Ransomware in the Automotive Industry

Delia-Iustina GRIGORIȚĂ[1], Elisabeta DIMA[1], Ioana-Alexandra BUICĂ[1] and Emil SIMION[2]
[1]Faculty of Computer Science, Alexandru Ioan Cuza University of Iași
[2]Department of Mathematical Methods and Models, Centre for Research and Training in Innovative Techniques of Applied Mathematics in Engineering, National University of Science and Technology
deliaiustinagrigorita@gmail.com, lizudim@yahoo.com,
ioana.buica2013@gmail.com, emil.simion@upb.ro

Abstract: As a result of complexity and integration of the automotive system and of the growing vehicle autonomy, ransomware attacks have become a growing threat in the automotive industry. Therefore, this paper assesses the evolution of ransomware and its main effects on the automotive systems and analyses specific case studies in order to highlight the risks related to the automotive supply chain. This paper also refers to the current cybersecurity standards and measures and to cybersecurity compliance with the purpose of laying the foundation for a solid cybersecurity practice.
Keywords: Ransomware, automotive, malware, cybersecurity, autonomous vehicles.

INTRODUCTION

Over the last few decades there has been a drastic shift in the automotive industry primarily because of the technologies adopted and the interconnectivity of vehicles. It has resulted in the design of intricate systems that as efficient as they are with regard to user convenience/ enjoyment, and security, have added new kinds of weaknesses to cyber threats. Specifically, ransomware has developed into a big problem.

Ransomware is currently among the most prevalent cyber threats around the world, which targets organizations of all types. In the automotive industry they can result in severe financial losses and risks to the users of automotive products. As a matter of fact, a ransomware attack is not only limited to an organization; all members of the supply chain are at risk. This paper focuses on how these attacks may affect the production, distribution, and maintenance of vehicles, especially given the current systems, which are interconnected within the automotive industry. The ever-growing trend of autonomous vehicles is important when it comes to identifying ways of enhancing the protection of key systems from cyber threats. Next, this paper looks at the new technologies that can be incorporated into the design of vehicles for safety. One of them is the end user awareness of such mobile technologies. Also, this paper focuses on the aspect of cybersecurity and on the consumers of cars and how they can help in fighting ransomware attacks.

RANSOMWARE

Ransomware is a type of malware that enters a computer or connected device with the purpose of locking down files belonging to a user (Aurangzeb et al., 2017). When the

https://doi.org/10.54851/v7i1y202501

files are encrypted, making the information on them non-readable and unavailable to the user, a message will appear in a pop-up demanding that the user pay a ransom, usually in cryptocurrencies that cannot be traced such as bitcoins (Pope, 2016). It not only hampers the availability of these sources of information but also creates unbearable pressure on victims to meet the demands, leading to additional financial and operative problems (Pope, 2016).

Traditional ransomware attacks focus on data stored on computer systems, carrying out the unauthorized encryption of user files (Bajpai et al., 2020) by using normal encryption methods such as AES and RSA encryption along with a secret key known only by the attacker (Bajpai et al., 2020). The symmetric encryption is used for faster or real-time large data encryption and the asymmetric encryption to cover the symmetric key and to make sure that only the person with the decryption keys will see it because it has not been paid yet (Bajpai et al., 2020).

The victim may see a pop-up on his or her screen that reads: „A virus has infected your computer. To fix the problem, click this link" (O'Gorman & McDonald, 2012). Some people comply with the demands by paying the ransom, either because they believe in the scammers' promise or because they hope to restore their system's functionality, only to be let down as most of the scammers don't restore functionality (O'Gorman & McDonald, 2012). Eliminating malware is the only surefire method to get functionality back (O'Gorman & McDonald, 2012).

Types of ransomware

According to Sgandurra et al. (2016), there are two primary categories of ransomware:

A) locker ransomware
B) crypto ransomware

The purpose of the first one (A) is to lock the victim's computer and eventually stop him/her from using it. The second one (B), which appears to be the most prevalent these days, encrypts private documents so that the victim cannot access them.

Because of its targeted nature, leakware—also known as doxware—poses a serious risk, especially to enterprises that handle sensitive data and institutions like banks. Leakware, in contrast to conventional ransomware, threatens to make private information publicly accessible rather than erasing data. The need for a speedy ransom payment may increase because of the possible harm to an organization's image (Rivera & Yoon, 2017).

Scareware is thought to pose relatively little danger. To trick people into downloading and installing malware on their computers, it uses social engineering tactics. Usually, it shows up as a seemingly authentic pop-up notification or one warning that there is an issue with their computer that has to be fixed right away. It's just another attempt to coerce the victim into paying money (Rivera & Yoon, 2017).

Further on, Ransomware-as-a-Service (RaaS) is implemented in affiliate schemes or networks whereby those who do not understand programming can get a share of the ransoms. These are distributors who spread the ransomware for the members of the networks and these RaaS vendors are focused on increasing the efficiency of their malicious software. RaaS can be expressed as a novel approach for threat actors. How it works: they create a friendly graphical user interface for ransomware then sell it as a service. The brain behind the program requires potential attackers to pay for subscription to the service and also get a percentage of the ransom received. This means that with this model, an attacker does not need to be a programmer because everything is structured to suit that purpose. Anyone with little or no knowledge of computer programming can develop their own malware, select the type of virus they wish to inject and commence an attack. The most famous RaaS services are Satan (complimentary), Stampado, Jigsaw, Karmen, Cerber, and Atom (Rivera & Yoon, 2017).

Windows malware likes to use ransomware tactics for its tasks against the targeted victims, while mobile malware also tends to get more used to the blackmail method to extort money from victims (Sgandurra et al., 2016). For example, the desktop Trojan called Kenzero will not only take a user's browser history but

upload it on the Internet alongside the user's name including a warning that they will delete it for a total of 1500 yen (Sgandurra et al., 2016). While no mobile malware has yet reached this level of public shaming for profit, one example exists: a Dutch worm (Sgandurra et al., 2016) that disables the phone screen and in return asks users for 5 euros in order to unlock their screens (Sgandurra et al., 2016).

Finally, multi-extortion ransomware or multifaceted extortion uses a variety of strategies to coerce victims into making a ransom payment (Das, 2024). This kind of cyberattack may use techniques like data exfiltration, distributed denial-of-service (DDoS) attacks or sending ransom demands to third-party affiliates in addition to encrypting files (Das, 2024).

In the automotive industry, to gain leverage over victims, ransomware is likely to implement various interruption attacks on the host systems such as denial-of-data: ransomware may struggle to demand high ransoms, pushing attackers to focus on critical services or privacy, denial-of-service: ransomware can exhaust system resources or block access with ransom screens, rendering the system unusable and denial-of-privacy: sensitive data (e.g., contacts, GPS) can be exploited for extortion, with ransomware lying dormant until enough private data is available (Bajpai et al., 2020). Table 1 includes a brief overview of the types of ransomware and explains the essence of each.

Table 1. *Ransomware Classification*

Type	Description
Locker Ransomware	Blocks access to the device, allowing only payment. Data isn't encrypted, so it can often be removed easily.
Crypto Ransomware	Encrypts files and demands ransom for the decryption key.
Leakware (Doxware)	Threatens to release sensitive data publicly instead of destroying it, pressuring victims to pay quickly.
Scareware	Tricks users into downloading malware by showing fake alerts about problems on their computer.
Ransomware-as-a-Service (RaaS)	Allows people with little technical knowledge to spread ransomware and earn a share of the ransom payments.
Multi-extortion ransomware (multifaceted extortion)	Utilizes multiple pressure tactics, such as data encryption, threats to leak data, and other means to ensure payment from victims.

