Security and Privacy in Wireless Payment Systems

Erin McBride, University of Oregon. Olga Korobova, University of Massachusetts Amherst.
Faculty Advisor: Kevin Fu. Graduate Mentor: Andrés Molina-Markham.

Abstract

The growth of Near Field Communication (NFC) equipped smart phones suggests that contactless mobile payment systems will be widely used in the near future. Such phones would replace conventional debit or credit cards, and can even function as point of sale (POS) terminals.

NFC is a wireless technology built around the concept of inductive coupling between a proximity coupling device (PCD), such as a phone, and a proximity integrated circuit card (PICC). Range is typically 4cm. Security for bank cards is handled by the Europay, Mastercard and Visa (EMV) protocol.

This research examines the security features implemented by bank PICCs, how much private information can be retrieved from them, and how those properties might be exploited.

Research Objectives

Our objective was to examine the security features implemented by bank PICCs. We worked to:

- Determine which security features are implemented by bank PICCs.
- Help design elements of a survey with the purpose of collecting information about bank PICCs in use.
- Explore ways in which an attacker might compromise a wireless transaction or PICC.

NFC-capable Android Nexus S

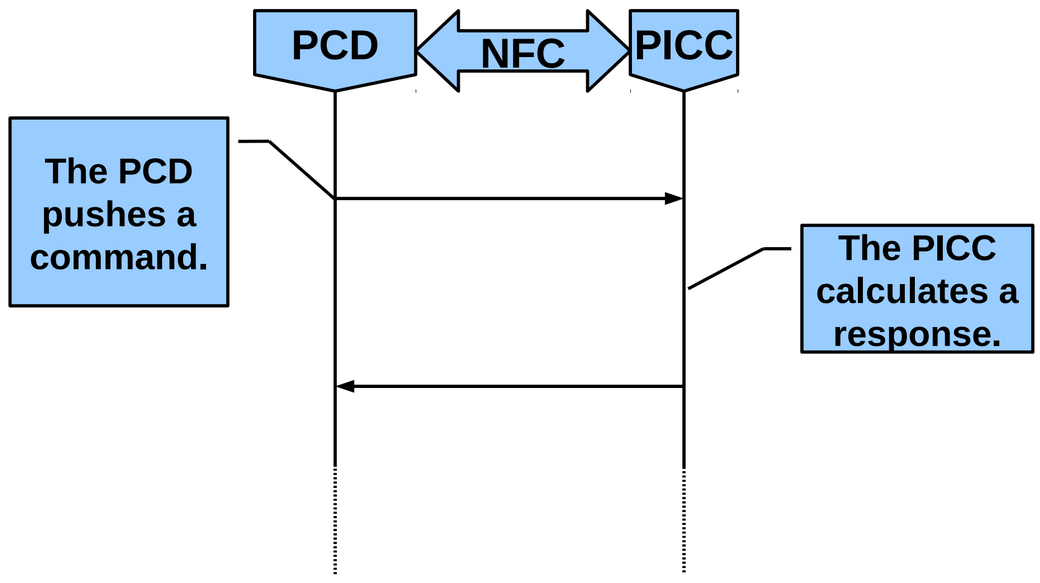
PN544 NFC Modem Chip

Progress and Results

We implemented the EMV protocol used by bank smart cards and POS terminals on the Android platform. By making the phone emulate a terminal, we can retrieve all static, non-secret information on a credit or debit PICC such as the cardholder's name and the expiration date.

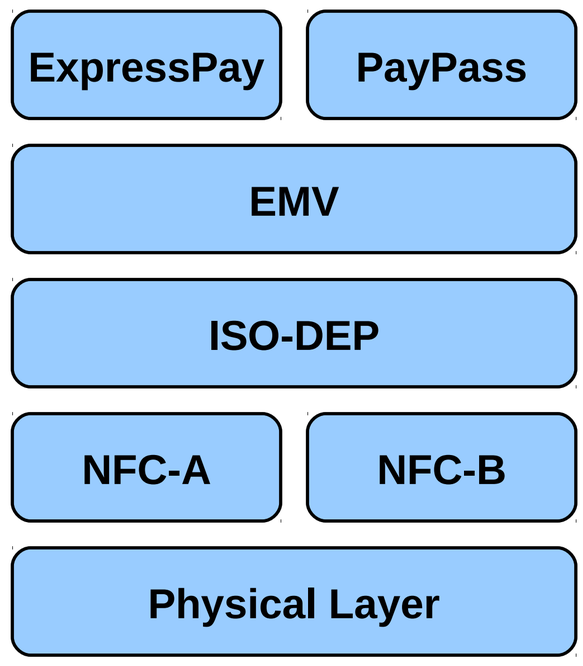
We also created software to allow an Android phone to forward traffic between an NFC device and the Internet, creating an IP tunnel. Combined with card emulation, it would be possible to perform a relay attack between a victim's PICC and a POS terminal that could be very far away.

Typical PICC-PICD System

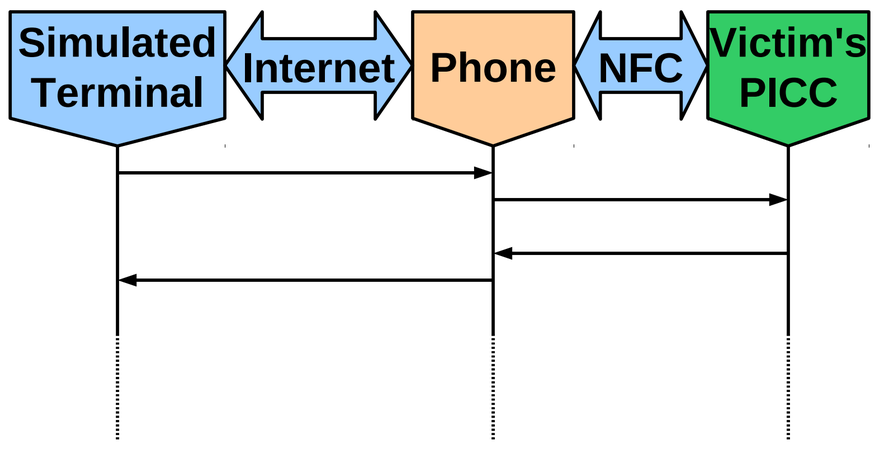


Phone and POS Terminal

Mobile Payment System



Partly Simulated Relay Attack



Completed Relay Attack

Future Work

- Enable card emulation on the Nexus S.
- Complete the relay system and study its efficacy.
- Design a kiosk for the information-gathering survey.
- Analyze the information from the survey with a focus on how much personal information cards readily gave up.

This work is supported by the Research Experience for Undergraduates Program of the National Science Foundation under NSF award number CNS-1062749. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the National Science Foundation.