



Automotive Cybersecurity in 2022

VicOne Report





Introduction

In the past year, energy production around the world has changed quickly and the automotive industry has kept up with this evolution. The energy crisis has pushed many governments to review renewable energy policies and, as a result, electric vehicles (EVs) have started to become mainstream. Automotive-related news has also become more visible to a public audience, and more people are aware of the industry's trends and issues. However, change is a double-edged sword. When people take bold steps forward, it is natural to also make mistakes. In the arena of technology, change generates new vulnerabilities and flaws.

Top Reported Automotive Security Issues

We surveyed news about the automotive industry from the start of 2021 to June 2022 and the results tell an interesting story while also highlighting current real-world threats. Keyless issues made up 26.1% of the discussions we monitored in 2021 and 24% in the months monitored in 2022. These keyless issues were an intuitive entry point for automotive security since this technology can unlock the door to a car or start the engine without physically inserting a key.

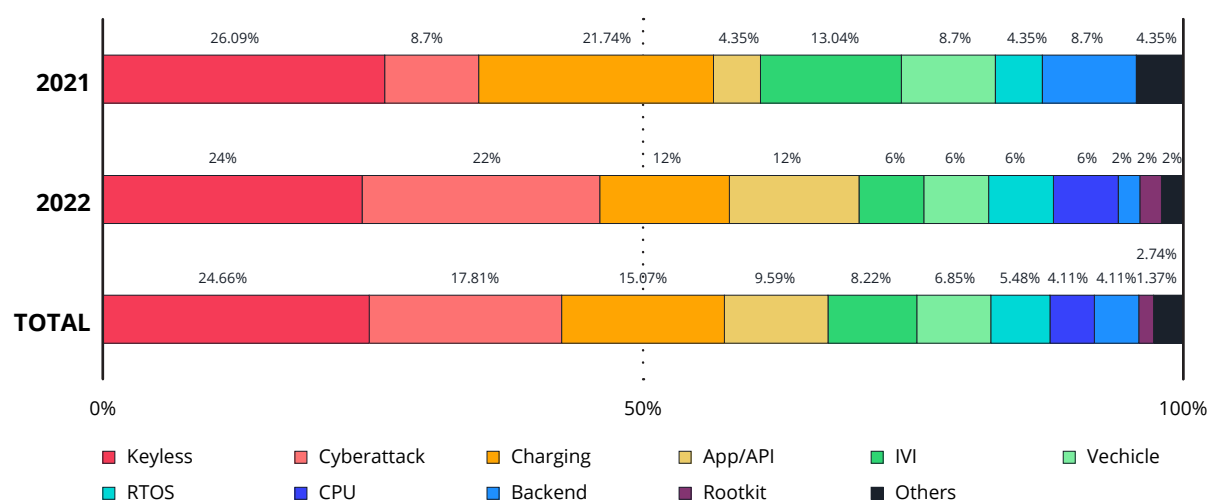


Figure 1. Security topics covered by automotive news

Typically, remote keyless entry systems use a radio frequency (RF) signal but also digital cards and mobile apps through RFID (Radio Frequency Identification), Bluetooth, NFC (Near Field Communication) and UWB (Ultra-Wideband). Sometimes these technologies can be used in conjunction with each other.

In-vehicle infotainment (IVI) was another topic discussed in the news. IVI is another channel for a user to communicate with the vehicle. Users can interact with it via USB, Bluetooth, Wi-Fi, SD card, DVD, touch screen, GPS, or cellular connection. Recently, users can remotely control a vehicle via internet connection, which increases the risk of vehicle internal network compromising via a remote connection. IVI also connects with other electronic control units (ECUs) via the CAN bus or Ethernet, effectively serving as a possible gateway for lateral movement of an attacker. Essentially, IVI has features that makes it more convenient and user-friendly but also gives the attacker more options to access the car. The attacker can modify IVI firmware, making the attack persistent and allowing the injection of malicious frames into internal vehicle network connections. Some IVI systems also have critical bugs; for example, one

navigation system has the Year 2022 bug (Y2k22), which resets the clock to January 1, 2002. Another bug is triggered when a system can't process image files without an extension, which will reboot and crash the system. Recently, we saw researchers demonstrate a remote code execution (RCE) vulnerability with CAN messages sent to switch on a target vehicle's headlights and wipers and open the trunk in Pwn2Own 2022.¹

Besides in-vehicle components, charging issues have been prominently discussed since charging stations or charging piles are likely targets. Charging stations and piles are like internet-of-things (IoT) devices — they have operating systems, debug ports, CAN protocol, and PLC (Power Line Communication) protocol. Users can use mobile apps or API, RFID, Bluetooth, Wi-Fi, or 4G to communicate with the charging stations or piles. They can also interact with them through webpages, so these stations also have a cloud back-end server.

There were significant charging station-related vulnerabilities reported in CVEs last year. Some researchers found that users can access charging stations for web hard-coded credential authentication, modifying configuration, or setting up remote root firmware. Attackers could also deploy web-based attacks such as cross-site scripting (XSS), cross-site request forgery (XSRF/CSRF), server-side request forgery (SSRF), and brute-force attacks to interact with users and get access permission or sensitive information. Some machines have injection vulnerabilities that could allow code execution and let attackers download new firmware. These vulnerabilities could also allow an actor to monitor and modify systems via a Wi-Fi network to deploy man-in-the-middle (MitM) attacks and get tokens or APIs, deploy a jamming signal to prevent a charging station from working, or even get free charging. For example, in 2022, we saw researchers investigate charging piles² and uncover a vulnerability in the Plug-and-Charge feature, enabling them to get free charging after exploiting the vulnerability.

One notable incident happened in February 2022. A popular automotive vendor³ suspended operations for two days after a supplier was hit by a cyberattack. After that, we saw more incidents of suppliers being hit by cyberattacks. The malicious actors usually steal data and threaten to publish the company's sensitive data.

Supply chains⁴ have been increasingly exposed in recent years, as many manufacturing facilities have begun to digitalize and most of them have given little thought to cybersecurity. Smaller businesses along the supply chain are easier targets and can attract attackers. This is also a threat for the automotive industry, because if a supply-chain attack can halt an operation, it will affect the whole enterprise.

Common Vulnerabilities and Exposed Attack Vectors

We collected automotive-related Common Vulnerabilities and Exposures (CVE) information from 2021 to June 2022 and also included Common Weakness Enumeration (CWE) information. CWE is a community-developed list of software and hardware weakness types. The following table lists the top 10 weaknesses we found:

CWE	2021	2022	Total
Buffer Copy without Checking Size of Input ("Classic Buffer Overflow")	30	3	33
Double Free	3	3	6
Improper Input Validation	14	0	14
Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	15	3	18
Integer Overflow or Wraparound	15	3	18
NULL Pointer Dereference	17	1	18
Out-of-bounds Read	29	3	32
Out-of-bounds Write	30	7	37
Reachable Assertion	22	0	22
Use After Free	22	9	31

Table 1. Top 10 CWEs from January 2021 to June 2022

These weaknesses might lead to data corruption, systems or programs crashes, denial of service (DoS), and code execution. If they are present in a vehicle, they could affect vehicle operation and vehicle security. Original equipment manufacturers (OEMs) and suppliers should pay attention to these vulnerabilities and weaknesses. We compiled our data in the following and showed several topics that automotive and security personal should be aware of. The top three topics are system-on-chip (SoC), kernel, and real-time operating system (RTOS).

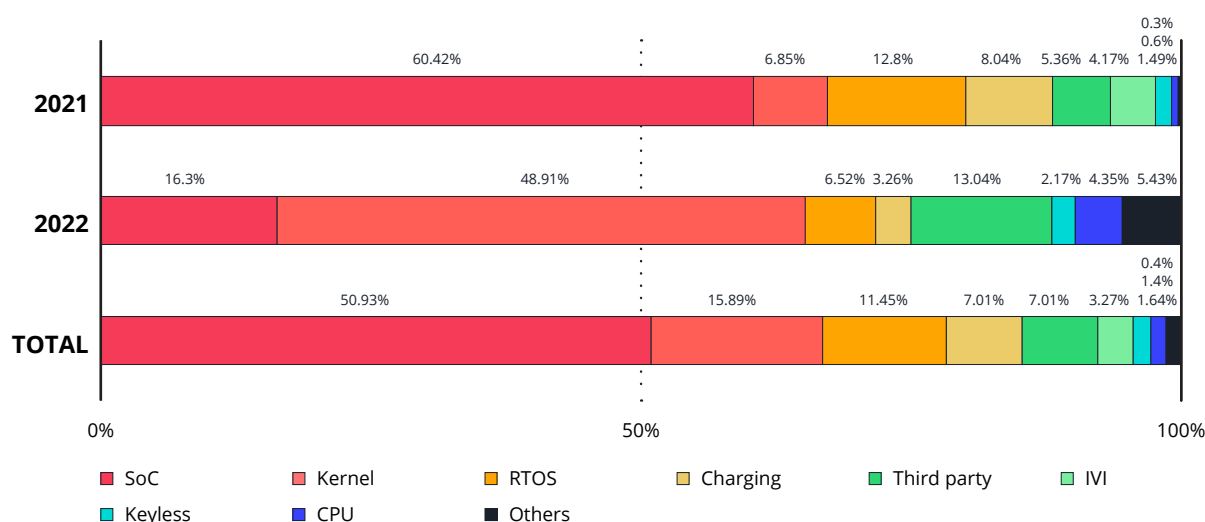


Figure 2. Security issue distribution within top CVEs

SoC Issues

A system-on-chip (SoC) is a processor that combines multiple types of computing modules, such as a central processing unit and a graphics card. Automotive connectivity SoC supports Wi-Fi, Bluetooth, 2G/3G/LTE/4G/5G, with C-V2X and Dual Sim Dual Active (DSDA). It also supports location features for automotive use cases such as wireless phone, camera, display, voice, music, headphones, speakers, positioning, and so on. A scalable computer architecture featuring SoCs is also used for developing advanced driver assistance technology and autonomous driving. Those related chipsets have security vulnerabilities, and they will impact core, audio, multimedia, data, modem, and event cryptographic issues. They can also bypass content protection and authentication.

