Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 78-100
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Multi-Factor Authentication for Keyless Entry Systems: An Innovative Approach to Automotive Security

Danilo Brito, Shakour Abuzneid

Cybersecurity Program, Roger Williams University, Bristol, USA
Email: dbrito192@g.rwu.edu, sabuzneid@rwu.edu

How to cite this paper: Brito, D. and Abuzneid, S. (2025) Multi-Factor Authentication for Keyless Entry Systems: An Innovative Approach to Automotive Security. *Journal of Information Security*, **16**, 78-100.
https://doi.org/10.4236/jis.2025.161004

Received: October 30, 2024
Accepted: December 24, 2024
Published: December 27, 2024

Abstract

Car manufacturers aim to enhance the use of two-factor authentication (2FA) to protect keyless entry systems in contemporary cars. Despite providing significant ease for users, keyless entry systems have become more susceptible to appealing attacks like relay attacks and critical fob hacking. These weaknesses present considerable security threats, resulting in unauthorized entry and car theft. The suggested approach combines a conventional keyless entry feature with an extra security measure. Implementing multi-factor authentication significantly improves the security of systems that allow keyless entry by reducing the likelihood of unauthorized access. Research shows that the benefits of using two-factor authentication, such as a substantial increase in security, far outweigh any minor drawbacks.

Keywords

MFA, Keyless Entry Systems, Automotive Security, Biometric Authentication

1. Background

Overview of keyless entry systems in vehicles Remote Keyless Entry (RKE) systems have ushered in a new era of car access. They offer a futuristic, easy-to-use option that surpasses the outdated mechanical key system. With these systems, drivers can unlock and start their cars without inserting a key into a lock or ignition switch. Instead, they rely on electronic signals sent from a key fob to the car's internal computer, showcasing cutting-edge technology in the automotive industry [1] [2]. The journey of keyless entry technology dates to the early 1980s, with the debut of the initial remote entry systems. These early models enabled drivers to lock and unlock their car doors with a basic remote. As technology progressed,

keyless entry systems have significantly improved their capabilities and security [3]. In the initial phase (1980s-1990s), the first keyless entry systems relied on infrared (IR) signals for communication between the key fob and the car. These systems were rudimentary, offering limited capabilities and a short range [2]. In the second phase (2000s), the shift to radio frequency (RF) technology significantly boosted the range and dependability of keyless entry systems. This period also saw new features like trunk release and panic buttons [2]. In the current phase (2010s-present), today's keyless entry systems are highly complex, featuring sophisticated encryption and rolling codes to thwart unauthorized entry. The advent of passive keyless entry (PKE) systems has added to their convenience, allowing users to unlock and start their cars without pressing any buttons, as long as the key fob is within a certain distance [3]. Today's cars are outfitted with an array of electronic control units (ECUs) that oversee everything from the engine's running to the entertainment features. The growth of cars that can interact with outside gadgets and networks has also made car systems more complicated. This ability to connect to the internet puts vehicles at risk of many cyber-attacks, highlighting the need for solid car security [4] [5].

Vehicle security risks can be generally divided into two main types: those related to the physical aspects and those related to cyber elements. Physical hazards include direct assaults on the car's mechanical components, like taking the key fob or breaking into the vehicle. Meanwhile, cyber risks exploit vulnerabilities in the car's software and communication networks. Specifically, keyless entry systems have emerged as a significant focus for cyber-attacks [6]. The economic consequences of car security breaches are considerable. When a car is stolen, it is not just a loss for the owners; it also drives up the cost of insurance for both the car owners and the car makers due to the need for recalls and improvements in security. Moreover, when cars are hacked, it can put the safety of the people inside at risk, potentially causing accidents and even deaths. Hacks that disrupt a car's ability to control itself can create hazardous driving situations. Strong security is essential to avoid these situations and ensure the safety of everyone on the road: car theft and damage cause billions of dollars in losses every year [7]. More robust security systems can help reduce these losses and lessen the financial strain on individuals and the car industry [8].

Governments and oversight agencies worldwide acknowledge the critical need for vehicle security and are implementing strict rules and guidelines to guarantee the protection and integrity of automobiles. Adhering to these rules is not just a matter of law but is also crucial for preserving consumers' confidence and the brand's image. Different guidelines, like the ISO/SAE 21434 [9], detail the expectations for cybersecurity in the automotive sector. Meeting these guidelines ensures that car manufacturers incorporate security considerations from the initial design stages to the vehicle's lifespan [9].

A 2FA is a security system that demands two types of confirmation before allowing entry to a system or device. It is commonly acknowledged as a powerful method for improving security by introducing an extra layer of defense above the

usual systems based on passwords [10]. 2FA uses two distinct verification methods to confirm a user's identity. Something You Know usually involves a password or a Personal Identification Number (PIN). Something You Have might be a tangible object such as a mobile phone, security device, or key ring. By requiring two unique pieces of information, 2FA significantly enhances security, reducing the risk of unauthorized entry. A potential intruder would need to breach both aspects to gain access, providing an extra layer of protection [10]. Within car safety, the threat of relay attacks and key fob duplication is a pressing concern. A 2FA can bolster defenses in keyless entry systems, making them more resistant to these prevalent threats. By incorporating an extra step for verification, such as biometric identification or a confirmation from a mobile app, cars can achieve a much higher level of protection [10]. Biometric identification is a crucial component of 2FA that involves using unique biological data, such as fingerprints or facial recognition, as the second factor. This adds an unparalleled layer of security to the system, ensuring that only the authorized user can access the car [10]. Mobile App Confirmation is a feature that requires users to validate their access through a secure mobile app. The process involves a series of steps, including user authentication and device verification, adding an extra security dimension to the system [10]. Using 2FA in car keyless entry systems brings many advantages. It improves safety by introducing an additional safeguard, making it harder for intruders to access without permission [1]. It reduces the risk of theft and unauthorized entry by dramatically lowering the chance of car theft and unauthorized access [1]. It boosts customer trust and shows dedication to safety, building customer trust and confidence [1]. Modern cars now have keyless entry systems, providing drivers with easy and convenient access. However, these systems are not immune to security issues. Even with the sophisticated technology behind keyless entry, multiple weaknesses leave cars vulnerable to theft and unauthorized entry. This part delves into the main security weaknesses in today's keyless entry systems and highlights the importance of implementing more robust security systems [11]. Can multi-factor authentication reduce car theft in vehicles with keyless entry systems? This inquiry delves into the possible advantages and feasible application of Two-Factor Authentication (2FA) in improving the safety of systems that rely on keyless entry, tackling existing weaknesses, and guaranteeing a strong defense against unauthorized entry.

The central aim of this study is to thoroughly investigate the potential of 2FA in enhancing the safety of vehicle keyless entry systems. To achieve this, the research will begin by identifying and examining the current vulnerabilities in existing keyless entry technologies, such as relay attacks and key fob duplication. It will then delve into the effectiveness of 2FA in mitigating these vulnerabilities by studying its principles and applications in other security domains. The study will propose a comprehensive theoretical framework for integrating 2FA into keyless entry systems, particularly emphasizing biometric and mobile app verification methods. Furthermore, the research will rigorously evaluate the ease of use and acceptance of the proposed 2FA system through extensive usability tests and user

feedback. Lastly, it will thoroughly investigate the legal and market implications of adopting 2FA, considering the need for compliance, potential costs, and the competitive advantage enhanced security can bring. The detailed and meticulous results are intended to provide essential insights for strengthening the protection of vehicles and influencing industry standards [8].

