTCIP Agent

50.254.1.162
Comcast Cable Communications, LLC
United States, Chicago                         Econolite ASC/3 SNMP/NTCIP Agent

166.143.105.207
Service Provider Corporation
United States, Newton                          Econolite ASC/3 SNMP/NTCIP Agent

166.144.104.185
Service Provider Corporation
United States, Sunnyvale                       Econolite ASC/3 SNMP/NTCIP Agent

63.40.251.217
Cellco Partnership DBA Verizon Wireless
United States, Fairless Hills                  [illegible] Econolite ASC/3 SNMP/NTCIP Agent

63.40.251.216
Cellco Partnership DBA Verizon Wireless
United States, Seaford                         [illegible] Econolite ASC/3 SNMP/NTCIP Agent

50.243.2.108
Comcast Cable Communications, LLC
United States, Salt Lake City                  [illegible] Econolite ASC/3 SNMP/NTCIP Agent

63.40.251.221
Cellco Partnership DBA Verizon Wireless
United States, Seaford                         [illegible] Econolite ASC/3 SNMP/NTCIP Agent
```

© 2013-2021, All Rights Reserved - Shodan®

Figure 9. Exposed Econolite ASC/3 traffic signal controllers in Shodan

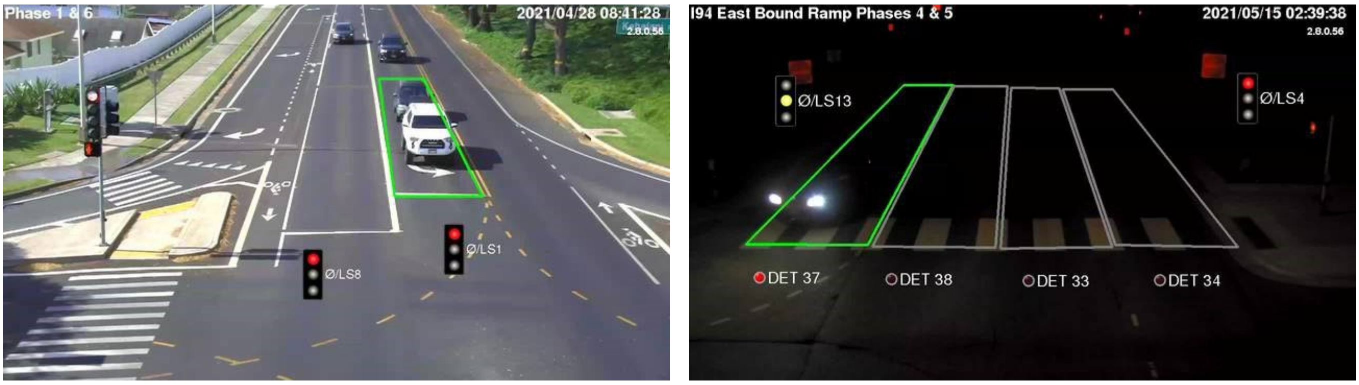


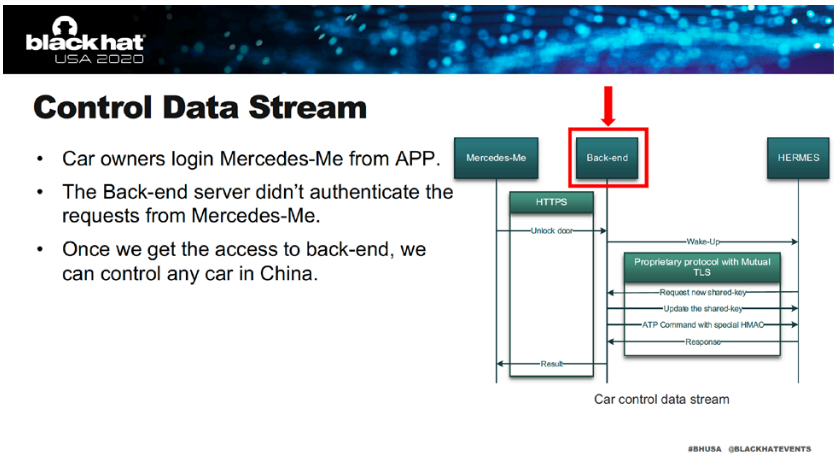
Figure 10. Exposed traffic signal cameras in Shodan

These demonstrate the ease of discovering internet-exposed roadway infrastructure in Shodan, adding to its risk is how they are also accessible to anyone from anywhere, creating a massive security hole. A malicious attacker can mount a DDoS attack against these roadway infrastructures or exploit a vulnerability to gain control of the device and cause dangerous road accidents. The overall cybersecurity of connected cars extends beyond the inside of the car, meaning the whole ecosystem needs to be protected.[28]

Compromised App-API Supply Chain

It is fairly common for modern cars to have fully digital cockpits without analog dials and buttons and everything is displayed or controlled using touchscreens and digital displays. The interior of the car looks like a giant touchscreen phone, wherein many of these head units natively support a rich third-party app ecosystem as well as Apple CarPlay and Android Auto. In addition to the apps that run on-board the vehicle, there are OEM-created apps installed on mobile phones that allow the driver to perform several key functions such as locking and unlocking their car, starting and stopping the engine, controlling the temperature inside the car, and locating their vehicle. These car apps access cloud services through a mobile phone or the vehicle's built-in eSIM.

