Relay attack survey

Tereza Burianova
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
xburia28@vutbr.cz

***Abstract*—This survey summarizes interesting research regarding relay attacks with focus on the most affected areas - Passive Keyless Entry and Start vehicles, contactless payments and NTLM. Implementations of the attack and possible countermeasures are presented, with one of the most universal measures being distance bounding protocols.**

***Index Terms*—Relay attack, Passive Keyless Entry and Start (PKES), car theft, smart cards, contactless payments, New Technology LAN Manager (NTLM), Distance Bounding Protocols.**

I. Introduction

The relay attack is a significant security threat, especially with contactless technology being more popular in general, and often no special equipment is needed to execute such an attack with mobile phones being equipped with NFC technology. Even after years of research, relay attacks are still prevalent and proposing effective countermeasures is difficult due to the attacker not needing to know any information about the relayed message for the attack to be successful, making the application-level countermeasures ineffective.

This survey summarizes critically affected areas with description of existing papers regarding the implementation and execution, possible countermeasures specific for the selected areas, including detection and prevention, examples of other interesting relay attack implementations and generally applicable countermeasures with focus on distance bounding protocols.

II. Relay attack

To execute the attack, the attacker generally relays the communication between the reader and the credential, e.g. a smart card or a car key fob, without the reader recognizing that the credential is not located in proximity. While the proxy credential communicates with the legitimate reader and the proxy reader communicates with the legitimate credential, the communication is relayed between the proxy reader and the proxy credential, increasing the distance over which the reader can still communicate with the credential without the owner's knowledge. The described process is shown in Figure 1. Additionally, the attacker can perform a man-in-the-middle attack, also referred to as an active relay attack by Hancke, in a similar way, exploiting a vulnerability in the security protocols and modify the relayed communication [1], [2]. The relayed data can be intercepted on the physical layer, or, recently more commonly, on the application layer in the form of application protocol data units, further increasing the capabilities of such an attack. There are also cases of software-based relay attacks, where the relay is realized through a connection between the device, infected with a malicious app, and the attacker's device [3].

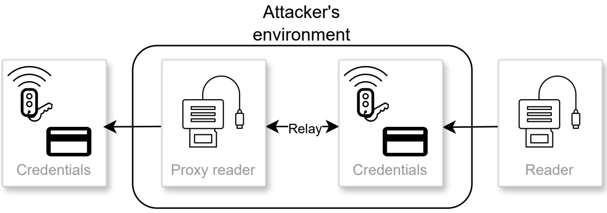

Fig. 1. Description of the relay attack principle.

III. Passive Keyless Entry and Start vehicles

According to a report by toronto.com, car theft is recently on the rise, with relay attacks being one of the most common methods [4]. The reason for the rise is the new PKES technology, where a key fob constantly emits signals, allowing the car owner to unlock and start their car by having the key fob in proximity, without need of any interaction. The attack does not require expensive specialised equipment, allowing the attackers to execute an attack with a relatively cheap custom device [5].

A. Protocol description

In a PKES system, an LF RFID tag is used for the short range and an UHF transceiver for the long range communication using the key fob. Typically, the car periodically communicates with the key fob using a wake up message sent through the LF RFID, checking the proximity of the fob. Once the key fob acknowledges the wake up message, a challenge is sent by the car. In some systems, instead of using a wake up message, the car communicates by directly sending the challenge. The key fob uses the UHF transceiver for the response [6]. An example of the communication between the car and the fob is shown in Figure 2.

B. Attack implementations

Francillon, Danev and Capkun [6] described and implemented a relay attack on PKES at the physical layer, independent of the used system and cryptography. In their attack, only the RFID LF communication was relayed, as the UHF range

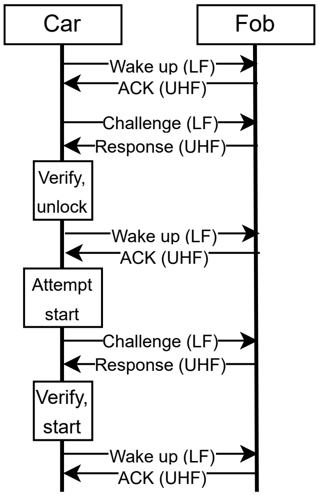

Fig. 2. An example of the PKES protocol communication [6], [7].

was sufficient as is. They described two ways of executing the attack, using wired and wireless equipment.

In the wired attack, attackers use two loop antennas connected with a coaxial cable with an added amplifier. By bringing one of the loops closer to the handle or the start button, the signal is captured, amplified and relayed to the key fob, which then sends the valid response.