Evolution of Ransomware

Due to the increasing usage of computerized networks and related technology, ransomware has gradually become a growing threat to the automotive industry. Experiences of ransomware in this industry over the years are a clear depiction of how advanced ransomware has been and the challenges that manufacturers, suppliers, and service providers have faced.

Originally known as PC Cyborg, the AIDS Trojan appeared to be the first ransomware of all

kinds, and it hit the healthcare sphere in 1989 (Sgandurra et al., 2016).

The first ransomware to employ the RSA encryption was released in 2006 in the form of the Archiveus Trojan, which heralded a shift to more dependable cryptographic methods (Razaulla et al., 2023). It encrypted all the files in the „MyDocuments" folder, this being its purpose and achievement according to its creators (Razaulla et. al., 2023). Archiveus was financially driven, which included ransoming its victims and forcing them to buy goods from an online pharmacy at the cost of a 30-digit decryption key (Razaulla et al., 2023).

The Cryzip ransomware searched for files with specific extensions (e.g. .doc, .jpg, .xls), it encrypted them, and then placed the encrypted files into a compressed, password-protected ZIP folder, this approach was effective in disrupting user access to important files and required the victim to pay for the decryption key (Zavarsky & Lindskog, 2016).

MBR (Master Boot Record) Ransomware can be traced back to 2010, the first strain of the malware being Trojan-Ransom.Boot.Seftad.a; the second one was bootlock.B in the following year. Some varieties of ransomware overwrite all files on the infected machine and substitute them with a copy of the ransomware as well as change the MBR to deny the user access to his system (Zavarsky & Lindskog, 2016).

Ransomware attacks started to target automobile industry peripheral systems, including supplier networks and dealerships, between 2010 and 2015 (Kim & Shrestha, 2020). The main goal of these attacks was to interrupt operations by encrypting important company files. Concerns over possible ransomware threats to vehicles themselves were raised once with the growth of telematics systems and connected cars during this time, which expanded the attack surface (Kim & Shrestha, 2020).

The new model of ransomware, Ransomware-as-a-Service (RaaS), appeared in 2018, allowing novices to use tools developed by experienced cyber attackers. Some examples are Maze and Ryuk that have affected diverse industries negatively (Nagar, 2024).

The rise of RaaS made ransomware campaigns more accessible, targeting critical systems in Honda and Kia. Honda's production was temporarily halted globally due to a ransomware incident in 2020 (Bajpai et al., 2020). Recent studies highlight scenarios where ransomware could lock drivers out of their vehicles or disable safety features. Researchers emphasize the importance of securing vehicle ecosystems as connected vehicles and autonomous driving systems are becoming more vulnerable.

THE EVOLUTION OF AUTONOMOUS VEHICLES

The actual beginnings of the car manufacturer and present foundation of Mercedes-Benz date back to more than one hundred thirty years ago when Karl Benz introduced the first motorized automobile. Much has changed in the automobile industry since then. These developments are aimed at helping to decrease the incidence of traffic accidents with the secondary aim of enhancing the safety and security of both the drivers and passengers, as well as enhancing the efficiency of the operation of the traffic system.

ITS (Intelligent Transportation Systems) research significantly expanded during the early part of the 1980s. Other ITS applications that were readily distinguishable included intelligent and automated automobiles (Kim & Shrestha, 2020). In 1984, DARPA (Defense Advanced Research Projects Agency) introduced the first automatic cars through its program known as the Autonomous Land Vehicle or ALV (Kim & Shrestha, 2020). Using computer vision technologies such as LiDAR (Light Detection and Ranging), GPS (Global Positioning System) and robotic control to manage the cars' route and direction during a test drive on the roads, this revolutionary project demonstrated the saving ability of on-road AVs (Autonomous Vehicles) (Leighty & Lane, 1986).

In 1980, Mercedes-Benz revealed a vision of an autonomous robotic car for hire on the public roads that did not have the characteristics of other conventional cars (Kim & Shrestha,

2020). This vehicle achieved a maximum speed of 63 kilometers per hour (Kim & Shrestha, 2020). Though it was innovative in automobile engineering, it did not grab the attention of the emerging automated vehicle industry at the time (Dickmanns & Graefe, 1988).

In 1989 the Carnegie Mellon University (CMU) improved on this model by using artificial intelligence (AI) on the earlier Autonomous Land Vehicle (ALV) (Kim & Shrestha, 2020). By developing a new connected scheme known as ALVINN (autonomous land vehicle in a neural network), they built the autonomous navigation test car, NAVLAB. This system applied artificial neural networks to enhance the level of the auto pilot of the car (Pomerleau, 1988).

Intelligent Vehicles (IV) were developed when artificial intelligence was incorporated in automated cars, making them to not only embrace navigation control mechanisms but also integrate IC perception to respond to their surroundings (Kim & Shrestha, 2020). GM (General Motors) struck at the right time when it developed the OnStar telematics system in mid-1990s (Kim & Shrestha, 2020). This invention signaled a major shift to automobile connectivity where customers received help in real time through navigation and emergency services by linking automobiles to central systems (Barabba et al., 2002).

The connectivity of intelligent vehicles increased, which allows vehicles to communicate with other vehicles and parts of the road infrastructure. The US Department of Transportation (US-DoT) coined the term „connected vehicle" to refer to automobiles that could communicate in this way (Kim & Shrestha, 2020). Though, this term does not mean that those vehicles are actually autonomous. However, the wireless communication based on the On-Board Unit (OBU) only warns the drivers of the possible risks, or an incoming crash and the driver is forced to adapt and change something to avoid these threats (Kim & Shrestha, 2020). This points to the fact that connected vehicles are characterized by a symbiotic relationship where technology and human decision are involved.

When it comes to vehicle communication, there are two primary forms of connectivity:

1. Dedicated Short-Range Communication (DSRC) and WAVE (IEEE, 1997)
   - Used for: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.
   - Extended to: Vehicle-to-Everything (V2X) communication, which has become the foundation of vehicular communication systems.
2. Cellular Technology (e.g. LTE, 5G):
   - Used for: Connecting vehicles to the Internet, cloud services, and other Internet of Things (IoT) devices.

It's necessary to remember that wireless connection capabilities are not always necessary for automated cars. Several sensors are used by Automated Driving Systems (ADS) to collect environmental information for driving (Kim & Shrestha, 2020).

Multi-sensor fusion was studied between 2005 and 2007 by academics from universities such as MIT (Massachusetts Institute of Technology), Stanford, and Carnegie Mellon University (CMU). Their experimental intelligent cars used a variety of sensors, including LiDAR, GPS, radars, inertial measurement units (IMUs), and multiple cameras (Kim & Shrestha, 2020). Google Inc. didn't release a high-precision mapping-based autonomous car until 2009. Other names for these automobiles include driverless cars, robotic cars, and self-driving autos (Kim & Shrestha, 2020). A computer-controlled car that uses the aforementioned sensors to sense its environment, recognize impediments, and recognize pertinent indications is called an autonomous vehicle. After this, the technology for driverless vehicles advanced quickly (Kim & Shrestha, 2020).

Elon Musk presented the Tesla Model S with conditional automation in 2014 as part of the Tesla Autopilot system, with such features as the parking of a car in a parking lot without the presence of the driver (Zhang, 2016). The driving features of Tesla are categorized as Level 2 driving automation by the SAE (Society of Automotive Engineers). Still, the autopilot

system was involved in a fatal Tesla crash that occurred in Hebei, China in 2016 (Kim & Shrestha, 2020). In the same year, utilizing prediction through output of cameras and the steering angle data in the context of deep learning, GPU maker NVIDIA made a major leap forward in developing the complete solutions for the Autonomous vehicles (Bojarski, 2016). A significant competition in the context of building intelligent and autonomous vehicles arose in 2017 between automakers and academic institutions, including Ford, Audi, Baidu, the University of Michigan, Mercedes, and many more. The first self-driving technology company to introduce and market a fully autonomous taxi service was Waymo, a division of Google Inc., in 2018 (Laris, 2018).