Usually, the hardware vulnerability is difficult to patch and its life cycle is longer than other vulnerabilities. Sometimes, vulnerabilities were introduced by circuit design, such as speculative processor vulnerabilities, and such vulnerabilities are permanently present in the ECU. The best practices for mitigation is to patch software and operating systems and avoid causing damage by limiting the usage scenario. Other hardware vulnerabilities might be fixed by upgrading firmware. In the past, upgrading firmware was almost impossible without recalling vehicles to an authorized service center. However, over-the-air (OTA) update technology is getting more mature, which demonstrates how manufacturers can handle issues more elegantly and effectively.

Kernel and RTOS Issues

The kernel is second in the list of top vulnerabilities, but both kernel and RTOS concerns are increasing. Vulnerabilities connected to both show a clear path of being rooted in software development. Using proprietary software does not mean it is secure, and closed-source software still has the same troubles as open-source. There is no doubt that the modern automotive industry leverages open-source software to rapidly build a solid software system and provide a variety of applications. However, it means the software will inherit the same legacy security concerns from existing software. Solutions to these issues are not clear-cut.

The ECU is a device that can be used to control the engine, wipers, brakes, and other electronic features in a car. Its status will heavily affect the vehicle's security and safety. There are many ECUs in an vehicle, and they are composed of microcontrollers (MCU, SoC, core) that contain one or more CPUs, memory, input/output (I/O), analog/digital (a/d) converters, and communication links, such as CAN bus or Ethernet, and embedded software. The embedded software includes an operating system (in most cases, some sort of RTOS with device drivers) written for hardware subsystems.

RTOS is an operation system that has critical time constraints for data and event processing without buffer delays. RTOS has different types, but it typically includes a hard real-time operating system, also called safety-critical system, which assures that tasks are finished and an accurate response is given within the specified time. Many OEMs and suppliers use Linux kernel-based software solutions (AGL or customized systems or even Android-based on upstream Linux Long Term Supported [LTS] kernels). According to the data we collected, there are existing vulnerabilities in a kernel that could be used to escalate privileges on the MCU and inject or execute codes.

Building a responsive and healthy software system is crucial, and the automotive industry should consider introducing source code auditing and vulnerability management systems, which can power up with a software bill of materials (SBOM). It is impossible to eliminate all vulnerabilities in one's systems, but efforts can be made to minimize risks.

Critical Cyberattacks on the Automotive Industry

Based on observations made over 2022 and an analysis of major cybersecurity incidents in the automotive industry, we collected 52 significant events to show the range of cyberattacks on the industry. These cover different levels of the supply chain from supplier to vendor and show that they were involved at almost every production stage. Incidents also happened several times each month without exception.

What are the major types of incidents? Ransomware and data breaches are first and second, respectively. Both incident types usually made a big impact on the victim’s company or factory. The most affected production stage is the supplier. Attacks on the supplier mean that production progress is suspended or stopped during the incidents. Also, recovery time is normally lengthy because most suppliers don’t have a plan to handle such attacks and threats. Because of this, they need more time than traditional IT companies.

The following sections provide more details.

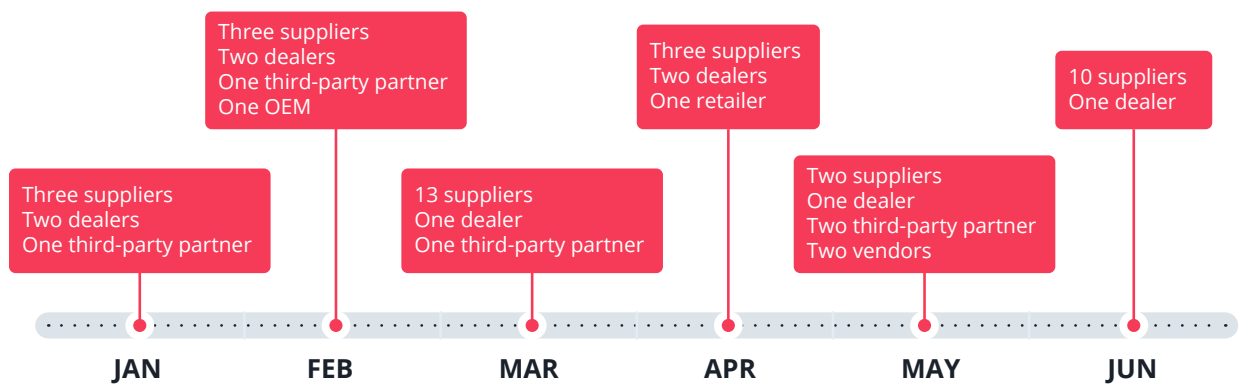


Figure 3. Six-month timeline of cybersecurity incidents involving the automotive supply chain

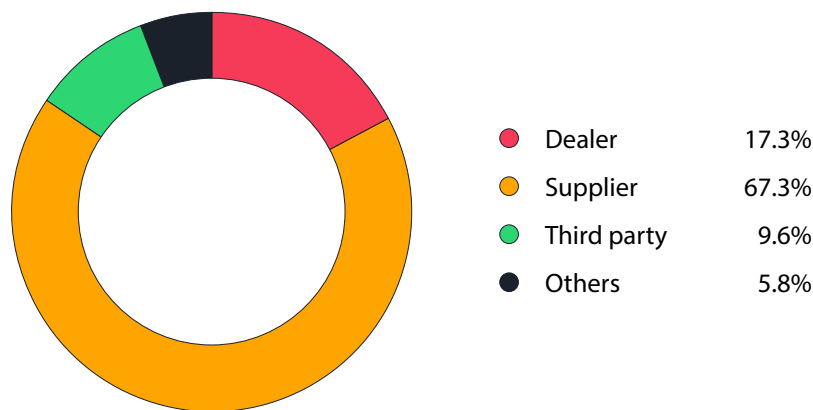


Figure 4. Percentage of affected supply-chain roles

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their systems, either by locking a system's screen or by encrypting users' files until a ransom is paid. Ransomware is already a critical security topic in every industry. Ransomware actors are not only attacking banking or payment systems but also all levels and departments of businesses.

According to our open-source intelligence (OSINT) in the first quarter of 2022, ransomware grew quickly. If we compare ransomware data with the first three months of 2021, we see that victims increased around 30%. These victims are across every industry, and the targets are not limited to big business — even smaller organizations have been hit.

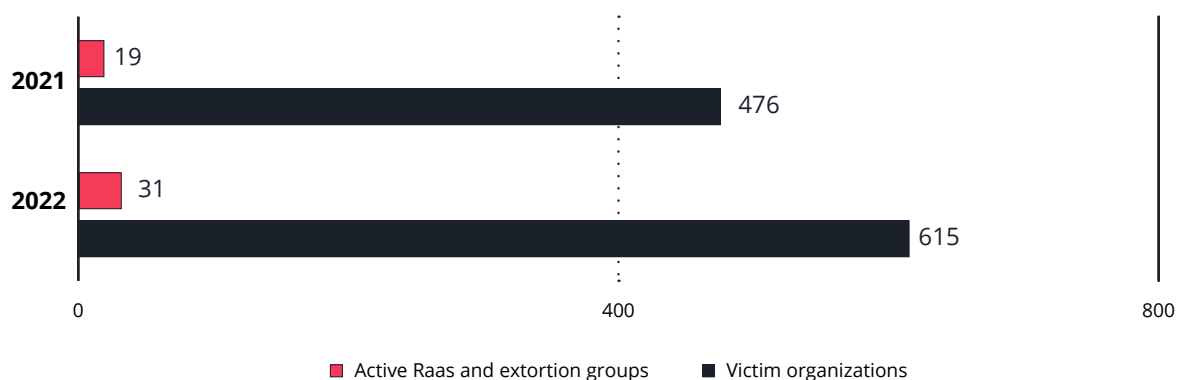


Figure 5. Comparison of ransomware victims and groups in the first quarter of 2021 and the first quarter of 2022

The automotive industry is no exception, having been transformed by the digital age over the years. Huge complex automotive factories need a lot of IT equipment in order to keep operations running smoothly. Any type of accident will affect operations and cause financial losses. If we look at data from January to June 2022, we see 43 automobile industry-related victims.

The ransomware families that have affected the automotive industry the most is Conti, followed by LockBit and Hive. These ransomware families are already infamous in the IT industry, and they leverage known techniques and tricks to break into systems in the automotive industry. There is no secret sauce or any brand-new techniques, but they still successfully compromise companies without getting into trouble.