The cloud is an API economy.[29] One example of this API economy is the data flow when turning on an internet-connected smart bulb via the Google Home App. Tapping the device's power button on the Google Home App sends a request to the Google Cloud, which then forwards the request to the bulb manufacturer's cloud, which finally sends the "turn on" command to the smart bulb. These actions are all accomplished using APIs. Hence, it is not unrealistic to expect that a connected car's cloud service makes API calls to a T1 supplier's cloud service, which in turn makes API calls to a T2 supplier's cloud service, and so on. Any compromise in this cloud supply chain could adversely affect the connected car. This is precisely what Qihoo 360's SkyGo team demonstrated at Black Hat USA 2020.[30]



Control Data Stream

- Car owners login Mercedes-Me from APP.
- The Back-end server didn't authenticate the requests from Mercedes-Me.
- Once we get the access to back-end, we can control any car in China.

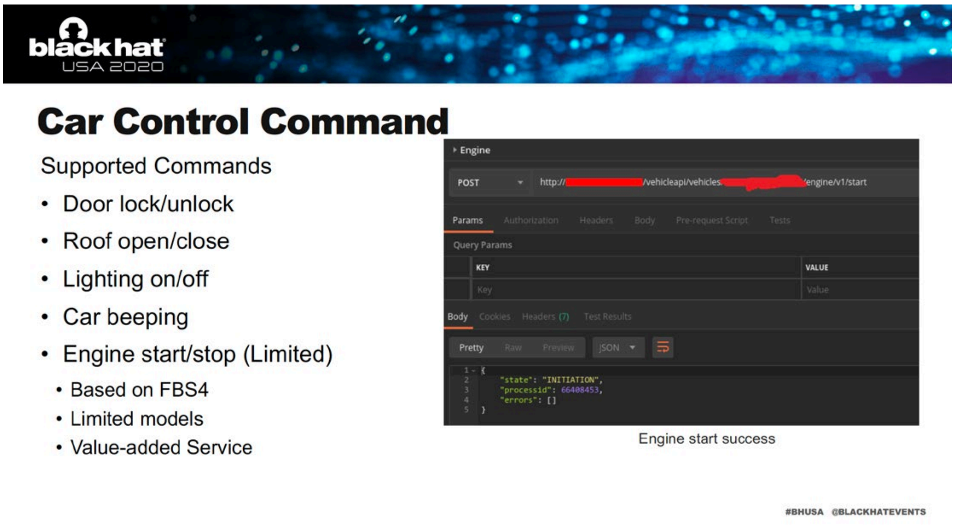
Car control data stream

#BHUSA @BLACKHATEVENTS

Figure 11. Illustrated control data stream used to compromise the cloud supply chain and control autonomous vehicles

Image source: Security Research on Mercedes-Benz: From Hardware to Car Control by Guy Harpak, Jiahao Li, and Minrui Yan[31]

The Sky-Go team successfully managed to access the Mercedes-Me (Mercedes-Benz's vehicle management App) backend servers that are serving the local Chinese market by physically removing an eSIM from one of their test vehicles and connecting it to a 4G router with a flexible printed cable (FPC) adapter. The 4G router then successfully obtained an intranet IP address from Mercedes's ISP in China. They next obtained a certificate from the ISP with which they were able to access the Mercedes-Me backend servers.



black hat USA 2020

Car Control Command

Supported Commands

- Door lock/unlock
- Roof open/close
- Lighting on/off
- Car beeping
- Engine start/stop (Limited)
  - Based on FBS4
  - Limited models
  - Value-added Service

POST http://[redacted]/vehicleapi/vehicles[redacted]/engine/v1/start

```
{
    "state": "INITIATION",
    "processid": 66408453,
    "errors": []
}
```

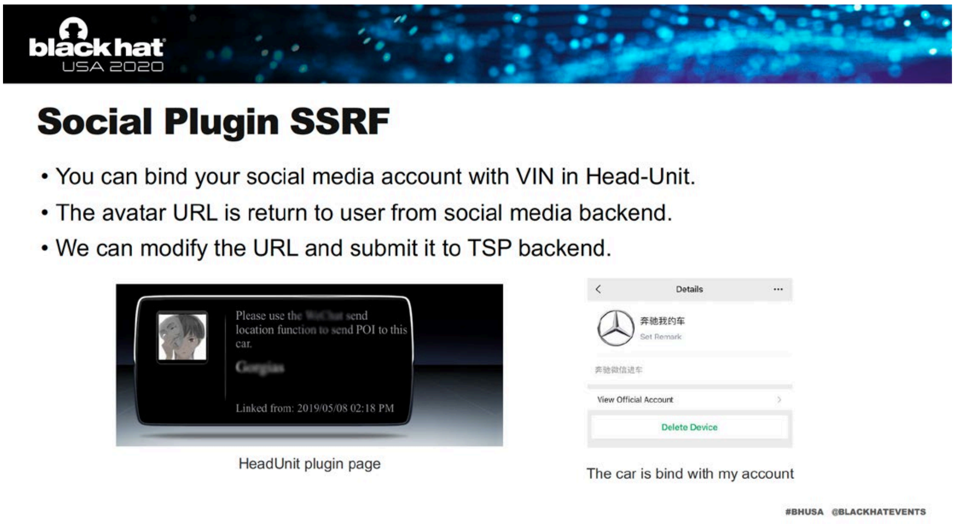
Engine start success

#BHUSA @BLACKHATEVENTS

Figure 12. Researchers having accessed car control commands after compromising the cloud supply chain

Image source: Security Research on Mercedes-Benz: From Hardware to Car Control by Guy Harpak, Jiahao Li, and Minrui Yan[32]

Once they gained access to the backend servers, they were able to use the APIs they extracted from the Mercedes-Me app to send commands to any Mercedes-Me-enabled vehicle in China. This attack worked because the Mercedes-Me backend servers did not authenticate the user requests it received from the app. Although this is an extreme example of an API supply chain compromise that involved unauthorized access to the backend servers, it does successfully demonstrate that this style of attack is possible against connected cars and can potentially impact an entire fleet.



