Security of NFC payments

Olga Korobova
Department of Computer Science
University of Massachusetts Amherst

Abstract

Our research objective was to examine the security features implemented by the bank cards with integrated circuits.
Contribution: During DREU program Erin McBride and I studied wireless transaction between a card and Android phone that was enabled as a terminal, a protocol of communication, and how it's design could lead to personal data leakage. We examined the information that could be retrieved from the card, and helped to design elements of the survey that would help determine the extend to which individuals expose their personal information through contactless cards they carry in their wallets. We also created software to allow Android phones forward traffic to each other through IP tunnel. Combined with card emulation mode, requests and replies could be forwarded between the card and the reader, making it feasible to enter in the middle of transaction and pretend to be the owner of certain credentials.

I. Introduction

The growth of Near Field Communication (NFC) equipped smartphones suggests that contactless mobile payment systems will be widely used in the near future. The phone is about to replace a plastic credit card and charge users by being waved near the reader. For example, Google's ambition to replace a wallet full of plastic cards led to the Google Wallet application, that would virtually fit all the cards in the NFC-enabled Android. Sensitivity of banking information and the large number of potential NFC-enabled phone users encouraged us to study the security of NFC contactless communication using Android phone.

Build-in NFC chip allows the phone to be not only a banking card, but a reader as well. It is interesting to know whether contactless credit cards are indeed secured against malicious actions. Is it possible to lift critical information of the card by just standing near the wallet?

II. Near Field Communication enabled Smart Phones

Near field communication, or NFC, is the wireless technology that traces its origin to RFID, but typically requires a distance of a few centimeters. NFC involves an initiator that generates RF field and a target that gets powered by that field. Passive tags, or targets, can take very simple forms and be cheap, which makes NFC technology very appealing.

The communication range of NFC is limited to a few centimeters, but it does not imply any security. NFC devices usually support ISO/IEC 14443 protocols, which provide no resistance to data eavesdropping or data modification.

Many smart phones now come with built-in NFC chips that enable the device to be a reader and a contactless card. NFC was approved as an ISO/IEC standard and supports dominant ISO/IEC 14443 A&B and JIS-X 6319-4 contactless card technologies [1]. Provided the hardware, software applications can enable the phone to communicate with smart cards and read its stored data.

Nexus S with Android 2.3.3 firmware includes access to Near Field Communication functionality. Every such phone is capable of discovering a tag and identifying the technology the tag supports. By bringing the smart card close to the Android phone, we could read a list of supported standards, and therefore, identify how to communicate with the card; to talk to the bank cards we had to use Europay, MasterCard and VISA (EMV) protocol.

III. Europay, MasterCard and VISA Standard for Card Transactions

EMV (Europay, MasterCard and VISA) is a standard that defines physical and application levels of transactions between integrated circuit cards ("smart cards") and terminals. Contact cards' standards are based on ISO/IEC 7816, and contactless cards transactions follow ISO/IEC 14443 standard. The protocol defines the command/response flow and data exchange that proceeds in application protocol data units (APDUs). Thus, the card receives Command APDU, computes the answer and sends Response APDU to the terminal [2].

EMV provides different security measures, but not all of them are required to implement; many are left for banks consideration. Researchers from Cambridge University in their paper "Chip and Pin is Broken" described how flawed EMV implementation resulted in successful man-in-the-middle attack [3].

Implementation's details depend on EMV features, card issuing banks, and terminal deployers. For example, PayPass, EMV compatible payment feature that lets you pay by tapping the card, does not require cardholders name to be on the card, and depending on the terminal facilities, skips some protocol steps to simplify the transaction [4].

IV. Card Relay

We created application that loosens the distance limitation, which is one of security assumptions of NFC technology, by forwarding traffic between an NFC device and the Internet, making devices communicate through the created IP tunnel. If NFC phone had card emulation mode enabled, a relay attack between a victim's card and a terminal would be possible with only two stock commercial NFC devices.

