Chameleon: A Lightweight Method for Thwarting Relay Attacks in Near Field Communication

Yafei Ji[1,2,3], Luning Xia[1,2(✉)], Jingqiang Lin[1,2], Jian Zhou[1,2], Guozhu Zhang[1,2,3], and Shijie Jia[1,2,3]

[1] State Key Laboratory of Information Security, Institute of Information Engineering of Chinese Academy of Sciences, Beijing, China
{jiyafei,xialuning,lingjinqiang,zhoujian,zhangguozhu, jiashijie}@iie.ac.cn
[2] Data Assurance and Communication Security Research Center of Chinese Academy of Sciences, Beijing, China
[3] University of Chinese Academy Sciences, Beijing, China

Abstract. Near field communication (NFC) is applied in payment services, setup of high-bandwidth connection and information sharing. Therefore, NFC devices represent an increasing valuable target for adversaries. One of the major threats is relay attack, in which an adversary directly relays messages between a pair of communication peers referred to as initiator and target device. A successful relay attack allows an adversary to temporarily posses a 'virtual' initiator/target and thereby to gain associated benefits. In this paper, we propose a lightweight and automated method featuring role transitions and thus called Chameleon to thwart relay attacks. The principle of the method is: Chameleon exchanges the roles of the two devices after every NFC session in a random manner. The information of exchanged role is included in the messages of every session and encrypted by pre-shared key of the two legitimate devices. In this condition, the adversary cannot decrypt the message and configure themselves to appropriate role during the connection. Consequently, the relayed communication will be interrupted and a transaction is aborted due to uncompleted data packet. This method is implemented in real communication scenario and works well on thwarting relay attack. Our experiments indicate that it is an easy-to-implement and effective defense against relay attacks.

Keywords: Near field communication · Radio frequency identification · Relay attack · Implementation · Role transition · Lightweight · Tradeoff

Y. Ji—This work was partially supported by the National 973 Program of China under award No. 2013CB338001 and the Strategy Pilot Project of Chinese Academy of Sciences under award No. XDA06010702.

S. Qing et al. (Eds.): ICICS 2015, LNCS 9543, pp. 346–355, 2016.
DOI: 10.1007/978-3-319-29814-6_29

1 Introduction

Near field communication (NFC) [1] is a promising and increasingly prevalent short-range wireless technology. Due to its shorter-range of operation and other characteristics, NFC is more suitable than RFID systems in many applications such as access control, payment services, and information sharing. With the release of Android 4.4 in Oct. 2013, Google introduced a new platform, Google Wallet,for NFC-based transactions. In Sept. 2014, Apple also announced support for NFC-powered transactions as part of its Apple Pay program.

With the popularity of NFC application, NFC enabled devices represent an increasing valuable target for adversaries [5,6] and one of the major threats is the relay attack [7]. It is executed by sitting in the middle of two communication parties and simply "relaying" request and response effectively making one invisible to either party. During relay attack, the adversary can employ a proxy-reader and a proxy-token to relay the communication, in either wired or wireless manner, between authenticating reader and token over a distance much longer than intended, which intends to deceive the real reader into believing that real token is in close proximity (while it is not).

To the best of our knowledge, relay attack can hardly been defended by any practical countermeasures. Since the adversary does not need to parse or apprehend the relayed messages, it is well understood that application-layer countermeasures like cryptographic approaches are incompetent at defending against relay attacks. According to [7], relay resistant measures for NFC include enforcing timing constraints [8], distance bounding [9], and additional verification [10–14]. Nevertheless, due to various technical and marketing reasons, effectively counteracting relay attacks is still a very challenging task.

In this paper, we propose a lightweight and automated method featuring role transitions and thus called Chameleon to thwart relay attacks. Chameleon is lightweight as it doesn't involve heavy encryption algorithm like ECC; On the other hand, it is based on software that needn't interact with users and thus is automated. Two NFC devices during communication are configured as initiator and target alternatively, and thus our scheme is named after Chameleon, a type of lizard that can quickly change the color of its skin. The principle of the method is: Chameleon exchanges the roles of the two devices after every NFC session in a random manner. The adversary cannot decipher the messages containing the information of exchanged role and thereby cannot configure themselves to appropriate role during the connection with legitimate devices. Consequently, the relayed communication can be interrupted and a transaction can be aborted due to uncompleted data packet. We also implement Chameleon in a real communication scenario, and the results show that it can work well on defending relay attack.