2. Literature Review

2.1. Trends and Vulnerabilities in Automotive Theft: Analyzing the Rise and Impact of Keyless Entry Exploits

The recent surge in motor vehicle thefts in the United States underscores a growing concern for vehicle security and the effectiveness of modern anti-theft technologies. Between 2019 and 2023, motor vehicle thefts have increased by approximately 25% [12], indicating a significant rise in this type of crime. Notably, three cities in Colorado rank among the top ten U.S. metropolitan areas most affected by vehicle thefts, with Pueblo leading the list at nearly 1100 thefts per 100,000 people. This alarming trend is further exacerbated by vulnerabilities in specific car models, particularly over 8 million Kia and Hyundai vehicles that lack engine immobilization devices [12]—a flaw that gained widespread attention due to a social media trend demonstrating how easily these cars could be stolen. The impact of this security weakness is not merely theoretical. Still, it has manifested in a tangible increase in thefts, revealing a critical gap in these vehicles' design and security measures [12].

A VicOne report analyzed media coverage of the automotive industry from early 2021 to June 2022, revealing significant insights into current threats. Keyless entry system vulnerabilities accounted for 26.1% of the discussions in 2021 and 24% in the monitored period in 2022. These keyless issues have emerged as a critical concern in automotive security, given that this technology allows unlocking a car or starting its engine without needing a physical key [13]. However, the growing frequency of thefts has left many car owners questioning the adequacy of such measures in deterring crime. According to the National Highway Traffic Safety Administration (NHTSA), approximately 1,000,000 vehicles are subjected to theft annually, with 40 percent of these incidents occurring at automobile dealerships. A motor vehicle is stolen every 32 seconds in the U.S., illustrating the urgency with which this issue must be addressed. The recent trends in auto theft highlight the need for enhanced vehicle security features and greater awareness among car owners about protecting their assets. This review of auto theft trends, sparked by data and real-world cases, serves as a crucial resource for understanding the scope of the problem and identifying potential solutions to mitigate the risk of vehicle theft in the current landscape [12] [14]. In January 2023, vehicle owners initiated a class action lawsuit after State Farm and Progressive announced that they would cease providing insurance coverage for particular Hyundai and Kia models older than 2019 due to thefts. These owners had either experienced the theft of their cars or had their insurance policies canceled. The presiding judge dismissed the proposed $200 million settlement, stating that it fails to offer "fair and adequate relief to vehicle owners [15]. This isn't just a problem in the United States; accord-

ing to Statista, in 2020, New Zealand had the highest rate of car theft in the world, with 1172 occurrences per 100,000 inhabitants [16]. Additionally, car theft in Canada has escalated into a significant issue, with recent data showing a 24% increase in thefts nationwide in 2023. Toronto has experienced a staggering 150% rise in car thefts over the past six years. According to the Insurance Bureau of Canada (IBC), over 105,000 vehicles have been stolen since 2022, with one car stolen every five minutes. Many of these stolen vehicles are being identified at ports of entry in other countries, particularly in Africa, where the demand for used cars is high due to a growing middle class [17]. The COVID-19 pandemic has exacerbated the situation, as shortages in auto parts and semiconductors increased the value of newer models already on the road, making them attractive targets for thieves. Car theft remains a lucrative and relatively low-risk crime for organized crime, contributing to its persistence and growth in Canada [17].

One of the major contributing factors is the exploitation of keyless entry systems. Despite their convenience, these systems have become a target for thieves using relatively simple devices that mimic the signals of key fobs. These devices are often called "emulators" [18], can intercept and retransmit signals, allowing unauthorized vehicle access in seconds. The accessibility of these devices, which can be bought online for just a few thousand dollars, means that even individuals with no technical expertise can easily steal cars equipped with keyless entry systems.

This trend has affected various car models globally. For instance, the Hyundai Ioniq 5, a modern electric vehicle, has been targeted in the UK, where owners resort to additional security measures like steering locks. This issue isn't new; automakers have been aware of these vulnerabilities for over a decade. A 2011 study by the University of California and the University of Washington highlighted these security flaws, but automakers underestimated the potential for exploitation. With the rise of these devices, car thieves have become more effective, contributing to a sharp increase in car thefts in regions like England and Wales, where incidents rose from 70,000 in 2014 to around 130,000 in 2023 [18]. Vehicles with keyless entry systems are significantly more vulnerable to theft. Recent data indicates that keyless cars are up to twice as likely to be stolen as non-keyless models. Keyless entry thefts account for a substantial majority of all car thefts in some countries. For example, in 2022, 94% of vehicles recovered by one vehicle tracking firm were keyless cars. The increase in thefts is primarily due to the ease with which thieves can exploit the signal emitted by key fobs using inexpensive and readily available devices. These tools allow criminals to relay or intercept the key fob's signal, enabling them to unlock and start the car without needing the key [18] [19]. Another car security company, Tracker, revealed that 92% of the vehicles it recovered last year were stolen without using keys. This marks an increase from 88% in 2018 and a significant rise of 26% compared to four years ago when the figure stood at 66% in 2016 [18]. This trend has been on the rise for over a decade, and the automotive industry is engaged in an ongoing "arms race" to improve security measures against these increasingly sophisticated theft methods [18] [19].

As shown in Table 1, California recorded the highest car theft statistics among U.S. states.

Table 1. Top 10 car theft statistics by state.

Rank	State	2022	2023	Percent change 2022-2023
1	California	208,668	202,685	3%
2	Texas	115,013	105,015	10
3	Florida	46,213	45,973	1
4	Washington	43,160	46,939	−8
5	Illinois	41,528	38,649	7
6	Colorado	34,068	42,237	−19
7	New York	32,715	28,292	16
8	Ohio	31,647	29,913	6
9	Georgia	28,171	26,529	6
10	Missouri	27,279	29,345	7

In 2023, vehicles manufactured by Kia and Hyundai recorded the highest theft rates, overturning the longstanding pattern where full-size pickup trucks have consistently occupied the top position in theft statistics. This shift was highlighted in a recent report released by the National Insurance Crime Bureau (NICB), an organization within the insurance sector that is committed to combating insurance-related crime and fraud [20]. Ford F-150 trucks made between 2018 and 2020 with push-button start are vulnerable to relay attacks, where thieves can use an antenna or receiver to amplify the key fob signal outside a home, tricking the truck into starting. Older F-Series trucks are even more accessible to steal due to their ignition switches under the steering column and easily removable door handles [21]. Similarly, full-size Chevy pickups, especially the Silverado 1500, have consistently ranked among the top 10 most stolen vehicles since 2016. Thieves can quickly steal a Silverado 1500, which is susceptible to relay attacks and can also be hacked through its built-in OnStar security system. Additionally, these trucks are targeted for their valuable components, which can be stripped and resold [21].