black hat USA 2020

Social Plugin SSRF

- You can bind your social media account with VIN in Head-Unit.
- The avatar URL is return to user from social media backend.
- We can modify the URL and submit it to TSP backend.

Please use the [redacted] send location function to send POI to this car.

[redacted]

Linked from: 2019/05/08 02:18 PM

HeadUnit plugin page

The car is bind with my account

#BHUSA @BLACKHATEVENTS

Figure 13. Researchers executing random malicious URLs in the head unit

Image source: Security Research on Mercedes-Benz: From Hardware to Car Control by Guy Harpak, Jiahao Li, and Minrui Yan[33]

In the same research paper, the SkyGo team demonstrated how they used a server-side request forgery (SSRF) attack against a third-party app installed in the vehicle's head unit and get it to execute random malicious URLs. These head units are commonly running customized versions of OS such as Linux and QEMU, and thus are susceptible to common IT-style attacks such as SSRF, script injections via banners, malvertising, SQL injections, XSS attacks, MitM, session hijacking, DNS spoofing, and many others.[34] With the vehicle head units supporting app ecosystems, as well as being able to load both authorized and unauthorized (jailbroken phones) apps via Apple CarPlay and/or Android Auto, the App-API ecosystem accessed by in-vehicle apps will quickly become a complicated security problem in the near future.

Social Engineering Attacks

Social engineering attacks use the art of deception for malicious end goals. These attacks are common in the IT security world and include things like phishing, spear phishing, baiting, social media scams, scary propositions, big news, and many others.[35] Given the ways modern cars interact with mobile devices and head units are all digital and touchscreen, it's not inconceivable to find cybercriminals adapting their social engineering toolkits to target connected car users.

A published research paper by Promon from 2016 shows how Tesla car owners were socially engineered into installing a malicious app with the promise of a free meal at a nearby restaurant.[36] The malicious app replaced the Tesla app with itself using a privilege escalation attack. The malicious app mimicked the genuine Tesla app and prompted the car's owner to input their Tesla username and password, which the app then exfiltrated to the attacker. The attacker can abuse the stolen credentials to unlock the target vehicle, start the engine, and steal the car.

This is not an extreme example of a social engineering attack as most car manufacturers have created apps for mobile phones that allow the driver to lock and unlock their vehicle, start and stop the engine, control the temperature, and locate their vehicle. Most head units support Apple CarPlay and Android Auto, which in turn support loading both authorized and unauthorized (on jailbroken phones) apps. The authorized app list is limited, but by jailbreaking their phone, the driver can load any app from their phone to the head unit.[37, 38] This presents the perfect opportunity for cybercriminals to socially engineer drivers into installing malicious apps that can then be loaded on the vehicle's head unit and steal a wide range of data, such as vehicle location, saved credentials, access tokens or hashes from other apps, other PII, and saved payment information.

Stealing data from a fleet of vehicles may become more profitable than stealing the physical vehicles themselves. Malicious apps do not necessarily have to be loaded via jailbroken phones — the previous section showed how the SkyGo research team successfully executed random malicious URLs via an SSRF attack against an authorized third-party app installed in the vehicle's head unit. Similar methods can also be employed to remotely or drive-by install malicious apps or malware. If middleware abstracts the E/E details of the vehicle and provides API access to apps to send messages to the ECUs, then malicious apps would be capable of potentially sending dangerous inputs to the ECUs while the vehicle is moving, seriously jeopardizing everyone's safety on the road.

Mitigating UN R155-Defined Threats

In discussing the solution, let us first recap what connected cars are and the general progression of their development. Connected cars are vehicles that have becomes a part of the ITS system, which consists of a network and back-end system that functions as an information and communication technology (ICT) terminal. The development of connected cars will happen in this order:

1. The terminal or vehicle that originally ran as stand-alone units will be connected to the internet and start to work by occasionally pulling out the necessary data from the back end.
2. It then starts to work with a more established connection to the internet and exchanging data in real time.
3. Finally, many features and processes, even those traditionally performed by hardware, will move to the cloud.

This is the same sequence that has happened within the IT world for the last few decades. However, we expect the speed of this evolution to be much faster than that of IT, because we've already experienced the development of IT. It should be noted, however, that this chain of events also applies to attackers.

In our previous research,[39] we found that the connected car attack chain looks uncannily like typical IT cyberattacks. The characteristic point is that after breaking through the entrance by exploiting a vulnerability, attackers would then successfully use lateral movement to straddle multiple systems. This is not surprising because connected vehicles share hardware, software, and communication protocols with that of the IT world. We can expect them to share more similarities.

Given these similarities, we recommend applying several methods based on learnings and experiences from the IT world and future threat predictions:

1. **Connected car threat intelligence.** It is built-in by integrating cyberthreat intelligence and automotive threat intelligence. This is the baseline protection technology that can detect, analyze, thwart, and respond to threats.