In the wireless attack, a RF link consisting of an emitter and a receiver is used to capture, amplify and relay the messages wirelessly, up-converting and down-converting it on the way to extend the relay distance. This method is not only less noticeable during the attack execution and possible even with key fobs behind walls, but also keeps the delay lower.

Wouters et al. researched automotive security in general, combining the opportunity of a relay attack with other existing vulnerabilities in the security system [7]. The main focus was on systems used in luxury cars, with an attack being successfully demonstrated on Tesla Model S. They were successful in building a protocol analyser and getting information regarding the protocol and the frame structure. According to their research, there is no implementation of a relay attack protection, e.g. a distance bounding mechanism, the protocols used in the analysed cars utilize the same 40-bit cryptographic key for opening and starting the car and a proprietary cryptographic algorithm proven to be unsafe, the correct response to a wake up message can be calculated and the key fob responds to any received challenge that has the correct frame format. These findings allow for an active relay attack, described in section II as a relay attack additionally utilizing vulnerabilities in the security mechanism. Additionally, the relay attack could lead to another dangerous attack by giving attackers access to communication ports, allowing them to install rootkits on the computer system and get control of the car.

C. Countermeasures

The countermeasures that can be implemented directly by car owners include using a protective case and removing the battery from the key. The protective case must create a Faraday cage around the key, making the attack more difficult. Combined with removing the battery, which changes the mode of the key fob and requires it to use a physical key to open the car and move the fob directly to the start button to start the car, these countermeasures considerably decrease the possibility of a relay attack [6].

Many car makers implemented a countermeasure that utilizes a motion sensor in the key fob. After not detecting any movement for a set period of time, the key fob enters sleep mode, not sending any signal. This countermeasure is efficient for the cases where the attackers gain access to the car directly in front of the owner's house, with the key fob laying in their house. However, the attack can still be executed before the key fob enters the sleep mode, and only works when the key fob is currently not carried by the owner [8].

In an attempt to prevent the frequent car theft cases, the Canadian government is taking steps to ban a popular tool Flipper Zero, used by hobbyists to experiment with communication protocols. It has been brought up that Flipper Zero is unable to bypass most security system used nowadays. The attackers presumably use custom or specialized equipment, rendering this measure inefficient [9].

Paniagua has proposed a concept of a detection system based on Random Forests, allowing the system to trigger appropriate reaction when detecting a relay attack [10]. Random Forest is a machine learning algorithm that allows to make predictions and classifications based on the combination of several decision trees. The model is designed in a way that assumes its integration directly in the security system, enabling immediate reaction to a possible relay attack.

Jeong and So propose an additional phase after the challenge-response phase, collecting the channel state information (CSI). Correlation between the last and the current CSI is then used, together with round-trip-time (RTT), to determine the proximity of the key based on more properties [11]. The communication protocol is shown in Figure 3.

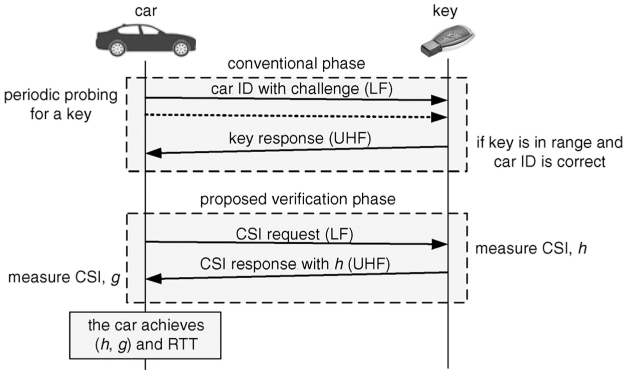
car
key
conventional phase
periodic probing for a key
car ID with challenge (LF)
key response (UHF)
if key is in range and car ID is correct
proposed verification phase
CSI request (LF)
measure CSI, h
CSI response with h (UHF)
measure CSI, g
the car achieves (h, g) and RTT

Fig. 3. An example of the PKES protocol communication with additional CSI phase proposed by Jeong and So. Source: [11].

Francillon, Danev and Capkun propose a solution that utilizes a secure distance bounding protocol to determine the proximity of the car and a verifiable multilateration protocol to verify that the key fob is located inside the car [6]. Distance bounding protocols are further described in section VII.

