Securing Keyless Entry Systems against Relay Attacks: A Systematic Literature Review

Lourenço Santos

February 20, 2024

Word Count: 4171
Module Code: 7CCSONCA

Abstract

A relay attack occurs when an attacker deceives a verifier by simulating a trusted prover, misleading the verifier into trusting that they are directly communicating with each other. This type of attack exploits the wireless communication between two honest entities. In a keyless entry system, the "honest prover" could be the key fob of the owner, and the "honest verifier" would be the vehicle's security system designed to unlock the car and allow ignition when the key fob is nearby. In this study we will also delve into how distance-bounding techniques can be subjected to attacks and many mitigation strategies proposed by researchers in the area, and by companies that are fighting this new emerging threat.

Index Terms Relay attack, Keyless entry systems, PKES, RFID, BLE

1 Introduction

The increasing issue of relay attacks in keyless entry systems is raising a concern in the automotive security industry. Relay attacks exploit the communication between a (e.g. key fob) and a verifier (e.g. vehicle) by manipulating the proximity-based authentication mechanism inherent to these systems.
This paper will further explore the security of protocols, delving deeper into BLE and RFID, the **two main technologies** in keyless entry systems in the **automotive industry**. This paper will also review some effective strategies recently employed by different brands to mitigate the risk of such attacks.

1.1 Motivation

In the past months there have been a lot of news articles talking about these kinds of attacks, generally used to forge the distance between the prover and the verifier. Recent news in vehicle theft have highlighted the vulnerability of keyless entry systems to relay attacks.

In an article from Fortune [1] discusses the drop in value of luxury Sports Utility Vehicles (SUVs), including Range Rovers, due to the ease with which they can now be stolen. The concern has escalated to the point where manufacturers are investing heavily in countermeasures to make these vehicles more secure.
Complementing this, a report by The Sun [2], highlights the speed at which thefts can occur, noting that some models can be compromised in as little as 18 seconds.
The urgency of the situation is further illustrated by the theft of a £350,000 Rolls-Royce, which was reported to have been stolen in just 30 seconds, with a 9000€ device as noted by a DailyMail article [3]. This incident showcases the critical need for enhanced security protocols.

Once again, we are confronted with the same old paradigm of security, where

the trade-off between usability and security remains a central challenge. Despite substantial investments in keyless technologies, the industry finds itself compelled to allocate additional resources towards fortifying these systems to address the vulnerabilities that have emerged as a result of this progress.

The Passive Keyless Entry and Start system (PKES) has emerged in recent vehicles. This provides usability to the consumer by automatically unlocking the vehicle without any need for pulling out the keys. The traditional PKES requires a key fob to confirm the user's proximity to the car. New models of Tesla, Volvo, and Lincoln allow owners to use their smartphones to enter and start their cars. [4]. This technology is known as Bluetooth Low Energy (BLE), an ultra-low power consumption and short-range wireless technology. Such systems are vulnerable to attacks, the one we will focus on this paper being are Relay Attacks.

1.1.1 Introduction to Relay Attacks

In a relay attack, the attacker intercepts the communication between an honest prover and an honest verifier, attempting to deceive the verifier into believing it's communicating with the honest prover when it's actually interacting with the attacker.

1.2 Structure of the Study

In the following sections, we will discuss the research methodology, detailing the systematic literature review process. This will be followed by a critical analysis of the key studies on relay attacks in PKES systems, along with mitigation strategies that have proven effective in reducing this risk. We will then discuss the findings and pose new questions, concluding with a summary of our discoveries and recommendations for future research.

2 Research Methodology

2.1 Research questions

RQ1: In what ways have relay attack methods been targeting keyless entry systems, and what tactics are currently mostly employed by attackers?

RQ2: What specific vulnerabilities in BLE and RFID protocols are vulnerable to exploitation through relay attacks, and how can these security gaps be effectively addressed?

RQ3: What are existing methods of defences and how are they effective against relay attacks in keyless entry systems, and in which areas can these defences be improved?