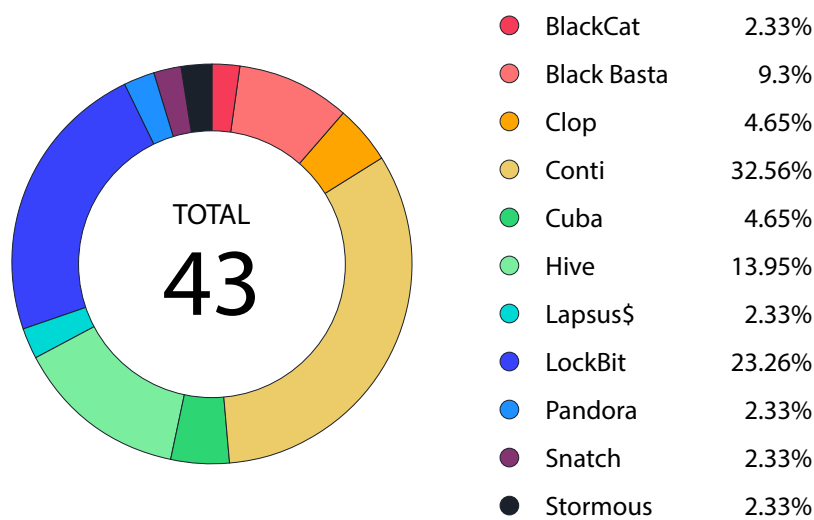


Figure 6. Top ransomware families affecting the automotive industry

Typical attacks begin with a vulnerability or some form of opening. One way that cybercriminals initiate attacks is by using system or network vulnerabilities to intrude into a vendor’s network. Another tactic involves gaining unauthenticated access permission, as seen in the attack on Nvidia⁵ this year. Like in most attacks, once cybercriminals are inside a system, they will proceed to encrypt data, after which they will demand a ransom in return for unlocking blocked systems. Most modern ransomware groups now either publish their victim list and the types of data they have stolen or threaten to do so in order to pressure their victims further into settling the ransom.

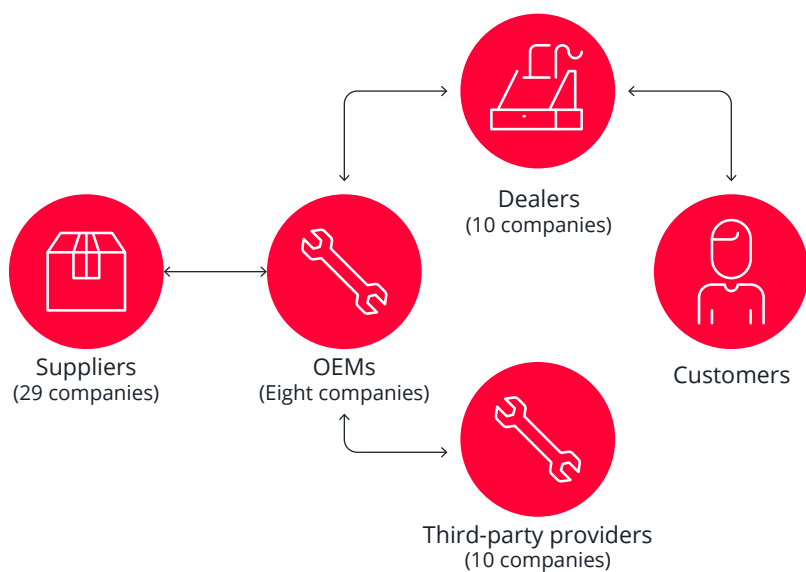


Figure 7. The overview of the roles that targets of cyberattacks have in the automotive supply chain and the number of attacked companies per role

Data Breach

A data breach is an incident in which information is stolen from a system without its owner’s knowledge or authorization. Depending on the type of data and from whom it is stolen, a data breach can have far-reaching consequences that can affect the lives of customers and affect an organization’s reputation regardless of its industry.

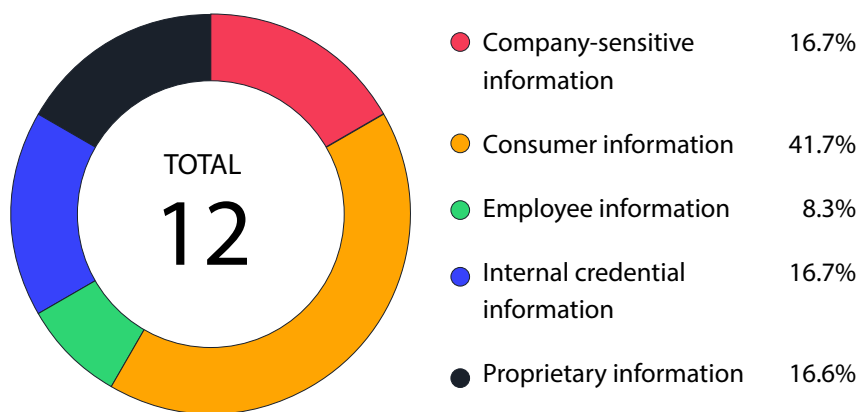


Figure 8. The types of information compromised in incidents of data breach in the automotive industry from January 2021 to June 2022

In our investigation, we reviewed published reports on data-breach cases within the automotive supply chain and noted the types of data that were stolen from each case. As seen in Figure 8, customer information and company-sensitive information are the top reported breaches from the last two years. In the wrong hands, these types of data can lead to more complicated attacks.

Stolen consumer information or any personal information can lead to individuals being directly targeted in scams or frauds. In credential stuffing, phone call fraud, and spear-phishing attacks, criminals leverage stolen data in order to target a specific person or particular groups using their own detailed information.

Stolen sensitive information and proprietary information affect companies directly. This kind of data leak might not have immediate implications, but once malicious groups have studied the information enough, they can launch unpredictable attacks.

Proprietary information, like the source code or infrastructure architecture, could allow threat actors to discover weaknesses or vulnerabilities more quickly. Because vehicles run on code and are essentially connected devices, the damage caused by exploits might be hard to calculate.

Stolen infrastructure architecture, on the other hand, can act like a treasure map by showing the path of the whole system and the source code used in a production vehicle.

Date	Business	Data
Jan 11, 2022	Data logger app for a car brand ⁶	Consumer information, internal credential information
Jan 25, 2022	Car dealership ⁷	Consumer information
Feb 1, 2022	Car dealership ⁸	Consumer information
Feb 10, 2022	Car dealership ⁹	Consumer information, employee information
Feb 23, 2022	Software company ¹⁰	Internal credential information, proprietary information
Mar 4, 2022	Ferrite manufacturer ¹¹	Employee information, company-sensitive information
Mar 9, 2022	Car dealership ¹²	Employee information
May 23, 2022	Vehicle manufacturer ¹³	Consumer information
Jun 1, 2022	Fabless IC company ¹⁴	Company-sensitive information, proprietary information

Table 2. List of data-breach cases from January 2021 to June 2022

Cyberattack Trends

These observations reveal some trends in the latest attacks on supply chains. The trends would likely continue in the near future, and the automotive industry should pay close attention to them.

- **The attacks would become more targeted.** Ransomware and data breaches are not new kinds of threats. In the past, threat actors might deliver their ransomware by spam email or drive-by download in order to spread their malware as broadly as possible. However, in recent years, they have adopted the tactics, techniques, and procedures (TTPs) of targeted attacks to make their operations more efficient and lucrative. Compared to the average individual user, a business is not only more likely to be able to afford the ransom, but also more likely to pay it to avoid disruption to its operations.
- **Interruption of operations is not the only problem.** Traditionally, threat actors make money from ransomware by making the device or data inaccessible to a user or company. Even for companies with good data backup plans, the shutdown operation before recovery can cost them a lot of money. However, this is not the worst scenario. As observed in some recent ransomware attacks, actors threaten to leak stolen data if victims refuse to pay the ransom. This is an intimidating situation for victims because the intellectual property involved might be critical to many companies. In some cases, the leaked data does not even belong to the victim companies but rather to their customers. Therefore, ransomware attacks or data breaches not only interrupt a business's operations but also damage its reputation.
- **It affects more than just the victims.** As we observed in some incidents, a ransomware attack or a data-breach incident affects not only the victim itself but also the upstream customers or downstream suppliers. As previously mentioned, threat actors have adopted the TTPs used by targeted attacks. Threat actors might use the collected information or credentials to attack other companies that have business relationships with the initial target. In several cases, we saw the upstream vendors pause manufacturing as a precautionary measure before their supplier sorts out a ransomware or data-breach incident.

Identified and Increasingly High-Risk Areas

EV Charging Stations

For more context on electric-vehicle charging stations and the security issues surrounding the technology and standards of charging, please see our Appendix.

Charging stations and battery management systems can easily become a hacker's target. In general, EVs usually use the lithium polymer (aka LiPo) battery and need comprehensive intelligent control mechanisms to work well. Compared to a traditional car, an EV has more sensors and communication protocols between the vehicle and a charging station, which leads to multiple security issues. Here are the top three attack surfaces we identified:

1. **CAN bus-based communication protocol between an EV and a charging station**

CAN bus-based protocols are often used on EV and charging station communications, and always transfer data by plain text. This gives hackers opportunities to hijack the sessions to deploy MitM attacks. They could also transfer malicious code to the EV or charging station.

2. **App/Cloud services for EV charging stations**

EV charging stations are usually connected to the cloud for transactions and billing procedures. Some EVs even have apps to give users a more convenient experience. In the context of cybersecurity, this is a traditional attack surface. An attacker could gain privileges to gather user information from mobile devices or penetrate the cloud server.

3. **Radio communications**

Radio communications, RFID, Bluetooth, and customized radio signals are frequently used on EV charging systems. These could become remote attack surfaces that attackers use to access the EV components. For example, hackers could remotely open the charging port or transfer malicious code to the EV or charging station to gain control.

Cloud APIs

Connected cars are an ongoing shift and evolution of automotive vehicles. Typical network architecture for these cars is illustrated in Figure 9. Most new car models sold in the market have built-in embedded-SIMs (eSIMs), although some of them are not activated. Built-in eSIMs are used to transmit telematics data, communicate with back-end cloud servers, create Wi-Fi hotspots, and get real-time traffic information, among other functions. Examples of cloud-based back-end server applications include smart apps that can remotely start, stop, lock, and unlock a car, and apps that can automatically send current road conditions data to the cloud and transmit to other vehicles subscribed to the same service. These are examples of the cloud services provided.