IV. Contactless smart cards and payments

While relay attacks on contactless payments are not as prevalent as the relay attacks in car theft cases, described in section III, they still may be problematic. Based on many analyses, the implemented relay attack protection is still not fully resistant against these attacks, with the mobile payment services like Apple Pay or Google Pay, adding a completely new layer of possible vulnerabilities in this area.

While the contactless payment relay attacks can also utilize the previously described hardware setup [12], they can also use a software setup, where the equipment needed by an attacker comprises of a card emulator and a relay software. The relay software is a malicious application installed on the user's device, which is able to relay the APDU communication between the user's device and the attacker's emulator [3]. Additionaly, with the widely used NFC technology, no additional hardware is needed to successfully perform a relay attack other than mobile phones with NFC and the required software, as shown by Francis et al. in the practical demonstration [2].

A. *Visa and Mastercard*

To mitigate relay attacks, Mastercard included a Relay Resistance Protocol (RRP) in their specification. RRP adds a nonce exchange on the EMV layer, which is repeated every time the time of communication is outside bounds. After three repeated exchanges, the payment is rejected.

Radu et al. analysed the RRP and recognized significant inconsistencies in response times on the EMV layer, caused mainly by different placement of the card on the reader. This could possibly leave a relay attack undetected, recognizing it as a legitimate card placed incorrectly. They observed more consistency in response times on the ISO 14443 layer and proposed that implementing the measures on the ISO 14443 layer would improve the functionality [13].

Visa suggests a measure that would bind ISO 14443 layer data to EMV layer data, assuming the ISO 14443 layer data cannot be tampered with by an attacker. The protocol has not yet been specified or implemented.

Radu et al. showed that the assumption about ISO 14443 layer data being tamper-proof is incorrect, due to the possibility of data forge using a rooted smartphone to change the UID of a card or a mobile phone.

They proposed a new protocol called L1RP, combining principles from both Mastercard and Visa countermeasure suggestions. This proposal moves the nonce exchange into the ISO 14443 layer. In the data binding suggested by Visa, ISO 14443 layer includes nonces issued from both the card and the reader. The protocol is shown in Figure 4 [13].

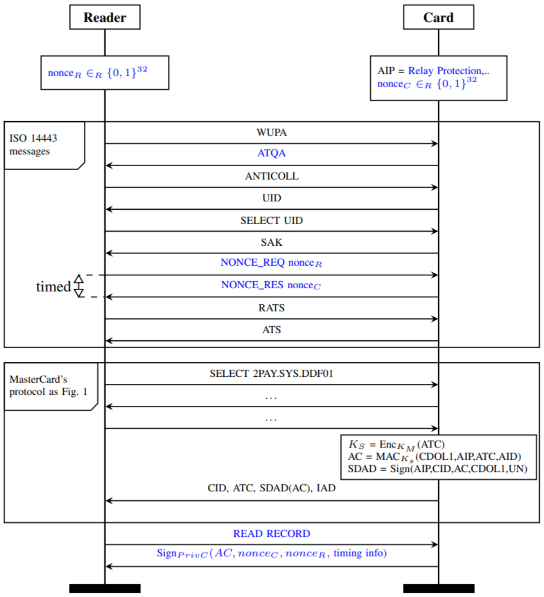
Reader
Card
$\text{nonce}_R \in_R \{0,1\}^{32}$
AIP = Relay Protection,..
$\text{nonce}_C \in_R \{0,1\}^{32}$
ISO 14443 messages
WUPA
ATQA
ANTICOLL
UID
SELECT UID
SAK
NONCE_REQ nonce_R
timed
NONCE_RES nonce_C
RATS
ATS
MasterCard's protocol as Fig. 1
SELECT 2PAY.SYS.DDF01
...
...
$K_S = \text{Enc}_{K_M}\text{(ATC)}$
$\text{AC} = \text{MAC}_{K_s}\text{(CDOL1,AIP,ATC,AID)}$
SDAD = Sign(AIP,CID,AC,CDOL1,UN)
CID, ATC, SDAD(AC), IAD
READ RECORD
$\text{Sign}_{PrivC}(AC, nonce_C, nonce_R, \text{timing info})$

Fig. 4. New L1RP protocol proposal against EMV relay attacks by Radu et al. Source: [13].

B. *Apple Pay Express Transit Mode*

In 2019, Apple introduced the Express Transit Mode for Apple Pay, which allows users to pay for transit at the station barrier without confirming the interaction by unlocking the iPhone. It was discovered by Radu et al. that the feature is invoked by receiving a set of magic bytes, allowing to bypass the lock screen. After checking certain conditions, a transaction is performed.