2. **Multilayered security.** The presence of a multilayered security solution would make it increasingly difficult for attackers to succeed. No defense is impregnable to determined adversaries, but a multilayered approach increases the cost, the time, and the resources needed by a malicious actor to mount a successful attack.

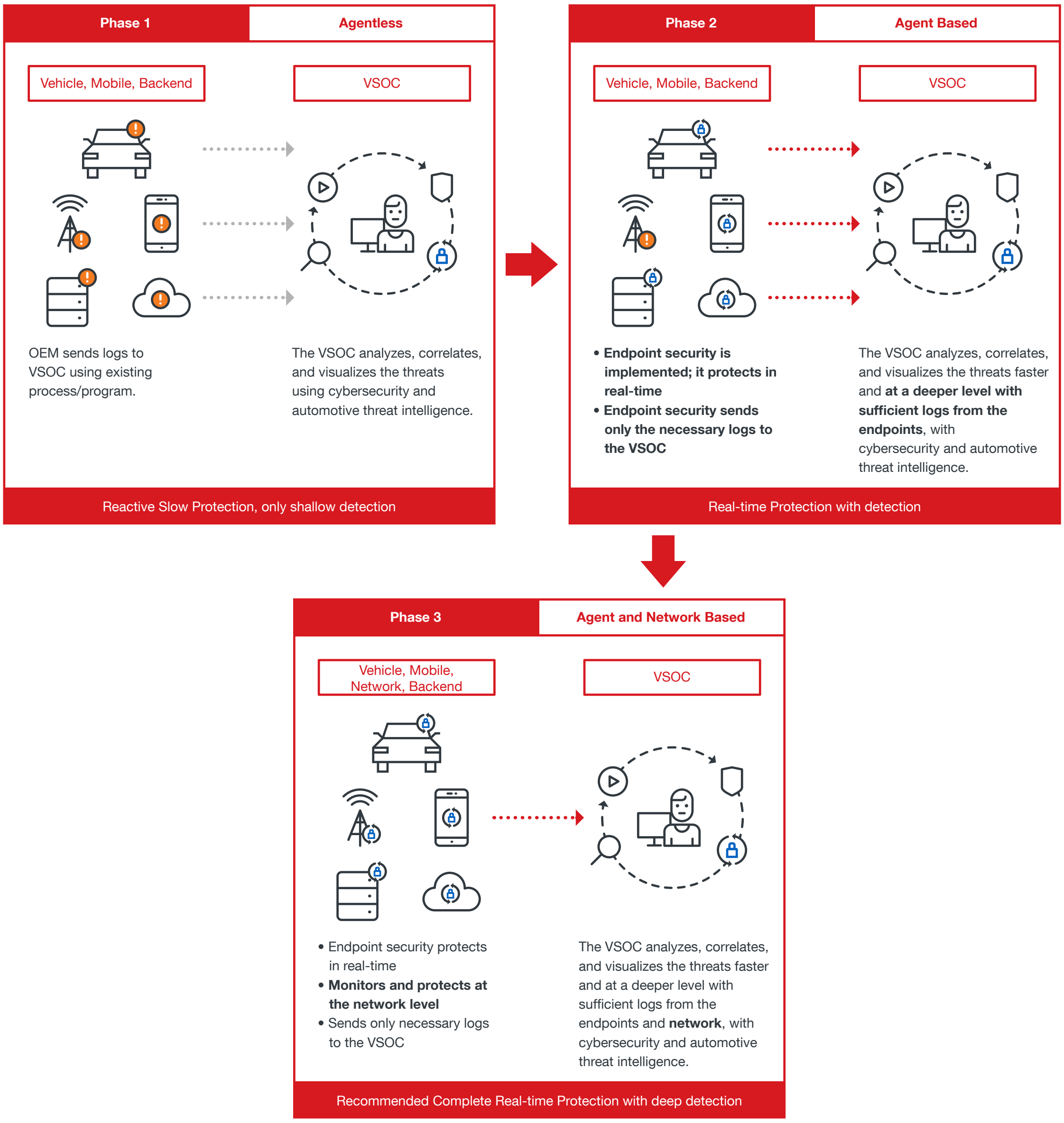
3. **Security covering a comprehensive ecosystem.** Connected car security needs to be designed with an integrated view of a comprehensive ecosystem, which is composed of an endpoint (vehicle), network, and back end. These are critical areas to monitor in order to secure the end-to-end data supply chain.

4. **Vehicle Security Operations Center (VSOC).** VSOC allows understanding the context of attacks typically carried out by lateral movements spanning system to system by correlating notifications from different components of a connected car ecosystem and then take the necessary actions or countermeasures.

Phased Approach

Finally, how can stakeholders implement security that covers expansive connected car ecosystems? In reality, security always comes as a trade-off and balance between benefits and cost.

Cybersecurity is an important business factor in connected cars, but it may not be possible to implement all security solutions at once due to various restrictions. Therefore, it is necessary to determine the priority of what to focus on and in what order, then determine the phased approach based on that prioritization. At this time, considering the speed with which threats evolve parallel to the evolution of technology, we recommend designing connected vehicles in a way that is oriented toward raising protection at a high speed. The following figures illustrate our recommended phased approach.



OEM sends logs to VSOC using existing process/program.

The VSOC analyzes, correlates, and visualizes the threats using cybersecurity and automotive threat intelligence.