THE CURRENT STATE OF AUTOMOTIVE CYBERSECURITY

Connected and autonomous vehicles (CAVs) have emerged on the automotive market which features unlimited opportunities ahead, along with the problem of cybersecurity. The specified domain of automotive cybersecurity has become an essential area for addressing the risks that could threaten the safety of vehicles, privacy and infrastructure. This section offers a review of the current state of cybersecurity systems, models, and measures that have been adopted in the automotive industry by using technical papers and guidelines.

As the complexity of cars is increasing, and new technologies such as machine learning systems and IoT devices, and new protocols become integrated into automobiles, the attack surface for malicious actors expands (Shan et al., 2020). Examples of existing risks are recovering passwords for ECUs (Electronic control units), remote attacks on telematics systems, as well as the exploitation of vulnerabilities of Over-The-Air (OTA) updates (Shan et al., 2020). Advanced security measures are strongly required since such attacks have the potential of causing loss of data, theft of vehicles, and interference with critical systems (Shan et al., 2020).

Existing Frameworks and Standards

Therefore, there is a need to create strong industry and regulatory standards to address the cyber security challenges emanating from the increased adoption of technology by automotive industries. This review examines the major frameworks and laws governing the developing cybersecurity environment in the context of the automotive industry:

- ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering: Recognized by this industry across the globe, ISO/SAE 21434 provides a structure for addressing cybersecurity throughout the build lifecycle of automotive systems (Standard, 2021). A risk-based approach is stressed through the standard, which requires manufacturers to perform threat analysis and risk assessments (TARA) in order to identify vulnerabilities and create plans to deal with them (ISO, 2021). To ensure that manufacturers are aligned with leading global standards and to ensure that cybersecurity engineering practices related to the manufactured products are standardized globally (ISO, 2021).
- UN Regulation No. 155 (UNECE WP.29 Cybersecurity Regulation): Strict cybersecurity standards for new cars are required by UN Regulation No. 155, which was created by the UN Economic Commission for Europe (UNECE) as part of the World Forum for Harmonization of Vehicle Regulations (WP. 29). The rule, which went into effect in 2022, mandates that automakers set up a Cybersecurity Management System (CSMS) in order to control risks along the whole supply chain (Costantino et al., 2022). Additionally, manufacturers are required by this rule to show that they can minimize risks like ransomware, data breaches, and illegal remote access to car systems. In more than 50 participating nations, including the European Union and Japan, adherence to UN R155 is required for vehicle type approval. Harmonizing international automobile cybersecurity standards is made possible to a large extent by this law (Costantino et al., 2022).

- Auto-ISAC Best Practices: Besides legal regulations, there is valuable guidance for improving cybersecurity capability in the automotive industry from industry-driven programs such as the Automotive Information Sharing and Analysis Center (Auto-ISAC) (Schlenoff et al., 2024). Risk management, information exchange about threats, and secure ways of software development are described in the Auto-ISAC guidelines. These best practices append AG/SAE 21434 as well as the UN Regulation No.155 (Schlenoff et al., 2024) and help the industry prepare for future risks by fostering cooperation between stakeholders.
- NIST Cybersecurity Framework (CSF): The fact that the NIST Cybersecurity Framework is not fully and directly tied to the automobile industry has not hindered the automobile industry from fully adopting it because of the structure of the Framework (White & Sjelin, 2022). The framework is mainly divided into five functions namely Detective, Responder, Protector, Identifier and Restorer (White & Sjelin, 2022). As such, the framework becomes a handy instrument for automakers to synchronize their actions with the existing norms since these conceptual pillars of thinking lay down a specific systematic approach regarding the cybersecurity threats (White & Sjelin, 2022).
- NHTSA Cybersecurity Best Practices for Modern Vehicles: Latest guidelines on how to address cybersecurity challenges in modern cars have been published by the National Highway Traffic Safety Administration (NHTSA) of the United States (Watney & Draffin, 2022). All these suggestions revolve around implementing new risk detection mechanisms, preserving OTA upgrades, and enhanced security layers. They are significant for manufacturers conducting business in the United States because these guidelines embody regulatory standards of vehicle safety and usage (Watney & Draffin, 2022).
- SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems: One of the first approaches for incorporating cybersecurity concepts into cars can be identified within the SAE J3061 standard. In doing so, it provides a framework for threat assessment, risk mitigation, and incident response planning; it provides the foundation for more modern standards like ISO/SAE 21434. It is an effective resource for suppliers and manufacturers who seek to tackle two issues of security and safety because the book focuses on integrating cybersafety with operational security measures (Schmittner et al., 2016).
- CIS Controls by the Center for Internet Security: The CIS Controls also have the best standards for IT system security, and automotive applications require them as they continually advance in their integration. Based on response management, vulnerabilities, and secure software development controls, this list provides implementable measures for improving the security of Automotive systems (Bashofi & Salman, 2022).
- ISO/IEC 27001: Information Security Management Systems: One of the widely used standards for implementing the framework of ISMS is the international standard ISO/IEC 27001. It helps automotive firms to deal with enterprise and product risks in the automotive industry. To ensure that the cybersecurity organizational measures match the requirements related to technical standards for automotive systems, this standard is often combined with ISO/SAE 21434 (Malatji, 2023).

While these guidelines offer a solid approach to addressing cybersecurity concerns related to automobiles, challenges arise when it comes to their implementation. Manufacturers are required to navigate an intricate supply chain, understand the legal environment and commit resources to continuous danger identification and controls establishment. In addition, there is still an option to look for a perfect balance between the growing popularity of innovation and usage, on the one hand, and the stringent approach to the security, on the other hand so that the industry can continue to embrace

the proper protection of automobiles and their resilience to the emergent cyber threats as highlighted by the application of ISO/SAE 21434, UN Regulation No.155 and other measures among them.

Model for Identifying Computer Security Threats

S.T.R.I.D.E. (abbreviation for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) framework is a heuristic for threat modeling, which is helpful for understanding what aspects of an environment ransomware might take advantage of. By pointing out these weak points and offering protective measures, this model shows that vulnerabilities will emerge as vehicles become more connected (Das et al., 2024):

- *Spoofing* means to pretend to be a particular service or workstation in order to gain unauthorized access to other computers or other computer networks. In the realms of automotive industry this type of vulnerability can be exploited by ransomware imitating trustworthy updated servers to deliver infected firmware to vehicle control units. The risk that can be associated with updates can be greatly minimized by employing mechanisms for strong authentication and digital signatures.
- *Tampering* involves unauthorized modifications of data or systems. The attackers can introduce themselves into cars by setting up ransomware through the help of OBD-II (Onboard Diagnostics II) ports, or weak wireless networks such as Wi-Fi and Bluetooth. This type of attack can be prevented by using integrity checks and good boot procedures.
- *Repudiation* enables attackers to refuse engagement by deleting logging information and creating false system records. Forensic investigation of vehicles is impeded because of repudiation. The combination of secure logging with cryptographic signing and remote logging and blockchain-based records offers solutions to keep track and for maintaining accountability over attacks.
- *Information Disclosure* becomes a major issue in ransomware attacks when it involves sensitive information. As far as this type of malware is concerned, a vehicle can be damaged because the attacker can threaten to expose a person's location history or other details if the person does not pay for their release.
- *Denial of Service (DoS)* leaves the critical car functions such as the steering or the brakes non-operational until a ransom is given. This is why it is possible to maintain fallback mechanisms so that the vehicle will have a minimum level of safety during such situations.
- *Elevation of Privilege* is when ransomware can be installed on all car systems and the attackers get administrative control. Attackers can then exploit these control units and also impact on other significant systems because of these openings. The risk arising here is significantly minimized if the principle of least privilege is implemented and strict controls on access are achieved.

