+300 pages of application knowledge about vehicle security according to UN Regulation No. 155, ISO/SAE 21434 & beyond

1000 THINGS WORTH KNOWING IN AUTOMOTIVE CYBERSECURITY

The Essential Guide to ISO/SAE 21434

SECOND EDITION

READING SAMPLE

CYEQT
KNOWLEDGE BASE

CYBERSECURITY AWARENESS

1

Chapter contents:

1. CYBERSECURITY AWARENESS

1. CYBERSECURITY AWARENESS

Cybercrime is on the rise in the connected world of today. It needs to be addressed by organizations who wish to protect their businesses. The growing threat landscape is also having an impact on regulators. More and more authorities are drafting and releasing documents which include specific requirements for handling cybersecurity. This includes directives such as the NIS2 (network and information systems directive 2022/0383) which includes measures for tackling cybersecurity in the EU by ensuring, among other things, a culture of security within organizations [353]. The NIS2 specifies penalties for non-compliance, including fines of up to €10mn or 2% of global annual revenue for failing to meet security requirements or failing to report incidents [354]. In addition to the organizational measures that are covered by the NIS2, the cybersecurity requirements for software and hardware products with digital elements are defined by the European Cyber Resilience Act (CRA). The CRA serves as a legal framework for ensuring cybersecurity throughout the product lifecycle [355]. Cybersecurity has therefore become the new feature of quality in the connected world of today. This applies to all industries, including the automotive industry. The wave of digital innovations, such as autonomous driving and connectivity which are driving a transformation of the automotive industry, is turning modern cars into tempting targets for cyberattacks. The failure to recognize the growing importance of cybersecurity has already led to a dramatic loss of consumer trust in brands and new vehicle features, due to the increasing threat to vehicle safety from malicious attackers. However, some organizations are still not aware that cybersecurity has become a value chain issue and a new feature of quality where road vehicles (including passenger cars, motorbikes, trucks, and trailers) are concerned.

Being aware of cybersecurity means understanding the specific cyber threats to the automotive ecosystem and their potential impact on vehicles, and the relevance of new regulations and standards. Emphasizing the importance and necessity of cybersecurity in the automotive industry requires a common understanding of what the term cybersecurity means. Several authorities and sources provide a definition of cybersecurity.

The ISO/SAE 21434 standard, “Road Vehicles – Cybersecurity Engineering”, defines cybersecurity as follows:

> *“Condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components [145].”*

The National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, defines cybersecurity as:

> *“The ability to protect or defend the use of cyberspace from cyberattacks [199]."*

The German Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik) describes cybersecurity as a discipline:

> *“Cybersecurity deals with all aspects of security in information and communication technology that extends the classical IT security to the entire cyberspace [45]."*

The European Network and Information Security Agency (ENISA) provides a more detailed description:

> *“Cybersecurity covers all aspects of prevention, forecasting, tolerance, detection, mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability, Robustness, Survivability, Resilience, Accountability, Authenticity and Non-repudiation [81]."*

Among the above definitions and the definitions of other relevant sources and references in the cybersecurity domain, we see the widening scope of cybersecurity as it becomes an increasingly relevant aspect of current industrial revolution. Nevertheless, it is essential to establish a common understanding of cybersecurity among organizations and individuals who work together to achieve the primary goal of cybersecurity:

> Protecting cyber assets against unauthorized access or attacks.

An asset is defined as any type of system, component, device, or data that supports information-related activities. It is worth to be protected and defines a property (i.e. confidentiality, integrity and/or availability) crucial for a stakeholder.

1.1 Cybersecurity incidents are not new

Over the years, we have seen several events that have demonstrated that security breaches and hacks in the automotive industry (as well as in other industries) occur through sophisticated attacks. Such incidents usually arise for a variety of reasons:

- Lack of cybersecurity awareness and implementation errors made by developers
- Technical weaknesses from improper cybersecurity design
- Poor quality of development (e.g. missing processes and documentation)
- Lack of attention from senior management and therefore fewer resources being allocated to cybersecure products
- Lack of clear responsibilities of distributed cybersecurity activities along the supply chain (i.e. between customer and supplier) or with service providers

This section gives an overview of the most prominent and significant hacks in the automotive realm.