Table 2 highlights the top 10 most stolen vehicle makes and models in 2023.

Table 2. National top 10 vehicles makes/models stolen 2023.

Rank	Make/Model	2023 Thefts
1	Hyundai Elantra	48,445
2	Hyundai Sonata	42,813
3	Kia Optima	30,204
4	Chevrolet Silverado 1500	23,721
5	Kia Soul	21,001
6	Honda Accord	20,895
7	Honda Civic	19,858
8	Kia Forte	16,208
9	Ford F150 Series Pickup	15,852
10	Kia Sportage	15,749

2.2. Keyless Entry Vulnerabilities

For over a decade, the "relay attack" has been a modern method for stealing vehicles, similar to old-school hot-wiring. Despite the introduction of ultra-wideband (UWB) communication in keyless entry systems, which was expected to fix this issue, Chinese researchers from GoGoByte [22] demonstrated that relay attacks are still effective, even against the latest Tesla Model 3. They were able to unlock and start the car using less than $100 worth of equipment. This vulnerability persists because the UWB feature isn't currently used for security distance checks. Tesla owners are advised to use the PIN-to-drive feature to prevent theft, as UWB alone does not guarantee protection from relay attacks [22].

1) CAN Bus Attack

The Controller Area Network (CAN) [23] bus was introduced in the 1980s as a specialized communication protocol designed specifically for automotive applications. Before the CAN bus, automobile manufacturers (Original Equipment Manufacturers or OEMs) relied on numerous point-to-point connections, resulting in a complex and extensive wiring infrastructure. Today, the CAN bus is a universally adopted standard within the automotive industry and is used in most modern vehicles [23]. The attacker accesses the CAN bus wiring, typically through the headlights, where the intelligent key receiver ECU is connected. The attacker repeatedly sends wake-up signals to the CAN bus by powering on a CAN injector until a response is received. The CAN injector then takes control of the bus by engaging a dominant override circuit, which blocks other devices from transmitting and disables the bus's error detection mechanisms. This allows the CAN injector to impersonate the smart essential ECU and send fake messages to the car's Gateway ECU, instructing it to deactivate the immobilizer and unlock the doors. The Gateway ECU forwards these messages to the engine control system and door ECU, effectively disabling the immobilizer and unlocking the car [23].

2) Relay Attacks

A significant weakness in keyless entry systems is their vulnerability to relay attacks. In such an attack, criminals use two devices to intercept and pass on the signal from the key fob to the car. This technique fools the car into thinking the key fob is nearby, enabling the criminals to unlock and start the vehicle [11]. Process: The initial device, located close to the key fob, picks up its signal and sends it to the next device, which is near the car. This second device then sends the signal back to the car, making it think the key fob is nearby and allowing the criminals to unlock and start the vehicle [11]. Relay attacks can happen rapidly and without the owner's awareness, resulting in car theft and unauthorized entry [11]. In **Figure 1**, we observe a demonstration of a relay attack targeting a vulnerable keyless entry system. This depiction illustrates how two individuals employ two separate devices to intercept and amplify the signal emanating from a key fob, thereby enabling them to unlock and commence the vehicle's operation without the key fob's proximity being present.

Figure 1. Simulation for relay attacks.

3) Signal Jamming

Intruders employ signal jamming to take advantage of systems that do not require keys. In this method, a device that interferes with signals disrupts the connection between the key fob and the car. This interruption stops the vehicle from locking correctly, making it susceptible to theft [11]. Intruders utilize a device that emits signals at the same frequency as the key fob, interfering with the connection between the key fob and the car's receiver [11]. Interference can prevent a vehicle from locking, making it easier for intruders to access. Owners must realize that their vehicles must be appropriately secured [11].

4) Code Grabbing and Replay Attack

Key fob interception and replay attacks occur when someone intercepts the signal from the key fob to the car and then plays it back to gain entry without permission. Even with improvements in encryption and rolling code technologies, specific systems are still at risk of these attacks [24]. The attacker employs a device to pick up the signal from the key fob to the car. This intercepted signal is returned to the car to unlock the doors or start the engine. These attacks can be carried out using low-cost and readily available tools, presenting a severe risk to vehicle security.

5) Key Fob Cloning

Key fob duplication, a process that allows intruders to create an exact copy of your key fob, poses a significant threat. This enables them to gain entry and operate your car without your knowledge. They can achieve this by physically obtaining your key fob or using advanced electronic techniques. Process: Intruders capture the unique signal of a key fob and manufacture a replica capable of unlocking and starting the car. They can do this by intercepting the signal or through proximity.

Attack	Process	Effect	Protection
Relay Attacks	The initial device captures the signal from the key fob and sends it to a second device near the car, which then sends the signal to the vehicle.	Car theft and unauthorized entry without the owner's awareness.	Store key fobs in signal-blocking pouches or boxes, use car alarms and disable keyless entry if possible.
Signal Jamming	A device emits signals at the same frequency as the key fob, disrupting the connection between the key fob and the car's receiver.	It prevents the car from locking, making it easier for intruders to access it.	Ensure the vehicle is locked manually and use additional security measures like steering wheel locks.
Code Grabbing and Replay Attack	An attacker intercepts the signal from the key fob to the car and replays it to gain entry.	Gains unauthorized access to the car using intercepted signals.	Use advanced encryption and rolling code technologies, and avoid using key fobs near potential attackers.
Key Fob Cloning	Intruders capture the unique signal of a key fob and create a replica capable of unlocking and starting the car.	Allows intruders to create a duplicate key fob, gaining entry and operating the car.	Keep key fobs secure, use signal-blocking pouches, and employ advanced security features in the car.

2.3. Applications of MFA in Various Industries

Within finance and banking, multi-factor authentication (MFA) has emerged and established itself as a standard procedure for safeguarding online transactions and securing customer accounts. Banks and financial organizations universally adopt MFA, underscoring its importance in guaranteeing that only legitimate users can access confidential financial data and conduct transactions. Frequently used techniques encompass text-based one-time passwords (OTPs), mobile application authentication, and physical tokens [25]. MFA is implemented in the digital shopping industry to safeguard user accounts and thwart illegal activities. E-commerce stores employ MFA to confirm customers' identity while logging in and before finalizing their orders, thus minimizing the chance of unauthorized transactions.

Research indicates that the adoption of Multi-Factor Authentication (MFA) can markedly improve vehicle security, particularly in safeguarding against digital threats, including unauthorized access to integrated vehicle systems. MFA, through its requirement for multiple verification methods, significantly increases intruders' difficulty gaining control over a vehicle's electronic systems, even if one security layer is breached [26] [27]. For example, integrating MFA into vehicle access systems can diminish the probability of unauthorized entry by as much as 90%, owing to introducing an additional authentication layer that is considerably more challenging to circumvent than conventional key fob systems on their own. This strategy is particularly efficacious in countering vulnerabilities associated with keyless entry systems, where intruders employ signal amplifiers or other devices to replicate key fob signals. By incorporating an extra verification step, such as a biometric scan or a one-time passcode, MFA can effectively prevent these attacks [26] [27]. Within the broader spectrum of cybersecurity, the deployment

of MFA has been demonstrated to significantly diminish the efficacy of hacking attempts, rendering it an essential element in the protection of contemporary vehicles increasingly dependent on digital systems [26].