2.2 Keywords and Phrases

To address the research questions, it was identified relevant keywords and developed phrases designed to explore specific aspects of the topic.
The **first** phrase provides a broad overview of security in keyless entry systems and the associated technologies. The **second** phrase focuses on methods to mitigate relay attacks, while the **third** phrase explores offensive strategies in this context. Finally, the **fourth** phrase delves into the underlying protocols of these systems.
Each phrase is tailored to a distinct facet of the research, ensuring a comprehensive analysis:

1: "security" **AND** ("RFID" **OR** "bluetooth") **AND** ("Keyless entry" **OR** "Keyless system" **OR** "PKES")

2: "relay" **AND** ("mitigation" **OR** "countermeasure") **AND** ("Keyless entry" **OR** "Keyless system" **OR** "PKES")

3: "PKES" **AND** ("relay" **OR** "exploitation") **AND** ("RFID" **OR** "BLE") **AND** "security"

4: ("PKES" **OR** "Keyless entry" **OR** "Keyless system") **AND** "protocol"

2.2.1 Search Engines

ACM digital library – returned a total of 68 results IEEE Xplore – returned a total of 15 results King's Library – returned a total of 28 results

2.3 Inclusion and Exclusion Criteria, and Quality Assessment Criteria

IC1: The paper discusses security in keyless entry systems.

IC2: The paper discusses relay attacks and/or countermeasures to it.

IC3: The paper discusses protocols, such as RFID and sub-type NFC OR BLE.

EC1: The paper is published before 2017.

EC2: The paper is not written in English.

EC3: The paper's primary focus is on non-security-related topics of keyless entry systems (e.g., user experience, design).

EC4: The paper lacks peer review or is published in a non-reputable journal.

2.3.1 Selection and validation process

From a total of 111 articles, the number was reduced to 20 research papers after applying the including and excluding criteria. Subsequent snowballing increased this number up to 25 articles.

3 Literature Review

3.1 Keyless Entry Systems - Background

3.1.1 Before Keyless Entry Systems

Before keyless entry systems appear, there were already many concerns about the security of the actual keys.
On credit cards there were already ways to clone the card with techniques such as phishing or card skimming, which is a technique where a device can be attached to an ATM machine to steal credit cards, and not really expensive (around €100) [5]
On key doors there were already known attacks, such as Lock Picking, which involves aligning pins or levers without the original key, while lock bumping uses a special key to momentarily align pins for unlocking.
These methods expose the limitations of traditional locks, highlighting the need for improved lock designs to enhance security.

3.1.2 Appearance Keyless Entry Systems

As technology evolves, new vulnerabilities appear, and this is where we will focus from now on. Keyless Entry Systems are known for their commodity to the user, but they also bring a lot of new challenges. "A traditional Remote Keyless System (RKS) refers to a locking system on a vehicle that can be unlocked by an electronic remote control, such as a key fob." [6]
When you unlock a vehicle it verifies the proximity of the key to the vehicle, that's why vehicles with PKES system don't need a user interaction anymore, as they automatically detect the proximity of the key fob to unlock the car, and lock it when exceeding the range.
Typically, the key fobs from PKES are equipped with RFID tags, which made them vulnerable to many new threats, specially to relay attacks. Some other vehicles use NFC or BLE to open their cars. As an example, Tesla use BLE technology to detect the proximity of the smartphone to the car, and also uses NFC, which is a sub-type of RFID, on the key card that unlock them.

3.2 Passive Keyless Entry Systems (PKES)

The first work on PKES appeared on 1990 by T. Waraksa et al. (US patent 4942393, 1990) [7].
In their patent, the authors talk about a system that is able to unlock the vehicle without any user action, by simply walking up to the vehicle it will be unlocked, or by moving away to lock it.
This system is characterized as 'Passive' as it doesn't need any action from the user. [8]
On these systems we can mention 3 different regions that allow for different actions:

- Remote distance to the vehicle (up to 100m): allows to lock or unlock the car by pressing the button on the key fob.
- Outside the car (between 1-2m from the door): allows to unlock and lock the car by using the door handle.
- Inside the car: allows to start the engine.