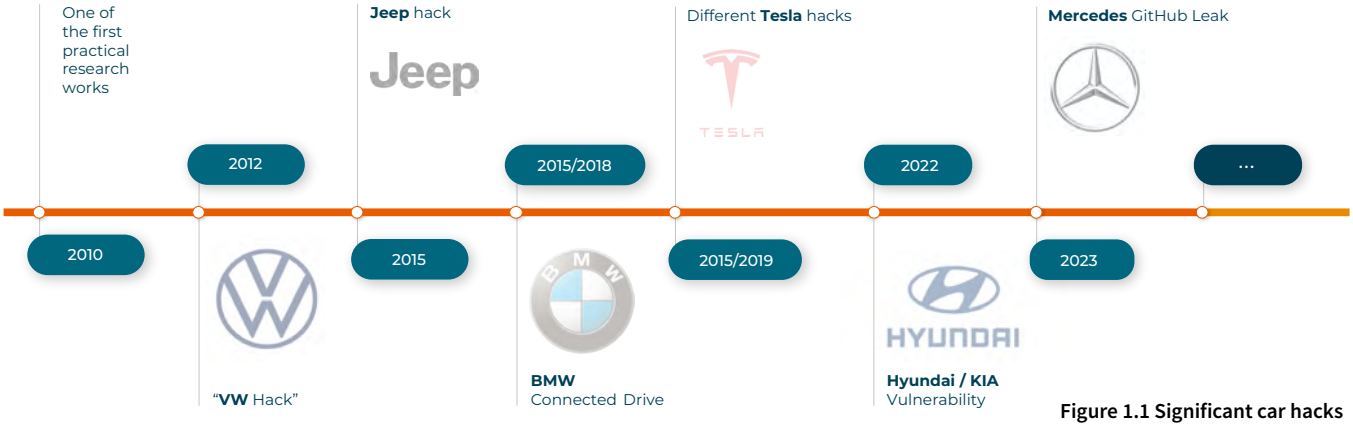

Figure 1.1 Significant car hacks

1.1.1 Experimental hack of a modern automobile (2010)

One of the first automotive hacks in a practical environment was performed by a group of researchers from the United States (US) [156]. The researchers evaluated the weaknesses specific to modern cars and revealed the vulnerability of the underlying system structure. One of the major findings was that the researchers were able to bypass critical safety systems and thereby control a variety of functions while ignoring the driver's input (e.g. disabling brakes or stopping the engine). This was possible because of the need for interconnection between multiple Electronic Control Units (ECUs). This interconnection is provided by several internal bus systems like Controller Area Network (CAN), which is a technology used for enabling communication between the different control units within the vehicle.

During the demonstration, the researchers gained access to the vehicle CAN bus network via an On-Board Diagnostics (OBD) port which provides direct and standard access to diagnostic and maintenance functions. These OBD ports are generally used in gerage or service stations The researchers were able to control different ECUs to brake selectively (per wheel), control the throttle and shift gears. First, they tested and tried out stationary changes by sitting in the car and having direct access to it.

The following hacks were possible:

- **Radio:** Control of the volume and preventing the user from resetting it, including the ability to produce disturbing clicks and chimes at arbitrary frequencies.
- **Instrument panel:** Display of arbitrary messages, falsification of fuel level and speedometer reading, adjustment of instrument lighting
- **Body controller:** Locking and unlocking the doors, jamming the door locks, popping the trunk, adjustment of interior and exterior lighting levels, sounding the horn, disabling and enabling the window relays and windshield wipers, continuously shooting windshield fluid
- **Engine:** Boosting the Revolutions Per Minute (RPM) of the engine momentarily by disturbing the engine timing by altering the learned crankshaft angle sensor error value which disables cylinders (even when wheels were spinning), and eventually disabling the engine (and making it impossible to restart it)
- **Brakes:** Locking of individual wheel brake or all brakes, e.g. locking of only one brake, locking against manual over-riding even when the power circuit is interrupted and the battery is removed
- **Heating, ventilation, and air conditioning:** Control of the Air Condi-tioning (AC) unit
- **Generic Denial of Service (DoS):** Preventing communication between individual components on the CAN bus