2.4. The Economic Consequences of Increased Motor Vehicle Theft

In 2022, the total value of motor vehicles reported as stolen amounted to $529.5 million. Notably, 43 percent of these vehicles were successfully recovered based on their value. Consequently, the value of the unrecovered vehicles was estimated to be $302 million. A total of 46,237 motor vehicles were reported stolen during this period. Among these, 60.8 percent were recovered, representing 28,313 vehicles. It is also observed that approximately one-third of the stolen vehicles, or 9340 to be precise, were returned to their owners, albeit with damages valued at $1000. Furthermore, it is estimated that 9340 vehicles were beyond repair and were subsequently totaled. To calculate the total loss incurred due to the theft of these vehicles, we must consider the value of the vehicles that were recovered but totaled, along with the value of vehicles that were returned with damages of $1000 and the total value of vehicles that were damaged to the extent of $1000. This computation yields a total loss attributed to the theft of motor vehicles in the year 2022 to be $386.4 million [28]. In 2014, Colorado passed legislation that lowered penalties for motor vehicle theft, basing the severity of penalties on the vehicle's value. At that time, Colorado ranked 18th nationally in motor vehicle thefts per capita. However, by 2020, the state experienced a 126% increase in thefts, leading the nation in motor vehicle thefts per capita. By 2022, the theft rate had surged to an all-time high of 801.2 thefts per 100,000 residents, representing a 233% increase from 2014. This rise in motor vehicle theft resulted in 46,237 stolen vehicles in 2022, valued at $530 million—a 545% increase from 2014. The economic consequences included $277 million in higher insurance premiums, amounting to $239 per household annually, the loss of 1530 jobs statewide, a $101 million reduction in personal income, a $158 million decrease in state GDP, and a 0.11% rise in inflation. These impacts have prompted legislative reconsideration of the 2014 reforms, with proposals to strengthen penalties for auto theft [28]. Manufacturers may be reluctant to invest in enhanced security measures because vehicle theft does not directly impact their financial incentives. The economic burden of these thefts primarily falls on dealerships and insurance companies, which bear millions of dollars in losses each year. As long as vehicle sales remain strong and profits continue, the urgency for manufacturers to prioritize additional security features remains diminished [28].

2.5. Real-World Examples of MFA

BMW is at the forefront with its Intelligent Personal Assistant, which uses voice recognition to enable seamless, hands-free control of in-car functions. Hyundai has also introduced fingerprint recognition in specific models, allowing drivers to unlock and start their vehicles with a touch. These technologies enhance both se-

curity and convenience, and customer feedback has been largely positive, highlighting the smooth integration into daily use and the improved driving experience. The success of these innovations encourages further development and broader adoption of biometric technologies in the automotive industry [21]. In 2022, Salesforce mandated Multi-Factor Authentication (MFA) across its platforms, including Sales Cloud and Service Cloud, as a proactive measure against the rising threat of cyberattacks. This initiative led to 100% employee compliance and significant security improvements for its extensive customer base. Salesforce's use of methods like the Salesforce Authenticator app and security keys has effectively protected against phishing and credential stuffing threats [29]. Google also saw a substantial reduction in account takeovers after implementing MFA, notably by introducing hardware security keys for high-risk users such as politicians and journalists. This approach significantly minimized phishing-related breaches, underscoring MFA's effectiveness in safeguarding sensitive accounts [30]. Microsoft has highlighted that enabling MFA can prevent over 99.9% of account compromise attacks. By making MFA a default security setting, particularly for privileged accounts, Microsoft achieved a marked decrease in unauthorized access, helping to secure its critical cloud services and applications [31].

3. Implementation and Analysis

3.1. Innovations in Biometric Vehicle Access: Trends, Technologies, and Patent Activity

The automotive industry remains a focal point for patent innovation, particularly in biometric vehicle access systems. This surge in innovation is fueled by growing consumer demand for convenience and security, advancements in biometric technology, government regulations, and competition among automotive manufacturers. Consumers increasingly seek secure methods to unlock and start vehicles, with biometric technology offering accuracy, reliability, and enhanced security. Government mandates for car safety features also contribute to this trend [32]. Recent advancements in biometric vehicle access include facial recognition, fingerprint recognition, and voice recognition. Facial recognition technology employs cameras to scan a driver's face and compare it to a stored image, granting access if there's a match. Fingerprint recognition uses sensors to verify a driver's identity against a stored fingerprint database. Voice recognition captures and analyzes a driver's voice, allowing access if it matches a stored voice print. Additionally, multimodal biometrics, which integrates two or more biometric technologies, offers even greater security and reliability in vehicle access [32]. According to GlobalData's report on cybersecurity in the automotive industry, over the past three years, more than 720,000 patents related to biometric vehicle access have been filed and granted, highlighting the rapid pace of innovation in this sector [32]. The analysis conducted by GlobalData's Technology Foresight, which utilizes more than one million patent documents to assess the level of innovation within the automotive sector, identifies over 300 distinct innovation areas expected

to impact the industry's future direction significantly [32].

Figure 2 provides a summary of patent volumes related to biometric vehicle access technologies [32].

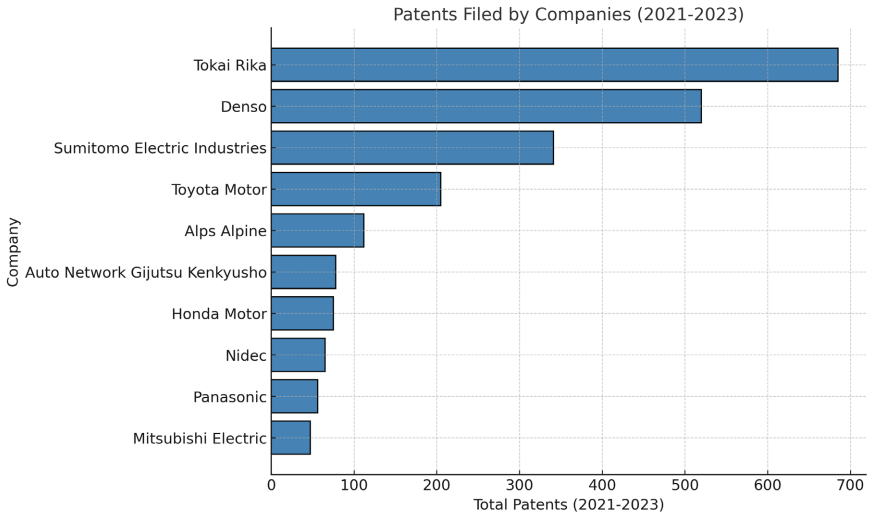

Figure 2. Patents filed by companies in the period 2021-2023.