- **Endpoint security is implemented; it protects in real-time**
- **Endpoint security sends only the necessary logs to the VSOC**

The VSOC analyzes, correlates, and visualizes the threats faster and **at a deeper level with sufficient logs from the endpoints**, with cybersecurity and automotive threat intelligence.

Real-time Protection with detection
Phase 3
Agent and Network Based
Vehicle, Mobile, Network, Backend
VSOC

- Endpoint security protects in real-time
- **Monitors and protects at the network level**
- Sends only necessary logs to the VSOC

The VSOC analyzes, correlates, and visualizes the threats faster and at a deeper level with sufficient logs from the endpoints and **network**, with cybersecurity and automotive threat intelligence.

Recommended Complete Real-time Protection with deep detection

Figure 14. Three recommended phases in developing security for the connected car

Trend Micro Solutions

To safeguard connected cars from the possibility of a successful attack, we prescribe a comprehensive cybersecurity strategy that considers the entire connected car ecosystem composed of the vehicle, network, back-end, and VSOC.[40] Those solutions are backed-up by connected car threat intelligence built by integrating automotive threat intelligence and cyberthreat intelligence from over 30 years of our history enabling protection from this ever-growing threat.

Working with industry leaders, we understand that the requirements and optimal solutions for each customer is different. Therefore, we provide customized solution for each customer. Trend Micro's customizable solution is not limited to technical solutions, and could, for example, include cybersecurity training and vulnerability research. In collaboration with industry leader partners, we offer a solution to support UN R155 compliance.

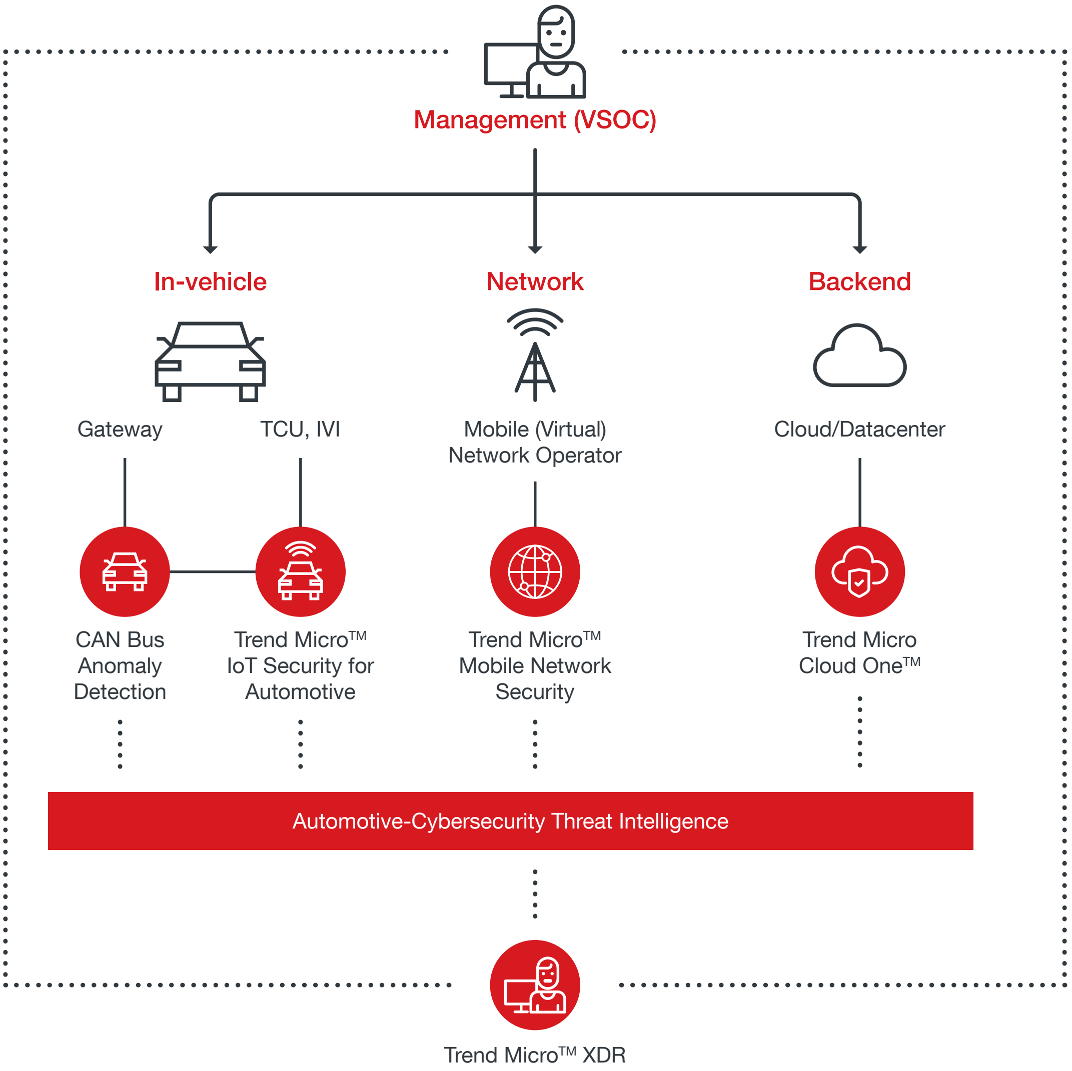

Management (VSOC)
In-vehicle
Network
Backend
Gateway
TCU, IVI
Mobile (Virtual) Network Operator
Cloud/Datacenter
CAN Bus Anomaly Detection
Trend Micro™ IoT Security for Automotive
Trend Micro™ Mobile Network Security
Trend Micro Cloud One™
Automotive-Cybersecurity Threat Intelligence
Trend Micro™ XDR

Figure 15. A comprehensive protection against cyberattacks at four points: vehicle, network, backend, and vehicle security operations center (VSOC).