The research was often criticized because it required immediate physical access to the vehicle. Later, the researchers demonstrated that they could also carry out the attacks remotely through the Moving Picture Experts Group Audio Layer 3 (MP3) parser of the radio, the Bluetooth stack and through the telematics unit.

1.1.2 Jeep hack (2015)

The 2015 Jeep Hack was carried out by two researchers from the U.S.: Charlie Miller and Chris Valasek [177]. Due to its media impact, it remains one of the most famous automotive hacks. At the center of the hack was the Jeep Cherokee, manufactured in 2014, which was chosen because its architecture made it easy to compromise two different CAN networks via the head unit of the infotainment system. The researchers gained access to ECUs in both the Controller Area Network - Interior High Speed (CAN-IHS), which is usually used by comfort systems and interior modules such as radio and climate controls, and the Controller Area Network - Class C (CAN-C), which connects, among other things, control units for engine management to all the physical components of the vehicle. During their demonstration, they identified several different attack vectors or, in other words, potential entry points for attackers [95]:

- Passive anti-theft system
- Tire Pressure Monitoring System (TPMS)
- Remote keyless entry/start
- Bluetooth
- Radio data system
- Wireless Fidelity (Wi-Fi)
- Telematics/Internet/apps

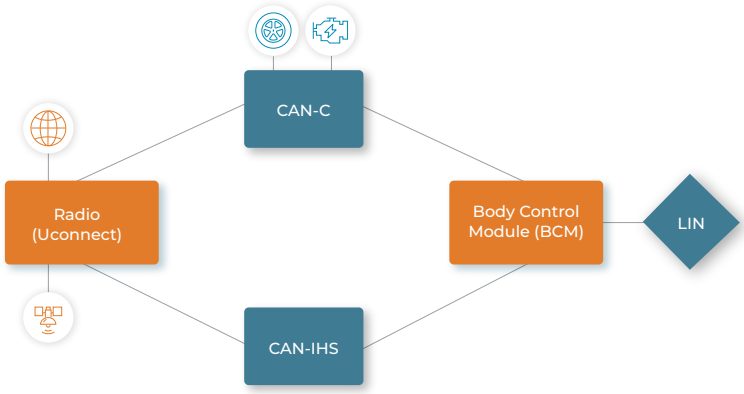

Figure 1.2 Simplified Jeep Cherokee architecture diagram [95]

In this particular hack, the infotainment system (i.e. the Uconnect radio, which is manufactured by Harman Kardon and includes a cellular modem) was hacked. By analyzing the attack surfaces, it was possible to identify the design of the Uconnect infotainment system network as the most vulnerable feature of the vehicle. The head unit of the Uconnect system communicates with other safety-relevant electronic modules in the car via the CAN-IHS bus. Uconnect also uses electronic message communication with other electronic modules in the vehicle via CAN-C. The Uconnect head unit has a point-to-point (PPP) interface with Sprint's (a telecommunications company) Third Generation (3G) services. PPP protocols are direct data link layer communication protocols between two routers without any intervening host or network.

By exploiting the cellular network, a remote attack was possible. The researchers were also able to access all the vehicles in the Fiat Chrysler fleet which had been equipped with the Harman Kardon infotainment system. In other words, it was possible to hack (remotely) other cars in the Fiat Chrysler fleet because every car that had this head unit was on the cellular network.