Tokai Rika, a prominent global player in the automotive industry, is a leading patent filer in biometric vehicle access. The company has patented a system that utilizes facial recognition technology for driver authentication. Other notable patent filers include Denso and Sumitomo Electric Industries [32]. Regarding application diversity, Panasonic ranks at the forefront, with Mitsubishi Electric and Mazda Motor securing the second and third positions, respectively. Global Mobility Service is leading regarding geographic reach, followed by Brose Fahrzeugteile and Abus Security Centre [32]. Some other leading companies in the biometric vehicle access systems market include BioKey International, Inc., VOXX International Corporation, Fujitsu Ltd, NEC Corporation, Antolin, Hitachi Ltd, Thales Group, Synaptics Incorporated, Fingerprints AB, and Biometric Vox. These firms are dedicated to continuously innovating fingerprint recognition, facial recognition, and other biometric technologies to deliver more precise and reliable vehicle access solutions. The Asia-Pacific biometric vehicle access systems market reached a valuation of USD 255 million in 2023, driven by technological advancements, increasing automotive sales, and a growing emphasis on security [33]. According to a research study by Global Market Insights Inc., the market for biometric vehicle access systems is anticipated to reach a valuation of USD 2.5 billion by 2032.

The growing adoption of electric vehicles (EVs) will expand this market. As the global automotive industry increasingly focuses on sustainable transportation, the incorporation of advanced technologies, such as biometric access systems, is becoming more prevalent. EV manufacturers prioritize integrating cutting-edge features and biometric systems to ensure secure and convenient vehicle access. Moreover, several industry players contribute to market growth by developing innovative

solutions that blend state-of-the-art technology with visually appealing designs. For instance, in January 2024, Continental introduced the Face Authentication Display, setting a new standard for vehicle access management through enhanced biometric user recognition [33]. Automakers are increasingly focusing on advanced, contactless access solutions, which are boosting the adoption of facial recognition due to its smooth authentication process for unlocking doors and starting vehicles. Additionally, rising consumer demand for sophisticated and secure features is expected to fuel growth in this segment further [33]. On December 24, 2018, Hyundai Motor Company introduced the world's first smart fingerprint technology, allowing drivers to unlock doors and start the vehicle using just their fingerprint. This technology was initially set to debut in the Santa Fe SUV model [34]. To access the vehicle, the driver places a finger on the sensor embedded in the door handle. The encrypted fingerprint data is then processed and verified by a fingerprint controller inside the vehicle. The driver can also start the vehicle by touching the ignition, which is similarly equipped with a fingerprint-scanning sensor [34]. Hyundai has addressed potential security concerns with this smart fingerprint technology by utilizing capacitance recognition, which detects variations in electrical levels across different parts of the fingertip. This method effectively prevents the use of forged or fake fingerprints. The technology boasts a misrecognition rate of only 1 in 50,000, making it five times more secure than conventional vehicle keys, including smart keys. Additionally, the system is equipped with a "dynamic update" feature, enabling real-time learning and continuous improvement of fingerprint recognition accuracy [34].

Hyundai's smart fingerprint technology is depicted in **Figure 3** [34].

Figure 3. Hyundai's smart fingerprint technology.

Ford Motor Company has filed a patent for a facial recognition entry system that could be used in future vehicles. The patent, submitted on November 21, 2022, and published on May 23, 2024, describes a camera-based biometric security system allowing vehicle access through facial recognition [35]. This system would use a camera to scan the driver's face and verify their identity before unlocking

the vehicle. The patent also includes a backup authentication method for situations where the facial recognition system may fail due to poor lighting, changes in the user's appearance, or technical issues. This alternative method involves entering a secret code, ensuring that users can still gain access to their vehicle even if the primary biometric system is unavailable [35]. This innovation is part of Ford's ongoing research into advanced vehicle access technologies. As early as 2015, Ford announced the implementation of advanced passenger-observing systems, including eye-tracking and other biometric technologies, to enhance vehicle interior designs, with the Ford GT being among the first to feature such advancements [35]. Beyond the confines of Ford, in 2022, LG Electronics submitted a patent application for the innovation of a novel biometric ignition system. This system is designed to enable vehicle start-up through touchless facial expressions or hand gestures. It employs facial recognition technology to calibrate settings for authenticated drivers, while gesture recognition controls in-vehicle functions, ensuring minimal distraction [36].

3.2. Implementation

Biometric technologies are increasingly integrated into vehicle systems, enhancing security and personalization. They allow for secure engine start-up using fingerprint or facial recognition and automatically adjust vehicle settings to individual preferences. This technology also supports secure vehicle sharing by recognizing multiple users and adapting to their preferences, paving the way for more convenient and collaborative mobility solutions. As biometric integration evolves, it transforms the driving experience into more secure, personalized, and adaptable. The automotive industry is actively working to improve the accuracy and efficiency of biometric technologies. This includes refining algorithms to reduce errors, implementing multi-modal biometrics for greater reliability, and developing adaptive systems to overcome environmental challenges [21]. Advancements in sensor technologies, such as better infrared and 3D imaging, are being pursued to mitigate issues related to poor lighting and to enhance overall biometric performance. Future developments in automotive biometric security are expected to impact the field significantly. Research is focused on integrating AI and ML to improve biometric recognition, allowing systems to adapt and evolve continually. Exploring additional biometric methods, such as palm recognition and iris scanning, expands the possibilities for secure access control [21].

Integrating biometric technologies in vehicles is governed by a complex regulatory landscape that balances innovation with privacy and security concerns. Various countries and regions have established frameworks to ensure the responsible use of biometrics in the automotive industry, with compliance playing a pivotal role in adherence to these guidelines. The General Data Protection Regulation (GDPR) sets strict rules for processing biometric data in the European Union, requiring explicit consent and emphasizing data minimization. Manufacturers operating in the EU must ensure their practices align with these stringent requirements

[33]. In the United States, regulations like the California Consumer Privacy Act (CCPA) and other state-level privacy laws influence how biometrics are applied in vehicles. As technology advances, legislators are considering additional measures to address the unique challenges of biometric data in the automotive sector [21] [33].

1) Biometric Authentication (Something You Are)

The first factor of our proposed 2FA model is biometric authentication, which uses the user's unique physical characteristics. This can include fingerprint recognition, facial recognition, or iris scans. The biometric data is stored securely within the vehicle's onboard computer system, protecting the user's personal information. A fingerprint Scanner can be installed on the vehicle's door handle or dashboard. A Facial Recognition Camera can be integrated into the rearview mirror or an external camera near the driver's door. The Iris Scanner is positioned on the driver's side for convenient access.

2) Mobile App-Based Verification (Something You Have)

Description: The second aspect involves a verification process through a mobile application. The user's smartphone, the primary interaction device with a secure app installed, creates a highly secure one-time password (OTP) or receives a push notification to confirm the request for entry. The application uses secure Bluetooth or Near Field Communication (NFC) signals to the car's system. A specially designed app for iOS and Android devices offers a convenient and user-friendly way to interact with the car's security system. One Time Password (OTP) empowers the user by producing a time-sensitive OTP that they have full control over and need to input into the car's interface. Push Notification, where the application sends a notification that the user needs approval to unlock the car.

