Research Archive of
Rising Scholars (preprint)
Where bright minds share their learnings

Driving into the Digital Age: Understanding Communal Knowledge and Cybersecurity in Modern Vehicles

Ronan Wong, *John A. Rowland High School*
Noah T. Curran, *University of Michigan – Ann Arbor*

Abstract

In recent years, concerns in the automotive industry have grown significantly more diverse as car manufacturers continue to push new technologies into their vehicles. Cybersecurity is becoming crucial in modern and previous vehicle models due to additional reliance on digital components, creating a larger attack surface that endangers many cars. Many consumers remain unaware of the specific risks that recent developments have cultivated that put their hard-earned vehicles in jeopardy. This paper examines the crucial knowledge gaps surrounding vehicle cybersecurity by analyzing responses of those living within the Orange County area and thus generating solutions from said responses. The information in this paper can be seen as a baseline of knowledge that can assist the broader population with quickly implementable methods and potentially prevent vehicular robbery.

1 Introduction

The rapid-paced evolution of technology has led to digitalization throughout the automotive industry. A belief as technological advancements are made is that they maintain the same level of safety or become even safer. Unfortunately, new implementations have created new vectors for thieves to steal cars, such as in-vehicle network packet injections and signal replication. Automakers utilize over-the-air software updates to counteract these exploits, which provide routine security updates. However, it is not uncommon for software updates to unintentionally introduce a new round of vulnerabilities, enabling hackers to exploit a new attack vector. Automakers introduced other methods, such as the Intrusion Detection System (IDS) and CAN encryption, to compete in this so-called cat-and-mouse game. However, they must still be advanced enough to shield a vehicle's most vulnerable areas flawlessly. How does hacking cause car theft?

Within the Los Angeles area alone, theft has increased by over 64% since 2020 [1]. This surge is primarily attributed to technological advancements that enhanced vehicle convenience and function, creating new attack vectors for car thieves. Gateways, such as keyless entry systems, enable thieves to gain entry without physical interaction. Whether through signal recordings emitted from critical fobs or even by gaining access to newer cars' proximity-unlocking features. With the increase in car theft incidents that use such tactics, wireless systems and internet-connected features like over-the-air software updates may make remote vehicle theft easier. These hacking techniques continue to grow more complex and evolve frighteningly, emphasizing car owners' need for better security practices as cars modernize.

How are we trying to stop this problem? Standard rules exist, such as ISO 21434, that provide a basis for what car security infrastructure should be but are considered non-binding recommendations. Due to a lack of enforcement, major flaws have exponentially increased CVE (Common Vulnerabilities and Exposures). Many of these CVEs will continue to be apparent in future car models.Moreover, with a projected 11.5 million new car units awaiting manufacturing in the US [2], the vulnerabilities become much more widespread. Due to this, there cannot be a reliance on the car to remain secure. Coincidentally, Ian Tabor [3], an automotive cybersecurity researcher, had his RAV 4 fall victim to a CAN injection, which was made possible due to ease of access to the in-vehicle network via the car's headlights. Seeing how a person with extensive knowledge can become a victim of an easily performed hack, it is even more important to stress the need for basic vehicle security knowledge. It is uncommon for an average person to know what their car is and is incapable of. Thieves often abuse this gap of knowledge, with unsuspecting victims finding out their car had been stolen through a method they were unaware of. Recognition and implementation are of utmost importance when preventing these types of attacks. Once a person on a local level can realize an issue, implementation becomes straightforward. Word of mouth is essential, enabling others to perform the exact solutions and creating a more cohesive environment that ensures vehicle safety.

I have conducted thorough interviews that reiterate the information gathered through numerous papers and gathered the responses from citizens in my local community about their personal experiences and thoughts regarding

how their concern for their vehicles has changed. I have recognized the need to communicate these issues directly, find the underlying gaps in knowledge, and formulate effective solutions on a local level. However, it also creates flexible and effective solutions and applies them on a broader scale. Readers will be briefed on the technologies discussed as if they were interviewees and be able to learn easily applicable solutions to strengthen cybersecurity within their vehicles and ensure their safety.