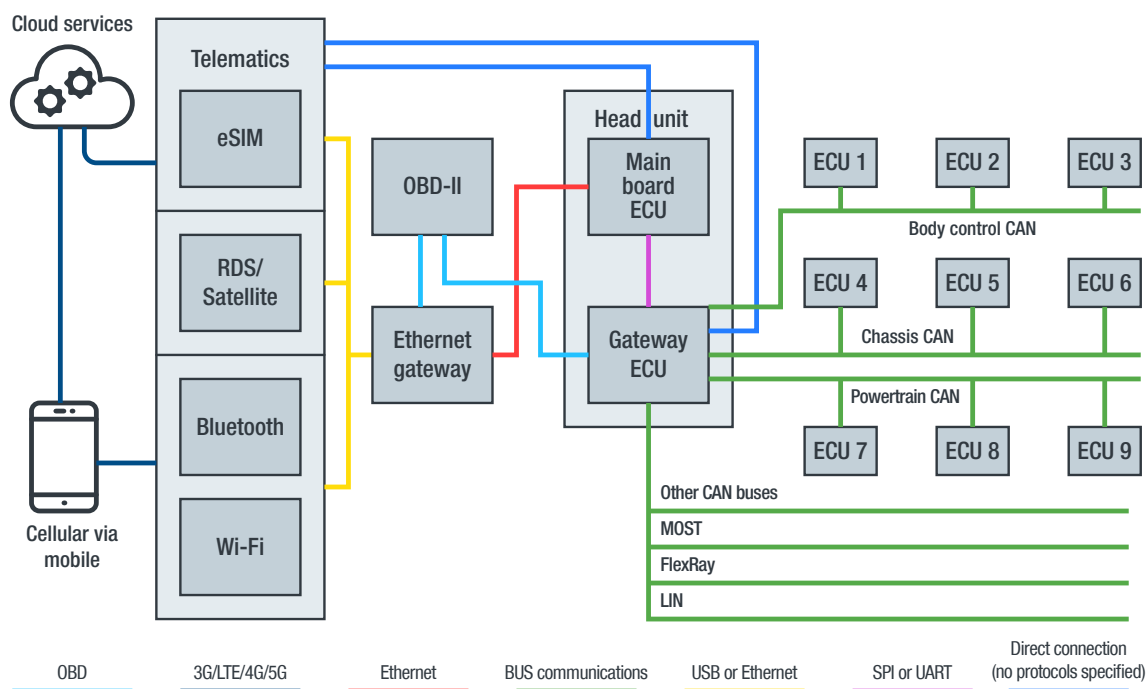


Figure 9. A theoretical visualization of a generic network architecture¹⁵ for a modern connected car

A cloud API is the main character of the whole network architecture that provides variables functions. The developer can leverage its data and functions to archive different purposes. It is similar to a simple GPS tracker OBDII dongle, allowing a user to track or deploy simple commands to a targeted car. However, an API provides more than that, and modern cloud APIs are already highly integrated with the car itself. Advanced functions are available to the user.

The Tesla API is a good example of this. This API's access control depends on an access token: Once you get the secret sauce, the car is yours. In early 2022, a teen hacker gained control of more than 25 Tesla cars¹⁶ remotely in an experiment, exposing the importance of API tokens to vehicle security and presenting a glimpse of what could happen should API tokens become lost or stolen. The incident explains some basic security rules that we can't just ignore. For example, a token must follow the principle of least privilege, meaning one API token should not be used to rule all functions. This way, even if breaches do happen, one has the measures to contain them. A complete access log is also very important, as it will be key to solving unauthorized access and alerting the user before things go bad.

In the traditional IT industry, API security already has its own set of best practices. The domain is mature, and related toolsets are ready. It is worth leveraging existing techniques and following guidelines. The Open Web Application Security Project or OWASP's top 10 list reminds developers of the top security issues every year, while MITRE's CWE gives a list of software and hardware weaknesses. The only problem is adapting and working with security as a mindset.

Remote Keyless Entry (RKE)

From January 2021 to June 2022, a long-standing issue regarding remote keyless entry systems was repeatedly raised. Although this topic has not been lacking in discussion over the years, it has not been effectively mitigated due to cost considerations of vehicle manufacturers, consumer habits, and market patterns. Some examples are the car theft incident¹⁷ reported by NBC News in June 2022 and the Honda key fob issues (CVE-2021-46145, CVE -2022-27254, and CVE-2022-37305), which have been uncovered for two consecutive years.

In the past, radio devices were both a high barrier and mystery to the general public; nowadays, with the popularization and affordability of software-defined radios, the radio field has become relatively more accessible. For example, the Flipper Zero is a software-defined radio device being sold in 2022 for about US\$165. It features the customizable Arduino-like Integrated Drive Electronics (IDE) interface, which further reduces the difficulty of coding software-defined radios. As a tweet by user inf0sec1 shows,¹⁸ the Flipper Zero can easily perform replay attacks on older Ford vehicles. Such replay attacks can be circumvented by changing the solution used by the manufacturer — for example, by using the rolling code mechanism — but few manufacturers paid much attention to it in the past, given the cost and user experience. For example, Honda has adopted the rolling key mechanism in its new models, but some actors still found ways to bypass this protection.¹⁹

The evolution of remote keys²⁰ in the automotive industry is somewhat similar to the evolution of protocols in the industrial internet-of-things (IIoT) environment. Industrial RF remote controllers appear as rugged remotes with multiple buttons, and so do vehicle RKE key fobs. RF remote controllers are based on packet radio protocols, which involve modulating a byte-stream as radio waves. Their increased connectivity with other devices (such as Anybus and CAN bus) makes them an interesting target for attackers.

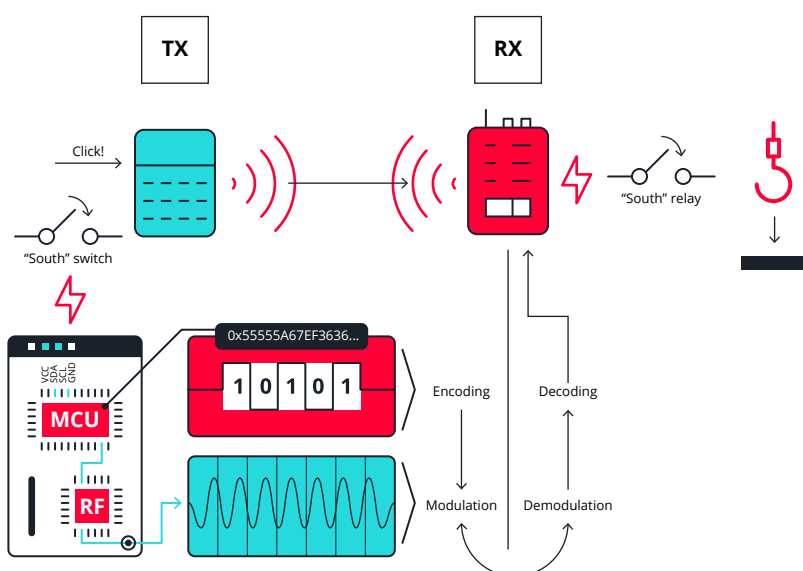


Figure 10. Scheme of connection between transmitter, receiver, and controlled equipment

Given that RF waves are “accessible” to anyone within range, this technology must include proper safety and security measures to prevent abuse.

Vulnerability pattern	Description	Attack class	Patch development	Patch deployment
No rolling code	Each packet is self contained and requires no dynamic secret to be interpreted. Any captured packet is always valid in the future.	1, 3	Very easy	Difficulty in terms of accessibility; there are millions of units already deployed and the components are not easily accessible.
Weak or no cryptography	The data exchanged between transmitter and receiver is not encrypted or is weakly obfuscated and predictable.	1, 2, 3, 4	Easy	Difficult in terms of coverage; in addition to the patching problems explained previously, firmware-only solutions may be insufficient because the hardware may not support cryptography.
Lack of software protection	The software used to upload firmware on the transmitter and receiver does not prevent unauthorized reprogramming.	5	Very easy	Easy; vendors just need to implement proper access control in their software.

Table 3. Vulnerability patterns that we identified in our research

In a previous research paper, Trend Micro identified the usual remote-controlled system vulnerabilities. We found that vehicle RKE systems also shared the same vulnerabilities as the industrial operational technology (OT) area.

As Trend Micro found earlier, the car remote control basically works on ISM channels, but more commonly between 315 and 915 MHz:

“...in which the most common 915 megahertz (MHz). Although the actual frequency band can vary from country to country, the ISM bands are internationally reserved for industrial, scientific, and medical requirements, and not for communications. More recently, industrial radio remote controllers in the 2.4 gigahertz (GHz) band are emerging, mainly as a solution to the overcrowded 315, 433, 868, and 915 MHz bands.”²¹

In the ISM band, we have many common modulation methods to choose from, such as frequency-shift keying (FSK), phase-shift keying (PSK), minimum-shift keying (MSK), and others. In the case of automotive remote control, FSK is the most used because most automotive remote controls do not require much transmission capability. Simplicity, ease of use, low cost, and the need for reliability dominate the choice of technology.

In common internet protocols, such as 802.11 family Ethernet, we do not directly transmit the data we need at the physical or modulation layer. The transmission method of most car remote controls is relatively simple and brutal, directly transferring the specific bit pattern to the ISM band via FSK Modulate.

This design might be fine for home appliances, but it will definitely be a problem for car doors, as we cannot share the same remote control for the same car model. Therefore, there is usually a set of codes to distinguish different vehicles to avoid the problem of key sharing. In the early days, this code was relatively short and could be found as a six-digit or even a four-digit finger switch after the key was removed, which allowed the vehicle's controller to accept the open/close signal from the key by adjusting the remote control to the same six-digit code as the car's controller.

This design is the same as the luggage combination lock — in fact, an attacker with enough time to test would soon be able to crack the code, so this design is relatively rare today. Most RKE key fob designs, called fixed code, usually have a flash memory (either built into the chip or externally) that stores a relatively long set of fixed codes for use as a match.