Based on experiments, it has been found out that after replaying and relaying the messages, it is possible to carry out a fraudulent transaction for any amount when a Visa card is used. For Mastercard, this attack could not be performed due to the check if the value of the Merchant Category Code is set as transportation services.

When resolving the threat, Apple believed the fault to be on Visa's end, suggesting checks similar to the ones performed by Mastercard. They rejected a system similar to Samsung Pay, which only performs zero-value payments in the transport mode and has an arrangement with the banks to receive payments based on the amount of the zero-value transactions. Apple also did not pay the advertised bug bounty to the researchers. Visa suggested the mistake is on Apple's end, due to the issue only occurring with Apple pay. Based on experiments, the attack would be mitigated by implementing the L1RP protocol, shown in Figure 4 [13].

C. *Google Wallet*

In 2012, Roland, Langer and Scharinger performed a software-based relay attack on Google Wallet [3]. This was performed using an Android application that maintains a persistent TCP connection with attacker's card emulator. The app can imitate opening the Google Wallet and entering a valid

PIN by selecting the corresponding component and sending the unlock command. The attack required rood access to the device.

After discussions with the Google team, an update was issued where the credit card applet could no longer be accessed from the application processor. This update did not change the locking and unlocking system, still allowing the attacker to unlock Google Wallet without entering a valid PIN.

D. ISO 14443 - proximity identification cards

Conactless payment cards are an implementation of ISO 14443, alike other identification cards using contactless technology, like biometric passports or ID cards. As shown by Hancke, relay attacks, in this case hardware-based, can be used similarly to contactless payments for any of those implementations [12].

V. NTLM RELAY

NTLM (New Technology LAN Manager) relay attacks have been a currently addressed topic. Based on an article by The Hacker News [14], a Russian hacker group has been targeting critical organizations in 2022 and 2023 with the goal to access private information. The attackers utilized security flaws in Microsoft Outlook and WinRAR to gain user's NTLM hash, which allowed them to perform a NTLM relay attack. According to a recent article by Help Net Security, a large number of servers are vulnerable due to being outdated and not having the security patches for known security flaws [15].

A. Attack explanation

Initially, the attacker needs to access the user's NTLM authentication. This can be done by taking advantage of a security flaw or by forcing the user to authenticate to a malicious server. The NTLM messages then can be relayed over various protocols due to NTLM being independent of the application protocol. This allows the attackers to bypass multi-factor authentication, gain the password hashes, escalate their privileges and possibly obtain sensitive data [16], [17].

B. Countermeasures

a) Security patches: It is important to maintain servers up-to-date with new security patches. This does not completely stop the attacks due to possible unfixed or unknown security flaws, but makes the attacks more difficult [15].

b) Manual detection: The ability to detect the attack means that the attacker has already executed the attack successfully, meaning the reaction has to be quick. To access the logs for manual analysis, Audit Security System Extension must be enabled. Events with ID 7045 or 4697, logging a new service installation, should be analysed in case of suspected relay attack [17].

c) Tools for detection: There are tools that can be used for NTLM relay detection in various ways, like the LDAP Relay Scan [1] The Network Execution Tool [2] [16].

d) Session signing: Requiring session signing can mitigate some relay attacks, but only works for SMB and LDAP. The messages themselves, including the signing, cannot be tampered with due to Message Integrity Code (MIC).

e) Kerberos: Using Kerberos for the authentication can mitigate the relay attacks, but is not entirely effective, as Windows automatically uses NTLM in case of Kerberos not working [17].

VI. OTHER EXAMPLES OF RELAY ATTACKS

A. Unlocking doors

Haskins and Stevado successfully demonstrated an attack targeting the Seos credential system [18]. Using inexpensive hardware, they were able to unlock their door that was more than 1900 km away. The attack could possibly also work for other systems based on ISO 14443A. The researchers suggest that a simple distance pounding protocol would mitigate the attack.

B. Electric Vehicle Charging System

Conti et al. presented an electric vehicle charging station relay attack [19]. The stations utilize the Vehicle-To-Grid method based on ISO 15118. The attack allows the adversary to charge their car with energy paid by the victim and, in some cases, to even sell the energy from the victim's car. The researchers proposed a distance bounding protocol adapted to ISO 15118.