Table 2 shows the correlation between threats according to the S.T.R.I.D.E. model and the desired security properties for mitigating them.

Table 2. *S.T.R.I.D.E. Threats and the Security Properties for mitigating them*

Threat	Desired property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

The Cyber Kill Chain

The Cyber Kill Chain, created by Lockheed Martin, is a component of the Intelligence-Driven Defense paradigm, which aims to detect and stop cyber assaults. The model determines what the opponents need to accomplish to reach their goal (Tarnowski, 2017).

The Cyber Kill Chain's seven steps can improve an analyst's comprehension of an adversary's strategies, tactics, and processes while also increasing visibility into an assault (Tarnowski, 2017). When ransomware targets automotive systems, the kill chain involves identifying how the attackers gain access, spread and actively attack the systems:

1. Reconnaissance: During this phase, the attackers obtain information about the target organization including System vulnerabilities, networks, and employees. In the context of the automotive industry, this could mean, therefore, collecting information on vehicle to vehicle and vehicle to infrastructure communication, the OBD-II interfaces, and integrated applications including navigation systems. For instance, a hacker may look for weaknesses in the car's Bluetooth or Wi-Fi systems.
2. Weaponization: After the accumulation of enough data has led to the identification of the weaknesses or vulnerabilities of a target, they devise a payload, usually in the form of ransomware. These activities can include creating viruses which can negotiate important operations such as steering or braking or even encrypting car information. For example, the hacker develops ransomware that specifically affects a car's firmware which then blocks the access to mechanisms that are critically important until a certain amount of money is paid.
3. Delivery: Some of the attack approaches aim at the onboard systems directly, including the use of websites containing Virus/hack links, phishing e-mails among others. Delivery in automobile cybersecurity can take place through a USB device or by utilizing compromised updated servers. For example, the ransomware is delivered through a USB stick, connected to the car's computer or a computer update.
4. Exploitation: The attacker controls how a person will launch the ransomware by exploiting the weaknesses of the infected system. To achieve this, a typical phase of such an attack requires the exploitation of the vulnerabilities found in the hardware interfaces, in the software or the communication protocols of the vehicle. The ransomware is able to infiltrate the main car control systems by exploiting a vulnerability in a car's infotainment system.
5. Installation: Ransomware installation becomes possible when the attacker compromises a vulnerable vehicle system. The malware operates within the firmware together with the operating system and connected control modules in order to ensure uninterrupted access.
6. Command and Control (C2): After installation the attacker sends a delivery confirmation message to the compromised system. This

allows them to send commands, receive information or change the response of the vehicle. The C2 phase of ransomware may involve the sending of other instructions like further encryption of data or shutting down critical systems. For instance, the attacker starts controlling the car, the additional networks no longer communicate with other networks and then the attacker demands a ransom to release such systems.

7. Actions on Objectives: This is the final stage, where the attacker achieves his/her objective, which often entails sacking or encrypting the targeted systems for the sole aim of being paid a ransom by the owners of the compromised computers. A typical implementation is a ransomware attack when the attacker's purpose is to seize control of the car or its key components and then ask for money to regain access.

In the context of the Cyber Kill Chain, an attack can be prevented at any stage up to the Installation phase, via good practice such as vulnerability scans, and a good user authentication mechanism. After the Installation phase, it becomes somewhat difficult. By discovering the Cyber Kill Chain, the automotive manufacturers and cybersecurity experts can reduce the impact of ransomware attacks and improve the defense mechanisms in each stage, particularly to enhance the likelihood of recovery against cyber threats in the automotive industry.

VEHICLE ARCHITECTURE AND ATTACK VECTORS

Before enumerating some real-world examples of ransomware attacks, it is necessary to understand what the automotive industry is and how its supply chain is operated, as well as how modern cars are constructed and interconnected. According to Binder & Rae (2020), the automotive industry is comprised of 'all those companies and activities involved in the manufacture of motor vehicles, including most components, such as engines and bodies, but excluding tires, batteries, and fuel'.

This means that the production of a single car involves multiple companies and organizations, each with its own role in the supply chain: raw material sourcing, component manufacturing, assembly, quality control, distribution, aftermarket support, and so on. If any of these steps is compromised by a malware attack, the whole supply chain suffers, and the production of a car may be delayed.

Ransomware attacks can target many steps in this process. However, not all of them are considered to be directly related to the automotive industry, since it consists of a complex network of service providers, manufacturers, and suppliers. Ransomware – and any type of malware, for that matter – can appear on any computer in a company that works more or less directly in the automotive industry – anywhere from automotive design to an appointment application. A more direct approach, where the attacker targets the automobile itself, requires a change of strategy (Bajpai et al., 2020).

Intelligent Vehicle Architecture

A modern intelligent vehicle relies on multiple (70 to 100) ECUs which communicate with each other (Figure 1). An ECU is an embedded system (a small computer) that controls different electrical parts of a car. ECUs include the following modules: engine control, powertrain control, transmission control, brake control, central control, central timing, general electronic, body control, and suspension control. These systems are illustrated in Figure 2.