PKES keys use a low-frequency (LF) RFID chip and ultra-high-frequency (UHF) RFID signal to unlock or start the vehicle. [9]
By using the LF, the vehicle can forward a message, also known as "challenge" to tell the key to get ready for communication. [9] This challenge is a cryptographic challenge from the car sent to the RFID on the key fob, and solved by the microcontroller on the key fob, which then responds over the UHF signal. When the key is within distance, it responds with challenges over the UHF. When the key is far, meaning that the LF RFID isn't seen, and the vehicle receives UHF signals from the key fob, they are ignored.

The protocols for PKES systems may differ based on the vehicle manufacturer. Usually, these systems are designed to function in two distinct modes: the normal and the backup mode.
The normal mode operates effectively when the battery is charged and functioning properly. On the other hand, the backup mode is designed to work even in the absence of a functional battery. [10]
On the backup mode, if the key fob has no battery, the owner of the vehicle is still able to open and start the car. They can do this because manufacturers usually embed a physical key within the key fob.
The most common types of relay attacks on PKES systems are: relay attacks and amplified relay attacks.

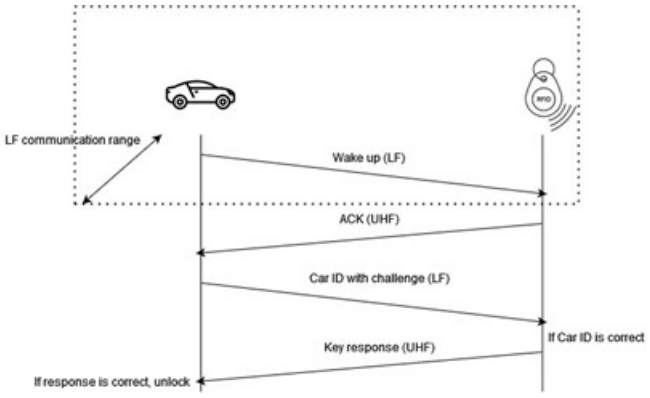

Figure 1: Example of PKES authentication

3.2.1 Usage of BLE in PKES

Bluetooth Low Energy (BLE), is an emerging short-range wireless technology aiming at low-power, low-latency, and low-complexity communications. (available on almost all smartphones, tablets and laptops). [11]
While in RFID the vehicle keeps searching for the signal from the key fob, in BLE PKES systems they typically rely on Received Signal Strength Indicator (RSSI) to estimate the proximity between the key fob, often in the form of a smartphone, and the vehicle.

Advantages of BLE This technology was designed for low power consumption, making it ideal for devices smartphones. Despite its low energy consumption, BLE supports high data transfer rates, and has low-complexity communication, which makes this communication between the key and the vehicle faster.

Disadvantages of BLE Unlike RFID, where proximity is determined by signal presence, BLE's use of RSSI for proximity measurement can be more susceptible to manipulation. Attackers may try to amplify or attenuate signals to trick the system. Ensuring secure pairing and continuous authentication between a device and the vehicle is crucial, as poorly managed pairing can leave openings for unauthorised access.

3.3 Relay Attacks

As previously mentioned, there are two possible attacks on a PKES system, but we will focus more on the relay attack. In a relay attack, an attacker sets one device close to the car and another close to the key fob's owner. These devices then act as a bridge, transmitting signals between the key fob and the vehicle. This process allows the attacker to start the car.
An amplified relay attack uses the same principles but with only an amplifier. The target stands by the target car and amplifies the signal, if the target is nearby with the key fob, then the car will be unlocked. What this amplifier does is increasing the range of the vehicle's sensor so that the key fob is able to communicate with it.
A book written by Smith (2016) provides an in-depth analysis of these techniques [9].

3.3.1 RFID Relay Attacks

Radio-frequency identification technology (RFID) involves using electronic methods to identify, record, and note the presence of an object using a radio signal. [14]
RFID-based relay attack usually means that communication messages are unexpectedly passed between two parties that include an RFID tag (T) and a reader (R). It is unexpected since the two are not physically close to each other as is required for such communication to take place. [15]

Figure 2: Example of a Relay attack with a signal repeater, from [12]

Figure 3: Example of an Amplified Relay attack using wire antena, from [13]

The studies conducted by Azadeh Rad et al (2018), Abdellah, Maatallaoui et al. (2023) and Yu-Ju Tu et al. (2019) provides us a good foundation in the domain of RFID Relay Attacks.