The remainder of the paper consists of Sect. 2 which provide a brief background summary of NFC and relay attack. Section 3 presents Chameleon, our lightweight solution dedicated for NFC devices to deter relay attack. Evaluation and discussion is presented in Sect. 4. Section 5 discusses related work, and finally concluding remarks are in Sect. 6.

2 Background and Preliminaries

In this section we present a brief overview of NFC characteristics including standard, communication speed, and operation mode, and then introduce the mechanism of relay attack.

NFC Characteristics. NFC is a specification for contactless communication between two devices. It is based on existing Radio Frequency Identification (RFID) technology [4] by allowing two-way communication between endpoints.It is accredited with standard ISO/IEC 18092 [2]. According to this standard,NFC devices operate at 13.56 MHz and are required to be compatible with ISO/IEC 14443 and FeliCa. This standard specifies the interface and protocol for simple wireless communications between close-coupled devices that communicate with transfer rates of 106, 212, 424 kbps. In 2012, NFC also earned a further international accredited standard ISO/IEC 21481 [3].

NFC devices are defined to work in two roles: initiator and target. Initiator generate RF filed and start the NFCIP-1 communication; target responds to initiator command either using load modulation scheme or using modulation of self generate RF field. NFC devices can communicate in either active mode or passive mode. In active mode both initiator and target devices provide their own power supply and create a magnetic field to transfer data between each other. They do this in half duplex, deactivating their RF field until no other devices is transmitting. In passive mode, initiator is the only device that generates an RF signal; the target device answers by modulating the existing field for which the initiator device listens out, and then processes therefore transfers the data.

Relay Attack. Relay attacks exist already for RFID systems and have been perfect to work with regular NFC devices (e.g. phone) by just installing specific pieces of software. Figure 1 shows schematic diagram of relay attack.

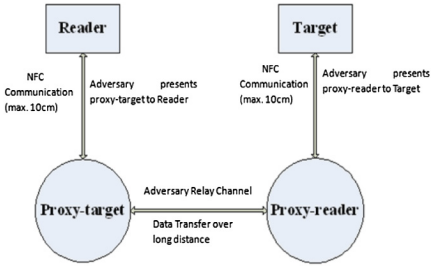

Fig. 1. Schematic diagram of NFC Relay attack setup

In order to execute a relay attack, an adversary needs two devices to act as proxies to relay communication, in either wired or wireless manner, between authenticating reader and target over a distance much longer than intended.

The two devices are connected via suitable communication channel such as Bluetooth to relay information over a greater distance. One proxy device interfaces with the NFC target device of a victim functioning as a proxy-reader. It forwards all messages over the high speed link to the second proxy device imitating a NFC target to interface with the actual NFC reader. The target assumes that it is communicating with the actual reader and responds accordingly. The response is then relayed back to the proxy-target, which will transmit the messages to the reader. The intention of the attacker is to ensure that the reader is unable to distinguish between the real target and the proxy. If he succeeds the reader will assume that the target is in close proximity and grant access to the attack.

Relay attack has serious security implication as it can bypass any application layer security protocol, even if such protocols were based on strong cryptographic principles. It doesn't matter what application layer protocol or security algorithms are used, and the attacker even requires no prior knowledge about the relayed data. If the overarching protocol contains security vulnerability the attacker could also modify the relayed data in real time which is often referred to as "active" relay.

3 Chameleon

According to the principle of NFC, we propose a lightweight and automated method featuring role transitions and thus called Chameleon to thwart relay attacks. In this section the detail of Chameleon is described in the following three parts: security goal and assumption, Chameleon protocol and Chameleon characteristics.

Security Goal and Assumption. The main security goal of Chameleon is to block the communication established by adversary while do not influence normal communication. To achieve this goal we should better disrupt the relayed communication thoroughly or force the adversary to miss at least one data packet. During the communication,two real NFC devices convert their role between initiator and target randomly. The two real devices should reach an agreement on the role transition that indicates which role each device will use for next session. The agreement is unpredictable by adversary while it is manipulated by the two real devices.For the purpose of confidentiality, consistency and integrity of data, the real devices are assumed to pre-share a secret key.

To execute the Chameleon method there are also some assumptions must be proposed. The feature of the Chameleon is role transition and unpredictable by adversary. Unpredictability can be obtained by random number generated by randomizer. Moreover, confidentiality, consistency and integrity of data are considered, the two communicating devices should have a pre-shared secret key and symmetry encryption algorithm such as AES can be applied.