However, such a design is obviously subject to replay attacks, as shown in Figure 11.

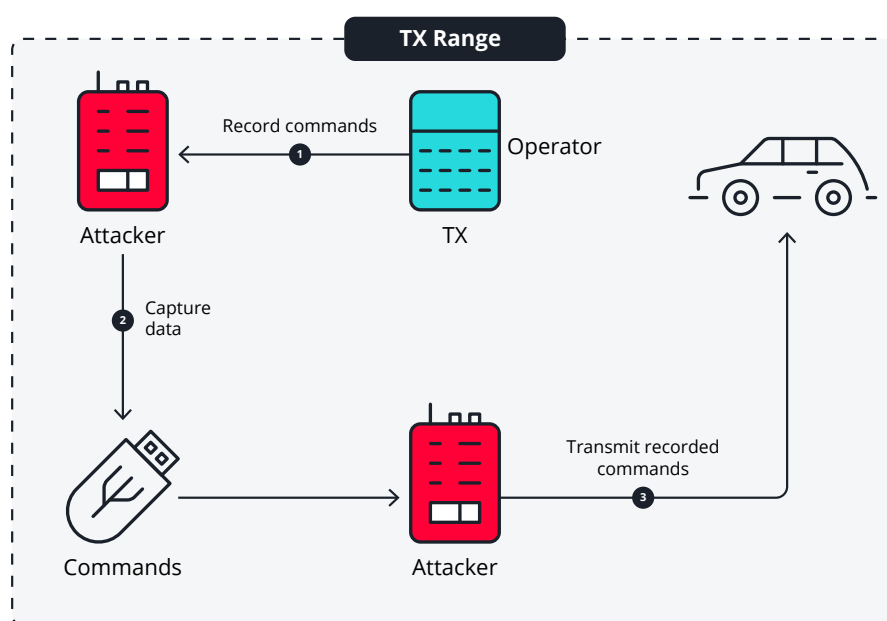


Figure 11. Illustration of replay attacks on vehicles

In this concept, the attacker recorded the user's remote control signal and sent it directly to the vehicle to achieve the same function. As illustrated previously, Flipper Zero, an entry-level software-defined radio device, can unlock older Ford vehicles.

In a previous research project on GitHub,²² it was found that a high percentage of Honda vehicles used simple FSK modulation, and there was even a design flaw in the use of fixed code that made the problem worse. The authors of "Unoriginal-rice-patty" (a report on a replay-based attack on Honda and Acura vehicles)²³ found that the RKE signal used in a large number of Honda vehicles uses the fixed code design, but the opening signal is the result of bit-flipping the lock signal. This means that the difficulty of replay attacks on Honda vehicles affected by this design is halved, since the attacker does not need to wait until the owner presses the door-open button to record it.

As aforementioned, there is a very effective way to prevent the replay attack called the rolling code mechanism.

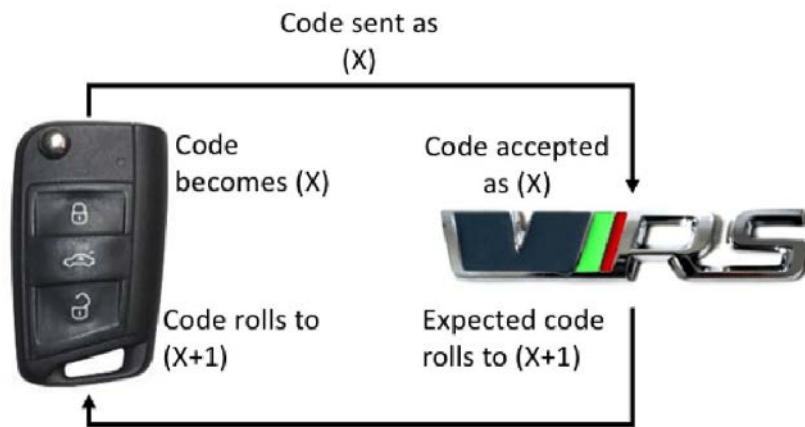


Figure 12. Illustration of the rolling code mechanism²⁴

Image credit: Colin Urquhart et al/Researchgate.net

The preceding diagram is a conceptual demonstration of the core concept of rolling code, which is a one-time discarded signal. Whenever a successful command is accepted by a vehicle, the key and the vehicle side will discard the current key, so this design is highly effective in limiting the occurrence of replay attacks. However, the use of rolling code in the real world does have a number of limitations; for example, it needs a set of cryptographic tables.

In terms of a solution, the first step is to generate a cipher table and place it in the key fob's memory during the pairing phase. The other focuses on design and requires the use of a proprietary cryptographic algorithm with PRNG dynamic generation. The Microchip HCS301 chip family (widely used in European cars) uses this design.

The Keeloq problem is one of the most famous cases, discussed by Samy Kamkar at Defcon23 in 2015.²⁵ The Keeloq algorithm is designed without a time parameter, which means that if the owner presses or mistakenly touches the remote control when it is out of range or disturbed, the attacker can record the signal for the next time. In addition, most of the devices that use Keeloq have a short password length. The early 32-bit design can be easily cracked within two weeks, but later products have extended to 66-bit. However, with the rapid development of semiconductor technology, this is only a stopgap measure.

Rolling code design is also limited by another problem: the user experience issue. As shown in the concept diagram of the rolling code mechanism, the core of the mechanism is the discarded code. In other words, if a key has discarded the previous code and the car does not know about it, the next time the key is used, the passcode on both sides cannot be matched effectively and the key is considered faulty. To deal with this user experience problem, Honda introduced a sliding window-like design.

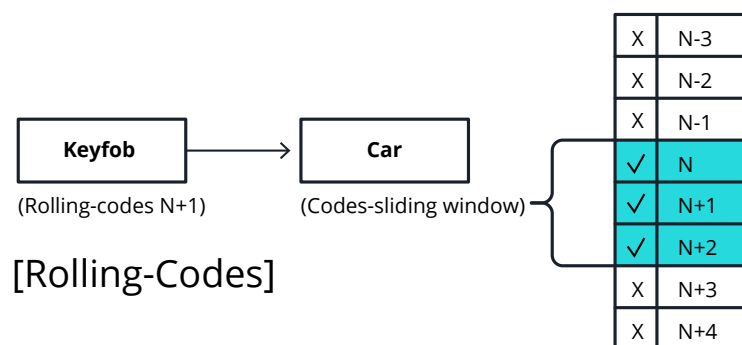


Figure 13. The sliding window design²⁶

Star V lab researchers found that Honda 2012 vehicles have been designed to allow a certain range of codes to be used for the resync process. However, this design dismantles the protection of the rolling code itself, making the replay attack possible again:

*"By replaying the previously eavesdropped Lock/Unlock commands in a special sequence to the Honda-Civic, it will be resynchronizing the counter. Once the counter resync, commands from the previous cycle of the counter can be replayed again."*²⁷

Tesla's key uses a new idea, abandoning the traditional RKE design to use Bluetooth Low Energy (BLE) with a data layer/application layer authentication and encryption design to produce key fobs. As the cost of BLE devices decreases, more car manufacturers are following up with this design in their advanced vehicles. By shifting the work of pairing and passcode to the data layer, we can enjoy the various encryption and authentication solutions that have been developed in the IT area.

However, this design has been repeatedly defeated by cost issues, and in May 2022, Sultan Qasim Khan, a senior security consultant at NCC Group, posted his research²⁸ alluding to such on the company's blog. Additionally, due to the flexibility of the BLE key fob used by Tesla on latency, the relay attack became feasible and was successfully used on the 2022 Model 3.

In 2021, Lennert Wouters discovered a series of vulnerabilities²⁹ in the Tesla model X's keys, including an OTA function that did not implement security mechanisms and a faulty pairing protocol. The protocol allowed him to build a chain of attacks by brushing malicious firmware onto the same chip as the key fob and triggering a rekeying process that allowed the attacker to directly (and without contact) mass-produce the keys to the target vehicle.

We, the VicOne research team, conclude these RKE problems in this mind map:

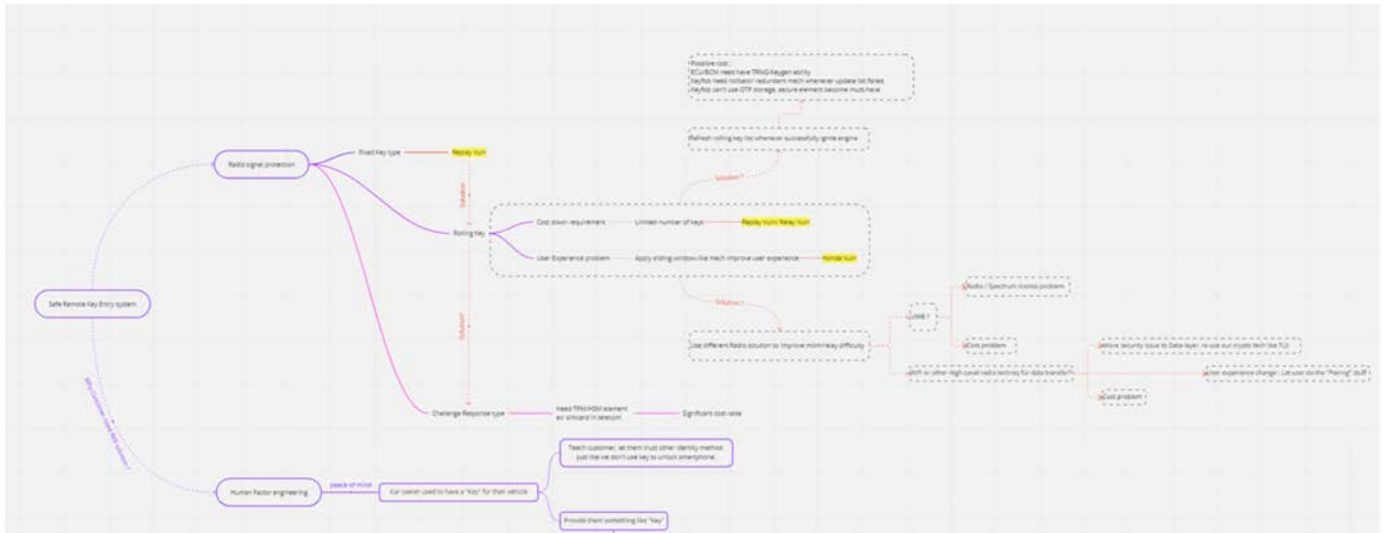


Figure 14. A mind map of issues related to RKE systems in connected cars

RKE's vulnerability is a series of compromises between cost and experience. This is not something that can be changed over time, but there are some countermeasures and necessary strategies:

