In-Vehicle Infotainment (IVI) Systems

[redacted]
Wireless Sec. & Tech., Section #27729
Purdue School of Engineering, IUPUI
Indianapolis, Indiana

Jake Simpson
Wireless Sec. & Tech., Section #27729
Purdue School of Engineering, IUPUI
Indianapolis, Indiana

[redacted]
Wireless Sec. & Tech., Section #27729
Purdue School of Engineering, IUPUI
Indianapolis, Indiana

[redacted]
Wireless Sec. & Tech., Section #27729
Purdue School of Engineering, IUPUI
Indianapolis, Indiana

I. Introduction

As technology rapidly becomes an integral part of the automotive industry, in-vehicle infotainment (IVI) systems have transformed into indispensable components within modern vehicles. These systems, evolving from basic entertainment features to sophisticated platforms, now manage critical functions such as gear selection, powertrain management, navigation, and even autonomous driving [1]. The industry's reliance on various operating systems like Android and Automotive Grade Linux contributes to the complexity of IVI systems, raising concerns about their vulnerability to wireless attacks and potential impacts on driver and vehicle safety [2].

The evolution of in-vehicle infotainment systems from basic music or video players to sophisticated platforms necessitates an understanding of the challenges posed by their proprietary characteristics, rapid industry innovation, testing constraints, and ethical considerations. The investigation into vulnerabilities within In-Vehicle Infotainment (IVI) systems presents challenges that require a holistic understanding and approach. These systems are comprised of a wide array of components from various suppliers, introducing inherent complexities in testing procedures [1]. The proprietary nature of many IVI systems further compounds the intricacies, limiting access to vital information and making analysis challenging for researchers. Rapid industry innovation leads to frequent system overhauls, making vulnerability research a continually evolving pursuit.

During our research into the vulnerabilities of In-Vehicle Information (IVI) systems, we built a test environment, incorporating a Raspberry Pi 4, a CrowPi, and several other pieces of equipment. The software we chose for our IVI emulation was Automotive Grade Linux (AGL) and ultimately tested with three different versions in an attempt to replicate the Car Whisperer attack. Much of our research was inspired by the Cyber Security Challenge 2021 competition, which showcased several successful attacks using AGL [2]. We used several tools throughout our research including the HackRF One, Wi-Fi dongle, and Bluetooth dongle. In addition to the Car Whisperer attack other Bluetooth attacks were performed including Bluetooth Sniffer, and Car Blues attack, with varying success. Blue Smack, a Bluetooth Denial of Service attack, was successful every time it was demonstrated.

II. Problem

In consideration for the ever-increasing integration of technology in the automotive industry, our research focuses on In-Vehicle Infotainment (IVI) systems wireless vulnerabilities. These infotainment systems have become an integral part of modern vehicles as they aim to provide communication, navigation, and entertainment features to users. While the primary user interface is recognizable as the screen located front and center on the dashboard, these systems are fully integrated into nearly every aspect of vehicle operations [1]. The automotive industry's increasing integration of technology has led to more intricate in-vehicle infotainment systems, which now manage numerous mission-critical features. Consequently, vulnerabilities in these systems have the potential to cause significant impacts on both the driver and the vehicle.

This topic sparked our interest, particularly after reading a news article about Ford Motors reporting a drive-by Wi-Fi hacking vulnerability in its vehicles due to a flaw in Ford's infotainment systems [3]. Ford disclosed a buffer overflow vulnerability in SYNC 3, one of its infotainment systems, although there was no evidence of exploitation, and it would not affect vehicle safety if exploited [4]. Our research revealed other manufacturers infotainment systems may be vulnerable to attacks similar to this buffer overflow attack, and it may compromise vehicle safety. The growing concern surrounding the vulnerability of these systems to wireless attacks is a key motivator for our research.

