Exploiting Vulnerability of NFC-Based Mobile Systems

Jesus Toxtle, Igor Lyebyedyev, and Kiho Lim
Department of Computer Science, William Paterson University

Introduction

The objective of this project is to investigate the security issues of NFC-based Mobile Payment systems and NFC-enabled "contactless" credit and debit cards. As more and more retail businesses begin to offer cashless transactions for their customers, the security of the emerging contactless payment systems and contactless payment cards is being put under further scrutiny. There have been studies on exploits and operating systems pertaining to the vulnerability of this technology, and attempts have been made to patch these flaws and remove the user's ability to acquire the unsecure software from the open web. In our research, we investigated the ability of a potential perpetrator to steal a victim's credit card information, and then conduct unauthorized transactions, all without the victim's knowledge.

Capturing Payment Information

We designed an experiment in which a contactless credit card's details would be skimmed and transmitted to a payment terminal over network. We used a standard contactless RFID credit card, a contactless NFC POS terminal, and two rooted NFC-enabled Android phones. The first phone acted as the skimming device, reading the credit card information when near the victim's wallet and transmitting it over WiFi. The second phone acted as a receiver at the other end of the network, storing the skimmed information to be used later. Both devices were running an app called NFCProxy, which facilitated the skimming and transmission of credit card details. [1]

Relay and Replay Attack toward Payment System

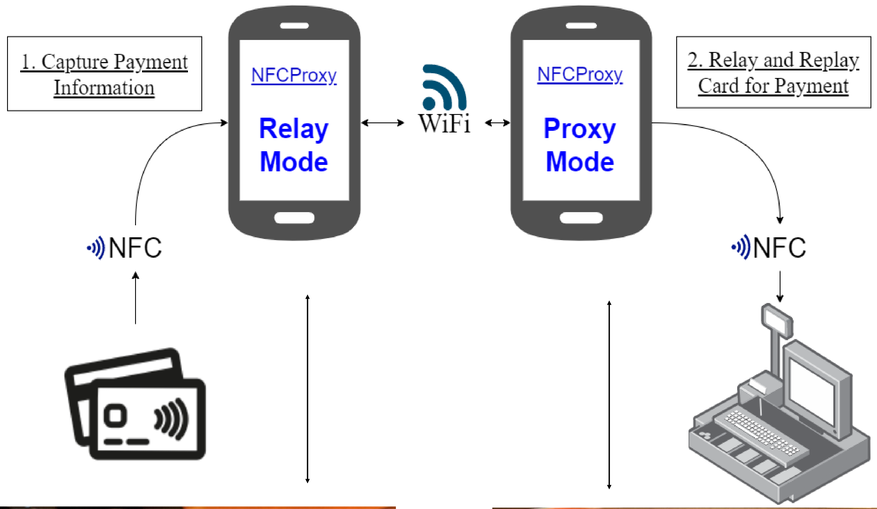
Using port forwarding for both relay mode and proxy mode, we were able to send credit card information over the same network. [1] Then with the second phone being in proxy mode, payment was cleared at a POS credit card reader. [1] We knew that the payment was cleared when the credit card information appeared on the screen and was verified via the Status tab. The attack was successful and can be done in a matter of seconds without the victim ever knowing.

Procedure

- Two devices are paired using a shared IP address and a WiFi network [2]
- Card is skimmed using the NFC receiver on the first device and read by NFCProxy [2]
- Data is transmitted over WiFi to the second device
- Second device transmits card data using NFC to a payment terminal and makes a purchase

- The pictures shown inside the testing environment were taken from the two Android phones. The figure a shows the first phone in relay mode. After putting the phone on top of the credit card, the status tab states that the phone finish reading the tag. The figure b shows the second phone in proxy mode. After making sure beforehand, that they had the same IP address and set to the same port, the phone is then scanned at a POS terminal. The card then successfully displayed this upon scanning which is the credit card information.

Testing Environment



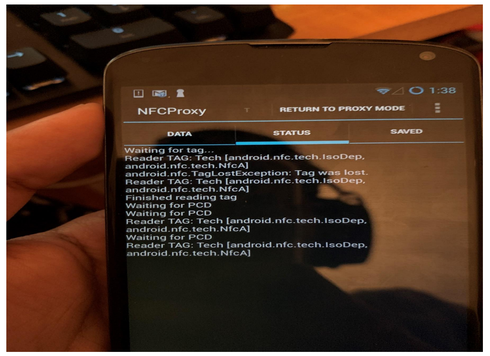


Figure A. First phone

Figure B. Second phone

Conclusion

In our testing environment, the first phone was successfully able to capture the credit card information with an app called NFC Proxy, and then transmit it to the second phone. We then scanned the second phone in Proxy Mode and tap it on a contactless credit card reader and payment was cleared.

Our findings indicate that individuals' contactless credit cards can be skimmed easily with such setup and the information captured can be used for unauthorized transactions. Credit cards can still be scanned even in leather wallets. Some possible consumer solutions to this issue is to secure their card inside an RFID-shielded wallet to block a hacker from skimming the card as a countermeasure. Another way is for consumers to constantly update their phones with NFC patches. Lastly, consumers should turn off NFC if it's not being used.

Reference

[1] Lee, E. (2012) "NFC Hacking the Easy Way",
[2] Bocek, T., Killer, C., Tsiaras, C., & Stiller, B. (2016). An NFC Relay Attack with Off-the-shelf Hardware and Software. *Management and Security in the Age of Hyperconnectivity Lecture Notes in Computer Science*, 71–83. doi: 10.1007/978-3-319-39814