2 The Modern Car Theft Procedure

2.1 Types of Car Hacking

Car hacking methods exploit vulnerabilities in modern vehicles' digital and physical security systems. In this section, we will explore several prevalent methods of car hacking, including their respective vulnerabilities, the tools used to exploit these vulnerabilities, and the potential outcomes.

2.1.1 CAN-BUS (Physical Injection)

The CAN-BUS method [4] injects malicious commands into a car's internal system via physical and digital entry points. This process begins by physically tampering with the vehicle, such as breaking through a headlight to access the CAN-BUS system—a crucial component that controls the vehicle's reactivity. Once access is gained, attackers flood the CAN-BUS network with false commands, forcing the car to unlock or perform other unauthorized actions. Vulnerability: Access to the CAN-BUS system through the vehicle's physical components, such as headlights. Tool: Specialized hacking tools used to inject malicious commands into the CAN-BUS. End Result: Unauthorized access to the vehicle, allowing the attacker to unlock and steal it.

2.1.2 Digital Key Abuse (Network-Based Attack)

Digital critical abuse [5] is a network-based attack that exploits vulnerabilities in a car's mobile unlocking feature, a relatively new feature implemented by many manufacturers in recent years. This proximity-based attack allows attackers to unlock and start the car if they are near the vehicle once they compromise the owner's smartphone security. Vulnerability: Compromised mobile phone security and the mobile unlocking feature. Tool: Hacking techniques to gain unauthorized mobile app or phone access. End Result: The attacker can remotely unlock, start, and steal the vehicle.

2.1.3 Relay Attack (Network-Based Attack)

Two thieves working together to extend the authentication signal from the victim's key fob to the car perform a relay attack. One thief stands near the house, capturing the key fob's signal, while the other stands near the car, relaying the signal to authenticate and unlock the vehicle. Vulnerability: Key fob proximity authentication signal can be intercepted and relayed. Tool: Signal relaying devices extending the critical fob's authentication signal range. End Result: Unauthorized access and control of the vehicle without the key fob being physically present.

2.1.4 Flipper Zero (Network-Based Attack)

The Flipper Zero [6] is a legally available device that records AM and FM signals emitted by crucial fobs. Due to a delay in resetting authentication codes, some modern vehicles allow thieves to record and use a signal to unlock the car within a short time frame. Although the tool itself is legal, its misuse for unauthorized access poses a significant security risk. Vulnerability: Authentication signals from key fobs can be recorded and reused before expiration. Tool: Flipper Zero or similar signal-capturing devices. End Result: Thieves can create a one-time-use digital key, unlocking the vehicle.

2.1.5 Bluetooth (Network-Based Attack)

Bluetooth vulnerabilities present a risk to sensitive information, but due to the complexity of the encryption involved, Bluetooth is less commonly used for car theft. While Bluetooth can potentially expose private data, the likelihood of it being a vector for direct car theft remains low. Vulnerability: Weaknesses in Bluetooth encryption. Tool: Exploitations of Bluetooth encryption vulnerabilities. End Result: While vehicle theft through Bluetooth is uncommon, this vulnerability can expose personal data, posing other risks to the owner.

2.2 Vulnerability Analysis

Car thieves exploit both physical and digital vulnerabilities in modern vehicles. The most common vulnerabilities include physical access to the car's CAN-BUS system and the interception or relay of authentication signals. Below, we examine how these vulnerabilities are exploited.

2.2.1 Headlight Access

The CAN-BUS, the network controlling the flow of commands in a car, is located behind the headlights, making it a prime target for thieves. By removing the headlight, thieves can access the wiring system and inject commands directly into the vehicle's network, manipulating the system to unlock doors or turn off alarms.

2.2.2 Emitted Signals

Signals emitted by vehicles and key fobs, such as those for locking and unlocking, open a window for interception and replication. Despite implementing features like rolling codes and proximity-based use, these signals are vulnerable to being recorded or redirected by malicious actors to perform unauthorized actions [7].

2.2.3 CAN-BUS (Control Area Network)

The CAN-BUS controls communication between a vehicle's electronic control units (ECUs), which manage everything from engine performance to security features. Once thieves gain access to the CAN-BUS, they can send commands that manipulate the car's responses, leading to theft [8].