3.3. Process Flow of the Two-Factor Authentication Model

User-Initiated Entry: The process begins when the user, a pivotal figure in the system, interacts with the vehicle. They kickstart the entry process using a biometric authentication device, such as the fingerprint scanner, demonstrating their active role in the system [37]. Thorough Biometric Authentication: The vehicle's system, with its meticulous attention to detail, rigorously examines the biometric data provided by the user. It then cross-references this data with the stored information, ensuring high accuracy in the authentication process [37]. Mobile Application Verification: The vehicle initiates a request to the user's mobile application through Bluetooth or NFC technology. The application, acting as the second factor in the two-factor authentication, may generate an OTP or dispatch a push notification to the user [38]. User Authorization: Upon receiving the OTP or push notification on their mobile device, the user is in the driver's seat and empowered to choose how to proceed. They can either input the OTP directly into the vehicle's interface or approve the push notification, giving them a strong sense of control and security [38]. Access Granted: After successfully verifying the second factor, the vehicle's system unlocks the doors, permitting the user to proceed into the

vehicle.

3.4. Security Features and Advantages

1) Improved Security: The Two-Factor Authentication (2FA) model substantially diminishes the likelihood of unauthorized entry by necessitating two distinct verification processes. This means that an attacker would have to circumvent the second factor even if one of the initial factors is compromised [37]. 2) Convenience for Users: Incorporating biometric technology and mobile application verification mechanisms offers a smooth and intuitive user experience. This allows users to access their vehicles effortlessly while maintaining high security [37]. 3) Resistance to Frequently Employed Attacks: The 2FA model is engineered to withstand prevalent attacks such as relay attacks, signal interference, and code interception. Using biometric data presents a significant challenge for replication, and the communication between the mobile application and the vehicle is encrypted [37]. 4) Scalability: The proposed 2FA model can rapidly adapt to various vehicle models and manufacturers. It provides versatility regarding biometric authentication techniques and mobile application functionalities [38]. 5) Compliance with Regulatory Standards: The 2FA model is crafted to comply with the evolving standards of automotive cybersecurity regulations. This ensures that manufacturers fulfill industry benchmarks and safeguard consumer data, thereby securing the support of stakeholders [37].

3.5. Implications of Implementing Two-Factor Authentication (2FA) for Keyless Entry Systems in Vehicles

Adopting two-factor authentication (2FA) for keyless entry systems within automobiles presents many significant implications, encompassing both advantages and disadvantages. These implications could impact a range of stakeholders, such as vehicle manufacturers, users, and the wider automotive sector.

1) Positive Implications

a) Reducing Vehicle Theft Rates: 2FA plays a crucial role in this reduction, introducing an additional security measure that makes it significantly more challenging for unauthorized persons to access vehicles. This results in a decrease in the occurrence of vehicle theft incidents [39].

b) Effective Defense Against Relay Attacks: Two-factor authentication (2FA) plays a crucial role in our defense strategy. By necessitating a second authentication method, it significantly reduces our vulnerability to relay attacks, a common method used to exploit conventional keyless entry systems [39].

c) Perception of Security: Individuals will likely experience a heightened sense of peace knowing that sophisticated security protocols safeguard their vehicles. This increased perception of security may lead to higher satisfaction levels and a stronger commitment to the brand [11].

d) Ease of Use: The contemporary biometric and mobile application-based verification techniques are engineered to be intuitive, ensuring enhanced security

features do not compromise convenience [11].

e) Adherence to Security Regulations: With the tightening of automotive cybersecurity regulations, implementing 2FA can assist manufacturers in adhering to both present and forthcoming standards, thereby circumventing possible legal and financial consequences [9].

f) Leadership in the Industry: The prompt adoption of sophisticated security protocols can establish manufacturers as pioneers in automotive security, thereby securing a competitive advantage.

g) Insurance Premium Reduction: Vehicles equipped with sophisticated security mechanisms, such as 2FA, may be eligible for reduced insurance premiums, thereby offering financial benefits to consumers.

h) Innovation in Automotive Security Technologies: Adopting 2FA could stimulate additional research and development efforts in automotive security technologies, culminating in developing more inventive and efficient solutions.

2) Negative Implications

a) Increased Manufacturing Expenses: The incorporation of supplementary hardware components, such as biometric sensors and communication modules, alongside the development of secure software solutions, escalates production expenses. However, a comprehensive cost-benefit analysis shows that the long-term benefits of these investments often outweigh the initial costs, making them sound financial decisions [8].

b) Maintenance and Updates: The continuous maintenance and updates required for the 2FA system are a testament to its robustness and reliability. While they contribute to manufacturers' and users' long-term financial obligations, they also ensure the security and integrity of the manufacturing processes, making it a worthwhile investment [8].

c) User Complexity: Certain users may perceive incorporating additional steps within the authentication process as inconvenient or burdensome, potentially resulting in resistance or dissatisfaction.

d) Technical Failures: The reliance on biometric sensors and mobile applications introduces potential vulnerabilities. Problems such as errors in biometric recognition or malfunctions within the mobile application could hinder legitimate users from accessing their vehicles.

e) Biometric Data Security: The storage and processing of sensitive biometric data pose considerable privacy concerns. Safeguarding this information from potential breaches presents a significant challenge.

f) Compatibility Challenges: Integrating 2FA systems with current vehicle architectures and keyless entry technologies is a technically intricate process that requires considerable engineering resources and time investment.

g) Legacy Systems: Modifying or retrofitting older vehicle models with 2FA systems might prove impractical or exorbitantly costly, restricting the broad implementation of this technology.

h) The Reliability of Mobile Applications: The efficiency of the two-factor au-

thentication (2FA) system is, to a certain extent, contingent upon the dependability and security of the user's mobile device and associated application. Problems such as device loss, software defects, or cyber-attacks targeting the mobile application can undermine the system's efficacy.

Implementing 2FA within vehicle entry systems can markedly augment security measures, particularly for high-risk or high-value vehicles, including police vehicles, those involved in transporting monetary assets, and luxury automobiles. Although 2FA introduces an additional layer of protection, it is essential to acknowledge that it may also introduce certain inconveniences that must be mitigated. This guide outlines practical strategies for addressing these challenges [40].

3.6. Mitigating User Discomfort with 2FA

1) Delay in Unlocking the Car

Issue: One of the challenges associated with 2FA is the potential introduction of a minor delay in unlocking and initiating the vehicle, which may prove to be an inconvenience for users who are in a hurry. Proposed Solution: We propose adopting rapid and intuitive 2FA mechanisms, such as biometric authentication (utilizing fingerprint or facial recognition technology) to address this issue. This user-centric solution significantly expedites the verification process, providing a seamless user experience without causing undue delay [41].

2) Renewing the PIN Regularly

Issue: Regularly updating the PIN can become cumbersome and may lead to forgetfulness. Proposed Solution: Implement a solution that integrates biometric authentication and a PIN, with biometric authentication as the primary method. This approach minimizes the necessity for frequent PIN updates. Furthermore, it is advisable to employ user-friendly interfaces to facilitate the ease of PIN renewal [41].