There are two main types of RFID-based relay attacks.
Let's start by the RFID-based **Mafia fraud** relay attack. This attack occurs when the prover and the verifier are both not aware of the attack and are authenticated. Normally, there's a communication between an honest tag and an honest reader. However, an attacker can employ a malicious reader in between to mimic the honest reader to the honest tag and then relay the message from the honest reader to the honest tag. Similarly, the attacker can use a malicious tag to impersonate the honest tag and then relay the honest tag's message to the honest reader. [15]
This attack can be detected by using Distance-Bounding Protocols (DBPs) to measure the additional delay in the round-trip time of the signal, by including two parameters, a secret key and a random number when generating a response. [16]

The second RFID-based relay attack we will discuss is the **Terrorist fraud** relay attack. In this attack a dishonest tag is aware of the unexpectedly relayed data, but the honest reader isn't. The main difference is that the dishonest tag is part of the attack and helps fooling the reader. As an example, when a customer completes a transaction using mobile payment, there's a risk of falling to RFID-based relay attacks. Additionally, if a customer is complicit, they can permit an attacker to relay their payment details for making a purchase remotely, in a place where the customer is not present. Consequently, since the customer can claim they were elsewhere, they might dispute the transaction. This leaves the credit card issuer to deal with the financial loss. In such a

situation, a dishonest customer exploiting compromised payment methods can perform a relay attack. [15]

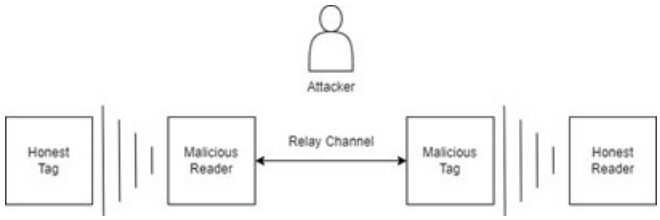

Figure 4: Mafia Fraud relay attack

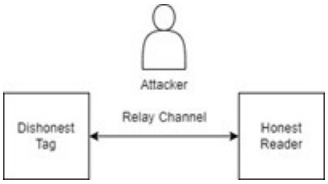

Figure 5: Terrorist Fraud relay attack

3.3.2 Prevention and Mitigation Strategies

Rolling Codes: One of the first mitigation strategies that appeared were rolling codes. Before these rolling codes were implemented, if an attacker captured a Radio-Frequency(RF) from a key fob, he would be able to repeat the same signal repeatedly, meaning that he would have access to the device until it was changed.
The rolling code, also known as hopping codes, counter this threat by using an algorithm that changes the code transmitted by the key, every time it is used. This way, if an attacker intercepts the signal, it will only be valid once.
In most systems, there will be only 1 valid code, so if the attacker wanted to save a lot of different codes, he wouldn't be able to do so. [17]
If the owner of the key fob unlocked the car with the code n+3, in most systems, all the other codes intercepted by the attacker would become meaningless. However, if the attacker replayed the last code, in this case n+2 before the key fob sent the code n+3, then the car would be unlocked. Additionally, advanced rolling code implementations already have precise timestamps besides the counters (e.g. Ultimate KeeLoq) avoid any practical replay attacks because of the time difference between the vehicle and the key fob's signal. [17]
In the following example, we can see the interaction between the key fob and the vehicle, and we have an adversary trying to intercept the codes sent by the key fob.

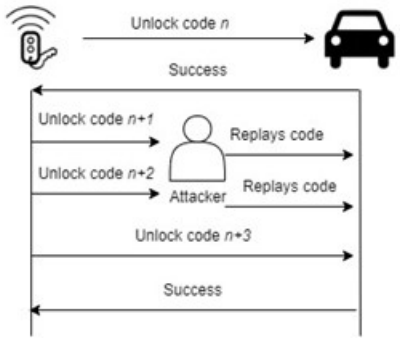

Figure 6: Intercepting signal with rolling code technology

Temperature Sensors and Round-Trip Measurements: This method was proposed by P. Urien et al. [5] This authentication protocol contains two components for measuring the physical proximity of the reader and the tag to each other: tag temperature and physical distance as measured by signal round-trip time.
The idea is to use a temperature sensor-enabled RFID tag that can measure the tag temperature. The measured temperatures are then exchanged between tag and reader and the difference in their temperatures is then checked for validity. When both tag and reader are physically close, the temperature delta should be minimal.
Since relay devices add a delay to the signal, the round-trip time would be longer than expected, and the temperature may differ if the key is not in the expected environment (e.g., outside vs. inside a pocket)