Our project began with an exploration of the evolution of IVI's and their security history. Throughout this project, our focus was on identifying wireless vulnerabilities in automotive infotainment systems. We explored potential attacks and attack vectors that In-Vehicle Infotainment (IVI) systems might encounter, investigating the potential impact of these vulnerabilities. To facilitate our investigation, we established a testing environment specifically designed to assess certain vulnerabilities. Our testing platform was assembled with

equipment provided by Dr. Feng Li, without his generosity none of our testing would have been possible.

The main goal of our testing environment was to showcase the exploitation of specific attacks and attack vectors that we suspected the emulated In-Vehicle Infotainment (IVI) system might be susceptible to. We sought to exploit these vulnerabilities within the emulated IVI environment, using open-source software, specifically Automotive Grade Linux (AGL). To achieve this, we compiled a list of potential attacks intended for execution on the AGL system.

III. Background

In-Vehicle Infotainment systems have become a key component of modern vehicles. You would probably recognize it as the screen at the front of your car where you can play music or video. As society has become more connected with our mobile devices many people expect the features of our mobile devices to be available everywhere [5]. Just look at how watches and TVs have become smart watches and smart TVs. Car infotainment systems have followed this trend as well. The auto industry has focused on developing In-Vehicle Infotainment systems with a wide variety of services such as AM/FM radio, music playback, video, hands-free communication with a mobile device, navigation, internet access, etc. [5]. They have evolved to offer more features due to the pressure of customers.

Looking more closely at in-vehicle infotainment systems, they are tightly coupled to a vehicle via heterogeneous networks such as a Controller Area Network (CAN), Bluetooth, Wi-Fi, cellular, automotive ethernet, and other vehicle-to-everything communications [2]. The IVI system also comes with a smartphone-grade CPU, and user-convenient human-machine interface, such as a touch screen [2]. As in-vehicle infotainment systems have evolved over time they have taken control of many more critical features. For example, the Tesla Model 3's IVI system is in charge of nearly all the features including gear selection, powertrain/chassis management, seat positioning, HVAC, music streaming, navigation, autonomous driving, etc. [5]. They can even monitor, manage, and diagnose a vehicle via the in-vehicle network [2]. They additionally deal with sensitive information like current geolocation/destination, phonebooks, SMS, and driver's voice [2]. This makes them prime targets for attackers as they can potentially steal valuable information as well as cause considerable damage to a vehicle or driver.

Diversity is something to be aware of in IVIs as well. Many In-Vehicle Infotainment systems will run operating systems such as Windows CE, Linux, QNX, Green Hills, or Android VM. Automakers will tailor their systems to meet specific requirements and integrate new features for the numerous amounts of different car types. One of the most popular OS systems is Android as it is now being used by companies like GM, Ford, Nissan, Honda, BMW, Volkswagen, and Porsche [6]. This is notable because the attack surface of these Android IVIs will be similar to that of an Android mobile phone [5]. This shouldn't be that shocking as both the IVI and mobile phone would be running on the same operating system. Attackers could potentially use this knowledge to try to exploit IVIs via vulnerabilities that exist in the Android OS. Our project, however, focused on Automotive Grade Linux.

No matter what OS IVIs use they all have big wireless attack vectors such as Wi-Fi and Bluetooth. Which is what we focused on. The modern infotainment systems have Wi-Fi and Bluetooth capabilities which allow it to connect with other personal mobile devices such as a mobile phone or laptop, which the IVI can act as a hotspot [5]. While this allows users to get convenient features such as the internet, it also opens an attack vector which outside adversaries could try to exploit.

Despite the efforts of car makers, it is impossible to identify and resolve all the vulnerabilities in an In-Vehicle Infotainment system [2]. This is why documentation is so important. During our research, we came across multiple good IVI documentation. Some of the most useful were security guidelines, penetration testing reports, user manuals, software updates/security patches, educational papers, and open-source documentation. These were important because they were not just a guide, but they were a tool which we used to find potential vulnerabilities that we would later attempt to execute against the Automotive Grade Linux system.