The Jeep hack caused a recall of 1.4 million vehicles manufactured by Fiat Chrysler, including Jeep, Dodge and Ram Trucks. Besides the media attention and reputational loss, the stock price of Fiat Chrysler was significantly impacted, and the stock value collapsed [177]. In the event of cyberattacks, all automotive players can face similar consequences in the form of financial losses and loss of reputation.

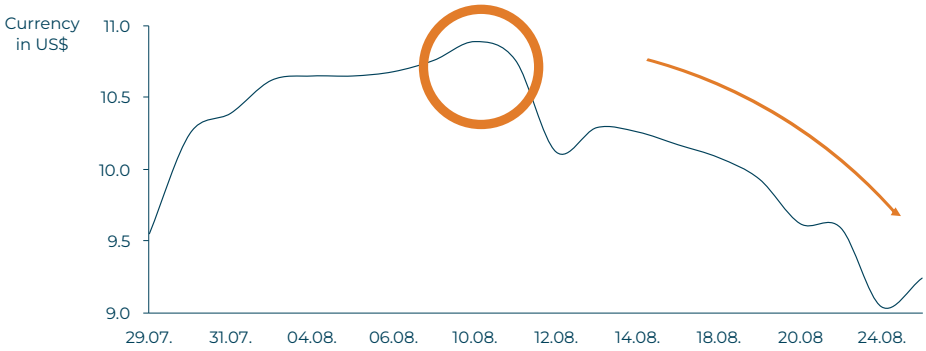

Figure 1.3 Impact of Jeep hack on Fiat Chrysler stock value in 2015

1.1.3 Other relevant hacks

Listing every single hack or cybersecurity incident that has occurred in the automotive industry over the last ten years is far beyond the scope of this section. The following is therefore just a selection of relevant examples that show that even small security gaps and weaknesses can lead to serious consequences if cyber risks are not properly managed.

2012: VW hack

A group of researchers from the University of Nijmegen and the University of Birmingham managed to gain access to the systems of various automobiles using the Radio Frequency Identification (RFID) chips (built into the Megamos immobilizer transponder system developed by Motorola) using a brute-force attack to start the vehicles by remote ignition [309]. However, this problem was not confined to the Volkswagen (VW) group. The immobilizer was used by several other car manufacturers including Volvo, General Motors (Chevrolet, Holden, Cadillac) and Fiat Chrysler Automobiles (Fiat, Jeep, Maserati, Ferrari). In 2013, Volkswagen filed a lawsuit against the scientists in a British court in an attempt to prevent them from publishing their findings. As a consequence, the hack of the Megamos system became known as the "VW hack".

2015: BMW hacked via ConnectedDrive

In 2015, a security expert was able to unlock BMW (Bayerische Motoren Werke) cars equipped with ConnectedDrive within minutes. The "ConnectedDrive" function is essentially based on a Subscriber Identity Module (SIM) card permanently installed in the car, which enables the vehicle to maintain contact with the manufacturer's data center [52]. Via a browser or the corresponding app, the user can also exercise corresponding functions depending on the license which is activated.

A key tool during the researcher's security analysis was a particular control unit. This was extremely helpful at one point because the hacker initially overcame almost all the obstacles to the break-in but did not succeed in hacking the car [119]. This was because the hacker's message to the car did not include the chassis number of the BMW car which was the target of the attack. However, instead of breaking off communication with the hacker, the control unit responded with an error message which included, as the sender, the missing chassis number. This enabled the hacker to succeed on the second attempt. As the same symmetrical keys are used for the cryptographic functions in all vehicles equipped with ConnectedDrive, accessing one car meant that the entire fleet of BMW cars was vulnerable.

This hack can be regarded as the starting point for dedicated automotive cybersecurity activities in the E/E development of BMW.