- Use rolling code and avoid excessive cost cutdowns as much as possible.
- Separate the door control and engine unlock functions to avoid the problem of simply opening the door to drive the vehicle away.
 - For example, many of today's vehicles are equipped with what is commonly known as a chip lock. This lock uses an RFID tag on the key body to achieve further security by utilizing the characteristics of RFID's own signal transmission over long distances.
- Keep in mind the concept of "easy to lock, hard to unlock."
 - In terms of human-factor engineering, owners rarely need to unlock their car doors from a distance. For car owners, whether they want to get something from the car or drive, they need to open the door when they are nearby. Therefore, is it really necessary to have a long-distance unlocking function? For example, it is worth discussing the use of UWB signals with high-precision positioning capability to carry the unlocking signal. This will help prevent long-distance attacks.

For the foreseeable future, we believe that these RKE attacks will become more common. As SDR devices become cheaper and the supply chain becomes more global, vehicle manufacturers should take a serious look at key fob design and abandon the old defensive mindset. For example, the integration of keyless systems, which are increasingly accepted by car owners, can make attacks more difficult by combining the use of multiple wireless telecommunication systems.

In the end, it is often more efficient for car thieves to break the glass and enter the car directly. For example, the teenage car theft incident³⁰ in North America for the so-called Kia Challenge was a thorough demonstration of this, as the car involved was driven away via a simple USB interface after its windows were broken. Therefore, we would recommend that vehicle manufacturers focus more on engine startup anti-theft if cost is a constraint.

Security Recommendations and Predictions

We highlighted the high-risk attack surfaces in the previous sections, as well as the current cyberthreats that the automotive industry is facing as a whole. Many of these threats are well-known in the cybersecurity industry, and automotive organizations should use the experience and knowledge from other industries to create a tailored plan for their specific needs. As previously discussed, it is worth leveraging existing techniques and following proven security tactics.

Here are some security recommendations that decision-makers in the automotive industry should be aware of:

Although there are various kinds of open-source software that can be used to build car software quickly, these often do not include security. The ongoing Tesla Pwn2Own³¹ competition has also proven the importance of the software development life cycle (SDLC), as it shows that weaknesses in software can be used to attack users years later. Real progress is all about maintaining relative security while developing rapidly — therefore, we must invest more in security.

- OTA updates are an indispensable part of modern vehicle design, not only to improve the functionality of the vehicle through online updates but also to repair problems after they are discovered without having to return the vehicle to the factory. This not only increases safety but also saves possible costs in the future.
- Maintenance is valuable for vehicles. For increased convenience, modern vehicles have plenty of electronic equipment and are actually powerful mobile computers. Taking this into consideration, security requirements also need to increase, just as there should be real-time reporting of the vehicle's situation. This helps identify possible problems and prevent future issues. The existence of vehicle security operations center (VSOC) has also become indispensable.

Malicious actors evolve as quickly as the industry does, so we have a few predictions that automotive professionals should also be aware of:

- Ransomware will continue to affect the automotive supply chain in the near future and extend its target base to include cloud vendors and in-car components.
- Open-source vulnerabilities will affect more components in the automotive industry. Open-source software is common in the automotive industry and is heavily used in chips, hardware, firmware, operating system, and application levels. One illustrative case is the Log4j vulnerability, which puts Tesla vehicles and charging stations at risk.

- Radio signal attacks (replay, relay, jamming, MitM, and more) will increase.
- Malware will be implanted in IVI/telematics control unit (TCU) systems.
- AI-driven detection devices, such as advanced driver assistance systems (ADASs), will be affected more by generative adversarial networks (GANs). Since the introduction of GANs in 2014, many studies have suggested that they can be used to enhance the safety of ADASs. In the area of functional safety, GANs can be applied to image-to-image translation for super resolution and environmental light enhancement and object detection. In information security, GANs have been proposed for detecting forged information. Conversely, their design can also be used to help attackers avoid abnormal detection.
- There will be chip-level vulnerabilities and attacks. The chip-level design is not secure. In the past, hackers could use the vulnerability and pass through upper-level security protection (like operating system-level or application-level security protection).
- OTA will be a target. OTA is a critical component for modern cars to update to the newest or subscription-based software. Hackers can exploit this mechanism to compromise the flow or implant malicious code in upgraded software.
- Attackers can bypass the digital locks that manufacturers impose on a vehicle. Hackers will exploit vulnerabilities in digital locks to open/bypass the features that manufacturers try to place behind a paywall.

APPENDIX

Electric Vehicle Charging

According to the International Energy Agency's (IEA) Global EV Outlook 2022,³² electric vehicle ownership tripled from 2018 to 2021. The number of public charging stations has risen linearly along with this, not even taking into account home chargers and private charging stations by brand.

The International Electrotechnical Commission (IEC) 62196³³ report specifies the main types of charging piles currently in circulation.

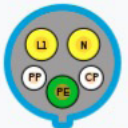
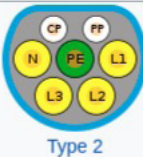
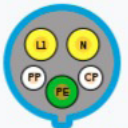
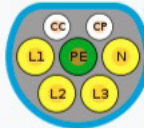
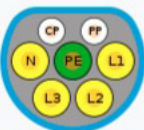
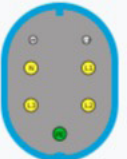
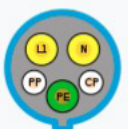
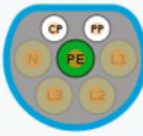
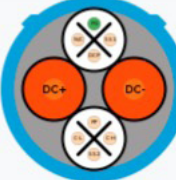
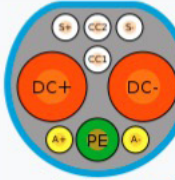

Power supply	United States	European Union	Japan	China
1-phase AC (62196.2)	 Type 1 (SAE J1772)	 Type 2 (DE, UK)	 Type 1 (SAE J1772)	 Type 2 (GB/T 20234.2)
3-phase AC (62196.2)	 Type 2 (SAE J3068)	 Type 3 (IT, FR; now deprecated)	—	—
DC (62196.3)	 EE (CCS Combo 1)	 FF (CCS Combo 2)	 AA (CHAdeMO)	 BB (GB/T 20234.3)
	—	—	 ChaoJi (planned)	—

Figure 15. Main types of charging piles from the IEC 62196 report³⁴

Image credit: International Electrotechnical Commission/IEC Webstore

Due to the different design objectives and safety regulations, we can basically classify the charging pile specifications in several ways.

AC/DC

Almost every battery is a direct current (DC) device, and this means we can only charge it with a DC charger. Currently, household electricity is usually supplied by alternating current (AC) power, so most vehicle manufacturers design on-board chargers on EVs to facilitate charging at home. This is also why EV charging stations use AC.

Due to various factors such as size, heat dissipation, energy efficiency, and of course, cost, the power of an on-board-charger is often relatively limited. In the case of the SAE J1772 type used in North America, charging with AC only provides up to 19.2 kilowatts of power, without taking into account conversion losses.

By connecting directly to the battery management system or battery-charging Ucharging stations, using DC charging can often provide far more power than AC charging. For example, the CCS1 charging specification inherited from J1772 can even provide up to 100 kilowatts of energy in DC mode.

CAN bus or PLC-charging piles must be designed to serve different vehicle types and even vehicles of different makes. Therefore, regardless of the charging system, the specifications and settings are initiated from the vehicle side. The charging pile passively provides the power to the vehicle within the pile specifications. Earlier J1772 charging piles did not necessarily use digital data transmission to communicate with vehicles but used a set of PWM signals to communicate with vehicles. This communication protocol is standardized in IEC61851, and this communication method reserves a status for CAN bus or PLC protocol (typically, reducing the duty cycle to no more than 5% will trigger handover status, which tells both electronic vehicle supply equipment [EVSE] and EVs to switch to CAN bus or PLC for further communication).

Security Issues Surrounding EV Charging

In this section, we will discuss the security situation around charging stations and technology connected to charging EVs. One of the challenges manufacturers and users face is the power of “analog.” For example, DC fast charging is high-voltage and high-current. This makes DC fast charging dangerous in many ways, and original design manufacturers (ODMs) and vehicle manufactures know it. This means there is not only a software interlock on CAN bus but also a timeless failsafe design.

TrendX research has also analyzed the weakness and the security design on the SCPI/VISA (Standard Commands for Programmable Instruments/Virtual Instrument Software Architecture) protocol,³⁵ which is widely used on test instruments. The security issues on SCPI are close to those surrounding the fast-charging protocol; for example, old data buses are without security design. Newer standards will cover security issues like TLS usage, but these are still on the way.

These problems are definite cybersecurity risks and will affect user safety if successfully exploited. Currently, ODMs implement multiple failsafe mechanisms to prevent fires or emergency situations. However, manufacturers and users shouldn't rely on these. Failsafe designs such as resistance monitoring, ultra high-speed fuses, or proximity sensors are the last barriers for user safety, and hence they should not be the first response to a cybersecurity issue.