IV. Challenges

Researching potential vulnerabilities in In-Vehicle Infotainment (IVI) systems presents numerous challenges. These challenges begin with the vast array of components from various suppliers used to build these systems, making testing inherently difficult. Further complicating matters, many of these systems are proprietary, restricting information available to researchers. Additionally, rapid innovation in the automotive industry often results in complete system changes, turning vulnerability research into a continuously moving target. To add to the complexity, creating a test environment is becomes increasingly challenging, and as with any research, ethical concerns must also be addressed.

The diversity in IVI systems, each with different architectures, software, and security measures, complicates the development of universal testing methodologies and tools. The integration of a variety of serial and parallel bus communication systems contributes to the diverse communication protocols and architectures inherent in different IVI setups [7]. The interfaces designed for drivers and passengers alike reflect this diversity, encompassing entertainment and information, active noise reduction, security systems, GPS navigation, in-vehicle and internet connectivity, safety features, and visual sensors [7]. Each of these systems is composed of components from various suppliers, creating a complex supply chain. Identifying and addressing vulnerabilities across this supply chain is challenging and may require collaboration among researchers and manufacturers.

IVI systems are often proprietary and closed source, making it challenging for researchers to access the necessary hardware, software, and firmware for analysis. Obtaining the necessary permissions and tools for testing can be difficult. Proprietary

software, such as QNX and Microsoft's Windows Embedded, currently dominates the field [8]. QNX is used in vehicles from Audi, BMW, Ford, GM, Honda, Mercedes, and Toyota. Windows Embedded powers Ford's successful Sync system and is utilized by other automakers like Kia and Fiat. Cooperation with automakers can be challenging due to concerns about proprietary information, reputational damage, and differing priorities. Establishing productive relationships with the automotive industry is crucial for addressing vulnerabilities responsibly.

The automotive industry is rapidly evolving, with frequent updates to software and hardware. This dynamic environment makes it difficult for researchers to keep up with the latest technologies and security measures. While some manufacturers opt to develop in-house software for their distinct vehicle infotainment systems, others choose to leverage existing ecosystems [9]. Both approaches necessitate ongoing development and maintenance of software applications. To keep up with this continuous software development, the hardware of these infotainment systems must also be improved. As functionality expands the need for increased computing power, larger memory capacity, and more efficient power management becomes increasingly important [10].

Comprehensive security assessments require significant resources, and not all researchers or organizations may have the necessary capabilities. Many researchers may face limitations in terms of time, funding, and expertise. Setting up an experimental test environment that realistically simulates an In-Vehicle Infotainment (IVI) system and the Electrical/Electronic (E/E) architecture of a vehicle can be incredibly complex [11]. In many cases, acquiring the exact model of IVI and related equipment may be necessary to perform the required testing. Unfortunately, even when using reduced-cost solutions, such as a salvage yard to obtain the needed equipment, this type of manufacturer-specific research may not be feasible for those without ample funding. The cost of many development IVIs, such as the Nexcom VTC-1000, can be too high for many researchers [11]. Even lower-cost options, such as emulating an IVI in a virtual environment, can be rife with complexity. Additionally, conducting real-world tests can be challenging due to potential risks involved. Striking a balance between realistic testing scenarios and ensuring that our actions do not pose a danger to users on the road must be found.

Ethics is a significant aspect of penetration testing; hacking a system without the owner's permission is illegal. Testing and probing in-vehicle systems might violate laws and regulations, presenting potential legal challenges. Researchers need to navigate legal and ethical considerations to avoid legal consequences and ensure responsible disclosure [12]. In some cases, it might be necessary to first establish an agreement with the manufacturer whose equipment you are testing. Responsible disclosure is crucial to allow the manufacturers time to patch any vulnerabilities found during testing [12]. Additionally, research involving in-vehicle systems often deals with sensitive data, such as location information, personal preferences, and communication records. Safeguarding user privacy can present its own challenges. Yet another challenge could result from publishing or sharing results prior to disclosing your findings to the manufacturers, potentially placing the public in unnecessary danger. In-vehicle systems are critical for the safe operation of vehicles and the disclosure of vulnerabilities intentionally or inadvertently that compromises the safety of drivers, passengers, and other road users should be avoided at all cost.

