Cybersecurity in modern cars: awareness and readiness of auto workshops

David Hedberg
School of Informatics, University of Skövde, Skovde, Sweden

Martin Lundgren
Department of Computer Science, Information Systems, University of Skövde, Skovde, Sweden, and

Marcus Nohlberg
School of Informatics, University of Skövde, Skövde, Sweden

Received 9 November 2023
Revised 10 January 2024
Accepted 10 January 2024

Abstract

Purpose – This study aims to explore auto mechanics awareness of repairs and maintenance related to the car's cybersecurity and provide insights into challenges based on current practice.

Design/methodology/approach – This study is based on an empirical study consisting of semistructured interviews with representatives from both branded and independent auto workshops. The data was analyzed using thematic analysis. A version of the capability maturity model was introduced to the respondents as a self-evaluation of their cybersecurity awareness.

Findings – Cybersecurity was not found to be part of the current auto workshop work culture, and that there is a gap between independent workshops and branded workshops. Specifically, in how they function, approach problems and the tools and support available to them to resolve (particularly regarding previously unknown) issues.

Research limitations/implications – Only auto workshop managers in Sweden were interviewed for this study. This role was picked because it is the most likely to have come in contact with cybersecurity-related issues. They may also have discussed the topic with mechanics, manufacturers or other auto workshops – thus providing a broader view of potential issues or challenges.

Practical implications – The challenges identified in this study offers actionable advice to car manufacturers, branded workshops and independent workshops. The goal is to further cooperation, improve knowledge sharing and avoid unnecessary safety or security issues.

Originality/value – As cars become smarter, they also become potential targets for cyberattacks, which in turn poses potential threats to human safety. However, research on auto workshops, which has previously ensured that cars are road safe, has received little research attention with regards to the role cybersecurity can play in repairs and maintenance. Insights from auto workshops can therefore shed light upon the unique challenges and issues tied to the cybersecurity of cars, and how they are kept up-to-date and road safe in the digital era.

Keywords Connected car, Vehicle cybersecurity, Auto workshop security

Paper type Research paper

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-11-2023-0211

Introduction

Cars have been at the forefront of human society for the last century, enabling people to travel across vast distances. But cars have also evolved into something much more than a means of transportation. Each year, new features are added. Modern cars can be described as a distributed computer network on four wheels (Ring, 2015), with computers handling everything from antilock braking systems to adaptive cruise control. Lately, communication between these computer systems has extended outside the car itself. Ring (2015) explained vehicle-to-vehicle communication, which is a tool whereby cars communicate with each other. One purpose for such a tool is crash avoidance, as cars can relay their positions to each other in real time and thereby help to avoid potential collisions. However, this extended communication can also be exploited. Cars have been shown to be a legitimate target for cyberattacks. In one famous example, two security researchers were able to hijack and take remote control of a Jeep Cherokee's breaks and steering (Levi *et al.*, 2018). In another example, security researchers managed to take control of a Ford Escape (Greenberg, 2013).

Although security in cars is discussed and studied by researchers and car manufacturers, one seemingly overlooked area is the auto workshop. There are, however, indications that more research tied to auto workshops in cybersecurity is needed. For example, Martínez-Cruz *et al.* (2021) mentioned car repair as a requirement for new systems to increase cybersecurity in cars. Eiza and Ni (2017) mentioned how a modern car has between 30 and 100 electrical control units, and they all deal with different subsections of the car's different systems. If an auto workshop mechanic were to accidentally disable communication to any of the subsystems, the car may be more vulnerable to cyberattacks. Cars should therefore not only be seen as a means of transportation but rather as cyber assets in need of protection. This has been identified to some extent by manufacturers, as modern cars contain several security functions integrated into their internal computer systems. However, a security feature only works as well as the person using it. The auto mechanics working in auto workshops are not educated IT or security professionals. Yet, improper actions taken during car repair or maintenance may lead to vulnerabilities in the car's system being overlook or even introduced, which can be exploited later on in a cyberattack. Every car needs to go to a workshop at some point. Auto workshop mechanics therefore face unique challenges and issues tied to cybersecurity of cars and keeping up-to-date on every car model and their latest features. While auto workshop mechanics are well versed in traditional car security and safety, the question remains – to what extent is cybersecurity considered?