VII. GENERAL COUNTERMEASURES

A. Distance Bounding Protocols

One of the most promising countermeasures for relay attacks are the distance bounding protocols. These protocols introduce new ways to reliably determine the distance between entities. According to a survey by Avoine et al., the various implementations can be based on various properties and measures like the Received Signal Strength (inverse relationship between signal strength and distance), the Angle-of-Arrival (directions of signals), noise levels, physical properties of communication channels, ambient environments and Time-of-Flight (measured time of an exchange). These methods vary based on the exact types of attack they can reliably detect, the implementation practicality or the amount of security flaws. Implementation and deployment of an effective distance bounding protocol is not an easy task and the various methods have been in research since the 1990s [20].

According to Clulow et al., the following principles should be followed when building a secure distance bounding protocols, with emphasis on Time-of-Flight usage [21]:

1) The propagation speed of the used communication medium should be as close as possible to the speed of light in vacuum.
2) The communication format should transmit only a single bit at a time, allowing the recipient to immediately react.
3) The output energy, distinguishing the two possible bit values, should be timed as short as possible.

[1] https://github.com/zyn3rgy/LdapRelayScan

[2] https://github.com/Pennyw0rth/NetExec

4) The protocol should be able to handle higher bit error rates due to the previous limitations.

These principles ensure the reliability of the distance bounding protocols, but also introduce new possible challenges, like the impossibility of utilizing conventional error correction methods or the exclusion of usable communication mediums.

a) Secure, Accurate, and Practical Narrow-Band Ranging System: As an example of a distance bounding protocol implementation, the proposal from Abidin et al. from 2021 has been selected [22]. The researchers propose an approach based on the combination of Narrow-Band ranging and Time-of-Flight, creating a proposal that strives for both accuracy and security. Narrow band signals include technologies like Bluetooth, Bluetooth Low Energy (BLE), IEEE 802.15.4, with the research focusing on the widely used BLE.

The proposed protocol has three stages: authenticated key exchange, distance bounding and authentication and authorisation. In the process, it is assumed that the prover and the verifier know each others' public key. In the first phase, communicating entities establish a shared secret, using the SIGMA protocol based on a Diffie-Hellman key exchange. In the second phase, distance bounding is performed using Multi-Carrier Phase Difference (MCPD) method to accurately estimate the distance based on phase differences and the ToF method to stop the adversary from delaying the signal and influencing the phase shift. Finally, in the third stage, encrypted measurements are shared with the verifier, who compares the measured values with various threshold values and decides whether to grant access.

In the performed security analysis, it has been shown that the proposed protocol is resistant against generic attacks, like the impersonation attack and the relay attack, and also the physical-layer attacks, like the early-detect late-commit attack or the phase manipulation attack.

B. NFC Relay Detection Based on RF Fingerprinting

Countermeasures can also be implementing in the form of detection systems based on various parameters. In their research focused on ISO 14443-A, Wang, Zou and Zhang proposed a detection system based on deep learning [23], using features extracted from the physical-layer wireless communication of radio-frequency devices. Data of the usual and the relayed communication have been collected and used to train a deep convolutional neural network. Based on experiments, the method has been quite successful, with 99% of the cases being correctly classified.

VIII. Conclusion

The article summarized several affected areas, including the passive keyless entry and start vehicles, contactless payments and NTLM. Based on research, the relay attacks were successful even with luxury vehicles, allowing the attacker to unlock and start the car and to access the car computer ports, opening the door to more attacks. Countermeasures can be also implemented by users themselves, e.g. using a protective case or removing the battery.

While Visa and Mastercard have proposed relay attack protection methods, research shows that the protection can be bypassed. Additionally, when using Apple Pay in transit mode with a Visa card, the attacker can steal any amount of money even from a locked iPhone.

NTLM relay is a special kind of attack, where an attacker can gain access to the user's NTLM authentication and relay it to bypass multi-factor authentication, gain password hashes and escalate their privileges. This attack is frequently used by hackers to gain sensitive data, especially when used servers are not up-to-date.

A general countermeasure are distance bounding protocols, which allow to reliably determine the distance between two entities. There have been many researched protocols with various principles and different properties which are used for the computations. Proposing such a protocol is difficult, because protocols are prone to security flaws and different protocols are more effective for different attack executions.

References

[1] G. Hancke, K. Mayes, and K. Markantonakis, "Confidence in smart token proximity: Relay attacks revisited," *Computers & Security*, vol. 28, no. 7, pp. 615–627, 2009.

[2] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," Cryptology ePrint Archive, Paper 2011/618, 2011.

[3] M. Roland, J. Langer, and J. Scharinger, "Applying relay attacks to google wallet," in *2013 5th International Workshop on Near Field Communication (NFC)*, 2013, pp. 1–6.