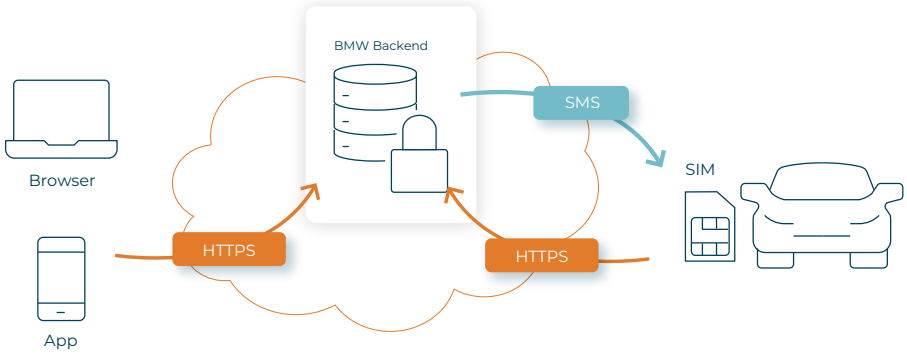

Figure 1.4: "ConnectedDrive" function

2018: Security vulnerabilities in infotainment systems of BMW vehicles

Further weaknesses in BMW vehicles were discovered by security researchers in 2018 [248]. The researchers exploited a vulnerability in the infotainment system used in various BMW models to gain access to the vehicles. In their publication describing 14 security gaps discovered in various BMW models, the researchers explained that attackers could gain root access to the CAN bus of the cars, both locally and remotely.

2019: BMW and Hyundai targeted by OceanLotus (Advanced Persistent Threat (APT) 32)

In 2019, the cyber espionage group OceanLotus (APT32) conducted a targeted operation with the aim of spying on BMW and Hyundai [231]. The hackers used a program called Cobalt Strike to infiltrate a BMW computer. The tools which were used probably triggered an alarm in BMW's network monitoring system. The South Korean car manufacturer Hyundai was hit by fake websites. The aim was to obtain information about the target of the attack and possibly access login details. This attack had an impact on the infrastructure rather than the vehicle itself. However, these two areas are always interdependent, e.g. when providing software updates over the air [323]. The targets of OceanLotus, whose operations are allegedly in line with Vietnamese state interests, are “international companies investing in Vietnam’s manufacturing, consumer goods and hospitality industries” [231]. Vietnam is home to a number of fast-growing vehicle manufacturers and various manufacturing plants of foreign companies. VinFast, the country’s first domestic brand, was launched in 2017 and the first vehicles were introduced a year later. The initial public offering (IPO) on the stock market was launched in 2023 [324].

2019: FordPass security flaw

Strictly defined, the FordPass incident was not a hack. But it demonstrated the presence of a small bug in Ford’s FordPass system [111]. FordPass is a smartphone app that allows drivers to use their phone to access several vehicle functions and obtain additional information about the car. This includes starting, locking and unlocking the vehicle remotely, and tracking the vehicle’s precise location. A man who rented a Ford Expedition and connected the car to the FordPass app was still able to control vehicle features for five months after returning the rental car. Although he immediately informed Ford about the issue, his access was not revoked for a long time. This shows a lack of awareness and attention to cybersecurity and data protection on the part of the company, which would cause damage to their reputation and a loss of trust among customers.