For the Vehicle

Trend Micro IoT Security for Automotive provides multilayered security including system protection and application protection for critical devices connecting in-vehicle systems and outside networks, such as telematic control units (TCU), IVIs, domain systems, and digital cockpits, while CAN Bus Anomaly Detection monitors traffic in the CAN bus. It works as a sensor reporting critical logs to VSOC and HIDPS, capable of filtering a tremendous amount of logs by ML models and threat expert rules to reduce network bandwidth and resource consumptions at VSOC.

For the Network

Trend Micro Mobile Network Security (TMMNS) is a hybrid cybersecurity solution that ensures the network security and identification integrity of vehicles connecting via cellular network. Based on the European Telecommunication Standards Institute (ETSI) Network Functions Virtualization (NFV) framework, TMMNS

Network Protection offers VNF that can flexibly deploy at the mobile edge or core network for connected cars to monitor traffic, detect, and take countermeasures with high performance and low latency. In the meantime, the TMMNS Endpoint Protection will identify the anomalous behavior and deny it access. TMMNS Endpoint Protection is deployable on any subscriber identity module (SIM), such as physical SIMs, eSIMs, and iSIMs, allowing users to harden vehicle security. TMMNS bridges the gap between information and communication technologies (IT/CT) to provide comprehensive protection against cyberattacks in 4G/LTE and 5G networks, covering the network and vehicle seamlessly.

For the Back End

Among the various connected technologies used by connected cars are applications and systems hosted on back-end infrastructures. Many more of these applications and systems are bound to be built as the adoption of connected cars continues to grow. The Trend Micro™ Cloud One™ security services platform can be used to secure back-end cloud and data center environments without affecting performance. Through the Trend Micro™ Zero Day Initiative™ program, it can detect and disclose vulnerabilities to keep cloud environments and vehicle systems secure, especially since it is common for new and evolving technologies to have known and unknown vulnerabilities. The platform also continuously analyzes and identifies new malware, ransomware, and indicators of compromise that could be used in attacks. In addition to ITS back-end systems, ITS endpoints need to be secured. The Trend Micro IoT Security™ solution can be used for this purpose, providing risk and anomaly detection and in-system protection for a wide range of IoT devices, including traffic lights and surveillance cameras.

For the VSOC

From our own experience, the following are the threats seen and pain points of most SOCs:

- Stealthy threats that continue to evade even the best of defenses
- Disconnected security layers with siloed tools and data sets that make it difficult to correlate information and detect critical threats
- Too many alerts and overloaded organizations that don’t have the time or resources to conduct a thorough investigation

  Consolidated visibility into an organization’s current security status, trending over time, is hard to come by and limits the ability to know what to focus on and where action should be taken

To ensure that the VSOC is able to correlate events quickly and effectively, the Trend Micro™ XDR® analyzes, correlates, and visualizes events from the endpoint, the network, and the back end, with individual notifications for each. It provides a comprehensive look at events alongside vital contextual data, thereby helping organizations identify and thwart threats.

Conclusion

More than 125 million passenger cars with embedded connectivity are forecasted to ship worldwide between 2018 and 2022,[41] and the annual production of semi and fully autonomous vehicles are expected to reach more than 14 million by 2025.[42] The sheer volume of network-connected cars will both create and expand new attack surfaces for the ITS ecosystem. Connected cars will be connected via 5G or Direct Short-Range Communications (DSRC) (implemented using 802.11p or 802.11bd) to V2X and will become one of the heaviest users of cloud infrastructure. Future vehicles will have functions from their E/E architecture migrated to the cloud and communicating back to the vehicles via high-speed, low-latency networks. Connected cars with their all-digital cockpits will support a rich ecosystem of third-party apps that will provide a host of innovative functionalities to both drivers and passengers. This opens up many interesting attack scenarios against connected cars via cloud infrastructure attacks or through E/E architecture agnostic middleware and cloud APIs.

Given the high level of expectations for connected cars and their potential exploitability, it is crucial to ensure that automotive cybersecurity technologies stay well ahead of adversary TTPs. This is the Red Queen hypothesis at play: a never-ending arms race with our competitors, the cybercriminals.

In this research paper, our assessment and insights about the attack vectors (listed in the UN Regulation No. 155) against connected cars had a two-fold goal. First, we wanted to inform the various stakeholders about the threats and challenges they are going to face on the roadways in the next couple of years and which threats they should prioritize. Second, identifying and addressing the cybersecurity risks faced by connected cars in their early development stages gives us the opportunity to influence both legislative and technological developments in this domain. We threat modeled the attack vectors listed in the UN Regulation No. 155 by applying current technologies, hacker TTPs, and learnings from published research in the car hacking domain. Within the next decade, especially with the global rollout of 5G networks, the available technology stack and TTPs are going to significantly change, and thus the threat profiles will also shift. Finally, while the WP.29 document already lists an impressive array of cyberattack vectors, we discovered additional attack vectors and focus areas that also need protection to ensure the overall safety and security of connected cars.