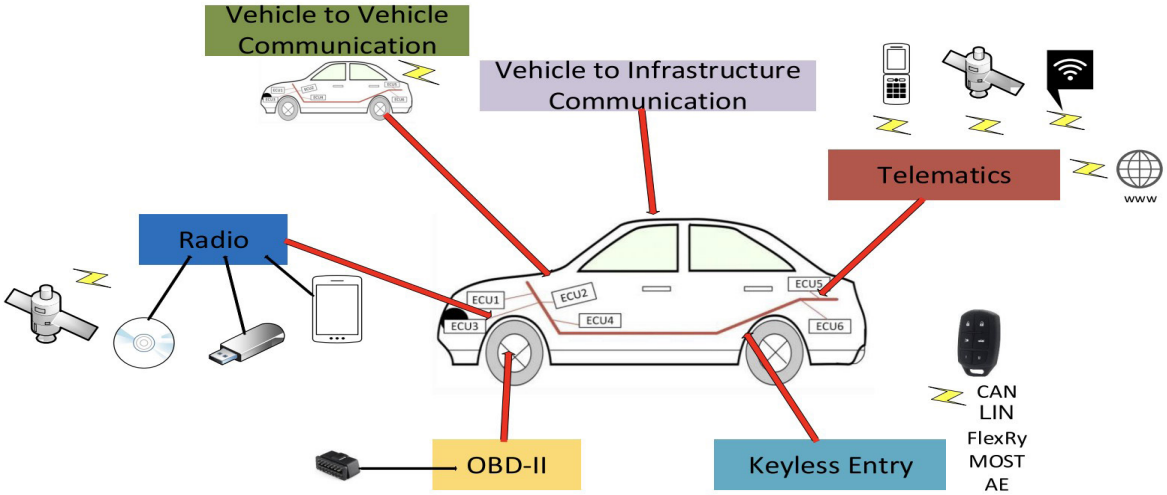

Figure 1. *The architecture of an intelligent vehicle (Elkhail et al., 2021)*

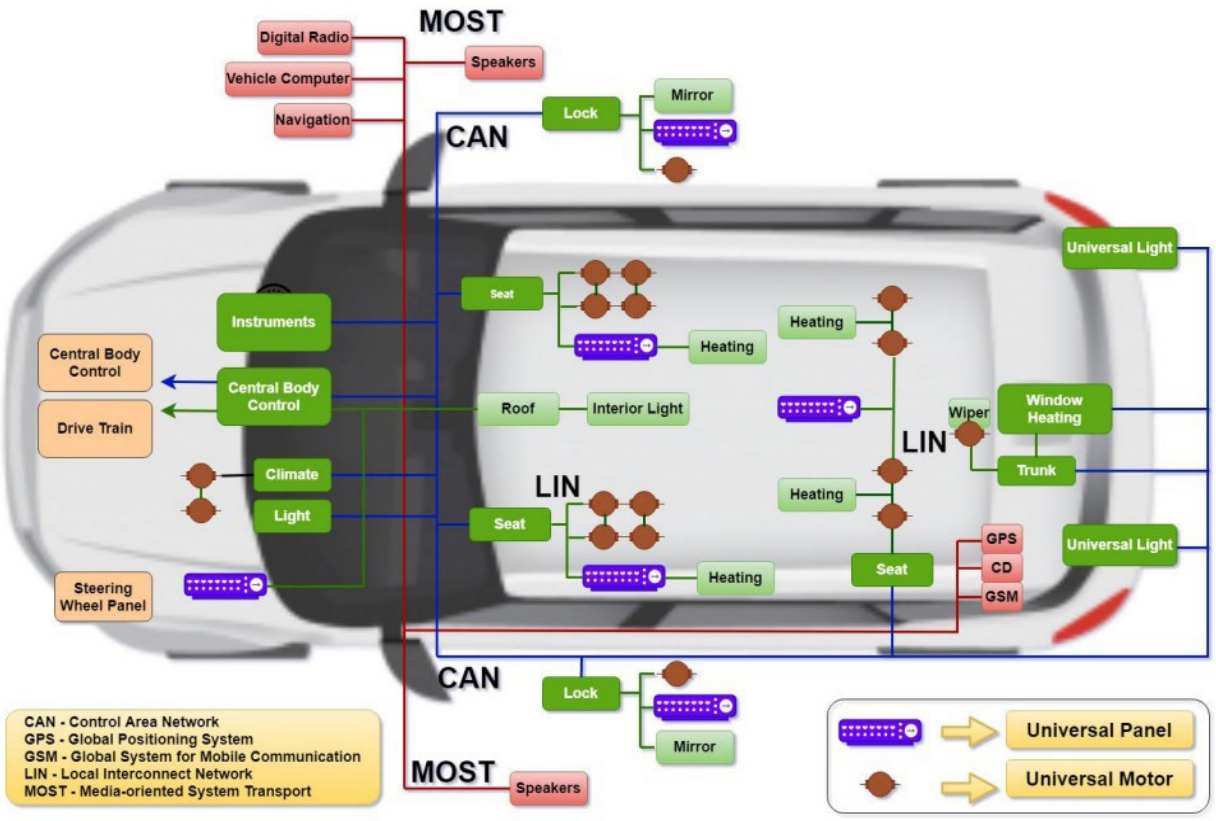

Figure 2. *The network architecture of an intelligent vehicle (Elkhail et al., 2021)*

Modern intelligent cars integrate in-vehicle network systems accessible through the OBD-II port for generating diagnostic reports. Entertainment systems equipped with USB connectivity or CD players allow users to sync and access content from mobile devices, and remote key entries and RFID (Radio Frequency Identification) car keys facilitate functions like door unlocking, flashlight activation, and, in some cases, ignition control. As stated in Section 3 about the evolution of autonomous vehicles, connectivity extends via Wi-Fi, Bluetooth, and cellular networks (LTE, 3G, 4G, 5G). Wireless phone connections enable infotainment systems to support Apple CarPlay and Android Auto, while Wi-Fi and 5G provide GPS, digital radio, and traffic updates. Additionally, Dedicated Short Range Communications (DSRC) technology supports V2V and V2I communication. By utilizing radio frequency channels, DSRC enables vehicles to share data with nearby vehicles and infrastructure, enhancing autonomous driving capabilities. Moreover, all intelligent vehicles have multiple and various sensors: high-resolution camera, Light Detection and Ranging (LiDAR), ultrasonic (sonar), RADAR, intelligent vision systems, and others (Elkhail et al., 2021).

Ransomware Attack Vectors

To be able to perform an attack on a vehicle, the attacker needs to access it in some way. Access points to the vehicle can be the following (Checkoway et al., 2011):

- **Short-range wireless access:** some examples include Remote Keyless Entry, RFIDs, and Bluetooth.
- **Long-range wireless access:** an example is GPS.
- **Physical access:** can be either direct (access to the ECUs through the OBD-II port or the OBD connector) or indirect (communicating with the ECUs through the entertainment system using devices such as CDs and USBs).

A ransomware attack can be carried out on an intelligent vehicle only if the following prerequisites are met (Wolf et al., 2017):

- A ransomware with both client and server software.
- An anonymous botnet for the global distribution and management of the ransomware vehicle clients.
- An in-vehicle security exploit, often paired with a Trojan software, to access and infect a connected in-vehicle system.
- A mechanism to lock or disable a critical vehicle component that is difficult to restore, bypass, or tolerate if inoperative for extended periods, ideally with a secret unlock command to restore functionality after ransom payment.
- An anonymous payment method to receive the ransom while protecting the attacker from identification and legal repercussions.

CASE STUDIES

Ransomware has significantly impacted the automotive industry, targeting both its supply chain and digital infrastructure. This section examines real-world ransomware incidents that have affected automotive suppliers, dealerships, and service providers, as well as hypothetical attack scenarios that illustrate potential threats to connected vehicles, highlighting how ransomware could compromise critical in-vehicle systems.

Real-World Incidents

Ever since *CryptoLocker* popularized crypto ransomware in 2013, the era of modern ransomware began, and this malware rapidly evolved into one of the most dangerous types we know today. The most infamous ransomware to this date is *WannaCry* (2017), which used the *EternalBlue* exploit software developed by NSA to spread globally. Later, in the 2020s, more ransomware families appeared, some of them playing major roles in attacks on the automotive industry, for instance *Conti* (2020),

BlackCat/ALPHV (2022), and *LockBit 3.0* (2022) (Razaulla et al., 2023). Below, some incidents of ransomware attacks that have indirectly affected the automotive industry are discussed.

LockBit 3.0 ransomware gained notoriety in 2022 due to its adaptable ransomware-as-a-service model. This group was involved in attacks on suppliers and software vendors critical to the automotive sector. For example, the group exploited a software vulnerability in one of the biggest dealership management systems in the UK, Pendragon PLC, affecting dealership operations across several countries. LockBit performed a double extortion ransomware attack and (allegedly) demanded US$60 million, however, the representatives of the company stated that they refused to pay. Another giant in the automotive industry, the German company Continental AG, faced a similar attack from LockBit 3.0 in 2022. Due to the fact that they also refused to pay the ransom, some of the stolen sensitive data and private information was leaked from their sites. These attacks demonstrated how important it is to secure not only internal networks, but also third-party software.

In June 2024, a ransomware attack targeted CDK Global, a major provider of digital solutions for auto retailers, impacting approximately 15,000 dealerships, predominantly in the US. The attack disrupted the systems used to manage client appointments, negotiations, and dealer operations. To regain access to encrypted data, the company reportedly paid US$25 million in Bitcoin, although it took days for the systems to recover fully. The dealerships faced significant operational challenges, with many resorting to manual processes like using pen and paper, while others were temporarily closed. The attack, attributed to the BlackSuit ransomware group – linked to the Royal and Conti groups – highlighted the vulnerabilities in the automotive supply chain. Although the company's primary focus is dealership management, the impact of the attack extended to sales and customer experiences across the industry, illustrating how a single vendor can create widespread disruption.