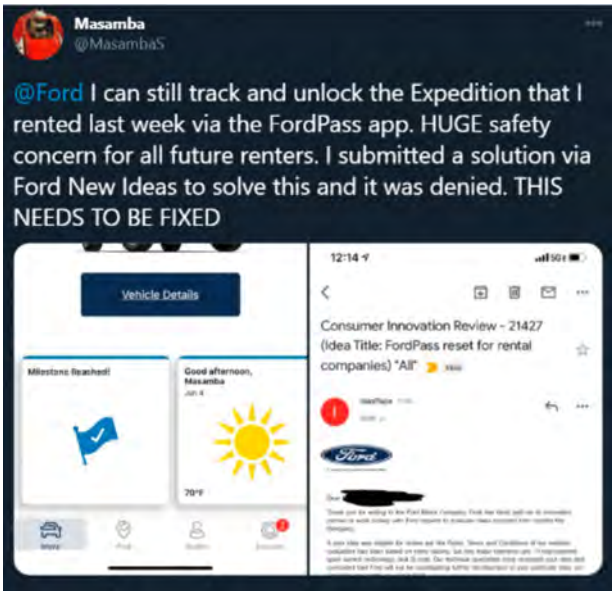

Figure 1.5 Customer addresses FordPass bug on Twitter

2019: Tesla gets stolen by means of key fob hack

Most modern cars allow their owners to remotely unlock the doors or sometimes even start the engine using a key fob. Though certainly not new, key fobs are now one of the most used car technologies and are regarded as a standard feature when buying a new car. However, this convenience goes hand in hand with small risks of the exploitation of security flaws in the key fobs that allow hackers to unlock the car. The risk of being subject to such a key fob relay attack seems to be quite low as the hacker must be close enough to scan it with an RFID device. But there are plenty of cases where the thieves simply stand outside the house and capture the signal.

Nevertheless, in 2019 two accomplices were able to unlock a Tesla Model S in less than 30 seconds [121]. While one hacker reached the location of the original key with a gadget capable of picking up the signal from the key fob, another hacker stood next to the car with a device anticipating the key fob signal. When the signal was found, it could be relayed from one unit to another, allowing the vehicle to be activated and operated. As Tesla is offering their cars at an upscale price, customers consequently have higher expectations. Such attacks can therefore easily lead to a loss of reputation and financial value.

2020: Cyber researchers fool autonomous vehicle systems

In a paper with the title “Phantom of the Advanced Driver Assistance System (ADAS)”, researchers demonstrated that they could enable an autonomous vehicle’s autopilot to apply the brakes incorrectly in response to "phantom images" projected onto a road or billboard [88]. This was achieved by tricking the cars into perceiving depthless projections (phantoms) of objects such as a person standing on the street or fake street signs. The researchers showed that they could deceive the ADAS into believing that phantom traffic signs projected for 125 milliseconds in advertisements on digital billboards are real, as in Figure 1.6 [244]. Such demonstrations show how easily, in the course of what are called adversarial attacks, attackers can exploit the perception of vehicles in order to manipulate them and harm the driver, passengers or pedestrians. This can be done without special expertise and solely by using, for example, a commercial drone or an inexpensive image projector.

Figure 1.6
Tesla’s autopilot fooled by phantom images

2022: Software developer cracks Hyundai car security with Google search

This hack is a perfect example of why cybersecurity-related information should always be kept confidential. In this case, a hacker was able to exploit the infotainment system in his 2021 Hyundai Ioniq SEL. To start with, he needed to obtain the firmware image, which was encrypted. Secondly, to get the system to accept a software update containing his maliciously crafted software, he needed to sign it with the correct key.

By searching the website of the IVI manufacturer, Mobis, he discovered that the algorithm used to decrypt the software was AES-CBC (Advanced Encryption Standard-Cipher Block Chaining). As it turned out, Mobis were using the exact same key from the example in the AES-CBC specification document. He was therefore able to decrypt the extracted software. After modifying it, he had to sign it correctly for the system to accept it. In the decrypted source code, he found the public key used to verify software updates. He then searched for this public key online and, almost unbelievably, found that it appeared in a tutorial on implementing RSA. RSA stands for Rivest–Shamir–Adleman and is a public-key cryptosystem, one of the oldest of those which are widely used for secure data transmission. The tutorial included the corresponding private key, which the hacker then used to sign his malicious software. This means that for both cryptographic operations (AES-CBC and RSA) Hyundai used secret keys that can be found online [325]!

2023: Mercedes-Benz source code exposure

To emphasize the need for cybersecurity awareness, let us consider the incident at Mercedes-Benz, where it was discovered that an employee's authentication token had been shared in a public GitHub repository. Using this token, anyone could gain access to Mercedes-Benz's GitHub Enterprise server, which contained design documents, passwords, API keys, Mercedes source code and other highly confidential information. This incident highlights the strength of the connection between product security and classical information technology (IT) security, since the exposed information could be used by an attacker to prepare an exploit against the product. Mercedes declined to disclose whether any third party had accessed their private repository [326].