[4] K. Jiang, "Canada has a car theft epidemic. here are simple ways to protect your vehicle from being stolen." [Online]. Available: https://www.toronto.com/news/crime/canada-has-a-car-theft-epidemic-here-are-simple-ways-to-protect-your-\vehicle-from/article_ebf2c10e-f7d6-5935-972d-1b2cc8a9c3d8.html

[5] A. Greenberg, "Just a pair of these $11 radio gadgets can steal a car." [Online]. Available: https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/

[6] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars." *IACR Cryptology ePrint Archive*, vol. 2010, p. 332, 01 2010.

[7] L. Wouters, E. Marin, T. Ashur, B. Gierlichs, and B. Preneel, "Fast, furious and insecure: Passive keyless entry and start systems in modern supercars," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 3, p. 66–85, May 2019.

[8] J. Allen, "Motion sensor fobs are only short term fix for keyless car thefts, say security experts." [Online]. Available: https://www.driving.co.uk/news/motion-sensor-fobs-short-term-fix-keyless-car-thefts-say-security-experts/

[9] D. Goodin, "Canada declares flipper zero public enemy no. 1 in car-theft crackdown." [Online]. Available: https://arstechnica.com/security/2024/02/canada-vows-to-ban-flipper-zero-device-in-crackdown-on-car-theft/

[10] S. Paniagua and H. Inc, "Enhancing automotive security: A random forest-based relay attack detection system," 11 2023.

[11] H. Jeong and J. So, "Channel correlation-based relay attack avoidance in vehicle keyless-entry systems," *Electronics Letters*, vol. 54, no. 6, pp. 395–397, 2018. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/el.2017.4360

[12] G. P. Hancke, "A practical relay attack on iso 14443 proximity cards," 2005. [Online]. Available: https://api.semanticscholar.org/CorpusID:1493166

[13] A.-I. Radu, T. Chothia, C. J. Newton, I. Boureanu, and L. Chen, "Practical emv relay protection," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1737–1756.

[14] "Russian apt28 hackers targeting high-value orgs with ntlm relay attacks." [Online]. Available: https://thehackernews.com/2024/02/russian-apt28-hackers-targeting-high.html

[15] Z. Zorz, "17,000+ microsoft exchange servers in germany are vulnerable to attack, bsi warns." [Online]. Available: https://www.helpnetsecurity.com/2024/03/26/vulnerable-microsoft-exchange-servers/

[16] "Ntlm relay." [Online]. Available: https://www.thehacker.recipes/a-d/movement/ntlm/relay

[17] E. Kuehn, "Ever run a relay? why smb relays should be on your mind." [Online]. Available: https://www.secureideas.com/blog/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html

[18] S. Haskins and T. Stevado, "Unlocking doors from half a continent away: A relay attack against hid seos," Cryptology ePrint Archive, Paper 2023/450, 2023, https://eprint.iacr.org/2023/450. [Online]. Available: https://eprint.iacr.org/2023/450

[19] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," in *Computer Security – ESORICS 2022*, V. Atluri, R. Di Pietro, C. D. Jensen, and W. Meng, Eds. Cham: Springer International Publishing, 2022, pp. 488–508.

[20] G. Avoine, J. Munilla, A. Peinado, K. Rasmussen, D. Singelée, A. Tchamkerten, R. Trujillo-Rasua, S. Vaudenay, M. Bingöl, I. Boureanu, S. Capkun, G. Hancke, S. Kardaş, C. Kim, C. Lauradoux, and B. Martin, "Security of distance-bounding: A survey," *ACM Computing Surveys*, vol. 51, pp. 1–33, 09 2018.

[21] J. Clulow, G. Hancke, M. Kuhn, and T. Moore, "Near and yet so far: Distance-bounding attacks in wireless networks," in *European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS)*, vol. 4357. Springer-Verlag, 2006, pp. 83–97.

[22] A. Abidin, M. E. Soussi, J. Romme, P. Boer, D. Singelée, and C. Bachmann, "Secure, accurate, and practical narrow-band ranging system," Cryptology ePrint Archive, Paper 2021/070, 2021, https://eprint.iacr.org/2021/070. [Online]. Available: https://eprint.iacr.org/2021/070

[23] Y. Wang, J. Zou, and K. Zhang, "Deep-learning-aided rf fingerprinting for nfc relay attack detection," *Electronics*, vol. 12, no. 3, 2023.