3) Possibility of Forgetting PIN or Code

Issue: Users may accidentally forget their PIN or code, which could result in system lockouts. Proposed Solution: To mitigate this risk, it is advisable to implement a comprehensive recovery mechanism that is flexible and adaptable to different user needs. This could include practical mechanisms such as email or SMS verification and the integration of secure password management systems capable of storing and auto-filling PINs. Additionally, biometric authentication methods could be an alternative to the reliance on PINs [41].

4. Cost Estimation for Implementing Two-Factor Authentication in Keyless Entry Systems

Implementing 2FA within automotive keyless entry systems can have considerable associated costs, contingent upon whether the solution is developed internally or contracted to a specialized provider. For instance, developing a rudimentary 2FA solution utilizing SMS-based verification generally requires 5 to 6 weeks of dedicated developer time. For systems that demand enhanced security measures, such as time-based one-time passwords (TOTP) or biometric solutions, the devel-

opment phase may extend to 8 to 10 weeks [42]. The expense associated with in-house development may vary between $15,000 and $20,000, contingent upon the weekly cost of a developer, which is estimated to be between $1800 and $2000. Should outsourcing this task be pursued, the costs are anticipated to escalate by approximately 50%, reflecting the inclusion of external expertise and service fees [42]. Furthermore, the additional expenses encompass the perpetual maintenance, updates, and integration with current systems. These aspects necessitate allocating specialized resources and overseeing service quality and delivery mechanisms [42].

Integrating Two-Factor Authentication (2FA) into keyless entry systems is designed to augment security by introducing an additional layer of verification, thereby mitigating the risk of unauthorized entry and vehicle theft. This enhancement is achieved by applying advanced encryption techniques and implementing robust authentication protocols, encompassing the utilization of Personal Identification Numbers (PIN codes) and biometric authentication methods. These measures collectively contribute to developing a more secure system fortified against prevalent hacking methodologies [42]. The adoption of 2FA in keyless entry systems holds the potential to markedly decrease the incidence of vehicle theft, although conclusive evidence regarding this reduction is still emerging. Incorporating such technologies is in harmony with the prevailing trend towards adopting more robust cybersecurity practices across various sectors, underscoring a dedication to safeguarding confidential information and assets. Through a strategic blend of in-house development capabilities and external service providers, the automotive industry can optimize costs while maintaining the highest security standards for their keyless entry systems [42].

1) Suggestions for Vehicle Manufacturers regarding the phase-in of MFA and collaboration with tech firms

a) Start with High-End Models: Introduce MFA in luxury vehicles where customers are more security-focused and can afford advanced features such as biometric authentication (e.g., fingerprint and facial recognition).

b) Expand to Mid-Range Models: Once proven effective, extend MFA to mid-range vehicles, offering it as a standard feature in higher trims or as an optional add-on. Simplify the technology for affordability, such as offering fingerprint-only authentication.

c) Integrate into Mass-Market Models: Eventually, MFA will be deployed in everyday vehicles, focusing on cost-effective solutions like biometric and PIN combinations to ensure wide accessibility.

2) Collaborating with Tech Firms:

a) Partner with Biometric and Cybersecurity Experts: Collaborate with specialized tech firms to close the expertise gap and ensure the development of secure, robust systems.

b) Accelerate Deployment: Partnerships can accelerate MFA implementation through pre-built APIs and SDKs, enabling quicker and more secure integration into vehicle systems.

c) Joint R&D Initiatives: Work together to develop next-gen biometric technologies, including AI-driven threat detection and multimodal biometrics, to stay ahead of emerging cybersecurity threats.

d) Co-Branding for Trust: Co-brand MFA solutions with established tech firms to enhance credibility and boost consumer confidence.

3) Long-Term Vision

a) Ensure Regulatory Compliance: Collaborate with tech companies to ensure MFA systems adhere to evolving cybersecurity standards, such as ISO/SAE 21434.

b) Industry Leadership: Position early adopters of MFA as leaders in automotive cybersecurity by actively participating in setting industry-wide security standards.

5. Conclusion

The surge in vehicle thefts globally, particularly in regions like the United States, Canada, and the United Kingdom, highlights critical vulnerabilities in modern automotive security systems, especially those relying on keyless entry technology. This research has underscored that while keyless entry systems offer convenience to users, they also present significant risks, as evidenced by the alarming increase in thefts facilitated by relay attacks and CAN bus attacks. The analysis has shown that criminals have largely exploited these vulnerabilities due to inadequate security measures. The failure of existing systems to prevent signal interception and manipulation has led to a widespread surge in vehicle thefts, with specific car models being disproportionately affected. Introducing multi-factor authentication (MFA), specifically two-factor authentication (2FA), in vehicles with keyless entry systems could serve as a robust countermeasure to these threats. By requiring an additional layer of verification, such as a biometric check or a mobile-based confirmation, MFA can significantly reduce the ease with which unauthorized individuals can access vehicles. This additional security layer would mitigate the risk of relay attacks by ensuring that possession of the key fob alone is insufficient for vehicle access. The evidence gathered in this research supports the notion that MFA and 2FA are not just theoretical improvements but necessary enhancements to modern automotive security protocols. As the automotive industry continues to innovate, integrating these authentication methods could provide a crucial safeguard against vehicle thieves' evolving tactics. Ultimately, this thesis concludes that implementing multi-factor and two-factor authentication systems in vehicles is a feasible and effective strategy to curb the rising trend of car thefts associated with keyless entry systems. Such advancements would protect vehicle owners and restore confidence in the security of modern automotive technologies.

6. Future Research

MFA for automotive security should focus on several key areas to strengthen vehicle protection and improve user experience. Investigate the feasibility of using more advanced biometric methods such as iris recognition, palm-vein authenti-

cation, and behavioral biometrics (e.g., gait analysis). These technologies can offer higher accuracy and security, especially for high-end or specialized vehicles. Research how to integrate multimodal biometrics efficiently, combining multiple biometric factors (e.g., fingerprint, facial, and iris recognition) without significantly compromising processing time or user convenience. Examine how artificial intelligence (AI) and machine learning can be integrated into vehicle MFA systems to detect abnormal behavior patterns and adapt authentication processes dynamically. AI could also predict and respond to new cybersecurity threats in real-time.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Mason, S. (2012) Vehicle Remote Keyless Entry Systems and Engine Immobilisers: Do Not Believe the Insurer That This Technology Is Perfect. *Computer Law & Security Review*, **28**, 195-200. https://doi.org/10.1016/j.clsr.2012.01.004

[2] Rogalski, A. (2012) History of Infrared Detectors. *Opto-Electronics Review*, **20**, 279-308. https://doi.org/10.2478/s11772-012-0037-7

[3] How Do Car Key Fobs Work? Phoenix EZ-Keys. https://www.capitalone.com/cars/learn/finding-the-right-car/how-do-cars-withkeyless-entry-work/1178

[4] How Many Semiconductor Chips Are in a Car? Polar Semiconductor, Nov. 30, 2023. https://polarsemi.com/blog/blog-semiconductor-chips-in-a-car/

[5] Alrabady, A.I. and Mahmud, S.M. (2005) Analysis of Attacks against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. *IEEE Transactions on Vehicular Technology*, **54**, 41-50. https://doi.org/10.1109/tvt.2004.838829

[6] Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J. (2022) In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, **22**, Article No. 6679. https://doi.org/10.3390/s22176679

[7] Garcia, F.D., Oswald, D., Kasper, T. and Pavlidès, P. (2016) Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems. 25*th USENIX Security Symposium* (*USENIX Security* 16), Austin, 10-12 August 2016, 929-944.