Coordinate Tracing System: This system, also known as PKES Forcefield, will use the vehicle as the center point and then trace the authenticated key, as shown in figure 5. This method was proposed by Syed Rizvi et al. [10] By using a developed algorithm to calculate the exact longitude and latitude of the authorized key. The PKES Forcefield also traces the movement through the coordinate system, and this information prevents relay and amplified relay attacks, as the attacker cannot simply impose a key signal right next to the vehicle. When a key leaves the area covered by the vehicle, the car anticipates that the same key will come back within range. Although the key may not return from the same direction it left, it must come back into the system's area to be recognized.

Sleep Mode for Key Fobs: This countermeasure to prevent relay attacks from happening, consists of, when the key fob stopped moving for the last seconds/minutes depending on the vehicle, it will stop emitting signal, this way, amplified relay attacks will not succeed, as there is no signal being emitted from the key fob that could be relayed to the honest verifier. Ford is an example of a

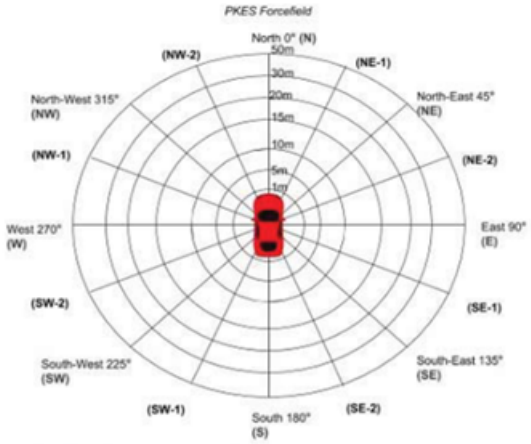

Figure 7: An illustration of PKES Forcefield graph, from [10]

vehicle brand that has been keeping up to date with this new security threats. The new motion-sensing key fob enters sleep mode after 40 seconds of inactivity, blocking relay box hacking attempts. Simply moving the fob reactivates it, ensuring functionality as you approach your vehicle. Ford's fobs work within a 2-meter range of their paired cars.

Pin to Drive: This mitigation strategy should be seen more as an additional security layer. In this case, even if your car is opened, the car wouldn't start just because you're inside the car, it would first prompt you for a PIN. "PIN to Drive allows you to set a secure four-digit verification that must be entered before your vehicle is driven." [18] There are concerns about the actual safety provided by this feature, as this was a feature implemented by Tesla, and anyone within a 9 feet range would be able to see you type the code on the big screen.

SecuriCode: Similar to Pin to Drive, this countermeasure prompts you for a code, differing from the Tesla Pin to Drive, due to the fact that the code is actually asked you before entering the vehicle. The SecuriCode keypad, located on the driver's door, lets you enter a code to lock or unlock your vehicle. Depending on your vehicle model, it may have physical buttons, or it may be invisible until you touch it. [19]

Figure 8: SecuriCode, from Ford

4 Discussion

In this study, it was conducted a comprehensive evaluation of how the PKES systems work, how they can be exploited by different types of relay attacks and countermeasures that have been lately employed by different companies. The discussion of the security of these systems sheds light on the challenges that remains on usability against security.

4.1 Security Analysis

The analysis revealed a spectrum of strategies deployed to mitigate relay attacks, from rolling codes, to more sophisticated techniques proposed by researchers, such as temperature sensors and round-trip measurements and coordinate tracing systems, to strategies offered by companies concerned with this security threat, such as the sleep mode functionality for key fobs, the pin to drive and SecuriCode.