V. Methods & Solutions

IVI system security vulnerabilities were evaluated using a carefully developed test environment incorporating both software and hardware elements. The hardware we used for the testing environment consisted of a Raspberry Pi 4, USB speakers, speakers with an auxiliary jack, and a CrowPi. To emulate an IVI, several versions of Automotive Grade Linux (AGL) were used for testing, starting with the demo image, then we moved on to AGL v16.0.2 Prickly Pike, finishing up our testing with v12.0.0 Lucky Lamprey. We chose Automotive Grade Linux primarily because it was open-source and was compatible with the equipment we used for our test environment. Additionally, AGL supports many automotive applications, including infotainment, instrument clusters, heads-up displays, telematics, advanced driver assistance systems, functional safety, and autonomous driving [5], [13].

To carry out our testing several tools were used including the HackRF One Software Defined Radio, a Wi-Fi dongle capable of being placed in Monitor Mode, and a Bluetooth dongle. Our attack strategies were inspired by those successful attacks carried out by the teams participating in the Cyber Security Challenge 2021 [2]. The most successful attacks demonstrated against an Automotive Grade Linux Infotainment system during this event included a command injection that exploited a services client authentication vulnerability, a resource exhaustion that relied on improper input validation and resource management in the IVI services, at least one insecure external communication attack, and a Bluetooth pairing attack due to a vulnerability created by a Bluetooth library that was in use.

Our test environment had limited attack vectors, it lacked a cellular connection, GPS, as well as Digital or XM Radio capabilities. This left us with the opportunity to exploit either Bluetooth or Wi-Fi vulnerabilities and since most of the Wi-Fi attacks, we could find exploited vulnerabilities in our test equipment instead of those found in AGL, many of our attacks focused on the Bluetooth capabilities in the infotainment system.

At the top of this list is the Car Whisperer, which relies on standardized passkeys to allow the attacker to send an audio file to be played over the cars speakers or record audio picked up on the in-car microphone, which is saved on the attacker's machine as a .wav file [6]. We tried every way we could think of to pull off a successful Car Whisperer attack, but was ultimately unsuccessful. We were unable to initiate audio playback, but couldn't access the onboard microphone.

To remedy this, we first attempted to compile an image of AGL version 16.0.2 with no additional success [14]. Next, we compiled an image of the older AGL version 12.0.0 and again was not successful in replicating the attack. After more research we believe that to get audio working on AGL we would have needed to implement several applications into our image, which was ultimately beyond our capabilities at the time.

We also researched and successfully deployed a Bluetooth Sniffer, utilizing the HackRF One to actively listen for and capture Bluetooth Low Energy packets from devices within range. The captured data was saved to a .pcap file, which could be viewed in WireShark. Subsequently, we attempted to execute the Bluedump attack, leveraging information gathered by the Bluetooth Sniffer, specifically the Bluetooth device addresses from a set of paired devices. In this attack, the attacker spoofs the address of one device and attempts to connect to the other. Since the attacker lacks a link key, when the target device requests authentication, the attacker's device responds with an 'HCI_Link_Key_Request_Negative_Reply.' In some cases, this response causes the target device to delete its own link key and enter pairing mode. While we encountered no issues spoofing the Bluetooth address of one of these paired devices, we were unable to successfully force the other device to enter pairing mode.