Chameleon Protocol. According to the ISO/IEC 18092 the two NFC devices intending to communicate should first configure themselves as initiator or target respectively, and then the they can pair with each other. The standard also

indicates that only initiator and target device can communicate while two initiator or two target devices cannot because the two devices with identical role are impossible to pair successfully. In other words, each device needs to determine the role of the counterpart, otherwise, it cannot configure to appropriate role and therefore pairing will fail. The characteristic of this method is to configure the device before transmitting message. For example, device A is configured as initiator to transmit first data packet to B, and then the role of device A and B may be changed before next session. The role of the two devices may be configured in two possible ways: first, device A and B can continue transmit next data packet with original role; second, the two devices exchange role, which means if A is initiator at first and then it should be configured as target to transmit next packet. Device A and B choose one of the two way randomly, and thus proxy devices may unable to receive messages from real devices as they cannot configure to an appropriate role.

The two legitimate devices should reach an agreement of role transition in order to communicate successfully. We use additional four control bytes C1, C2, ID1 and ID2 to indicate the information of role transition. All of the messages including the agreement are encrypted by pre-shared key. The coding structure of control byte C1 is shown is Table 1. MI represents whether all of the data packets are already transmitted. If MI is set to ONE, it indicates there are still some data packets should be transmitted while ZERO means data packets are transmitted completely. E1 represents which role will be used for transmitting next packet. If E1 is set to ZERO it means to use current role while ONE means the two devices exchange their roles. If E1 is set to ONE, a new ID with ID1 and ID2 should be set for the new target devices so that new initiator can find new target device with it. Control byte C2 is equal with data length modulo packet size, which indicates the data length in last packet.

Table 1. Coding structure of control byte C1

Bit	Bit7-Bit2	Bit1	Bit0
Function	Reserved	E1	MI

Chameleon Characteristics. The main characteristic of the Chameleon is that a pair of NFC devices negotiate and exchange their role randomly in communication. The messages including role information are encrypted by pre-shared key, and therefore the adversary is unable to determine the role of each device. As a result, the proxy devices may not be configured to an appropriate role to pair with legitimate devices and thus pairing would fail. On the other hand, communication or transaction could be aborted once data packet missing is detected.

4 Evaluations and Discussion

In this section, efficiency of the Chameleon on communication and thwarting relay attack is evaluated, and further discussion as well as the experiment results is also presented.

4.1 Experiment

We develop and test a relay attack of our own in order to better understand the level of difficulty an attacker might face in doing the same, as well as to see the strengths and weaknesses of the attack. Then, the Chameleon is applied to thwart the attack.

Attack Setup. We use NFC development board C and D to act as proxy devices to relay communication between A and B. The main component of the development board is PN532 and its associated circuit. The PN532 is a highly integrated transmission module for contactless communication at 13.56 MHz including micro-controller functionality based on an 80C51 core. The transmission module utilizes a modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocol at 13.56 MHz Two blue modules are used to establish relay channel between C and D. Microcontrollers STM32F407 from STMicroelectronics are served as "relay centers" to control proxy devices and Bluetooth modules.

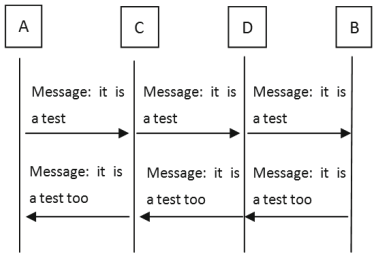

Fig. 2. Schematic diagram of the implemented relay attack

In this experiment device C worked as proxy-target is presented to legitimate device A while D worked as proxy-initiator is presented to legitimate device B. We manage to launch the relay attack between A and B. Figure 2 shows schematic diagram of the implemented relay attack. Adversary presents proxy device C to legitimate device A to trigger NFC communication. Proxy device C interacts with D via Bluetooth modules which act as relay channel. Proxy device D simply relays all messages received over the relay channel. Message "it is a test" is successfully relayed between two distant NFC-enabled devices.

Defense Result. From the above relay attack experiment, we can find that the proxy device can receive message from legitimate devices once it is configured to an appropriate role. In other words, adversary must know which legitimate device is initiator and which one is legitimate target, otherwise, they may not implement a successful relay attack. Figure 3 shows the result of using Chameleon to thwart relay attack.

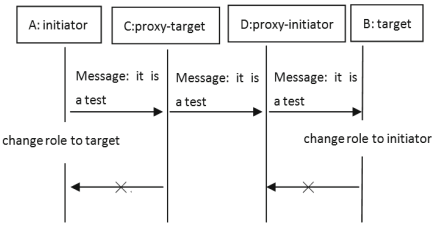

Fig. 3. Thwarting relay attack using Chameleon

When the Chameleon is not applied during the communication, the message "it is a test" can be relayed successfully from legitimate device A to B. However, the attack is thwarted once the Chameleon is executed. The proxy devices fail to pair with legitimate devices and thereby the communication is aborted. In order to measure the effect of this method on message interactions, we set up another experiment to quantify the time for transmitting 1 K bytes. Table 2 shows the required time for transmitting 1 K bytes.