This paper sets out to shed light on auto mechanics awareness of repairs and maintenance in relation to a car's cybersecurity and is an extension of the study carried out by Hedberg *et al.* (2023), with a rewrite of the empirical insights and an expanded discussion. The remainder of this paper is outlined as follows: First section discusses related research on the topic of cybersecurity in connected cars and its relation to auto workshops, followed by second section, which presents the research approach. Third section presents an overview of the identified themes and empirical insights gained, and fourth section discusses the result of the study and highlights its conclusion and future work.

Related research

In their article, Amin and Tariq (2015) discussed the issue of "glue code" present in the computer systems of modern cars. The concept refers to when suppliers outsource the development of tools and software that are then integrated using so-called "glue code" to make them work together because the components may have been developed by different outsourced companies. The manufacturer then integrates the tools, firmware and software

into the car. This type of integration paves the way for cybersecurity-related issues between the car and the implemented module (Amin and Tariq, 2015). Glue code has been responsible for numerous well-published hacks against cars (Pike *et al.*, 2017).

A possible solution to the issues caused by glue code is a more intrusive approach by the manufacturer, in which they oversee the development (Pike *et al.*, 2017). Procedures such as information sharing, progress checkups and meetings to make sure whatever is being developed through outsourcing will fit in with the other outsourced programs and tools may also prove useful.

While Amin and Tariq (2015) did not elaborate on auto workshops, the structure of the issue is similar for workshops. Communication and information from the manufacturer can create a better aftermarket, as glue code may be the root cause of issues that occur during reparations as well.

Mousavian *et al.* (2018) discussed the possible implications when integrating connected cars, especially electronic vehicles, into infrastructure. They mention how the smart grid may be vulnerable to cyberattacks from cars. Smart grids are already working at a high capacity with automation protocols and systems that face security challenges of their own. When connected vehicles are added to the smart grid, security will become even more complex. Mousavian *et al.* (2018) noted how connected cars are being pushed onto the market in the race to beat competitors (Humayed and Luo, 2015). Instead of carefully considering how each feature and how more connections might create possible issues or vulnerabilities, new updates and features are pushed with each new model.

Making cars smarter and connecting them has brought along cybersecurity issues. Dibaei *et al.* (2020) covered several such examples, where cars have been hacked through different means. BMW, Tesla, Chrysler, Toyota and Ford are all examples of manufacturers with exploited models, which shows how the issues are industry-wide and not tied to a specific manufacturer or model of car. Dibaei *et al.* (2020) showed different potential attack vectors for connected cars. The examples include both direct attacks and attacks via proxies such as infrastructure – such as an auto workshop, even though the study does not explicitly mention it.

Most software devices eventually need updates: phones, computers and smart TVs. The difference between such devices and a car is that the car was not created with constant updates being sent across the internet in mind. The area of over-the-air software and firmware updates for cars is covered by Halder *et al.* (2020). In their study, they discussed the importance of updates as the dependency on electrical components and software increases in cars. This has led to an increase in cybersecurity issues as well, increasing the number of recalls by manufacturers. Over-the-air updates can help alleviate this issue. Halder *et al.* (2020) gave examples with several benefits. They include lower cost, as recalls are expensive, and better safety, as patches can be sent at a more regular interval. However, the solution is not without its issues – such as a need for connectivity and a new attack vector for hackers. This relates to auto workshops as well, because the computer systems that handle the updates and the hardware that receives the connection still need occasional repairs. If cars start relying more on wireless updates, the need for these to function properly increases.

Morris *et al.* (2020) did a study where they focused on digital communications capabilities in connected cars and how cybersecurity is inadequate in its current state within the car industry. Digital communication issues can lead to cybersecurity issues when different components are integrated that are not cyber-resilient. The issue is similar in fashion to the concept of glue code, which mainly exists to combine incompatible software components (Amin and Tariq, 2015). The study also covers how the heavier reliance on electrical

components and the introduction of connected cars have led to a decrease in communication, such as software and updates, between different manufacturers and other actors, such as independent workshops. This, in turn, means less collaboration with secondary companies such as those who create spare parts, after-market components, and auto workshops. The study put forth that this might originate in a lack of trust between manufacturers and suppliers, as things are seen as more secure if as few people as possible know how they function. Manufacturers keeping knowledge to themselves only increases the chance that a cyberattack happens against a car in a workshop. Although this problem is mainly attributed to the manufacturers themselves, workshops also have their part to play in integrating secure ways to share information and the proper utilization of security systems.