We also researched and attempted to deploy the Car Blues attack, which could allow an attacker access to stored data from devices previously synced to the In-Vehicle Infotainment (IVI) system. This includes stored contacts, call logs, text logs, and, in some cases, full text messages. However, since we had no success pairing with the IVI, this attack ultimately failed.

Additionally, we also researched Bluetooth jammers, a piece of equipment that transmits interfering signals that prevent other devices within its transmission area to be unable to connect to any other device. Because of the price for these jammers and questionable legality, we didn't end up building or purchasing one of the devices. Instead to perform a more focused DoS attack we used the Blue Smack attack against our IVI.

Blue Smack is a Bluetooth Denial of Service (DoS) attack which is focused on a single device [15]. We did need to know the targeted devices Bluetooth address, but it was successful every time, this was also one of the unsuccessful ways we attempted to de-authenticate connected devices to force them to pair with our attacker. Proximity for this attack is an issue, and it alone achieves little, but as part of a more comprehensive attack it may be useful.

Some important cases, such as the Uconnect vulnerability (CVE-2015-5611) [16], were discovered during our vulnerability investigation, revealing the actual dangers of having remote control over vehicle operations. As a result of this vulnerability, attackers within the same cellular network could control basic vehicle operations, including movement. The Bluetooth stack vulnerability in the BMW 330i (CVE-2017-9212) [17] demonstrated the possibility of a remote CD/Multimedia software crash, underscoring the extensive consequences of vulnerabilities in automotive systems.

The identified flaws underscore the vulnerability of In-Vehicle Infotainment (IVI) systems to intrusions that pose risks to user privacy and critical vehicle functionality. Immediate action is essential to implement robust security measures, particularly focusing on firmware updates, user authentication systems, and communication protocols. The growing interconnectivity of automobile systems increases the potential for sophisticated cyber-attacks, necessitating proactive and vigilant cybersecurity measures.

Addressing the identified issues requires prioritizing the development and implementation of secure firmware updates. Safeguarding the integrity of the update process is crucial to prevent the introduction of malicious code into the IVI system [18]. Strengthening user authentication systems involves enforcing robust password rules and exploring multi-factor authentication to minimize unauthorized access attempts [3]. To ensure secure data transfer, enhancing communication protocols should include rigorous validation, verification procedures, and encryption requirements [5]. A comprehensive cybersecurity strategy must encompass timely patching of identified vulnerabilities and regular vulnerability assessments. To keep IVI systems resilient in the rapidly evolving automotive cybersecurity landscape, continuous research into emerging threats and the adoption of proactive measures to mitigate potential vulnerabilities are imperative.

VI. Pros & Cons

The evaluation of In-Vehicle Infotainment (IVI) system security vulnerabilities revealed crucial insights into risks and countermeasures. Our test environment comprised a Raspberry Pi 4, a CrowPi, and the Automotive Grade Linux (AGL) operating system. While the assessment demonstrated the effectiveness of certain security measures, it also exposed vulnerabilities that warrant immediate attention.

Utilizing AGL as the operating system, along with the hardware ensemble, was a significant pro choice, given that it is open-source and useful for many automotive applications. The variety of services the operating system and hardware provided allowed us to have many different testing point opportunities. The use of specialized tools such as HackRF One Software Defined Radio, Wi-Fi dongles, and Bluetooth dongles enabled a thorough evaluation of potential attack vectors, providing a holistic view of IVI system vulnerabilities. Our study, focusing on Bluetooth and Wi-Fi risks, allowed for focused mitigation strategies, including the identification of effective countermeasures against Bluetooth-centric attacks.

Our research successfully identified various attack vectors, including command injection, resource depletion, unprotected external connections, and Bluetooth pairing vulnerabilities. This knowledge is vital for strengthening security procedures. However, our investigation also helped to reiterate real-world vulnerabilities. Examples include the Uconnect vulnerability (CVE-2015-5611) [16] and the Bluetooth stack vulnerability in the BMW 330i (CVE-2017-9212) [15], emphasizing the tangible risks associated with IVI system vulnerabilities.