Rolling Codes and Encryption Techniques The introduction of rolling codes has been the first big step in mitigating the risks associated with replay attacks on PKES systems. Despite their efficiency, the security afforded by rolling codes is not enough. Attackers, equipped with sophisticated tools, have developed techniques to exploit vulnerabilities in the transmission process. This highlights the need for continuous research in encryption technologies and the development of more robust key generation algorithms to stay ahead of these emerging threats. [17]

Temperature Sensors and Round-Trip Measurements Integrating temperature sensors and leveraging round-trip timing measurements introduce a new layer of security that focuses on the physical properties of the communica-

tion environment. This method authenticates signals based on the assumption that interactions occur within specific environmental parameters, including temperature. However, the effectiveness of this approach is heavily dependent on the accuracy of the sensors and the calibration of the hardware, with environmental changes posing a significant challenge to its reliability. [5]

Coordinate Tracing System The adoption of coordinate tracing systems represents a great improvement in securing PKES systems against relay attacks. However, the practical application of such systems is not that easy. They demand considerable computational power and sophisticated algorithms to accurately process geographical data in real time, which PKES architectures might not be able to accommodate yet. [10]

Sleep Mode for Key Fobs Implementing a sleep mode feature in key fobs addresses the vulnerability of stationary key fobs. By stopping to transmit signal after a period of inactivity, this measure reduces the risk of signal interception and unauthorized relay attacks. [20]

4.1.1 Usability versus Security

Although fortifying PKES systems against cyber threats is an urgent topic, the main challenge remains on doing so without affecting user experience. As security protocols become more complex, the risk of limiting the user experience with heavy procedures grows. Security mechanisms that demand additional user actions, such as Pin to Drive and SecuriCode, perfectly illustrates this challenge, while all it takes for this additional layer of security to be bypassed is some social engineering. Future innovations must, therefore, aim to integrate advanced security features without reducing the usability of the system.

4.1.2 Future Directions

The landscape of automotive security is constantly evolving, driven by technological advancements and the emergence of new cyber threats. To maintain the integrity of PKES systems, future research should delve into the potential of biometric authentication and the application of machine learning for anomaly detection.

Biometric Authentication The integration of biometric authentication technologies, such as fingerprint, face print, or palm print, offers a promising future not only for strengthening the security of PKES systems, but also other types of authentication such as passwords, ID cards. [21] Biometrics provide a unique layer of security based on individual physical or behavioural characteristics, making unauthorized access considerably more challenging. However, as every technology mentioned in this paper, it might face some new challenges as well. An example of that are deep fakes, a new technology emerging and posing a great risk for this new generation.

Machine Learning for Anomaly Detection Anomaly detection refers to "the problem of finding patterns in data that do not conform to expected behavior" [22] [23] [24].
Incorporating machine learning techniques into PKES systems represents a significant step forward in detecting and preventing security breaches. By analyzing patterns and identifying deviations from normal behavior, these systems can instantly flag potential threats, offering a dynamic and adaptive layer of protection. This approach could quickly adapt to new methods of theft or unauthorized entry, as machine learning algorithms learn from each attempted breach, continuously improving the system security.
Nevertheless, the effectiveness of such systems will depend on the ongoing collection of robust and diverse data sets to train the algorithms effectively.

5 Conclusion

The aim of this study was to analyse PKES systems and reveal a fundamental need for a security paradigm that does not compromise user convenience for the sake of protection. As the automotive industry progresses, the implementation of sophisticated, user-friendly security strategies will be crucial in defending against relay attacks, thereby ensuring the enduring security and convenience of PKES technology. Failing to accomplish this mission could lead to a reconsideration of more traditional key entry systems, compromising the technological advancements achieved so far.

References

[1] R. Hogg, "Range Rovers are plummeting in value because theyve become so easy to steal—now its makers are spending millions trying to make the luxury SUVs theft-proof," https://fortune.com/europe/2023/12/14/range-rovers-value-steal-theft-proof/, Dec. 2023.

[2] J. Gratton, "STOLEN IN SECONDS Keyless car can be broken into in just 10 seconds and some popular models are easier to break into than others," https://fortune.com/europe/2023/12/14/range-rovers-value-steal-theft-proof/, Aug. 2019.