In conclusion, the UN Regulation No. 155 and similar initiatives are the correct regulatory step forward to ensure safe and secure roads, but it also needs to be flexible so that they can easily adapt with fast paced technological developments and changes in human behavioral patterns.

References

1 United Nations. (n.d.). *UNECE*. “WP.29 - Introduction.” Accessed on July 26, 2021, at https://unece.org/wp29-introduction.

2 United Nations. (n.d.). *UNECE*. “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.” Accessed on July 26, 2021, at https://unece.org/sites/default/files/2021-03/R155e.pdf.

3 United Nations. (n.d.). *UNECE*. “WP.29 - Introduction.” Accessed on July 26, 2021, at https://unece.org/wp29-introduction.

4 United Nations. (June 24, 2020). *UNECE*. “Virtual meeting of the (WP.29) World Forum for the Harmonization of Vehicle Regulations (181st session).” Accessed on July 26, 2021, at https://unece.org/transport/events/virtual-meeting-wp29-world-forum-harmonization-vehicle-regulations-181st-session.

5 United Nations. (n.d.). *UNECE*. “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.” Accessed on July 26, 2021, at https://unece.org/sites/default/files/2021-03/R155e.pdf.

6 Bob O’Donnell. (June 28, 2016). *USA Today*. “Your average car is a lot more code-driven than you think.” Accessed on July 26, 2021, at https://www.usatoday.com/story/tech/columnist/2016/06/28/your-average-car-lot-more-code-driven-than-you-think/86437052/.

7 Irwin Bambrah. (Dec. 16, 2020). *Tesloid*. “How to update Model 3 software when there is no Wifi?” Accessed on Aug. 20, 2021, at https://tesloid.ca/2020/12/16/how-to-update-tesla-model-3-software-when-there-is-no-wifi/.

8 John Cusimano. (2011). *SCADA Hacker*. “Assessing the Security of ICS Using Threat Modeling.” Accessed on July 26, 2021, at https://scadahacker.com/howto/howto-threatmodeling.html.

9 United Nations. (June 23, 2020). *UNECE*. “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.” Accessed on July 26, 2021, at https://undocs.org/ECE/TRANS/WP.29/2020/79.

10 Microsoft. (July 14, 2010). *Microsoft*. “Chapter 3 Threat Modeling.” Accessed on July 26, 2021, at https://msdn.microsoft.com/en-us/library/aa302419.aspx.

11 Dawid Czagan. (May 21, 2014). *Infosec*. “Qualitative Risk Analysis with the DREAD Model.” Accessed on July 26, 2021, at https://resources.infosecinstitute.com/topic/qualitative-risk-analysis-dread-model/.

12 United Nations. (June 23, 2020). *UNECE*. “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.” Accessed on July 26, 2021, at https://undocs.org/ECE/TRANS/WP.29/2020/79.

13 Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro*. “Cybersecurity for Connected Cars – Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on July 26, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

14 Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro*. “Cybersecurity for Connected Cars – Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on July 26, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

15 InetSoft. (n.d.). *InetSoft*. “InetSoft Webinar: The Data Supply Chain - Its Definition and How to Use It.” Accessed on July 26, 2021, at https://www.inetsoft.com/business/solutions/definition_of_data_supply_chain/.

16 Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro*. “Cybersecurity for Connected Cars – Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on July 26, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

17 Numaan Huq, Rainer Vosseler, and Morton Swimmer. (Oct. 24, 2017). *Trend Micro*. “Cyberattacks Against Intelligent Transportation Systems.” Accessed on Aug. 2, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/high-tech-highways-securing-the-future-of-transportation.

18 Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro*. "Cybersecurity for Connected Cars – Exploring Risks in 5G, Cloud, and Other Connected Technologies." Accessed on July 26, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

19 German Sharabok. (Sep. 2, 2020). *Towards Data Science*. "Why Tesla Won't Use LIDAR." Accessed on Aug. 2, 2021, at https://towardsdatascience.com/why-tesla-wont-use-lidar-57c325ae2ed5.

20 AutoPilot Review. (April 27, 2019). *YouTube*. "Elon Musk on Cameras vs LiDAR for Self Driving and Autonomous Cars." Accessed on Aug. 2, 2021, at https://www.youtube.com/watch?v=HM23sjhtk4Q.

21 Nir Morgulis, Alexander Kreines, Shachar Mendelowitz, and Yuval Weisglass. (June 30, 2019). *Research Gate*. "Fooling a Real Car with Adversarial Traffic Signs." Accessed on Aug. 2, 2021, at https://www.researchgate.net/publication/334161359_Fooling_a_Real_Car_with_Adversarial_Traffic_Signs.

22 Jonathan Gitlin. (Sept. 2, 2017). *Ars Technica*. "Hacking street signs with stickers could confuse self-driving cars." Accessed on Aug. 2, 2021, at https://arstechnica.com/cars/2017/09/hacking-street-signs-with-stickers-could-confuse-self-driving-cars/.

23 Jonathan Gitlin. (Sept. 2, 2017). *Ars Technica.* "Hacking street signs with stickers could confuse self-driving cars." Accessed on Aug. 2, 2021, at https://arstechnica.com/cars/2017/09/hacking-street-signs-with-stickers-could-confuse-self-driving-cars/.