2024: Hacking the infotainment system of a 2023 Dacia

There is now a growing number of automotive hacking enthusiasts who are sharing their “hobby” through blog posts which are available to the public. On the one hand, this should raise the awareness of car manufacturers regarding the vulnerability of their products and the need to fix the problem. On the other hand, it shows that there is a growing number of attack surfaces that are open to hackers.

In one such example, a white-hat automotive hacker exploited the infotainment system of his Dacia Sandero. He discovered a hint of a potential vulnerability (in this case, a script that allows the running of a root called “autorun.sh”) in other hacking forums. By reverse engineering the firmware of his target device, he discovered that this “autorun.sh” backdoor is missing in the latest version, so he decided to create his own new exploit. He eventually fooled the infotainment into accepting a fake map update from his device and was able to acquire root access. This example is one of many in which individual enthusiasts are able to find vulnerabilities and exploit them [327].

2024: Extracting Secure Onboard Communication (SecOC) keys from a 2021 Toyota RAV4 Prime

As cybersecurity becomes more prominent in the automotive ecosystem, hackers are becoming smarter and getting better at circumventing cybersecurity measures. For this attack on Toyota cars, the hackers were able to bypass multiple measures, starting with extraction of the firmware from the debug ports, although they were protected. The hackers used fault injection to bypass the debug port protection. Then, by reverse engineering the firmware they found out which UDS (Unified Diagnostic Services) routines were used for updating the SecOC keys. Through further reverse engineering, they figured out that the keys were stored in RAM rather than in a protected memory region. They were even able to reverse engineer the bootloader software to perform an update to flash their own code and finally extract the keys.

Of course, such a sophisticated attack required a lot of time and expertise. But it only takes a single exploit to clear the way for hackers to take advantage of this vulnerability [328].

2024:Troy PD busts ‘prolific’ auto-theft ring responsible for over 400 cars being stolen

In the U.S., an auto-theft ring was discovered and the thieves arrested in early 2024. Four hundred vehicles worth $8 million were stolen in Oakland, Washtenaw, Macomb, and Wayne counties. The vehicles were stolen from both pedestrian drivers and dealerships. The thieves managed to steal these cars by hacking them: Using a so-called “pro-pad”, which can connect to the diagnostics interface of the ECUs, they were able to reprogram the key fob in the vehicle in order to be able to unlock the vehicles with their keys. Such a hack demonstrates the lack of cybersecurity measures to protect against unauthorized modifications of the vehicle [329].

1.2 The value at risk from cybercrime

Cybercrime now ranks alongside natural disasters as one of the biggest global threats. As outlined in the following sections, it targets both organizations and individuals, and even small gaps in cybersecurity can have serious consequences. Poorly managed cyber risks can expose organizations and individuals to a wide range of cybercrimes, with implications ranging from data loss to financial ruin or even prison.

1.2.1 Risks for organizations

Over the past ten years, the number of security breaches in public and private sector organizations has increased rapidly [34]. This trend is worrying. The number of confirmed incidents in public and private sector organizations involving unauthorized access and/or disclosure of sensitive, confidential, or protected data increased by 67% from 2013 to 2018, representing a compound annual growth rate (CAGR) of 10.76% [166]. More recently, the World Economic Forum highlighted an increase in global data breaches of 72% between 2022, which was already a record year, and 2023. The breaches had primarily affected major tech companies with vast numbers of customers [349].

These trends also affect the automotive industry, in which the number of automotive hacks has risen rapidly in recent years. During only five years between 2018 and 2023, there was a more than threefold increase in the number of hacks. The resulting emerging risks can have serious financial and other consequences for organizations and individuals who underestimate cybersecurity risks [301].

CYEQT

KNOWLEDGE BASE