2.2.4 Proximity Unlocking (Network-Based Vulnerability)

Modern vehicles equipped with proximity-based unlocking allow key fobs to automatically emit authentication signals to unlock the car when the owner is near. Thieves exploit this by using signal replicators to record and replay the signal when the owner is out of range, allowing them to steal the vehicle.

2.3 Built-In Car Hacking Countermeasures

While car hacking presents significant risks, manufacturers have developed countermeasures to enhance security. Below are some of the most notable defense mechanisms to thwart modern car theft attempts.

2.3.1 Rolling Codes

Rolling codes [9] are a security feature designed to change the signal emitted by a critical fob each time a button is pressed. The key fob and the car are synchronized with an algorithm that tracks the previously used codes, making it harder for thieves to reuse a captured signal. However, this system can still be bypassed if a thief jams the signal, preventing the rolling code from advancing and allowing them to capture and reuse the same code.

2.3.2 Improved Headlight Protection

Since headlights provide access to the CAN-BUS system, manufacturers have implemented several protections to prevent unauthorized access. Mercedes-Benz, for example, has introduced tamper-proof screws, while BMW has integrated sensors into newer models that trigger alarms if the headlights are tampered with.

2.3.3 OnStar

OnStar is road assistance software installed in many modern vehicles. When a car is reported stolen, OnStar can track its location and even slow it down to aid in the recovery and apprehension of the thief.

2.3.4 Over-The-Air (OTA) Updates

Over-the-air updates allow car manufacturers to remotely deploy software fixes and security upgrades to their vehicles [10], protecting them from newly discovered vulnerabilities. This proactive approach helps keep cars secure from evolving threats.

2.3.5 Intrusion Detection Systems (IDSes)

Intrusion detection systems (IDS) [11] are designed to monitor vehicle activity and detect potential hacking attempts. Security sensors in the car feed data into algorithms that detect anomalies, which are then logged in the Security Event Memory. If a threat is detected, it is flagged and sent to the manufacturer for further analysis. This data is also stored for future reference to help identify patterns in cyber attacks.

2.4 Real-World Examples of Hacking-Based Car Theft

Both modern and previous car eras are extremely susceptible to cybersecurity vulnerabilities. Aged technologies are susceptible to the newer exploits developed over the years and are not manufactured to combat said attacks. The privilege of having OTA software updates is not an option for car models that never had this privilege in the first place. Cars with this technology have new features that older models need to improve, but the new implementations pose new threats that older cars are not vulnerable to. An example is in Irvine, a nearby city in Orange County, where a man gained access to a car keycard, a new method of access introduced by Tesla and other modern manufacturers. Through this easily accessible device, the thief ransacked the victim's car and stole all of their belongings without any access to the ECU or any technical method of breaching. Similar incidents have plagued the Orange County area, largely because most cars within the region are attractive targets for vehicle theft. The most common cars within the Orange County area are the Honda Civic, Toyota Rav 4, Toyota Camry, Honda Accord, and the Tesla Model 3. These cars make up over 70% of the cars popular in Orange County, providing many opportunities for car thieves to pick and choose their next victims. These cars remain susceptible because of their mid-newer age range (2012-2023 models), with many possessing newer technologies or flawed and aged vehicle cybersecurity infrastructure.

3 Interview Process

The content of the interviews consists of responses from civilians across Orange County to assess public knowledge and concerns regarding vehicle cybersecurity. The study aimed to explore pre-existing knowledge and general awareness of current vulnerabilities and record reactions to vulnerabilities that may be unknown to the general public. The culmination of interviews would distinguish strong, weak, and unknown areas of knowledge, enabling pattern recognition of what issues needed to be addressed or were already well known. But most importantly, each interview aimed to inform each individual and address their specific needs and questions regarding their respective vehicles.