Theoretical Attack Scenarios

While ransomware attacks on automotive suppliers and dealerships have dominated the headlines, direct attacks on vehicles themselves have also surfaced as a concerning trend, mostly due to articles and research papers that highlight potential risks and outline actual attack vectors that can be used.

Considering the necessary conditions for a ransomware attack detailed in the previous section, a possible attack scheme described by Wolf et al. (2017) is as follows. A cybercriminal creates ransomware and distributes it to target vehicles via an anonymous botnet, often using technologies like TOR (the onion routing). The malware is injected into vehicles either directly or through a secondary exploit via wireless or wired interfaces. Once inside, it exploits a primary in-vehicle security vulnerability to install and run on a central unit, such as the infotainment system. The ransomware may connect to the attacker for further commands or payloads or directly lock a critical vehicle component, like the ignition system, via in-vehicle bus systems. The malware then displays an extortion message on the in-car display demanding a ransom. Upon payment through anonymous methods (usually Bitcoin), the attacker communicates with the malware through the botnet to issue a secret unlock command, restoring the vehicle's functionality.

Generally, an attack scheme requires the attacker to identify a vulnerability in a connected vehicle system, for instance in the infotainment or telematics system. Then, the infiltration takes place, the malware being injected through physical or wireless methods. Once inside the system, the ransomware executes its payload: it encrypts vehicle control files, locks functions like ignition, brakes, or navigation, and then it displays a ransom message on the infotainment screen demanding cryptocurrency for unlocking. Theoretically, if the user refuses to pay the ransom, the attacker could threaten with data leakage, but this is more difficult to do when dealing with personal cars rather than big companies with actual important information.

BEST PRACTICES FOR CYBERSECURITY

This section outlines the best practices for automotive cybersecurity. By following these principles, vehicle manufacturers may increase their cybersecurity defense against malicious attacks, unauthorized access, and system vulnerabilities and maintain consumer safety.

Implementing the Principles of Automobile Cybersecurity

ACEA (2017) states that they have identified a set of six key principles to enhance the protection of connected and automated vehicles against cyber threats:

- Cultivating a cybersecurity culture
- Adopting a cybersecurity life cycle for vehicle development
- Assessing security functions through testing phases
- Managing a security update policy
- Providing incident response and recovery
- Improving information sharing amongst industry actors

Cultivating a Cybersecurity Culture

Establishing dedicated cybersecurity teams and processes that can handle risk management, secure design, and penetration testing ensures that an organization has the specialized personnel and standardized approaches for managing cybersecurity risks effectively. (ACEA, 2017)

A strong cybersecurity culture must permeate the entire organization to strengthen the overall awareness of the company's staff. One way to achieve this is through training and awareness programmers (ACEA, 2017). Engineers and vehicle manufacturers should participate in training programs that incorporate standards such as ISO/SAE 21434, providing a foundation for integrating cybersecurity into a vehicle's life cycle. To mitigate system vulnerabilities, best practices from NIST and Auto-ISAC should be adopted. These include small group discussions, interactive learning activities, and targeted training sessions. Public campaigns can help raise customer awareness of ransomware risks, while producers and sellers can evaluate their preparedness through training initiatives.

As regulations encourage the establishment of Cybersecurity Management Systems (CSMS) covering threats across the entire supply chain, awareness of international standards like UNECE WP.29 is essential. A strong cybersecurity culture leads to faster responses to ransomware incidents, an increased reporting of suspicious behavior, and an improved adherence to best practices, ultimately enhancing trust in the intelligent connected automotive environment.

Adopting a Cybersecurity Life Cycle for Vehicle Development

As stated in Section 4, the ISO/SAE 21434 standard provides a structure to address cybersecurity throughout the build lifecycle of automotive systems. Macher et al. (2020) stated the phases of the ISO/SAE 21434 (2020) as follows:

- Concept Phase: Evaluating the cybersecurity relevance of a system under development (determining whether the system requires cybersecurity consideration), the item definition in a cybersecurity context, and the initiation of product development (starting product development with cybersecurity in mind).
- Product Development: Emphasizing the integration of cybersecurity into system, hardware, and software development.
  - System Development: Involves planning methods and measures for cybersecurity, including risk assessments at the concept and system levels.
  - Hardware Development: For hardware design, cybersecurity functionalities should include domain separation, self-protection of security functionalities, protection against bypassing of the security functionalities, and secure initialization of the security functionalities. The identification of

all hardware interfaces (physical and logical) is made according to their purpose, usage, and parameters.
    - Software Development: Derives software cybersecurity requirements from system-level requirements.
- Production, Operation, and Maintenance: Focuses on ensuring that cybersecurity measures are maintained throughout the production, operation, and maintenance phases of vehicle development.
- Supporting Processes: Outlines supporting processes for cybersecurity, focusing on management systems, customer-supplier relationships in distributed cybersecurity activities, and tool management.

Assessing Security Functions Through Testing Phases

Manufacturers should incorporate robust cybersecurity testing processes to enhance the security of critical systems. Qualified testers who have not been part of the development phase conduct tests to identify and eliminate known vulnerabilities and to evaluate the security functions (ACEA, 2017).

Testers examine a vehicle's hardware and software, evaluating overall product integrity and security. It involves conducting software-level vulnerability tests (e.g. unit and integration testing) and validating security systems at the vehicle level (ACEA, 2017).

Managing a Security Update Policy

As cyber threats evolve, vehicle cybersecurity systems must adapt accordingly, with security updates tailored to the unique requirements of connected and automated vehicles. These updates must consider diverse components, such as applications, secure elements, and ECUs, each requiring different update methods. However, they must be delivered securely to prevent tampering. The best practice is to use OTA (over-the-air) updates, sending them in a timely and efficient manner while verifying the integrity and authenticity of the updates before applying them to ensure they are not compromised (ACEA, 2017).

Security update policies vary, but generally, they include informing users when support for a vehicle or its components ends, applying workarounds if no fix is available, and planning for manual physical security updates when OTA options are not feasible (ACEA, 2017).

Providing Incident Response and Recovery

Automotive Quality Institute (2018) states that the Automotive Cybersecurity Incident Response (CSIR) process involves four core components:

- Detect and Register: The company detects and registers cybersecurity incidents (e.g. discovered events, reported vulnerabilities, and newly identified threats).
- Assess and Classify: The incident is analyzed technically and business-wise.
- Decide and Respond: The company decides and implements countermeasures with immediate actions in case of emergency.
- Learn and Optimize: The company reviews the incident to learn from it and improve the Automotive Cybersecurity Incident Response process, potentially leading to product or service enhancements.

When responding to an incident, the response teams focus on conducting a root cause analysis to understand the origin of that issue, assessing the risk of a broader impact on other vehicles from the same manufacturer, containing the incident to reduce its severity, developing effective methods to remedy its consequences, and restoring standard vehicle functionality whenever possible (ACEA, 2017).

Improving Information Sharing Amongst Industry Actors

Effective defense against cyberattacks in the automotive industry hinges on a robust collaboration and information sharing among stakeholders (e.g. vehicle manufacturers, component producers, and aftermarket

operators). This cooperative approach fosters trust, aids in developing industry-wide standards, and promotes the adoption of commonly accepted practices. Sharing information also helps in challenging and refining the security measures, enhancing the skills of security teams, and improving the detection and resolution of security issues (ACEA, 2017).