Data packet size represents the data field length in data exchange command of PN532. Table 2 shows that transmission time is inversely proportional to data packet size. The larger data packet is, the shorter time is needed. It can also be found that the time needed to transmit 1 K bytes and the data packet size is generally in linear relationship. "Normal" shown in Table 2 means to transmit data packet continuously without any role transformation. It can also be found from Table 2 that "Chameleon" needs more time to transmit 1 K data due to continuously configuration before transmitting every data packet. However, with the increase of packet size, the time difference between "Normal" and "Chameleon" decrease gradually. This method, to some extent, can defense or reduce the possibility of successful relay attack.

Table 2. Time measurements of 1 K bytes transmitted in different packet size (Unit:second)

Packet size	16 bytes	32 bytes	48 bytes	96 bytes	128 bytes
Normal	13.971226	6.992128	4.816253	2.44235	1.393672
Chameleon	21.363692	10.472058	7.290481	4.15893	2.584200

4.2 Analysis

The legitimate devices act as initiator or target reaching an agreement on the role before communication. As all the messages including the agreement are encrypted by the pre-shared key of the two devices, adversary is unable to precisely determine the role of each legitimate device which result the connection fail. This countermeasure can effectively defense against the relay attack implemented by using off-the-shelf NFC enabled devices. It can be found from the experiment and Table 2 that the "Chameleon" require reasonable overhead. Compared with "Normal" transmission, "Chameleon" spends much more time to transmit 1 K bytes due to re-configuration. The successful rate of the attack is related with data packet number N and equal to $\left(\frac{1}{2}\right)^{N-1}$. In our future work, in order to reduce the time for configuration and therefore to improve communication efficiency, we can use the "Chameleon" method every few data packets instead of each packet.

As mentioned above, our investigation is focused on the relay attack implemented by off-the-shelf devices. However, the Chameleon is invalid to the relay attacks that executed by custom-built devices. For example, adversary can relay in both ways by using custom-built device to listen on both sides and just replay the messages to the right side. This is one drawback of the Chameleon , and we leave this challenge as our future work. In addition to the Chameleon, some assistant facilities can be added to enhance security. For example, monitor can be installed around a door. In this condition, the adversary will give up attacking if he fails to unlock a door in five seconds. Moreover, once adversary fails to relay entire data during communication for several times, the communication will be locked for a while or even be aborted which will trigger a warning signal sent to control center.

5 Related Works

In recent years, more and more attentions have been paid to NFC and many works have been published. Some researchers considered that NFC is more secure than other wireless technologies [1,6]. In Reference [6], NFC is considered the de facto standard for radio communication and the dominator of the contactless payment market. On the other hand, Reference [1] draw a conclusion that NFC exhibits higher security than Bluetooth and ZigBee. Nevertheless, this very lengthy survey on NFC, as well as References [4] and [5], hardly covers the relay attack.

Although NFC is believed to be more secure than RFID, both technologies are subject to relay attacks. In an overview on relay attack [7], the authors raise the concern that even though relay attacks pose a serious security threat, they are often not considered a major risk (like eavesdropping or skimming); examples include certain academic surveys [4,5]. Francis et al. demonstrate the first successful attack in [15] with unmodified NFC-enabled mobile phones running application written with publicly available APIs. Likewise, a software-based

relay attack to Google Wallet, a well-known mobile payment system, is presented in [16]. Furthermore, in [17] sophisticated relay attacks are demonstrated using smart phones and improved using custom-made proxy device.

Research efforts to make system relay-resistant are categorized into three types: time-out constraint [8], distance bounding [9], and the use of additional (i.e., external) verification procedures [10–12]. As to detecting relay attacks, there could be other approaches. For example, Ref [13] addresses relay attacks through ambient condition measurement and proposes an authentication protocol. Like Ref [10–12] the proposal is also appliance-based, as specific sensors are required. Another proposal considering environment measurement is in Ref [18]. In Ref [19], NFC's resiliency against relay attacks is evaluated via a formal verification technique for analyzing protocols and systems.