Participants were selected based on convenience, primarily consisting of individuals within the Orange County area willing to participate when approached. Of those approached, 40 agreed to participate in an interview. Every interviewee was shown a fact sheet on statistics and standard technology regarding vehicle safety, allowing for a baseline for individuals to speak about. Interviews focused on participants' knowledge of their own vehicle's security features and incidents of theft or break-ins that may have affected them in the past. Questions address their familiarity with standard automotive security technologies such as mobile entry systems, alarms, and cybersecurity measures they were aware of. Interviews were kept very conversational and emphasized the experiences of the interviewees, but when they struggled to provide input, the following questions were asked:

Questions We May Have Asked
Have you or someone you know undergone a vehicle theft?
What security features are you aware of in your vehicle?
What steps, if any, do you believe vehicle owners should take to protect themselves?
Are you familiar with any vulnerabilities?
What do you know about vehicle security technologies?
What would you do if you learned your car was vulnerable to remote hacking?

Questions, as such, allowed for continued conversations where the interviewees previously knew little about the topics or had no prior concern. These broad and easily addressable questions allowed interviewees to answer or go into areas of discussion that we would not have otherwise touched upon.

After the initial interview, participants received information on modern cybersecurity risks affecting vehicles manufactured within the last two decades. This extra information covered keyless entry, ECU, and remote hacking threats. Those interviewed were made aware of real-world instances to highlight the practical implications of the vulnerabilities stated.

Participants were asked to provide input and reflect upon the digested information after the briefing. They expressed concerns regarding their vehicle's cybersecurity infrastructure and potential risks that they had yet to

consider in the car. This feedback allowed for an analysis of awareness and its effects on the perceptions of vehicle safety.

To tailor the information to each person interviewed, the Automotive Security Research Group (ASRG) vehicle database [12] was used to find specific vulnerabilities within each person's vehicle. The database provides current issues involved with car models and manufacturers, then rating on a scale from 1-10 using the Common Vulnerability Scoring System (CVSS) to indicate the significance of the vulnerability. Doing so provided personalized data on potential threats to each person's specific cars, with vulnerabilities ranging from physical vulnerabilities to software flaws that could cause remote exploitation.

After receiving the personalized data, participants were asked to provide additional feedback on their learning. This phase explored whether those interviewed expressed their feelings regarding their vehicle's safety features and whether they felt inclined to take action to secure their vehicle. Solutions from compiled research were provided to help meet each individual's needs, and their responses were fed into the research database as a reference for future interviews.

4 Summary of Interview Responses

4.1 General Consensus

In general, many vehicle owners possess a baseline understanding of modern vehicle cybersecurity through the media or basic car knowledge. Most people are aware of common vulnerabilities, such as relay attacks or signal emissions, but do not understand the processes that enable them. The vehicle owners interviewed often know about vulnerabilities that apply to all cars but little regarding those that specifically target their vehicles. Out of the 40 interviewees, just 5 demonstrated some understanding of how these vulnerabilities function, whereas the remaining interviewees could only explain in vague terms heard from media sources.

Despite the general lack of awareness, the discussions during the interviews unveil a tendency to overestimate the protection offered by existing car security measures. This misconception can be seen most prominent in car owners with newer vehicles, as the idea is often misconstrued that new technology correlates with better security. Many vehicle owners were under the assumption that their cars were protected against most forms of both physical and digital attacks. When asked what they attribute this improvement to, the consensus of responses consisted of better software, hardware improvements, and car infrastructure, but they could not point out the specifics. For example, 20% of those interviewed were Tesla owners, and nearly 80% of them had highlighted the brand's reputation for innovation, believing that because of this, security features have remained on par with advancements. However, many were unaware of their vulnerabilities, such as the weakness in keyless entry systems. Although there are notable improvements that car manufacturers have introduced in the past few decades, there remain significant vulnerabilities and gaps that infringe on vehicle safety.

4.2 Housing Dependency

The demographic interviewed mainly resided in large cities or suburban areas, where housing is either an apartment or a family home. Responses gathered depended very primarily on where the person had worked or lived as it determined whether parking or protection from their vehicles was readily available. Many living in apartment complexes struggled to find areas where physical protection was accessible, and parking on the street had led to incidents of carjacking and brute force forms of theft. On the other hand, those who lived in houses had garages or secured driveways, preventing an attack. When asked about pre-existing concerns, most responses came from those living in non-permanent housing or a housing complex. The divide highlights the importance of addressing both physical and digital aspects of theft, as neither alone provides guaranteed protection.