As cars get more and more systems, such as GPS transmitters and radars, mechanics may need to incorporate fixing these into their work routines, as they may become a staple of every car in the future (Bean, 2017). This may bring more issues along with it, as parts that are more vital to the cybersecurity of a car need to be changed or swapped by mechanics. Kirk (2015) speaks of how modern cars are a collection of parts from several different manufacturers, which leads to integration issues. This may also mean that computers need calibrations after repairs or when a radar, transmitter, or computer is changed. If these calibrations are done incorrectly, the security functions of the car may not work properly and create possibilities for cyberattacks. Also, considering that the demands to become a car mechanic are rather low with no demand for certificates, there is no pressure for mechanics to learn these new components instantly unless they break often or if every car has them (Holm, 2013).

Physical access to anything increases the cybersecurity risks tied to it, which is why server halls require high security, no matter the company. Hodge *et al.* (2019) mention two different threats tied to physical access. One of which concerns the changing of telematics devices. The report explains how after-market telematics devices can be used to hack vehicles. While getting physical access to a vehicle may be difficult, replacing a part before an unsuspecting mechanic acquires it is a possible risk. The mechanic then replaces the part without realizing it is dangerous, as he sees no difference between the two, which puts the car in a vulnerable spot and makes it susceptible to hacks. Auto workshops can also have access to specific software that, in the wrong hands, can be used for malicious intent. An example of such software is key programming software (Bergström, 2021). As reported by Bergström (2021), a new certificate will enter the Swedish market in August 2023. The new certificate will be required for unauthorized auto workshops to be allowed access to some software.

Against the backdrop of the related research, cybersecurity considerations in modern cars are becoming increasingly important. Cybersecurity does not only pose new challenges when ensuring the road safety of cars but also to the auto workshop mechanics tasked with repairing and maintaining them. Studying these challenges, along with the practices and awareness among auto workshop mechanics, addresses a knowledge gap that furthers the research stream on cybersecurity related to cars.

Study approach

Data collection

To capture the experiences with cybersecurity related to cars and any existing procedures or tools applied, a qualitative research approach was designed. A semi-structured interview was chosen to allow for richer insights gained from follow-up questions to further elaborate on points of interest (Humayed and Luo, 2015).

The respondents included in this study were managers of auto workshops, specifically those with a background as mechanics. The reason behind choosing managers is that they have the best overview of all parts of their workshop. They are also the ones most likely to know the administrative processes that can be used if a car is attacked, while also having some knowledge about the practicality of them. In addition to that, they may have knowledge of the broader perspective related to other workshops and thus be able to reflect upon the current landscape along with the role of a workshop and how it has evolved. The scope of the research and the research questions are more catered toward an administrative standpoint. Thus, managers and administrative information are deemed to be the primary information, while any practical information or work-life experience will also be relevant.

A total of eight respondents were interviewed (see Table 1). They were approached using personal contacts in the industry and through emails/phone calls.

An interview guide was developed based on the capability maturity model (CMM), developed by IBM (Buecker *et al.*, 2014). This version of CMM is targeted toward cybersecurity and is a part of a larger security framework that can be applied to the cybersecurity efforts of a company to evaluate how well they have prepared and if they have processes in place to deal with different threats and attacks. The interview questions responded to the four different domains of the model (see column headers in Table 2), and the correlating levels 1 to 3 (i.e., basic to optimized, as listed in the row headers in Table 2) of protection. During the interviews, respondents used the CMM as a base for their answers to get fewer abstract judgments and to create numerical data. This way, the respondents could judge that they were on "level X out of three in this category," thus providing a kind of self-evaluation from the respondents.

To ensure the high quality and relevance of the questions asked during the interviews, they were tested in a pilot interview on one person matching the inclusion criteria that were not used later in the actual analysis.

Respondent	Independent	Origin as a mechanic
Alpha	No	No
Beta	No	Yes
Gamma	Yes	Yes
Delta	No	Yes
Epsilon	No	Education, no work experience
Zeta	Yes	Yes
Eta	No	Yes
Theta	Yes	Yes

Source: Created by authors

Table 1.
Respondents

Optimized	Identity governance	Managing encryption keys	Vulnerability correlation	Anomaly detection
Proficient	Access management	Data loss prevention	Source code scanning	Asset management
Basic	Directory management	Encryption	Application scanning	Antivirus
	People	Data	Applications	Infrastructure

Source: Adapted from Buecker *et al.* (2014)

Table 2.
CMM overview

Data analysis

The analysis was done using a thematic analysis (Alhojailan, 2012) to interpret the data in a structured manner and gain an understanding of the thoughts and experiences of several respondents. The transcripts were first read through, and reoccurring answers were noted down as codes. Similar codes were then grouped together to form themes. Some codes were considered themes on their own, whereas others were too specific. For example, "changing telemetry devices" and "changing electronic control units" are similar processes and were therefore grouped together under a common theme. Some codes were simply rebranded to better reflect what they contained, such as "theoretical readiness" becoming "response," as that is what the respondents discuss in their answers. Initially, there were 12 identified themes, and in the second phase, they were compacted into seven themes:

(1) diagnostics computers;
(2) traceability;
(3) handling of electronic control units (ECU);
(4) manufacturer relationship;
(5) responsibility;
(6) theoretical response; and
(7) self-evaluation (using the CMM).