Practices for Cybersecurity Design

According to Clause 8.1.4.2.2.3 of ISO/SAE 21434 as cited by Macher et al. (2020) mentions the following best practices of cybersecurity design:

- Principle of least privilege: Limit access rights for users, processes, and systems to the minimum necessary to perform their tasks.
- Authentication: Implement secure authentication mechanisms to verify the identity of entities (users, devices, systems) interacting with the vehicle.
- Authorization: Define and enforce access controls to ensure that only authorized entities can access or modify resources.
- Audit: Record and monitor security-relevant events for accountability, incident analysis, and compliance purposes.
- End-to-End Security: Ensure data integrity, confidentiality, and authenticity throughout the entire communication flow across systems.
- Architectural Trust Level: Define and implement trust levels within the system architecture using measures such as the segregation of interfaces and defense in depth.
- Segregation of interfaces: Isolate and separate different system interfaces to simplify cybersecurity analysis and limit the potential vulnerabilities.
- Protection of Maintainability during service: Secure test interfaces and vehicle diagnostic points (e.g. OBD ports) to prevent misuse during maintenance.
- Testability during development and operations: Design systems that allow thorough testing of cybersecurity measures throughout their development and during operational use.
- Security by default: Ensure the system defaults to secure configurations, avoiding unnecessary complexity, obfuscation, or reliance on expert users for setup.

Ensure Up-to-date Cryptographic Algorithms

Cryptographic algorithms are a cornerstone of cybersecurity in modern vehicles (e.g. for protecting communication, data integrity, and system authentication). However, as computational power and attack techniques evolve, older algorithms can become vulnerable to exploitation. To maintain the security of vehicle systems, manufacturers must ensure the use of up-to-date, robust cryptographic algorithms throughout the vehicle's lifecycle.

On the Embitel Automotive & IoT Blog, Anand (2024) states that there are various encryption algorithms that are implemented in the development of automotive cybersecurity solutions. These algorithms are crucial for securing communications within the vehicle's network and between the vehicle and external networks or devices. The most used algorithms for automotive cybersecurity are:

- Advanced Encryption Standard (AES) is commonly used in vehicles to secure data transmissions between ECUs and external systems, such as encrypting vehicle performance data shared between the engine control module (ECM) and the infotainment system.
- Rivest-Shamir-Adleman (RSA) offers secure automotive software updates by verifying their authenticity through digital signatures, ensuring that OTA update packages are genuine and untampered.
- Elliptic Curve Cryptography (ECC) offers an efficient cryptographic security with smaller key sizes. It is used in keyless entry systems for a secure key exchange between the vehicle and the key fob, protecting communications against eavesdropping.

- Secure Hash Algorithm (SHA) ensures data integrity in automotive systems by creating hash values (e.g. SHA-256 verifies the integrity of a firmware package before installation to confirm it is unaltered).
- Transport Layer Security (TLS) secures vehicle communications with external servers, such as encrypting diagnostic data sent to manufacturers or traffic data retrieved from telematics services, safeguarding data from interception.

Choosing an encryption algorithm for automotive applications depends on balancing security needs with the system's limitations and on the type of data being protected (Anand, 2024).

AI-Powered Ransomware Detection Mechanisms

Ransomware defense in the automotive industry is using artificial intelligence (AI) as a critical tool for real time threat detection and mitigation. These models are able to analyze unexpected file modifications, abnormal CPU use, or inconsistent network traffic patterns and are highly effective weapons against the known and future strains of ransomware (Nwoye & Nwagwughiagwu, 2024).

The major strength of AI security stems from predictive analytics which uses machine learning algorithms to forecast ransomware patterns before they attack automotive systems by digesting data found in threat intelligence feeds and on the dark web (IBM Security, 2022). The integration of AI security systems includes honeypots and decoy ECU systems which divert ransomware attacks and simultaneously gather hacker behavior information during the process.

Performance-recovery capabilities powered by AI execute automatic rollback processes to save vehicle firmware from cyberattacks thus safeguarding essential vehicle functions (Norton Labs, 2023). The protection of control data through vehicle-to-vehicle communications and ransomware attacks depends heavily on AI-enhanced encryption which implements ECC and dynamic key rotation mechanisms (Anand, 2024).

Real-time ransomware detection capabilities based on AI cybersecurity will improve thanks to 5G connections and edge computing which ensures small interruptions in vehicle operations (Girdhar et.al., 2023).

Modern intelligent vehicles experience an improved security because automobile manufacturers use deception-based defenses and machine learning and predictive analytics along with automatic rollback mechanisms and machine learning (NIST, 2023).

FUTURE DIRECTIONS

Future directions point toward a collaborative approach involving manufacturers, governments, and consumers. The automotive industry should be proactive in combating ransomware threats by integrating advanced detection technologies, strengthening regulations, and fostering public awareness with regard to this issue.

New ways to combat the cyber threats in the automotive sector should also be analyzed, for example:

- Data Backups: Automakers can promote data backup systems that enable data restoration without paying a ransom.

Another area that should benefit from cybersecurity measures is that of military vehicles, including tanks, and automated or drone-based vehicles. These vehicles are more and more connected to each other, and therefore more and more exposed to cyber risks, the consequences of which may be disastrous. Stating the threats and weaknesses specific to those sectors is important for safeguarding the essential infrastructures and national security, as well as for providing safe novel technological applications in defense and autonomous transportation.

CONCLUSION

The increasing integration of connected systems with vehicles and the reliance on software has made the automotive industry a growing target for ransomware attacks. These threats can impact on manufacturers and also

end-users, leading to a compromised safety and significant financial and reputational losses. The rise of ransomware in the automotive industry underscores the critical importance of robust cybersecurity practices and of studying the old cases of cyber threats.

This paper presents the evolution of autonomous vehicles and ransomware. It also explores existing frameworks and standards, a model for identifying computer security threats, the Cyber Kill Chain, intelligent vehicle architecture, ransomware attack vectors, and real-life and theoretical case studies. Additionally, it discusses best practices for cybersecurity and explores AI-powered mechanisms for detecting ransomware attacks.

A secure automotive ecosystem is essential for consumer safety and for protecting a manufacturer's reputation and trust. Addressing ransomware vulnerabilities today ensures a safer, more resilient future for connected and autonomous vehicles.

REFERENCE LIST

ACEA (2017) ACEA Principles of Automobile Cybersecurity. Available at: https://www.acea.auto/files/ACEA_Principles_of_Automobile_Cybersecurity.pdf [Accessed: 16th February 2025].

Anand, V. (2024) Decrypting the Encryption Algorithms Implemented in Automotive Cybersecurity. *Embitel Automotive & IoT Blog*. Available at: www.embitel.com/blog/embedded-blog/decrypting-the-encryption [Accessed 7th December 2024].

Aurangzeb, S., Aleem, M., Iqbal, M.A. & Islam, M.A. (2017) Ransomware: A Survey and Trends. *Journal of Information Assurance & Security*. 6(2), 48-58.

Automotive Quality Institute (2018) *Automotive Cybersecurity Incident Response – Pocket Guide Version 1.0*. https://aqigmbh.de/wp-content/uploads/2022/03/201812_PocketGuideAutomotiveCSIR.pdf [Accessed 8th December 2024].

Bajpai, P., Enbody, R. & Cheng, B.H. (2020) Ransomware Targeting Automobiles. In: *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec '20), 18 March 2020, New Orleans, LA, USA.* New York, USA, Association for Computing Machinery. p. 23-29. doi: 10.1145/3375706.3380558.

Barabba, V., Huber, C., Cooke, F., Pudar, N., Smith, J. & Paich, M. (2002) A Multimethod Approach for Creating New Business Models: The General Motors OnStar Project. *Interfaces*. 32(1), 20-34. doi: 10.1287/inte.32.1.20.18.

Bashofi, I. & Salman, M. (2022) Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. *In: 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom), 16-18 June 2022, Malang, Indonesia.* Piscataway, IEEE. p. 58-62.

Binder, A.K. & Rae, J.B. (2020) automotive industry. *Encyclopedia Britannica.* Available at: https://www.britannica.com/technology/automotive-industry [Accessed 16th february 2025].