4.3 Gas-Powered vs. EV

All types of vehicles are seen throughout the Orange County area, with most being gas-powered and the rest being hybrid or electric. Interviewees with gas-powered vehicles were skeptical about the impact of cyber threats on their vehicles due to their belief in the lack of digital advancement. Hybrid car owners felt very similarly, believing that the only change in their vehicle was the slight electrical integration for better gas mileage and greener usage. However, electric vehicle (EV) owners have expressed more concern about cybersecurity risks when equipped with mobile apps, remote access, and advanced driver assistance systems (ADAS). EV owners conveyed fears of being hacked while driving or their car being stolen due to the digital components of their vehicle and attributed the weakness to the digital infrastructure of the car.

4.4 Personal Lived Experience

Personal experiences deeply influence owners' perspectives on the importance of cybersecurity, with noticeable patterns emerging that were caused by previous encounters with any vehicle-related crime or geographic location. For instance, a Kia owner from downtown Los Angeles experienced two previous car break-ins. Thus, her initial concerns consisted of break-ins, but after her prior experiences, she had taken the time to research physical defenses and switched cars since then. Similarly, those who had previous encounters with theft are much more attentive and open to answering questions, having experienced it firsthand.

In the case of one participant, who we anonymously call Bob, they are a delivery driver and primary provider for their family, and they illustrate the tangible consequences of vulnerabilities in modern vehicle security systems. Bob's vehicle, a Toyota Sienna SE, was stolen through a relay attack. This allowed the thieves to unlock and start the car as if they possessed the original key, bypassing the need for physical intrusion to access the vehicle. This theft not only deprived him of his means of transportation for himself and his family but also put him out of a job, leaving him in a financial crisis.

Another case of this was the theft of many delivery vehicles, with four of the forty people interviewed being business owners who had experienced theft in some way that had hindered their business. The woman, who we anonymously call Alice and who is in the restaurant industry, had faced a period when she was without her inventory transport van due to theft. Fortunately, she was able to get her vehicle back, but there were no signs of forced entry, suggesting the theft was carried out through key fob replication or some contactless form of theft. The minimal security measures in inventory transport vehicles make them particularly vulnerable to such attacks, which have created significant challenges for business owners like Alice who depend on these vehicles for day-to-day operations.

After these experiences with vehicle cyber theft, Alice and Bob both individually had their opinions on cybersecurity permanently altered. They are more vigilant about the security of their vehicles due to the devastating impact that the theft can have on their livelihoods.

4.5 Duration of Ownership

Consequently, those with little vehicle experience or newer car owners believed that their vehicles had "advanced security features" that prevented digital theft. Yet only some were able to explain how these protections work. However, their concerns were similar to those of those already aware and having questions about physical theft. All interviewed showed some concern, although some more than others, and even fewer have implemented changes to their vehicle to ensure its safety. However, all needed a basic understanding of common cybersecurity theft, with many needing to learn they existed.

4.6 ASRG Reports

All 40 vehicle owners used the ASRG Database to obtain more specific data regarding their car's vulnerabilities during the research process. This resource enabled participants to provide more detailed responses, offering personalized and illustrative examples of vulnerabilities.

Numerous ASRG findings have reported that remote vulnerabilities are enabled by mobile car apps such as HondaLink, Mercedes-Me, and Tesla. Many older car owners needed to be made aware of the existence of these apps. However, many newer and more expensive vehicle owners have utilized these newer features, especially in Teslas and Mercedes. This led to a discovery in the importance of pricing of each car, with more luxurious vehicles with pricing typically ranging from $30,000-$60,000 having significantly more digital implementation, thus increasing the vulnerabilities shown on the ASRG database with theft vulnerabilities and data.

Owners of budget-friendly cars, priced between $5,000 and $20,000, are notably more prone to frequent attacks. One such attack is the Rollback, which involves tampering with odometers and continues to be a problem in the used car market. While these vehicles typically do not have advanced digital systems, they remain susceptible to repetitive fraud.

5 Discussion of the Responses

A pattern that emerged is the lack of awareness of specific cybersecurity weaknesses in each owner's cars. For example, many of the interviewees owned the Kia Sorento and Ford Range Rover, which are particularly susceptible to the CAN-BUS attack (which affects the majority of modern car models), which has been shown in other metropolitan areas.