[8] Anderson, R. and Moore, T. (2006) The Economics of Information Security. *Science*, **314**, 610-613. https://doi.org/10.1126/science.1130992

[9] ISO/SAE 21434:2021, Road Vehicles—Cybersecurity Engineering. Beyond Security, 2021. https://www.iso.org/standard/70918.html

[10] Linda Rosencrance, M.C. and Loshin, P. (2023) Two-Factor Authentication (2FA). Tech-Target. https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

[11] Shechter, S. (2023, Oct. 18) How to Mitigate Vulnerabilities in Keyless Entry Systems. Automotive World. https://www.automotiveworld.com/articles/mitigating-vulnerabilities-in-keyless-entry-systems/

[12] Straughan, D. (2024, Sep. 12) Car Theft Statistics 2024. Market Watch Guides. https://www.marketwatch.com/guides/insurance-services/car-theft-statistics/

[13] Automotive Cybersecurity in 2022. Vic One Report, 2022. https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf

[14] Schmidt, E. (2024, Feb. 27) How Many Cars Are Stolen Each Year? (2024). https://www.consumeraffairs.com/automotive/vehicle-theft-statistics.html#vehicle-theft-statistics

[15] Neiman, T. (2023, Sep. 25) Did the Auto Industry Actually Invent Multi-Factor Authentication? Dynamic Edge, Inc. https://dynedge.com/did-the-auto-industry-invent-mfa/

[16] Car Theft Rate in Selected Countries Worldwide in 2018 Statista. https://www.statista.com/statistics/1238378/car-theft-rate-country/

[17] Klawans, J. (2024, Jul. 22) Canada Is Facing an Uphill Battle against Car Theft. The Week US. https://theweek.com/culture-life/cars/vehicle-theft-canada

[18] Bell, S. (2024, Mar. 3) Keyless Entry Car Thefts Soar as Hackers Don't Need Skills, Just Cheap Devices. Carscoops. https://www.carscoops.com/2024/03/thieves-can-now-exploit-keyless-entry-security-lapses-automakers-have-known-about-for-years/

[19] Mullen, D. (2022, Nov. 28) Keyless Cars Twice as Likely to Be Stolen as Non-Keyless Models. Driving. https://www.driving.co.uk/news/keyless-cars-twice-as-likely-to-be-stolen-as-non-keyless-models/

[20] New Report: Imports Top List for America's Most Stolen Vehicles. National Insurance Crime Bureau, May 9, 2024. https://www.nicb.org/news/news-releases/new-report-imports-top-list-americas-most-stolen-vehicles

[21] Jain, A.K., Ross, A. and Pankanti, S. (2006) Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security*, **1**, 125-143. https://doi.org/10.1109/tifs.2006.873653

[22] Teslas Can Still Be Stolen with a Cheap Radio Hack—Despite New Keyless Tech. Wired, May 22, 2024. https://www.wired.com/story/tesla-ultra-wideband-radio-relay-attacks/

[23] How to Get Away with Car Theft: Unveiling the Dark Side of the CAN Bus. Vic One, May 5, 2023. https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus

[24] Checkoway, S., *et al.* (2011) Comprehensive Experimental Analyses of Automotive Attack Surfaces. 20*th USENIX Security Symposium* (*USENIX Security* 11).

[25] F.F.I.E. Council (2005) Authentication in an Internet Banking Environment. Vol. 28, p. 2006.

[26] Taku, D. (2023, Aug. 24) Cybersecurity Lessons Learned from Data Breaches That Evaded MFA. RSA. https://www.rsa.com/resources/blog/multi-factor-authentication/cybersecurity-lessons-learned-from-data-breaches-that-evaded-mfa/

[27] Multifactor Authentication. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

[28] George Brauchler, S.B. and Morrissey, M. (2023, Apr. 26) The Economic Consequences of Increased Motor Vehicle Theft Rates. Common Sense Institute Colorado. https://www.commonsenseinstituteus.org/colorado/research/crime-and-public-safety/the-economic-consequences-of-increased-motor-vehicle-theft-rates

[29] Multi-Factor Authentication (MFA) Enforcement Roadmap. Salesforce, Jul. 12, 2024. https://help.salesforce.com/s/articleView?id=000389313&type=1

[30] Burt, J. (2024) Google Makes Implementing 2FA Simpler. Security Boulevard. https://securityboulevard.com/2024/05/google-makes-implementing-2fa-simpler/

[31] The Power of Multi-Factor Authentication: Enhancing Security on Office 365. DS Business Life Simplified. https://www.dsbls.com/resources/the-power-of-multi-factor-authentication-enhancing-security-on-office-365/

[32] Cybersecurity: Who Are the Leaders in Biometric Vehicle Access for the Automotive Industry? Just Auto, Aug. 12, 2024. https://www.just-auto.com/data-insights/innovators-cybersecurity-biometric-vehicle-access-automotive/

[33] Biometric Vehicle Access Systems Market to Reach $2.5 Bn by 2032, Says Global Market Insights Inc. Globa News Wire, Feb. 20, 2024. https://www.globenewswire.com/news-release/2024/02/20/2832366/0/en/Biometric-Vehi-cle-Access-Systems-Market-to-reach-2-5-Bn-by-2032-Says-Global-Market-Insights-Inc.html

[34] Cha, J. (2018, Dec. 24) Hyundai Motor Reveals World's First Smart Fingerprint Technology to Vehicles. Hyundai News. https://www.hyundainews.com/en-us/releases/2674

[35] Foote, B. (2024, May 27) Ford Vehicles Could Get Facial Recognition Entry System. Ford Authority. https://fordauthority.com/2024/05/ford-vehicles-could-get-facial-recognition-entry-system/

[36] LG Patent Filing Delves into Automotive Biometrics. Mobile ID World, January 8, 2022. https://mobileidworld.com/lg-patent-filing-delves-into-automotive-biometrics-7012204/

[37] Garcia, M. and Horwitz, J. (2015) Two-Factor Authentication: What and How. SANS Institute.

[38] Miller, C. (2015) Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA.

[39] Greenberg, A. (2015) Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired*, **7**, 21-22.

[40] Francillon, A., Danev, B. and Capkun, S. (2011) Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. *Proceedings of the Network and Distributed System Security Symposium* (*NDSS*), Eidgenössische Technische Hochschule.

[41] From Key Fob to UWB: How Hackers Hijack Vehicle Entry Systems. Vic One, Jun. 7, 2024. https://vicone.com/blog/from-key-fob-to-uwb-how-hackers-hijack-vehicle-entry-systems

[42] Tomikas, U. (2023, Jun. 26) How Much Does Two-Factor Authentication Cost? Messente. https://messente.com/blog/most-recent/2fa-implementation-costs