Analysis of Charging Protocols, Designs, and New Standards

Tencent X-in-the-Middle Attack on Tesla Pile

In Black Hat 2021, Tencent's security team published research³⁶ on the Tesla Plug-and-Charge pile. The charging pile they researched is a DC-type/CAN bus-based pile, and the team pointed out that Tesla is using part of the GB/T type protocol combined with their private protocol.

The main idea behind the MitM attack is the CAN bus message Tesla used to communicate with the charging piles. The CAN bus is widely used in vehicles and works as broadcasting topology. However, there's no authentication or auditing method, so the CAN bus can definitely suffer from an MitM attack.

We can also call this an example of spoofing apps or CAN bus messages to achieve free charging. The Tesla charging piles identify users by app or cloud and CAN bus vehicle identification number (VIN) information. The attacker spoofs the VIN between app or charging piles and EV or charging piles to freely charge their car.

CHAdemo's Unique Design

CHAdemo³⁷ (developed as a fast-charging system for battery-powered electric vehicles in 2010) is the only charging protocol that considers vehicle to everything (V2X) and vehicle to grid (V2G) in their specifications. The CHAdemo 2.0 even extends the V2G part to cover power outlets from the vehicle. TEPCO, also known as Toden, designed this technology and kept the future in mind while it made CHAdemo specifications. For example, it estimated the impact and benefit for the power grid in a city or even a country where EV takes the place of gasoline vehicles.

The company analyzed the impact of using quick chargers with the limitations of the Tokyo power grid. Its plan includes taking EV charging as part of power grids, and CHAdemo 2.0 gives EVs an option to outlet 500KVA back to grid. However, this plan, (and including EV charging into city grids in general) has critical infrastructure problems and security implications.

To recall, most charging piles are passive to EVs, and CHAdemo has the same design. The charging control unit on the EV will handle the charging procedure and even power outlets while acting as part of the power grid.

In previous research, we can see that most CAN bus traffic is in plain text and it's not hard to perform MitM attacks. Tencent's X-in-the-middle attack can achieve free charging by exploiting the billing procedure while in Plug-and-Charge. While considering EVs as part of the power grid, we can't take these security implications lightly.

IEC 15118 and the Plug-and-Charge System

In the authors' location, Taipei, Taiwan, most of the fast-charging stations are currently set up by the car manufacturers themselves. For example, Tesla owners go to Tesla's charging stations, and Toyota owners go to Toyota stores or their own for charging. However, Plug-and-Charge stations are starting to appear at highway rest stops and other places. It is expected that Plug-and-Charge will become the mainstream of charging piles in the future when EVs become popular.

Currently, different types of charging piles have different data chains, specifications, and even billing methods. This is obviously detrimental to the development of Plug-and-Charge, leading to the creation of the IEC 15118³⁸ standard.

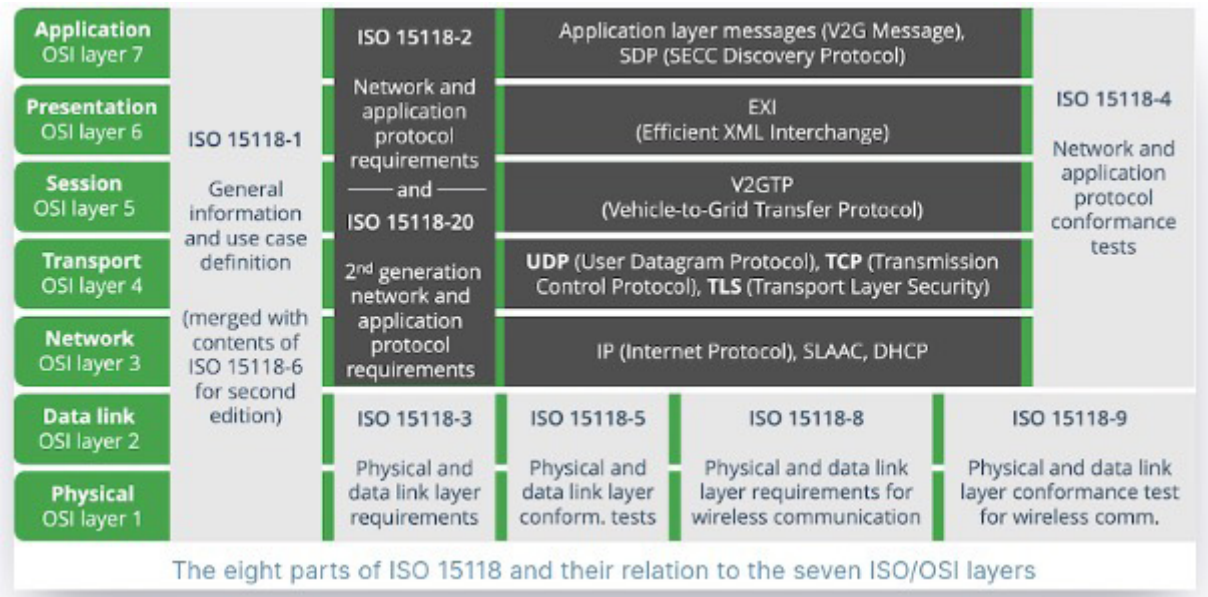


Figure 16. IEC 15118 standards³⁹

Image credit: Marc Mültin/Switch-EV.com

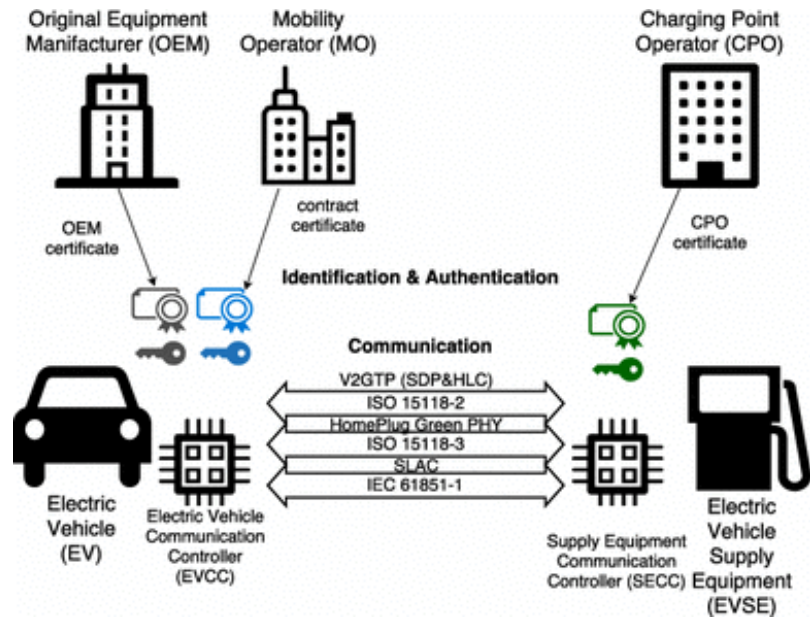


Figure 17. System overview of ISO 15118⁴⁰

Image credit: Kaibin Bao et al/Researchgate.net

If IEC 15118 becomes a common standard for charging stations in the future, we can see from the preceding diagram that the communication between charging stations and EVs will introduce various features of current modern networks such as OSI-7Layer, TLS, and HTTP/2 usage. By introducing Open Systems Interconnection (OSI) layering, it does not matter which communication method is used by the charging plug. The introduction of OSI layering will make it possible to use the same protocol stack to achieve universal Plug-and-Charge regardless of the communication method used by the charging plug, such as CAN bus or PLC.

However, in the current iteration of IEC 15118, some potential problems have been identified by relevant members, such as whether the process of key exchange is secure enough or whether the proximity response has not been designed with a timeout and therefore might lead to DOS attacks.

Issues With High-Risk Attack Surfaces

Plug-and-Charge Risks

The authors believe that Plug-and-Charge is a very important part of the future development of the EV industry, and that widespread and mature Plug-and-Charge stations will be an important key to overcoming the mileage anxiety of EV users. Although IEC 15118 is not yet on the road, the author has found some local fast-charging pile products⁴¹ in Taiwan that are Plug-and-Charge-ready.

We can see that the pile in Taiwan already supports multiple communication methods such as RFID, Ethernet, 3G/4G, Wi-Fi, and OCPP (Open Charge Point Protocol). This can easily seem to benefit Plug-and-Charge features, like billing and operator management. Compared to the current fast-charging piles set up by the manufacturers themselves, such charging pile products are more appealing targets for hackers.

EVs' Charging Port Can Be Hacked by Radio Signal Replay Attack

Because of the lack of radio secure protocol implementation, the Tesla charging port can be opened by using a simple radio record/replay attack. In a case⁴² reported by RTL-SDR, we can see that the charge port protocol doesn't have any rolling code features, and the same data can trigger different Tesla charge ports and acts like a super key.