Concerns about these vulnerabilities ran deeper than theft. One Nissan owner also expressed anxiety after referencing the ASRG database about the implications of data theft. Many modern vehicles store sensitive information like GPS location or contact information, and the idea that thieves could gain access to a car and the information stored inside it was troubling for many interviewees. This revealed a much broader fear of increasing vehicle interconnectedness compromising personal privacy.

Most ASRG reports brought attention to remote (Keycard and Mobile Unlocking) vulnerabilities. Similarly, new models like the newer Honda Accord (2018+) and Tesla Models Y and 3 have the function capabilities for both mobile and proximity unlocking via phone or keycard. While these technologies are convenient for users, allowing for entry without a key, they also present a significant security risk. The ASRG Database references vulnerabilities within manufacturers' respective apps, often ranking them 7+ on the CVSS scale, and are seen throughout the spectrum of most vehicles from after 2016.

In addition to using online educational resources, owners can take the initiative by implementing physical improvements to bolster their vehicles' security. Simple additions to a car, such as a steering wheel or pedal lock, do not protect its cybersecurity but create significant difficulty during thefts. These devices are apparent and may even dissuade intruders from targeting a vehicle by making it appear less attractive.

Other technical solutions, like OBD port locks, offer specialized vehicle infrastructure protection. These devices prevent unauthorized access to a vehicle's internal networks and prevent unwanted tampering with software and diagnostics. A secure OBD port mitigates the risk of exploitations that create false warnings on a vehicle, creating opportunities to unlock or even start the car.

Investing in a CAN-BUS Anti-Theft Shield provides further protection by creating a barrier between a thief and a car's internal networks. This shield reinforces against potential breaches, ensuring that communication within a car and the vehicle's components remain untampered. By combining physical and technical measures, vehicle owners can create a a comprehensive security strategy that strengthens their cars and prevents cyber threats.

Aside from making direct improvements to the car, owners may take a much simpler approach by securing their cars' signal emissions. In the interviews, many witnessed the procedure of a relay attack and the rare possibility of a rollback attack. These thefts continue to grow increasingly common due to advancing car networks that utilize proximity features. Many thieves rely on redirecting key fob authentication signals into the car to unlock a vehicle. However, Faraday pouches or essential fob protectors effectively block signals and prevent unauthorized access to a vehicle.

6 Future Work

Despite increasing awareness of vehicle cybersecurity, several issues still need to be addressed. One key factor is the complacency of vehicle owners, who often only investigate risks after experiencing a problem. Many consumers mistakenly assume their vehicles are inherently secure, a belief reinforced by technological advancements that create a false sense of safety.

Vehicle manufacturers often prioritize features that make their cars more appealing over improving security. Research shows that the rapid adoption of digital technologies has outpaced the development of adequate security protocols [13]. Despite being aware of these vulnerabilities, manufacturers are often reluctant to disclose them, fearing reputational damage or legal repercussions. This lack of transparency makes it even harder for drivers to find reliable information or take effective steps to improve their vehicle's security.

Another significant barrier is the lack of oversight in the automotive cybersecurity standards. Unlike industries such as finance or healthcare, the automotive sector has relatively loose regulations. This regulatory gap leaves manufacturers with the responsibility of establishing their own safety and security measures. As a result, there is little consistency in the cybersecurity protocols across the different brands and models of cars, which further complicates efforts to ensure a standard for industry-wide protection.

Broader solutions involve providing resources for car owners to become educated about their specified vehicle and obtain a basic knowledge of their car's capabilities. Consumer education increases awareness amongst vehicle owners about cybersecurity threats, which can be achieved through educational campaigns by the respective car manufacturers. Whether it be instructional videos or an informational website, manufacturers must outline the potential risks associated with their various vehicles to ensure their customer's safety.

However, change must also rely on car owners themselves. Vehicle owners should familiarize themselves with organizations like SAE International, which not only sets industry standards such as the SAE J3061 framework but also provides accessible guidelines and resources to promote best practices in automotive cybersecurity. Similarly, the National Highway Traffic Safety Administration (NHTSA), which enforces safety regulations and issues cybersecurity best practices for manufacturers, also offers educational materials that help consumers stay informed about security

updates and measures. By leveraging resources as such, car owners can complement industry efforts and ensure the safety of their vehicles.