The next step of the analysis was to extract relevant parts of text from the transcriptions into each of the identified themes. The extracted texts for each theme were then examined, where quotes of particular interest were highlighted for inclusion and differences and similarities synthesized into a coherent text that described the characteristics of the theme.

Empirical insights

The following section presents an overview of the empirical results with example quotes that highlight some of the points captured in each theme.

Diagnostics computers

The diagnostics computers theme captured the need for reliable diagnostic tools. Throughout the interviews, it was clear that a computer running a type of diagnostic software was almost always used when repairs or services on a car were conducted. Indeed, it was even noted by the interviewees that it would be difficult to get any service or repair done without such a diagnostic computer because its software is what informs the mechanics if there are any issues with any of the ECUs in the car, as well as display error codes and messages. However, how these computers were obtained and configured varied significantly between branded and independent workshops.

In the case of branded workshops, these diagnostic computers were readily installed and preconfigured directly from the factory. The computers and the software were not updated remotely; instead, the computer itself was replaced every few years by the manufacturer. Which, according to the interviewees representing branded workshops, caused them to be slow to use by the end of their cycle. While not a rule *per se*, trust was put into the mechanics not to use these computers for other things than diagnostics. But they were occasionally used for arbitrary computer use by the mechanics, such as for browsing the Web.

Independent workshops, on the contrary, did not have the benefit of access to such readily configured diagnostic computers, nor was it a guarantee that they were available for purchase from the manufacturers. Even if the diagnostics computers were available for

purchase, as an independent workshop, they would have needed to buy one such computer from each different type of car brand they served, which would simply have been too expensive. Instead, consensus among these independent workshops was to opt for after-market or third-party products that covered several car brands and could be used with common, off-the-shelf computers. However, these products, according to the interviewees, were often unreliable as they did not have any official support from the manufacturers themselves. As a result, they did not always support proprietary hardware, or they displayed incorrect information, such as error messages and codes. Theta explained that:

> Because we are an independent workshop, we get nothing from any general agent, so we must rely on after-market equipment from a third party. We don't get a ready computer, but rather a 'box' that we plug into any laptop [. . .] it is not always reliable, so we have several ['boxes'] from different providers so we can double or even triple-check error messages.

The consensus among the interviewees was that, no matter if it was a brand or third-party diagnostic software, the computer did not always notice modifications that had been carried out on an ECU. Indeed, one way to tune up a car is to do just that, modify the software of an ECU. Delta noted that "the computer doesn't always remark on such modifications," but also noted that branded workshops could easily solve such issues. For example, when ECUs were suspected of having been manipulated, Delta explained that the software used by branded workshops had privileges to "run an [ECU] update, and the tune-up software would be overwritten." However, making modifications to an ECU without the right diagnostic software or noticing such modifications is not possible. Furthermore, changes made to GPS or radar components relied on similar software, equipment and privileges as do ECUs, meaning that only branded workshops could maintain such components as well.

Traceability

Traceability highlighted the challenges of tracking who has conducted what tasks through a work order. This relates both to digital traces regarding who has used the diagnostic computer and to what end, as well as paper trails to log what mechanics have conducted which specific tasks. One reason given for the challenges around keeping track of the digital traces was that a mechanic often logs onto a computer, which is then passed around between different mechanics. Epsilon explained that "you can see that our workshop did the job, but saying exactly who is hard." Similar explanations were given by the other interviewees, forming a consensus around the issue. "You can see that our workshop did the job, but," noted Epsilon, "saying exactly who is hard."

Instead, the work order is used to track who did what. However, this document is meant for planning and not for tracking. As Eta put it, "I cannot check [what mechanic did what] in the computer, but I can see who did it through their work order. Complete with timestamps and such things." Interviewees from both the branded and independent workshops noted that there have been talks about new up-and-coming systems that will improve upon this, but there is no consensus on when such a system will be implemented.