These schemes [8–13] are appliance-based, which may not comply with commodity devices generally available from the market. Moreover, as summarized in [7], countermeasures mentioned above may result in significant increased system cost (e.g., modificate both reader and token), complicate the process (e.g., require user interaction), and/or need strong computation ability (e.g., implement ECC). These observations motivate us to pursue a lightweight and automated solution. This solution needn't additional hardware so as to reduce cost and it also doesn't require a large amount of computation.

6 Conclusion

We propose a lightweight and automated method featuring role transitions and thus called Chameleon to thwart relay attacks. The principle of the method is: Chameleon exchanges the roles of the two devices after every NFC session in a random manner unpredictable by the adversary. The information for exchanged role is included in the messages of every session and encrypted by pre-shared key of the two legitimate devices. The adversary unable to decipher the message and therefore may not configure themselves to the right role during the connection with legitimate devices. As a consequence, the communication may be interrupted and a transaction may be aborted due to uncompleted data packet. This method is implemented in real communication scenario and can work well on thwarting relay attack. Our proposal exhibits an intrinsic tradeoff between security and efficiency, and experiments indicate that it is an easy-to-implement and effectual defense against relay attacks.

References

1. Coskun, V., Ozdenizci, B., Ok, K.: A survey on near field communication (NFC) technology. Wireless Pers. Commun. **71**(3), 2259–2294 (2013)
2. ISO, IEC 18092:2013, Near Field Communication Interface and Protocol (NFCIP-1), March 2013
3. ISO/IEC 21481:2012, Near Field Communication Interface and Protocol (NFCIP-2), June 2012

4. Roberts, C.M.: Radio frequency identification (RFID). Comput. Secur. **25**(1), 18–26 (2006)
5. Haselsteiner, E., Breitfuß, K.: Security in near field communication (NFC): strengths and weaknesses. In: proceedings of 2nd Workshop on RFID Security (RFIDSec 2006), p. 11, July 2006
6. Nelson, D., Qiao, M., Carpenter, A.: Security of the near field communication protocol: an overview. J. Comput. Sci. Coll. **29**(2), 94–104 (2013)
7. Hancke, G.P., Mayes, K.E., Markantonakis, K.: Confidence in smart token proximity: relay attacks revisited. Comput. Secur. **28**(7), 615–627 (2009)
8. Reid, J., Nieto, J.M.G., Tang, T., Senadji, B.: DetectingRelay attacks with timing-based protocols. In: Proceedings of 2nd ACM Symposium on Information, Computer and Communication Security (ASIACCS 2007), pp. 204–213, March 2007
9. Drimer, S., Murdoch, S.J.: Keep your enemies close: distance bounding against smartcard relay attacks. In: proceedings of 16th USENIXSecuritySymposium (USENIX Sec 2007), pp. 87–1C102, August 2007
10. Kang, S., Kim, J., Hong, M.: Button-based method for the prevention of nearfield communication relay attacks. Int. J. Commun. Syst. **28**(10), 1628–1639 (2015)
11. Malek, B., Miri, A.: Chaotic masking for securing RFID systems against relay attacks. Secur. Commun. Netw. **6**, 1496–1508 (2013)
12. Čagalj, M., Perković, T., Bugarić, M., Li, S.: Fortune cookies, smartphones: weakly unrelayable channels to counter relay attacks. Pervasive Mobile Comput. **20**, 64–81 (2015)
13. Urien, P., Piamuthu, S.: Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. Decis. Support Syst. **59**, 28–36 (2014)
14. Stajano, F., Wong, F.-L., Christianson, B.: Multichannel protocols to prevent relay attacks. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 4–19. Springer, Heidelberg (2010)
15. Francis, L., Hancke, G., Mayesc, K.: A practical generic relay attack on contactless transactions by using NFC mobile phones. Int. J. RFID Secur. Crypt. (IJRFIDSC) **2**(1–4), 92–106 (2013)
16. Roland, M., Langer, J., Scharinger, J.: Applying relay attacks to Google Wallet. In: Proceedings of 5th International Workshop on Near Field Communication (NFC 2013), p. 6, February 2013
17. Korak, T., Hutter, M.: On the power of active relay attacks using custom-made proxies. In: Proceedings of 8th Annual IEEE International Conference on RFID (IEEE RFID 2014), pp. 126–133, April 2014
18. Kim, G.-H., Lee, K.-H., Kim, S.-S., Kim, J.-M.: Vehicle relay attack avoidance methods using RF signal strength. Commun. Netw. **5**, 573–577 (2013)
19. Alexiou, N., Basagiannis, S., Petridou, S.: Security analysis of NFC relay attacks using probabilistic model checking. In: proceedings of 10th International Wireless Communications and Mobile Computing Conference (IWCMC 2014), pp. 524–529, August 2014