Despite the opportunities provided by our hardware and software, limitations in our testing environment arose due to our software being a demo version. Furthermore, we lack the resources of a multi-million-dollar car company, limiting our ability to invest extensively in a testing environment. The absence of an LTE connection, GPS, and Digital/XM Radio capabilities in the test environment restricted the evaluation primarily to Bluetooth and Wi-Fi risks, potentially overlooking vulnerabilities associated with other communication channels. For instance, the inability of the Car Whisperer to access the onboard microphone underscored a limitation in the evaluation, highlighting the challenges in simulating real-world attack scenarios.

Our testing reveals the priority of safe firmware updates that automakers should continue to progress in. Safe firmware updates and development should be a top priority, ensuring the integrity of the update process. One thing we did not encounter during our testing was utilizing multi-factor authentication. Implementing multi-factor authentication is a necessary step to enhance user authentication systems and reduce illegal access attempts. While we highlight both strengths and weaknesses in the IVI system's security, it is important to be proactive in implementing recommended measures crucial to safeguarding user privacy and maintaining vehicle functionality in the continuous growing threat of cyber-attacks. The strengthening of protocols will also increase the security of IVI systems. Variables to consider, such as encryption requirements and authentication, should be incorporated. A successful cybersecurity plan addressing IVI systems will involve both timely patching of vulnerabilities and routine vulnerability assessments to address emerging threats.

VII. Future Work

The landscape of future In-Vehicle Infotainment (IVI) system vulnerability research is evolving. The prevalence of connected and autonomous vehicles is expanding, necessitating research into vulnerabilities associated with artificial intelligence, machine learning, and vehicle-to-everything (V2X) communication. As 5G connectivity becomes ubiquitous, researchers must explore the security implications of high-speed, low-latency connections, adding a new dimension to IVI system vulnerability assessments.

At the same time, the rise of edge computing within vehicles presents challenges and opportunities. Examining the security implications of distributed systems and the integration of edge computing into IVI architectures will be important. As IVI architectures evolve, researchers will need to adapt methodologies to address the security implications of diverse operating systems and software frameworks.

The complex automotive component supply chain, including IVI systems, will likely remain a key focus for researchers. Ensuring the overall integrity of IVI systems requires assessing and securing the supply chain, including the security practices of various suppliers. The development of specific regulatory frameworks for automotive cybersecurity may impact IVI system vulnerability research. Standardized testing environments are crucial to addressing the diversity of IVI systems. Virtual test beds replicating different setups offer researchers a controlled yet diverse space for security assessments. Advocating for open-source initiatives enhances transparency, granting researchers access to IVI systems for effective security contributions. Access to the continuous monitoring mechanisms and remote update capabilities are essential for researchers to stay informed and promptly address vulnerabilities amid rapid innovation.

We believe that, balancing simulated and real-world testing in In-Vehicle Infotainment (IVI) system vulnerability research will remain challenging. Researchers will continue to innovate methodologies to bridge these environments, prioritizing user safety and emphasizing ethical considerations, responsible disclosure, and safeguarding user privacy. Continuous collaboration, emerging technology focus, and ethical awareness are integral to shaping the future of IVI system vulnerability research.

Focusing on the increasingly sensitive user data handling practices of manufacturers, future research will emphasize the safeguarding of user privacy. This research may address privacy-preserving technologies and assess the effectiveness of privacy measures integrated into IVI systems. Collaboration between the automotive industry, cybersecurity researchers, and technology providers is expected to strengthen, prompting researchers to engage in cross-industry initiatives to share insights, methodologies, and best practices.