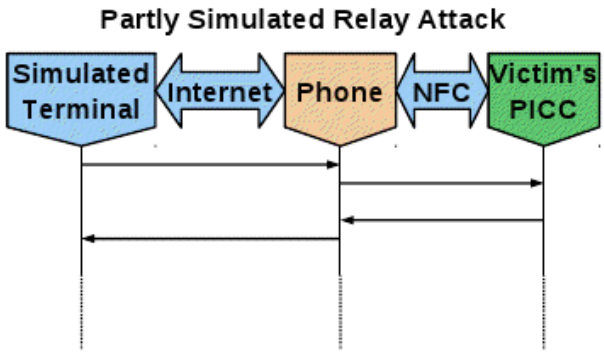

Figure 1. Our partial Card Relay implementation

If Phone A were in the card emulation mode, it would be able to present victim's private information to the terminal as it's own, because neither NFC, nor EMV protocol have protective measures.

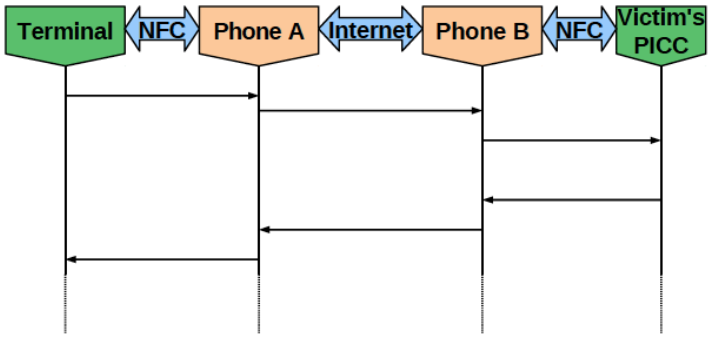

Figure 2. Full implementation

V. Card Emulation

NFC has three different communication modes: Reader/Writer mode, Peer-to-Peer mode, and Card Emulation mode. Enabling the phone to emulate a card is not trivial. The emulation is handled by the special hardware component called Secure Element (SE), which is activated under special privileges. Due to the sensitivity of payments transactions, by default the phone/tag is not available to external readers (the phone can recognize its own tag however). It is possible to tweak the Android source, remove required privileges, and thus to activate SE. However, both Erin and I could not recompile the code and successfully flash the system with the new image file.

Card emulation mode could be activated through UICC (SIM card) that supports the Single Wire Protocol, an interface for connection between the SIM card and NFC chip in a smart phone. This approach is technically very challenging, because SWP-enabled SIM card, and SWP-enabled NFC modem have to use the same standards to communicate. As of now, there is no off-the-shelve solution to easily enable card emulation through a SIM card and SWP protocol.

It could be possible to emulate a card with external hardware, but due to the time constraints we decided to adjust our plan and use a card + terminal node, where the phone sends out assumed (from the specifications) commands from the terminal (Figure 1).

VI. Conclusion

Payment systems are difficult to design and, because of the large number of its components and participants, their implementation is difficult to control. While some vulnerabilities relate to specific implementations of the system, practical man-in-the-middle attacks are possible because ISO/IEC 14443, and EMV therefore, provide no resistance to data eavesdropping or data modification.

Because Android NFC phone supports ISO/IEC 14443 protocols, its transactions are vulnerable to relay attacks. During DREU internship Erin McBride and I created Card Relay application that forwarded supposed reader's requests to the victim and relayed the answers back with no delay. If one of the devices is in the Card Emulation Mode, it can pretend to be the holder of the victim's smart card. Given the popularity of smart phones, this could be a very practical attack with only two off-shelf-devices.

References

[1] NFC and Contactless Technologies,
[2] EMV – Integrated Circuit Card Specifications for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.2 ed., EMVCo, LLC, June 2008.
[3] Steven J. Murdoch, Saar Drimer and Ross Anderson, *Chip and PIN is Broken*, IEEE Symposium on Security and Privacy, 2010.
[4] *PayPass POS Host/Payment Software Implementation Guide*.