[3] D. Boyle, "£350,000 Rolls-Royce is GONE in 30 seconds! Moment key-less car thieves steal luxury SUV on owner's driveway," https://www.dailymail.co.uk/news/article-12790145/350-000-Rolls-Royce-GONE-30-seconds-Moment-key-car-thieves-steal-luxury-SUV-owners-driveway.html, Nov. 2023.

[4] J. Li, Y. Dong, S. Fang, H. Zhang, and D. Xu, "User context detection for relay attack resistance in passive keyless entry and start systemuser context detection for relay attack resistance in passive keyless entry and start systemc," *Sensors*, vol. 20, no. 16, p. 4446, 08 2020.

[5] P. Urien and S. Piramuthu, "Elliptic curve-based rfid/nfc authentication with temperature," *Decision Support Systems*, vol. 59, pp. 28–36, 03 2014.

[6] J. Wang, K. Lounis, and M. Zulkernine, "Cskes: A context-based secure keyless entry system," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019.

[7] T. Waraksa, K. Fraley, R. Kiefer, D. Douglas, and L. Gilbert, "Passive keyless entry system," US Patent 4942393, 7 1990.

[8] Z. A. H. B. Z. Abidin, "Car key lock reminder (xbee wireless module implementation)," Master's thesis, Universiti Teknologi PETRONAS, Dec. 2010, dissertation Report.

[9] C. Smith, *The Car Hacker's Handbook*. No Starch Press, 2016.

[10] S. Rizvi, M. Tokar, J. Imler, and L. Ritchey, "Securing pkes against relay attacks using coordinate tracing and multi-factor authentication," pp. 1–6, 2019.

[11] J. Yanga, C. Poellabauer, P. Mitra, and C. Neubecker, "Beyond beaconing: Emerging applications and challenges of ble," *Ad Hoc Networks*, vol. 97, Feb. 2020.

[12] J. Cox, "Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds," https://www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars, Feb. 2020.

[13] R. Pattinson, "FAST & FURIOUS Shocking clip shows thieves stealing £350K Rolls Royce in 30 seconds using wire antenna to unlock car," https://www.the-sun.com/news/9701810/thieves-rolls-royce-aerial-clone-key/, Nov. 2023.

[14] T. T. Alshamri, M. M. Albakheet, and P. I. I. Kateeb, "Survey on radio frequency identification security and attacks," Dec. 2021.

[15] Y.-J. Tu and S. Piramuthu, "On addressing rfid/nfc-based relay attacks: An overview," *Decision Support Systems*, vol. 129, p. 113194, 02 2020.

[16] A. I. Rad, M. R. Alagheband, and S. B. Far, "Performing and mitigating force and terrorist fraud attacks against two rfid distance-bounding protocols," *Journal of Information Security and Applications*, pp. 87–94, Oct. 2018.

[17] L. Csikor, H. W. Lim, J. W. Wong, S. Ramesh, R. P. Parameswarath, and M. C. Chan, "Rollback: A new time-agnostic replay attack against the automotive remote keyless entry systems," Tech. Rep. 1, 01 2024.

[18] Tesla, "Vehicle Safety & Security Features - Tesla Support," https://www.tesla.com/en_my/support/vehicle-safety-security-features, accessed: 2024-02-11.

[19] "Ford Technology: SecuriCode Keyless Entry," https://casscountyford1.wordpress.com/2013/02/17/ford-technology-securicode-keyless-entry/, accessed: 2024-02-11.

[20] Ford, "Motion Sensing Key Fob - Ford Accessories," https://www.ford-accessories.ie/safety-+-security/antitheft-devices/motion-sensing-key-fob/2514050#, accessed: 2024-02-11.

[21] Y. Zhang, J. Qin, and L. Du, "A secure biometric authentication based on peks," *CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE*, pp. 945–1395, Mar. 2016.

[22] V. Chandola, A. Banerjee, , and V. Kumar, "Anomaly detection: A survey." *ACM Comput. Surv*, vol. 41, pp. 71–97, 2009.

[23] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," Tech. Rep., Dec. 2018.

[24] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78 658–78 700, 2021.