References

- 1 Dustin Childs. (May 18, 2022). *Zero Day Initiative*. "Pwn2Own Vancouver 2022 - The Results." Accessed on Nov. 14, 2022, at <https://www.zerodayinitiative.com/blog/2022/5/18/pwn2own-vancouver-2022-the-results>.
- 2 Wu HuiYu and Li YuXiang. (May 7, 2021). *Blackhat Asia 2021*. "X-in-the-Middle : Attacking Fast Charging Piles and Electric Vehicles." Accessed on Nov. 14, 2022, at <https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-Wu-X-In-The-Middle-Attacking-Fast-Charging-Piles-And-Electric-Vehicles.pdf>.
- 3 Reuters. (March 1, 2022). *Reuters*. "Toyota suspends domestic factory operations after suspected cyber attack." Accessed on Nov. 14, 2022, at <https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/>.
- 4 David Fiser. (March 3, 2021). *Trend Micro*. "Identifying Weak Parts of a Supply Chain." Accessed on Nov. 14, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/identifying-weak-parts-of-a-supply-chain>.
- 5 Dan Goodin. (March 30, 2022). *Ars Technica*. "Lapsus\$ and SolarWinds hackers both use the same old trick to bypass MFA." Accessed on Nov. 14, 2022, at <https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/>.
- 6 David Colombo. (Jan. 25, 2022). *Medium*. "How I got access to 25+ Tesla's around the world. By accident. And curiosity." Accessed on Nov. 14, 2022, at https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028.
- 7 Office of the Maine Attorney General. (n.d.). *Office of the Maine Attorney General*. "Data Breach Notifications." Accessed on Nov. 14, 2022, at <https://apps.web.maine.gov/online/aeviewer/ME/40/ec8e5dc7-e259-4847-8a94-23b789691b54.shtml>.
- 8 Coya Vallejo Hägi. (Jan. 13, 2022). *Digitec.ch*. "Cyber attack on car dealer Emil Frey." Accessed on Nov. 14, 2022, at <https://www.digitec.ch/en/page/cyber-attack-on-car-dealer-emil-frey-22420>.
- 9 Office of the Maine Attorney General. (n.d.). *Office of the Maine Attorney General*. "Data Breach Notifications." Accessed on Nov. 14, 2022, at <https://apps.web.maine.gov/online/aeviewer/ME/40/62ea1496-1f06-4120-aa97-fe1952bd418b.shtml>.
- 10 Ionut Ilascu. (March 1, 2022). *Bleeping Computer*. "NVIDIA confirms data was stolen in recent cyberattack." Accessed on Nov. 14, 2022, at <https://www.bleepingcomputer.com/news/security/nvidia-confirms-data-was-stolen-in-recent-cyberattack/>.
- 11 Mullen Coughlin LLC. (March 4, 2022). *New Hampshire Department of Justice*. "Notice of Data Event." Accessed on Nov. 14, 2022, at <https://www.doj.nh.gov/consumer/security-breaches/documents/fair-rite-products-20220304.pdf>.
- 12 Hayes Connor Solicitors. (n.d.). *Hayes Connor Solicitors*. "LHS Auto UK contact current and former employees to report data breach." Accessed on Nov. 14, 2022, at <https://www.hayesconnor.co.uk/group-actions/lsh-uk-contact-current-and-former-employees-to-report-data-breach/>.
- 13 Bill Toulas. (May 23, 2022). *Bleeping Computer*. "General Motors credential stuffing attack exposes car owners info." Accessed on Nov. 14, 2022, at <https://www.bleepingcomputer.com/news/security/general-motors-credential-stuffing-attack-exposes-car-owners-info/>.
- 14 Red Packet Security. (June 13, 2022). *Red Packet Security*. "Cuba Ransomware Victim: Etron." Accessed on Nov. 14, 2022, at <https://www.redpacketsecurity.com/cuba-ransomware-victim-etron/>.
- 15 Numaan Huq, Craig Gibson, and Rainer Vosseler. (Aug. 18, 2020). *Trend Micro*. "The Cybersecurity Blind Spots of Connected Cars." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.
- 16 Matthew Humphries. (Jan 13, 2022). *PCMag*. "Teenage Hacker Gains Remote Control of 25 Teslas in 13 Countries." Accessed on Nov. 14, 2022, at <https://www.pcmag.com/news/teenage-hacker-gains-remote-control-of-25-teslas-in-13-countries>.
- 17 NBC News. (June 16, 2022). *YouTube*. "Thieves Turning To Cutting Edge Technology To Steal Cars." Accessed on Nov. 14, 2022, at <https://www.youtube.com/watch?v=rx5mjOEixMY>.
- 18 inf0sec1. (July 10, 2022) *Twitter*. "Playing around with #FlipperZero..." Accessed on Nov. 14, 2022, at https://twitter.com/inf0sec1/status/1545804925522829313?t=4-n6SQ3H8OhD_WFXwiLZMg&s=19.

- 19 Rolling Pwn. (n.d.). *GitHub*. "Rolling Pwn Attack." Accessed on Nov. 14, 2022, at <https://rollingpwn.github.io/rolling-pwn/>.
- 20 Jonathan Andersson et al. (Jan. 15, 2019). *Trend Micro*. "A Security Analysis of Radio Remote Controllers for Industrial Applications." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
- 21 Jonathan Andersson et al. (Jan. 15, 2019). *Trend Micro*. "A Security Analysis of Radio Remote Controllers for Industrial Applications." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf.
- 22 Hacking Into Your Heart. (July 17, 2022). *GitHub*. "Replay-based Attack on Honda and Acura Vehicles." Accessed on Nov. 14, 2022, at <https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty>.
- 23 Hacking Into Your Heart. (July 17, 2022). *GitHub*. "Replay-based Attack on Honda and Acura Vehicles." Accessed on Nov. 14, 2022, at <https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty>.
- 24 Colin Urquhart et al. (Oct. 2019). *Research Gate*. "Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach." Accessed on Nov. 14, 2022, at https://www.researchgate.net/figure/Rolling-Code-Overview_fig2_336715499.
- 25 Samy Kamkar. (2015). *DefCon 2015*. "Drive It Like You Hacked It." Accessed on Nov. 14, 2022, at <https://samy.pl/defcon2015/>.
- 26 Starvlab. (n.d.). *Starvlab*. "Honda-Civic Keyfob system affected by counter resynchronization attack." Accessed on Nov. 14, 2022, at <http://starvlab.qianxin.com/?p=409>.
- 27 Starvlab. (n.d.). *Starvlab*. "Honda-Civic Keyfob system affected by counter resynchronization attack." Accessed on Nov. 14, 2022, at <http://starvlab.qianxin.com/?p=409>.
- 28 Sultan Khan. (May 15, 2022). *NCC Group*. "Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks." Accessed on Nov. 14, 2022, at <https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/>.
- 29 Lennert Wouters, Benedikt Gierlichs, and Bart Preneel. (Aug. 11, 2021). *Ruhr-Universität Bochum*. "My other car is your car: compromising the Tesla Model X keyless entry system." Accessed on Nov. 14, 2022, at <https://tches.iacr.org/index.php/TCHES/article/view/9063>.
- 30 Brad Anderson. (Aug. 2, 2022). *Carscoops*. "When Is This Going To Stop? TikTok's Latest 'Kia Challenge' Encourages Users To Steal Cars." Accessed on Nov. 14, 2022, at <https://www.carscoops.com/2022/08/social-medias-kia-challenge-has-led-to-a-spike-in-car-thefts/>.
- 31 Kieran Press-Reynolds. (May 20, 2022). *Insider*. "The world's top hackers are competing to break into a Tesla. The winner gets \$600,000 and keeps the car." Accessed on Nov. 14, 2022, at <https://www.insider.com/pwn2own-hacking-tesla-contest-cybersecurity-tesla-2022-5>.
- 32 International Energy Agency. (May 2022). *IEA*. "Global EV Outlook 2022." Accessed on Nov. 14, 2022, at <https://www.iea.org/reports/global-ev-outlook-2022>.
- 33 International Electrotechnical Commission. (Feb. 18, 2016). *IEC Webstore*. "Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories." Accessed on Nov. 14, 2022, at <https://webstore.iec.ch/publication/24204>.
- 34 International Electrotechnical Commission. (Feb. 18, 2016). *IEC Webstore*. "Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories." Accessed on Nov. 14, 2022, at <https://webstore.iec.ch/publication/24204>.
- 35 Philippe Lin et al. (Jan. 28, 2020). *Trend Micro*. "Security Dive: Devices Supporting SCPI, VIS Protocols." Accessed on Nov. 14, 2022, at https://www.trendmicro.com/en_us/research/20/a/security-analysis-of-devices-that-support-scp-i-and-visa-protocols.html.
- 36 Wu HuiYu and Li YuXiang. (May 7, 2021). *Blackhat Asia 2021*. "X-in-the-Middle: Attacking Fast Charging Piles and Electric Vehicles." Accessed on Nov. 14, 2022, at <https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-Wu-X-In-The-Middle-Attacking-Fast-Charging-Piles-And-Electric-Vehicles.pdf>.
- 37 CHAdeMO. (n.d.). *CHAdeMO*. "About Us." Accessed on Nov. 14, 2022, at <https://www.chademo.com/about-us>.

- 38 Marc Mültin. (Oct. 11, 2021). *Switch EV*. "What is ISO 15118?" Accessed on Nov. 14, 2022, at <https://www.switch-ev.com/knowledgebase/what-is-iso-15118>.
- 39 Marc Mültin. (Oct. 11, 2021). *Switch EV*. "What is ISO 15118?" Accessed on Nov. 14, 2022, at <https://www.switch-ev.com/knowledgebase/what-is-iso-15118>.
- 40 Kaibin Bao et al. (Feb. 2018). *Research Gate*. "A threat analysis of the vehicle to grid charging port protocol ISO 15118." Accessed on Nov. 14, 2022, at https://www.researchgate.net/figure/System-overview-of-the-ISO-15118-protocol_fig1_319431250.
- 41 E-value. (n.d.). *Fortune*. "DC Charging Pile." Accessed on Nov. 14, 2022, at <https://www.fortune.com.tw/tw/attached/product/evi/tw/DC%E7%9B%B4%E6%B5%81%E5%85%85%E9%9B%BB%E6%A8%81.pdf>
- 42 RTL-SDR. (April 5, 2022). *RTL-SDR*. "Tesla Charging Ports Opened With HackRF Replay Attack." Accessed on Nov. 14, 2022, at <https://www.rtl-sdr.com/tesla-charging-ports-opened-with-hackrf-replay-attack/>



Learn more about VicOne
by visiting www.vicone.com
or scanning this QR code