Handling of electronic control units

The interviewees shared a sentiment around the handling of ECUs, which was that these control units are not easily replaced. Indeed, upon replacing an ECU, that particular type of control unit had to be ordered blank. That is to say, without any configuration, and for a specific make and brand. The mechanics at the workshop must then provide the control unit with the configuration via the diagnostics computer using the manufacturer's software. No manual changes can be made by the mechanics. The handling of ECUs thus presents a

challenge for independent workshops because only branded workshops have access to the manufacturer's software. "You just press a button," explained Eta, "and then you go get coffee, and it does the work by itself." Which also meant that independent workshops had no option but to refer such jobs to the branded workshops.

What is more, all ECUs in a newer car must be configured with the same, unique chassis number of the car that it is being put into for it to work. From a security point of view, tying ECUs to the unique chassis number means that the car cannot be driven if a completely rogue component has entered the system. Instead, the car will alert the driver that something is amiss. However, it also means that a component cannot be salvaged from scrapyards and repurposed, which has otherwise been common practice. "A few years ago," explained Epsilon:

> [. . .] there were some cars where we could pick up a control unit from a scrapyard, re-code it, and put it into the car, but that is impossible now. As soon as [the ECU] is busted, there is no option but getting a new one.

Manufacturer relationship

The relationship between the manufacturer and the workshop was shown to play an instrumental role. Branded workshops can, for example, discuss issues and escalate them to be solved by the car factory's engineers. Indeed, "if our highest-tier technicians here cannot solve the issues," said Alpha "they can contact the factory through a hotline [. . .] which means the engineers who designed the car." Such a channel of communication provides branded workshops with exclusive, in-depth support. It also allowed the manufacturer's engineers to connect to the car remotely, via a secure network, so that "they can look directly into the car's system and read a lot of different values," explained Alpha. That way, the manufacturer's engineers can get additional information about the car, read error messages and even upload new software and firmware.

For an independent workshop, no such exclusive troubleshooting is available. Instead, they often resort to limited, third-party suppliers (e.g. to acquire official circuit or wiring diagrams for cars), trail-and-error approaches, or simply referring the customers to a branded workshop. Theta noted that independent auto workshops do not have the luxury of branded workshops, "the issue is cooperation between an independent workshop and a branded workshop [. . .] on knowledge, equipment, and competition." However, as Theta elaborated, such cooperation could be established, e.g. by contractual demands from the car manufacturer.

Responsibility

Who has the primary responsibility for keeping the car safe concerning cybersecurity? This was a question that popped up throughout the interviews while discussing the topic of a car manufacturer's role and was captured in this theme. Among the interviewees, consensus was that the general manager and the car manufacturer have the most responsibility for ensuring cars safety and security. The consensus was captured quite well by Zeta that their:

> [. . .] task is always to be as good as we can be, and make sure our mechanics get the education and are constantly learning. That is also very important, but the foundation for this [security] still needs to come from the manufacturer.

It was noted that the workshop mechanics have a responsibility to continuously learn and use the tools available to them in a correct, secure and safe manner. However, the consensus was that the manufacturer has the primary responsibility to create a secure product, starting

at the design stage. Or as Zeta put it, "[The main responsibility] should be on the manufacturer. In the end, they are the ones developing and providing the car."

Theoretical response

The theme "theoretical response" captured the reaction to various fictitious scenarios. Although possible solutions to the different scenarios were suggested by all respondents, there was also much uncertainty among them. The main difference between the respondent's proposed solutions were that branded workshops tended to refer to assistance from the manufacturer or general agents. For example, Beta explained that:

> We get the car here, connect it to the factory, and they will see if there's *anything weird with the ECUs, if they're* stolen or modified. They can see if anything seems off in the car since all components are registered via the chassis number, so they know what is supposed to be in the car.

In contrast, independent workshops do not have the luxury of receiving help directly from the manufacturer. Instead, they rely on traditional, manual troubleshooting as their first response. This poses a challenge in the event of a previously unknown issue with, for example, the car's ECUs or even recognizing that the car has been the target of a cyberattack. When asked about reacting to a car that showed signs of being infected with ransomware on its in-car entertainment system, Gamma jokily replied that they "would just pull the car out of the workshops and tell the customer that they are in trouble." While said as a joke, it captured the lack of an immediate solution for independent workshops.