In security research, ethics should be a priority. Developing and promoting ethical hacking guidelines, collaborating with legal experts, and establishing responsible disclosure frameworks ensure a culture of responsible and ethical IVI security research. Education through programs and certifications elevates researchers' and manufacturers' skills. Crowdsourced security testing and bug bounty programs incentivize active contributions to IVI security. Interdisciplinary research teams provide a holistic understanding of IVI vulnerabilities, considering both technical and industry-specific aspects. Advocating for regulatory standards and emphasizing user privacy protection strengthens the ethical, legal, and technical foundations of IVI security research, allowing the research community to collaboratively enhance the security posture of In-Vehicle Infotainment systems.

Researching vulnerabilities in IVI systems is a complex endeavor, requiring a comprehensive approach to overcome challenges. Collaboration is essential, with partnerships established among automakers, suppliers, and researchers, creating a network for information exchange on vulnerabilities and testing methodologies. Encouraging insights and best practices sharing through collaborative platforms fosters a collective and informed effort towards securing IVI systems.

VIII. Summary

In-vehicle infotainment (IVI) systems have evolved into integral components of modern vehicles, offering a wide array of features driven by customer demands. Connected to vehicles through complex networks of diverse components, they have

user-friendly interfaces, and control over critical functions, including autonomous driving and vehicle diagnostics. This full system integration makes IVI's attractive targets for attackers who may seek valuable information or aim to compromise vehicle safety. Despite security efforts by car manufacturers, identifying and resolving all vulnerabilities remains challenging, highlighting the importance of documentation, including security guidelines, penetration testing reports, user manuals, and software updates.

Our research focused on the wireless vulnerabilities of In-Vehicle Infotainment (IVI) systems, considering the increasing integration of technology in the automotive industry. IVI systems, crucial for communication, navigation, and entertainment in modern vehicles, have become intricately involved in various mission-critical functions. We were motivated by reports of a drive-by Wi-Fi hacking possibility in Ford's infotainment systems. The purpose of this project was to explore and identify wireless vulnerabilities that could compromise vehicle safety. Our research involved an overview of IVI's, emphasizing their evolution and security concerns. We established a dedicated testing environment, generously provided by Dr. Feng Li, to assess specific vulnerabilities. The goal was to showcase the exploitation of potential attacks on an emulated IVI system using open-source software, particularly Automotive Grade Linux (AGL).

Researching vulnerabilities in In-Vehicle Infotainment (IVI) systems poses several challenges. The diversity in components from various suppliers, proprietary and closed source nature of many systems, rapid industry innovation, and continuous system changes make universal testing methodologies difficult to develop. The complexity extends to communication protocols, architectures, and diverse interfaces for entertainment, safety, and connectivity. Proprietary systems restrict access for researchers and complicate collaboration with automakers. Rapid industry innovation, including frequent software and hardware updates, demands constant adaptation from researchers. Testing restrictions arise from resource limitations, the complexity of setting up realistic test environments, and potential risks involved in real-world tests. Ethical considerations, including legal implications, responsible disclosure, and safeguarding user privacy, further complicate penetration testing. Navigating these challenges requires careful collaboration between researchers and manufacturers to address vulnerabilities responsibly.

Our evaluation of In-Vehicle Infotainment (IVI) system security vulnerabilities involved a test environment with hardware components such as Raspberry Pi 4, multiple types of speakers, and a CrowPi, coupled with different versions of Automotive Grade Linux (AGL). The focus was on Bluetooth vulnerabilities, inspired by successful Cyber Security Challenge 2021 attacks [2]. Despite limitations in the testing environment, including the absence of a cellular connection and GPS, various attack strategies were employed, such as the Car Whisperer and Bluetooth Sniffer. Our research supports the need for robust security measures, including safe firmware updates, user authentication enhancements, and secure communication protocols. Our findings highlight the urgency of proactive cybersecurity measures amid the growing threat of cyber-attacks on IVI systems in the automotive industry.

REFERENCES

[1] C. Evans, "The Car Hacker's Handbook," No Starch Press, San Francisco, 2016.