7 Conclusion

The growing prevalence of cybersecurity vulnerabilities in vehicles reveals the urgent need for collective action from both manufacturers and car owners. While modern vehicles offer convenience and innovation, they also present unique security challenges that many older and newer models are ill-equipped to handle. Interviews with vehicle owners reveal a concerning gap in awareness about these threats, fueled by misplaced trust in vehicle advancements and a lack of transparency from the manufacturers.

To address these challenges, there must be both systemic and individual change. Manufacturers must prioritize security as much as functionality, adopting universal standards and providing clear, accessible resources that allow consumers to educate themselves. Organizations such as SAE International and NHTSA, offer invaluable guidelines, but their impact depends on manufacturers' willingness to integrate the necessary practices and consumers' engagement with the information

Car owners can significantly reduce risks by combining physical deterrents, such as steering wheel locks, with digit safeguards like Faraday Pouches and CAN-BUS shields. Many resources are readily available online, such as the ASRG database, which provides opportunities for owners better to understand the functionalities and vulnerabilities within their vehicles to take informed actions. Ultimately cybersecurity is not just a manufacturer's responsibility, but a partnership between the industry and car owners [14].

The future of automotive cybersecurity is reliant on balancing technological progress with robust protections. As vehicles become increasingly connected, the potential for hardship evolves beyond theft to risking personal privacy and safety. But through increased vigilance, education, and action, we can create a safer automotive ecosystem.

References

[1] T. Schlepp, "L.A. Vehicle Thefts Skyrocketing in This Area," *KTLA*, 2024. [Online]. Available: https://ktla.com/news/local-news/l-a-vehicle-thefts-skyrocketing-in-this-area

[2] GlobalData, "Global Top 10 OEMs Production Forecast (Q1 2024)," *MarkLines*, 2024. [Online]. Available: https://www.marklines.com/en/report/forecastprod_202404

[3] K. Tindell, "CAN Injection: keyless car theft," *CANIS*, 2023. [Online]. Available: https://kentindell.github.io/2023/04/03/can-injection/

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Cantor, D. Anderson, H. Shacham, and S. Savege, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*, Seattle, Washington 98195–2350, 2010.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *20th USENIX Security Symposium*. San Francisco, CA: USENIX Association, aug 2011. [Online]. Available: https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces

[6] J. Cahill, "The Technology to Steal Cars," *NICB*, 2023. [Online]. Available: https://www.nicb.org/technology-steal-cars

[7] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," *MDPI*, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/17/6679

[8] Cyber Threat Research Lab, "How to Get Away With Car Theft: Unveiling the Dark Side of the CAN Bus," *VicOne*, 2023. [Online]. Available: https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus

[9] L. Csikor, H. W. Lim, J. W. Wong, S. Ramesh, R. P. Parameswarath, and M. C. Chan, "RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems," *TCPS*, 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3627827

[10] M. Mehar, A. Waghole, A. Bharti, and P. Behre, "Over the Air (OTA) Update System – A Systematic Review," *Alohana*, 2024. [Online]. Available: https://alochana.org/wp-content/uploads/69-AJ2288.pdf

[11] F. Luo, J. Wang, X. Jiang, Z. Li, and C. Luo, "In-Vehicle Network Intrusion Detection Systems: A Systematic Survey of Deep Learning-Based Approaches Literature," *PeerJ*, 2023. [Online]. Available: https://peerj.com/articles/cs-1648/

[12] Automotive Security Research Group, "AutoVulnDB," 2024, last accessed 20 Nov 2024. [Online]. Available: https://asrg.io/autovulndb/#/

[13] C. V. Kifor and A. Popescu, "Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies," *MDPI*, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/18/6139

[14] Code Intelligence, "ISO/SAE 21434 compliance in 2024: what's new and how to act," 2023, last accessed 1 Nov 2024. [Online]. Available: https://www.code-intelligence.com/blog/iso-sae-21434-what-is-new-and-how-to-act#:~:text=From%20July%202024%2C%20the%20UN,to%20be%20ISO%2021434%20compliant