When responding to a similar question, Beta, who represented a branded workshop, noted that one immediate solution could be to put the car into "workshop mode." While this type of mode exists in many different cars, not all interviewees knew about it. Originally put there to ensure no feature or function (or even the car itself) was started that could potentially hurt the mechanic working on the car, the workshop mode also blocks all wireless connections with the car. A first preventative measure to ensure that the attack would not spread elsewhere.

Self-evaluation

The self-evaluation of the respondents presented some uncertainty as to where on the scale to place themselves. While there was an outlier on both ends of the spectrum, the majority of the respondents placed themselves in the grey area between basic (1) and proficient (2), with several saying that they were in the "1.5-zone." The results from the self-evaluation in the CMM is summarized in Table 3.

Respondent	Rating	Comment
Alpha	3	Confident in their rating. The only 3
Beta	1	One respondent said 1, the other between 1 and 2
Gamma	2	The technology exists, the knowledge does not
Delta	1	Between 1 and 2, but more leaning toward 1
Epsilon	1	Cybersecurity is rarely discussed as a subject
Zeta	1	1 with the preface that it is on the manufacturer to protect the cars
Eta	2	The protection depends on the brand
Theta	1	Quick to say 1, sure that their security is bad

Source: Created by authors

Table 3. Results from CMM, where 1 is low, 2 is proficient and 3 is high capability

After the self-evaluation, the respondents were asked what would be needed to improve their CMM score. The answers gravitated around the theoretical know-how, ranging from "simply a lack of knowledge" (Theta) to "missing education" (Beta). Beta further elaborated that the education, remarking that "information has to come from somewhere, we cannot just acquire knowledge from thin air."

Discussion

The different ways an attacker might exploit a car are mapped out in several articles. However, less attention has been given to research related to cybersecurity and the role of auto workshops. Much of the previous research was based on experiments and using the expertise of security experts to attack cars and develop security controls around them. Such research articles and the results presented in this study differ in that aspect, as this study focuses on people with little to no knowledge of cybersecurity. Yet, these are the people who will need to use, repair and implement the developed security controls. Thus, their thoughts and insights are important to further this research stream on cybersecurity related to cars. According to the interviewees, it seems that the auto workshop industry has an issue with not being trusted with different kinds of information. Manufacturers instead ask workshops to turn to them for expertise each time a new issue presents itself. Previous research mentions both a lack of knowledge and a lack of trust (e.g. Amin and Tariq, 2015 and Morris *et al.*, 2020), but how the two are correlated is also important. This was noticed in the interviews by the respondents, and it is an area ripe for further research.

For example, cybersecurity was not discussed much in their industry (at least not among auto workshop mechanics), both because of a lack of trust resulting in little to no information regarding the subject reaching them, but also a general disinterest in the field. This lack of interest is not mentioned much in existing literature but was discussed by all respondents as something that is developing naturally with the new generation. While interest in cybersecurity within the car industry might be changing with the next generation of workers, waiting for the entire industry to be replaced by personnel with an interest in the subject is not feasible. Furthermore, cybersecurity awareness and the skills needed to address such risks would mean continuous training for workshop mechanics as cars are becoming ever more interconnected and digitalized. This is no small challenge, considering other professions (such as software development [Salin and Lundgren, 2022], for example) that have long strived to incorporate such skillsets among their workers.

What exact skills would be required remains to be hashed out by additional research, and the needs that presents themselves over time to those working as auto workshop mechanics. However, glimpses of what such skills might look like can be seen from this study, such as cybersecurity awareness and incident response. Considering that the security of the cars is currently tied to the security of the diagnostics computer and how it is used to upload information into ECUs, an attacker could target the software updating the ECU by injecting malicious code into it before the program uploads the update into the ECU. Mechanics working in auto workshops should thus have some cybersecurity awareness, or insights, about related risks. Not just toward cars specifically but also the digital environment in general and the know-how required to mitigate these. For example, by keeping computers updated and having some form of antivirus software installed, along with strict policies for what the diagnostics computers may or may not be used for. Similarly, if something were to happen, it is currently said to be hard for mechanics to notice irregularities or potential threats. As such, some basic incident response capabilities in the form of initial intrusion detection would be beneficial. For example, access to log entries to

see what changes have been made to the ECUs, by whom and the knowledge for how to act thereafter should something be amiss in the form of mitigating or remediating actions.

However, support would be needed from the manufacturer of the car as well. In the same manner that DevSecOps was introduced to align development and operations with security best practices (Myrbakken and Colomo-Palacios, 2017), one could expect a similar approach to the culture around the car designer. For example, manufacturers security engineers could recommend tailored security methods for a particular car. These recommendations could then be used by both branded as well as independent auto workshop mechanics, as they are the ones who will maintain the vehicle over time (a sort of "DevSecMec," if you will).