[2] S. Jeong, M. Ryu, H. Kang, and Huy Kang Kim, "Infotainment System Matters: Understanding the Impact and Implications of In-Vehicle Infotainment System Hacking with Automotive Grade Linux," Apr. 2023, doi: https://doi.org/10.1145/3577923.3583650.

[3] B. Vigilarolo, "Ford SYNC 3 infotainment vulnerable to drive-by Wi-Fi hijacking," The Register, Aug. 14, 2023. [Online]. Available: https://www.theregister.com/2023/08/14/ford_sync_vulnerability/ (accessed Sep. 20, 2023).

[4] "Ford Provides Customer Guidance in Response to Supplier Disclosure of Cyber Security Vulnerability — Ford Media Center," media.ford.com. [Online]. Available: https://media.ford.com/content/fordmedia/fna/us/en/news/2023/08/10/ford_provides-customer-guidance-in-response-to-supplier-disclosu.html (accessed Sep. 26, 2023).

[5] E. F. M. Josephlal and S. Adepu, "Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability," 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), Hangzhou, China, 2019, pp. 241-246, doi: 10.1109/HASE.2019.00044.

[6] "Android Automotive," Wikipedia, Nov. 20, 2022. https://en.wikipedia.org/wiki/Android_Automotive.

[7] C. Loberg, "Taking In-Vehicle Infotainment into the Future," Tektronix, Feb. 8. 2022. [Online]. Available: https://www.tek.com/en/blog/taking-in-vehicle-infotainment-into-the-future.

[8] D. Newcom, "The Next Big OS War is in Your Dashboard," Wired, Dec. 3, 2012. [Online]. Available: https://www.wired.com/2012/12/automotive-os-war/.

[9] B. Tanygin, "Vehicle Infotainment Systems: The Tech Trend Redefining the Automotive Industry," Eleks, June 1, 2020. [Online] Available: https://eleks.com/blog/vehicle-infotainment-systems-automotive-industry/.

[10] M. Burk, "The Evolution of In-Vehicle Infotainment Systems," Micron. March 14, 2019. [Online]. Available: https://www.micron.com/about/blog/2019/march/evolution-of-in-vehicle-infotainment-systems-part-one.

[11] C. Smith, "The Car Hacker's Handbook: A Guide for the Penetration Tester," No Starch Press, San Francisco, 2016.

[12] P. Anderson, "Penetration Testing of an In-Vehicle Infotainment System," KTH Royal Institute of Technology, 2022. [Online] Available: https://www.diva-portal.org/smash/get/diva2:1708534/FULLTEXT01.pdf.

[13] J. Takahashi, M. Iwamura and M. Tanaka, "Security Threat Analysis of Automotive Infotainment Systems," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 2020, pp. 1-7, doi: 10.1109/VTC2020-Fall49728.2020.9348647.

[14] Automotive Grade Linux, "AGL Documentation: Build Process Overview," Automotive Grade Linux, [Online]. Available: https://docs.automotivelinux.org/en/pike/#01_Getting_Started/02_Building_AGL_Image/01_Build_Process_Overview/.

[15] N. Patel, H. Wimmer and C. M. Rebman, "Investigating Bluetooth Vulnerabilities to Defend from Attacks," 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2021, pp. 549-554, doi: 10.1109/ISMSIT52890.2021.9604655.

[16] NIST, "CVE-2015-5611", MITRE, December 23, 2016. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-5611.

[17] NIST, "CVE-2017-9212", MITRE, October 2, 2019. [Online] Available: https://nvd.nist.gov/vuln/detail/CVE-2017-9212.

[18] V. Renganathan, E. Yurtsever, Q. Ahmed, and A. Yener, "Valet attack on privacy: A cybersecurity threat in Automotive Bluetooth infotainment systems - cybersecurity," SpringerOpen, https://cybersecurity.springeropen.com/articles/10.1186/s42400-022-00132-x (accessed Sep. 24, 2023).