24 Nir Morgulis, Alexander Kreines, Shachar Mendelowitz, and Yuval Weisglass. (June 30, 2019). *Research Gate*. "Fooling a Real Car with Adversarial Traffic Signs." Accessed on Aug. 2, 2021, at https://www.researchgate.net/publication/334161359_Fooling_a_Real_Car_with_Adversarial_Traffic_Signs.

25 Nir Morgulis, Alexander Kreines, Shachar Mendelowitz, and Yuval Weisglass. (June 30, 2019). *Research Gate*. "Fooling a Real Car with Adversarial Traffic Signs." Accessed on Aug. 2, 2021, at https://www.researchgate.net/publication/334161359_Fooling_a_Real_Car_with_Adversarial_Traffic_Signs.

26 Shodan. (n.d.). *Shodan*. "Shodan." Accessed on Aug. 2, 2021, at https://www.shodan.io/.

27 National Transportation Communications for Intelligent Transportation System (ITS) Protocol (NTCIP). (2009). *NTCIP*. "National Transportation Communications for ITS Protocol ." Accessed on Aug. 2, 2021, at https://www.ntcip.org/file/2018/11/NTCIP9001v0406r.pdf.

28 National Transportation Communications for Intelligent Transportation System (ITS) Protocol (NTCIP). (2009). *NTCIP*. "National Transportation Communications for ITS Protocol." Accessed on Aug. 2, 2021, at https://www.ntcip.org/file/2018/11/NTCIP9001v0406r.pdf.

29 Kelly Sheridan. (March 6, 2020). *Dark Reading.* "7 Cloud Attack Techniques You Should Worry About." Accessed on Aug. 2, 2021, at https://www.darkreading.com/cloud/7-cloud-attack-techniques-you-should-worry-about/d/d-id/1337259?image_number=7.

30 Guy Harpak, Jiahao Li, and Minrui Yan. (Aug. 6, 2020). *Black Hat USA 2020*. "Security Research on Mercedes-Benz: From Hardware to Car Control." Accessed on Aug. 2, 2021, at https://i.blackhat.com/USA-20/Thursday/us-20-Yan-Security-Research-On-Mercedes-Benz-From-Hardware-To-Car-Control-wp.pdf.

31 Guy Harpak, Jiahao Li, and Minrui Yan. (Aug. 6, 2020). *Black Hat USA 2020*. "Security Research on Mercedes-Benz: From Hardware to Car Control." Accessed on Aug. 2, 2021, at https://i.blackhat.com/USA-20/Thursday/us-20-Yan-Security-Research-On-Mercedes-Benz-From-Hardware-To-Car-Control.pdf.

32 Guy Harpak, Jiahao Li, and Minrui Yan. (Aug. 6, 2020). *Black Hat USA 2020*. "Security Research on Mercedes-Benz: From Hardware to Car Control." Accessed on Aug. 2, 2021, at https://i.blackhat.com/USA-20/Thursday/us-20-Yan-Security-Research-On-Mercedes-Benz-From-Hardware-To-Car-Control.pdf.

33 Guy Harpak, Jiahao Li, and Minrui Yan. (Aug. 6, 2020). *Black Hat USA 2020*. "Security Research on Mercedes-Benz: From Hardware to Car Control." Accessed on Aug. 2, 2021, at https://www.blackhat.com/us-20/briefings/schedule/#security-research-on-mercedes-benz-from-hardware-to-car-control-20746.

34 Sébastien Dudek. (March 18, 2019). *Synacktiv*. "Modmob tools and tricks: Using cheap tools and tricks to attack mobile devices in practice." Accessed on Aug. 2, 2021, at https://www.synacktiv.com/ressources/Troopers_NGI_2019-Modmobtools_and_tricks.pdf.

35 Trend Micro. (n.d.). *Trend Micro*. "Social engineering." Accessed on Aug. 2, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/social-engineering.

36 Promon. (Nov. 23, 2016). *Promon*. “Tesla cars can be stolen by hacking the app.” Accessed on Aug. 2, 2021, at https://promon.co/security-news/hacking-tesla-app-stolen-car/.

37 iPodHacks142. (July 17, 2019). *iPodHacks142*. “How to Use ANY App with Apple CarPlay.” Accessed on Aug. 2, 2021, at https://www.ipodhacks142.com/how-to-use-any-app-with-apple-carplay/.

38 Tomasz Grobelny. (Dec. 17, 2020). *Opensource*. “How to hack Android Auto to display custom content.” Accessed on Aug. 2, 2021, at https://opensource.com/article/20/12/android-auto-open-source.

39 Numaan Huq, Craig Gibson, and Rainer Vosseler. (Aug. 18, 2020). *Trend Micro*. “Driving Security Into Connected Cars: Threat Model and Recommendations.” Accessed on Aug. 2, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-cybersecurity-blind-spots-of-connected-cars.

40 Trend Micro. (n.d.). *Trend Micro*. “Connected Car Security.” Accessed on Aug. 23, 2021, at https://www.trendmicro.com/en_us/business/solutions/iot/connected-car.html.

41 Internet of Business. (2020). *Internet of Business*. “Connected cars report: 125 million vehicles by 2022, 5G coming.” Accessed on Aug. 2, 2021, at https://internetofbusiness.com/worldwide-connected-car-market-to-top-125-million-by-2022/.

42 Nick Michell. (Dec. 5, 2016). *Cities of Today*. “Self-driving cars to reach 14.5 million by 2025, says new study.” Accessed on Aug. 2, 2021, at https://cities-today.com/self-driving-car-production-reach-14-5-million-2025-says-new-study/.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research