The work conducted within this study highlights some of the challenges in making auto workshops ready for the connected future the world is heading toward. The next logical step would be to discuss the findings with car manufacturers. For example, one important aspect to evolve is the relationship between manufacturers, branded workshops and independent workshops. As noticed in this study, branded and independent workshops work differently. Thus, the relationship between all three should be evaluated and further studied, be it through interviews or a case study. Manufacturers may, as argued by the respondents in this study, have the primary responsibility to make these cars as safe and secure as possible. Thus, the next step would be to investigate the trends and incentives in car cybersecurity development and their take on the development of transparency, education and knowledge sharing with both independent and branded workshops.

Conclusions

When it comes to discussing cybersecurity in auto workshops, it is important to make a distinction between branded and independent auto workshops. While a lot of the classic workshop jobs – changing brakes, general service or repairing a radiator – are the same, every job tied to the internal systems differs in some manner. Independent workshops do not have the equipment, communication or privileges that branded workshops do. This creates two rather different work processes where one side has clear guidelines and work orders, and the other is more flexible and solves issues in whichever manner they can with whatever tools they can acquire. When an independent workshop hits a roadblock and encounters an issue that they, for any reason, cannot solve, their only option is to refer the customer to another, branded auto workshop. The branded auto workshop can then use its escalation chain to acquire assistance straight from the factory if needed. Both approaches present their own unique security challenges while also having some overlap. Where branded workshops have a direct line of communication with the internal systems of the car via a computer that is connected to the internet and may or may not be particularly well secured, the independent workshop uses third-party diagnostics equipment meant to circumvent the internal systems to acquire error codes for the mechanic to work from.

Manufacturers are an integral part of how an auto workshop operates. All respondents discussed how cybersecurity related to cars is not an area ever really mentioned. It is not mentioned at conferences or in meetings between managers. As it is not brought up or discussed, the general knowledge is not improved. Most respondents expressed how they have never even thought about cars being targeted or hacked. Connected cars are still a fairly new concept, and attacks against them are still theoretical, which probably partly explains why they are never mentioned, but the first step to knowledge is general discussions and an interest in the area.

Although the path to security is a long one, auto workshops do have several precautions and general security. Secure networks for communication, placing diagnostic computers on a separate network, workshop mode in the cars, secure software for updates to ECUs,

certifications for technicians and general traceability are some of the current solutions. Although these are seemingly not enough, they are a step in the right direction. It is important to remember that auto workshops have existed for a lot longer than connected cars, and industry-wide changes do not happen overnight. However, preparing for a threat before it becomes reality creates safer, more secure environments and better cybersecurity – no matter the industry or area.

References

Alhojailan, M.I. (2012), "Thematic analysis: a critical review of its process and evaluation", *WEI International European Academic Conference Proceedings*, Citeseer, Zagreb, Croatia.

Amin, M. and Tariq, Z. (2015), "Securing the car: how intrusive manufacturer-supplier approaches can reduce cybersecurity vulnerabilities", *Technology Innovation Management Review*, Vol. 5 No. 1, pp. 21-25, doi: 10.22215/timreview/863.

Bean, T. (2017), *The Auto Repair Shop's Role in Connected Car Cybersecurity*, Ratchet Wrench, available at: www.ratchetandwrench.com/classification/require-subscription/article/11481132/the-auto-repair-shops-role-in-connected-car-cybersecurity-2017-11-13

Bergström, N. (2021), *Nya Krav på Verkstäder* (in Swedish), Motor Branschen, available at: https://motorbranschen.mrf.se/nya-krav-pa-fria-verkstader/

Buecker, A., Arunkumar, S., Blackshaw, B., Borrett, M., Brittenham, P., Flegr, J., Jacobs, J., *et al.* (2014), *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, IBM Redbooks, available at: www.redbooks.ibm.com/redbooks/pdfs/sg248100.pdf

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., *et al.* (2020), "Attacks and defences on intelligent connected vehicles: a survey", *Digital Communications and Networks*, Vol. 6 No. 4, pp. 399-421, doi: 10.1016/j.dcan.2020.04.007.

Eiza, H.M. and Ni, Q. (2017), "Driving with sharks: rethinking connected vehicles with vehicle cybersecurity", *IEEE Vehicular Technology Magazine*, Vol. 12 No. 2, pp. 45-51, doi: 10.1109/MVT.2017.2669348.