Bojarski, M. (2016) End to End Learning for Self-Driving Cars. *Arxiv*. arXiv preprint arXiv:1604.07316. [Accessed 12th December 2024].

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. & Kohno, T. (2011) Comprehensive Experimental Analyses of Automotive Attack Surfaces. *20th USENIX Security Symposium (USENIX Security 11), 10-12 August 2011, San Francisco, CA, USA.* Berkeley, CA, USA, USENIX Association. 6.

Costantino, G., De Vincenzi, M. & Matteucci, I. (2022) A Comparative Analysis of UNECE WP. 29 R155 and ISO/SAE 21434. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 6-10 June 2022, Genoa, Italy.* Piscataway, USA, IEEE. p. 340-347.

Das, P., Asif, M.R.A., Jahan, S., Ahmed, K., Bui, F.M. & Khondoker, R. (2024) STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. *Vehicles.* 6(3), 1140-1163. doi: 10.3390/vehicles6030054.

Das, R. (2024) *Generative AI: Phishing and Cybersecurity Metrics.* Boca Raton, FL, USA, CRC Press.

Dickmanns, E.D. & Graefe, V. (1988) Dynamic monocular machine vision. *Machine Vision and Applications.* 1(4), 223-240. doi: 10.1007/BF01212361.

Elkhail, A.A., Refat, R.U.D., Habre, R., Hafeez, A., Bacha, A. & Malik, H. (2021) Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses. *IEEE Access.* 9, 162401-162437. doi: 10.1109/ACCESS.2021.3130495.

Girdhar, M., Hong, J. & Moore, J. (2023) Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models. *IEEE Open Journal of Vehicular Technology.* 4, 417-437. doi: org/10.1109/OJVT.2023.3265363.

IBM Security (2022) *AI-driven threat intelligence: The future of predictive ransomware defense.* IBM Research Whitepaper. https://www.ibm.com/ai-cybersecurity [Accessed 6th February 2025]

IEEE (1997) 802.11-1997 – IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. *IEEE Std 802.11-1997, 18 November 1997. Piscataway, IEEE.* p. 1-445. doi: 10.1109/IEEESTD.1997.85951.

ISO (2021) ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering. Geneva, IEEE.

Kim, S. & Shrestha, R. (2020) Automotive Cyber Security: Introduction, Challenges, and Standardization. Singapore, *Springer.*

Laris, M. (2018) Waymo launches nation's first commercial self-driving taxi service in Arizona. *Washington Post*. 5 December. p. 6.

Leighty, R. & Lane, G. (1986) Autonomous Land Vehicles (U). *Proceedings of the 15th Army Science Conference, 17-19 June 1986, New York.* vol. 2. Fort Belvoir, Virginia, USA, Defense Technical Information Center. p. 246.

Macher, G., Schmittner, C., Veledar, O. & Brenner, E. (2020) ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell. In: Casimiro, A., Ortmeier, F., Schoitsch, E., Bitsch, F. and Ferreira, P. (eds) *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops: DECSoS 2020, DepDevOps 2020, USDAI 2020, and WAISE 2020, 15 September 2020, Lisbon, Portugal* (Lecture Notes in Computer Science, vol. 12235). Cham, Switzerland, Springer International Publishing. p. 123-135.

Malatji, M. (2023) Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference on Cyber Management and Engineering (CyMaEn), 26-27 January 2023, Bangkok, Thailand.* Piscataway, IEEE. p. 117-122. doi: 10.1109/CyMaEn57228.2023.10051114.

Nagar, G. (2024) The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *International Journal of Scientific Research and Management (IJSRM).* 12(06), 1282-1298. doi: 10.18535/ijsrm/v12i06.ec09.

NIST (2023) AI-enhanced cybersecurity frameworks: Integrating machine learning in automotive security. *NIST Cybersecurity Whitepaper.* https://www.nist.gov/cyberframework [Accessed 6th November 2024].

Norton Labs. (2023) Next-gen ransomware detection with AI: Trends and solutions. *Symantec Research Report.* https://us.norton.com/blog/emerging-threats/threat-report-q2-2024 [Accessed 12th February 2025].

Nwoye, C.C. & Nwagwughiagwu, S. (2024) AI-Driven Anomaly Detection for Proactive Cybersecurity and Data Breach Prevention. *International Journal of Engineering Technology and Management Sciences.* 08(11), 339-356. doi: 10.5281/zenodo.14197924.

O'Gorman, G. & McDonald, G. (2012) Ransomware: A growing menace. *Symantec Corporation Arizona, AZ, USA.* https://banadersanlat.com/wp-content/uploads/2012/12/ransomware-a-growing-menace.pdf [Accessed 2th November 2024].

Pomerleau, D.A. (1988) ALVINN: An Autonomous Land Vehicle in a Neural Network. *Proceedings of the 2nd International Conference on Neural Information Processing Systems, 1 January 1988.* Cambridge, MA, United States, MIT Press. p. 305-313.

Pope, J. (2016) Ransomware: Minimizing the risks. *Innovations in Clinical Neuroscience*, 13(11-12), 37-40.

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B.C. & Assi, C. (2023) The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access.* 11, 40698-40723. doi: 10.1109/ACCESS.2023.3268535.

Rivera, L. & Yoon, J., Ransomware: An overview of a global problem. *Prevention.* 14(17), 418.

Schlenoff, C.I., Kootbally, Z., Rachakonda, P., Lightman, S., Vassilev, A., Wollman, D.A. & Griffor, E. R. (2024) Standards and Performance Metrics for On-Road Automated Vehicles. *U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD Report number: NIST IR 8527.* doi: 10.6028/NIST.IR.8527.

Schmittner, C., Ma, Z., Reyes, C., Dillinger, O. & Puschner, P. (2016) Using SAE J3061 for automotive security requirement engineering. In: Skavhaug, A., Guiochet, J., Schoitsch, E. and Bitsch, F. (eds.) Computer Safety, Reliability, and Security: SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, 20 September 2016, Trondheim, Norway (Lecture Notes in Computer Science, vol. 9923). Cham. Switzerland. *Springer International Publishing.* p. 157-170.

Sgandurra, D., Muñoz-González, L., Mohsen, R. & Lupu, E.C. (2016) Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection. *ArXiv abs/1609.03020*.

Shan, H., He, K., Wang, B. & Fang, X. (2020) Road vehicles Cybersecurity system evaluation method. *Journal of Physics: Conference Series.* 1607(1), 012054. doi: 10.1088/1742-6596/1607/1/012054.

Tarnowski, I. (2017) How to use cyber kill chain model to build cybersecurity? E*uropean Journal of Higher Education IT.* https://api.semanticscholar.org/CorpusID:212413006.

Watney, C. & Draffin, C. (2022) *Addressing new challenges in automotive cybersecurity.* R Street Institute. Policy Study no. 118.

White, G.B. & Sjelin, N. (2022) The NIST cybersecurity framework. *Research Anthology on Business Aspects of Cybersecurity.* Pennsylvania, USA, IGI Global, pp. 39-55.

Wolf, M., Lambert, R., Schmidt, A.-D. & Enderle, T. (2017) Wanna Drive? Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles. *Proceedings of Embedded Security in Cars Conference (ESCAR), 7-8 November 2017, Berlin, Germany.*

Zavarsky, P. & Lindskog, D. (2016) Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. *Procedia Computer Science*. 94, 465-472. doi: 10.1016/j.procs.2016.08.072.

Zhang, B. (2016) *In 2 years your Tesla will be able to drive from New York to LA and find you.* Available at: https://finance.yahoo.com/news/elon-musk-two-years-car-202858960.html [Accessed 16th February 2025].