Greenberg, A. (2013), *Hackers Reveal Nasty New Car Attacks–with Me behind the Wheel*, Forbes, available at: www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

Halder, S., Ghosal, A. and Conti, M. (2020), "Secure over-the-air software updates in connected vehicles: a survey", *Computer Networks*, Vol. 178, p. 107343, doi: 10.1016/j.comnet.2020.107343.

Hedberg, D., Lundgren, M. and Nohlberg, M. (2023), "Cyberthreats in modern cars: responsibility and readiness of auto workshops", in Furnell, S. and Clarke, N. (Eds), *Human Aspects of Information Security and Assurance*, Springer Nature, Switzerland, Cham, Vol. 674, pp. 275-284, doi: 10.1007/978-3-031-38530-8_22.

Hodge, C., Hauck, K., Gupta, S. and Bennett, J.C. (2019), *Vehicle Cybersecurity Threats and Mitigation Approaches, No. NREL/TP-5400-74247, 1559930, p. NREL/TP-5400-74247, 1559930*, National Renewable Energy Lab. (NREL), Golden, CO, doi: 10.2172/1559930.

Holm, O. (2013), *Dags För Yrkesbevis Inom Fordonsbranschen* (in Swedish), MotorMagasinet, available at: www.motormagasinet.se/article/view/415473/dags_for_yrkesbevis_inom_fordonsbranschen

Humayed, A. and Luo, B. (2015), "Cyber-physical security for smart cars: taxonomy of vulnerabilities, threats, and attacks", *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, presented at the ICCPS'15: ACM/IEEE 6th International Conference on Cyber-Physical Systems, ACM, Seattle Washington, DC, pp. 252-253, doi: 10.1145/2735960.2735992.

Kirk, R. (2015), "Cars of the future: the internet of things in the automotive industry", *Network Security*, Vol. 2015 No. 9, pp. 16-18, doi: 10.1016/S1353-4858(15)30081-7.

Levi, M., Allouche, Y. and Kontorovich, A. (2018), "Advanced analytics for connected car cybersecurity", *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, presented at the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), IEEE, Porto, pp. 1-7, doi: 10.1109/VTCSpring.2018.8417690.

Martínez-Cruz, A., Ramírez-Gutiérrez, K.A., Feregrino-Uribe, C. and Morales-Reyes, A. (2021), "Security on in-vehicle communication protocols: issues, challenges, and future research directions", *Computer Communications*, Vol. 180, pp. 1-20, doi: 10.1016/j.comcom.2021.08.027.

Morris, D., Madzudzo, G. and Garcia-Perez, A. (2020), "Cybersecurity threats in the auto industry: tensions in the knowledge environment", *Technological Forecasting and Social Change*, Vol. 157, p. 120102, doi: 10.1016/j.techfore.2020.120102.

Mousavian, S., Erol-Kantarci, M., Wu, L. and Ortmeyer, T. (2018), "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks", *IEEE Transactions on Smart Grid*, Vol. 9 No. 6, pp. 6160-6169, doi: 10.1109/TSG.2017.2705188.

Myrbakken, H. and Colomo-Palacios, R. (2017), "DevSecOps: a multivocal literature review", in Mas, A., Mesquida, A., O'Connor, R.V., Rout, T. and Dorling, A. (Eds), *Software Process Improvement and Capability Determination*, Springer International Publishing, Cham, pp. 17-29.

Pike, L., Sharp, J., Tullsen, M., Hickey, P.C. and Bielman, J. (2017), "Secure automotive software: the next steps", *IEEE Software*, Vol. 34 No. 3, pp. 49-55, doi: 10.1109/MS.2017.78.

Ring, T. (2015), "Connected cars – the next target for hackers", *Network Security*, Vol. 2015 No. 11, pp. 11-16, doi: 10.1016/S1353-4858(15)30100-8.

Salin, H. and Lundgren, M. (2022), "Towards agile cybersecurity risk management for autonomous software engineering teams", *Journal of Cybersecurity and Privacy*, Vol. 2 No. 2, pp. 276-291, doi: 10.3390/jcp2020015.

Further reading

Cho, J.Y. and Lee, E.-H. (2014), "Reducing confusion about grounded theory and qualitative content analysis: similarities and differences", *The Qualitative Report*, Vol. 19 No. 32, p. 1.

Corresponding author

David Hedberg can be contacted at: davidhedberg@hotmail.com