NFC Hacking: The Easy Way

Eddie Lee
eddie(at)blackwinghq.com
About Me

★ Security Researcher for Blackwing Intelligence (formerly Praetorian Global)
   ★ New site live: blackwinghq.com

★ We’re always looking for interesting security projects

★ Member of Digital Revelation
   ★ 2-time CTF Champs – Defcon 9 & 10

★ Not an NFC or RFID expert!
Radio Frequency Identification - RFID
- Broad range of frequencies: low kHz to super high GHz

Near Field Communication - NFC
- 13.56 MHz
  - Payment cards
  - Library systems
  - e-Passports
  - Smart cards
- Standard range: ~3 - 10 cm
- Lots of new Android phones have NFC

RFID Tag
- Transceiver
- Antenna
- Chip (processor) or memory
RFID (tag) in credit cards
- Visa – PayWave
- MasterCard – PayPass
- American Express – ExpressPay
- Discover – Zip

Proximity Coupling Devices (PCD) / Point of Sale (POS) terminal / Card Reader

EMV (Europay, Mastercard, and VISA) standard for communication between chipped credit cards and POS terminals
- Four “books” long
- Based on ISO 14443 and ISO 7816
- Communicate with Application Protocol Data Units (APDUs)
Why create NFCProxy?

★ I’m lazy
★ Don’t like to read specs
★ Didn’t want to learn protocol (from reading specs)
   ★ Future releases should work with other standards (diff protocols)
★ Protocol Analysis
★ Make it easier for other people to get involved
★ Contribute to reasons why this standard should be fixed
Previous work

★ Adam Laurie (Major Malfunction)
  ★ RFIDIOt
  ★ http://rfidiot.org

★ Pablos Holman
  ★ Skimming RFID credit cards with eBay reader
  ★ http://www.youtube.com/watch?v=vmajlKJlT3U

★ 3ric Johanson
  ★ Pwnpass
  ★ http://www.rfidunplugged.com/pwnpass/

★ Kristin Paget
  ★ Cloning RFID credit cards to mag strip
  ★ http://www.shmoocon.org/2012/presentations/Paget_shmoocon2012-credit-cards.pdf

★ Tag reading apps
Typical Hardware

★ Contactless Credit card reader (e.g. VivoPay, Verifone)
  ★ ~$150 (retail)
  ★ ~$10 - $30 (ebay)

★ Card reader
  ★ OmniKey (~$50-90 ebay), ACG, etc.
  ★ Proxmark ($230-$400)

★ Mag stripe encoder ($200-$300)
Tool Overview

What is NFCProxy?
★ An open source Android app
★ A tool that makes it easier to start messing with NFC/RFID
★ Protocol analyzer

Hardware required
★ Two NFC capable Android phones for full feature set
  ★ Nexus S (~$70 - $90 ebay)
  ★ LG Optimus Elite (~$130 new. Contract free)
    ★ No custom ROMs yet*
  ★ Galaxy Nexus, Galaxy S3, etc. (http://www.nfcworld.com/nfc-phones-list/)

Software required
★ One phone
  ★ Android 2.3+ (Gingerbread)
  ★ Tested 2.3.7 and ICS
★ At least one phone needs:
  ★ CyanogenMod 9 nightly build from: Jan 20 – Mar 22 2012*
History for android_frameworks_base / core / java / android / nfc / tech / IsoPcdA.java

Feb 25, 2012
Revert back to the public api/current.txt and properly @hide the new ... 7839cbe614
koush authored 4 months ago

Jan 20, 2012
Added NFC Reader support for two new tag types: ISO PCD type A and IS... c80c15bed5
doug yeager authored 6 months ago
android_packages_apps_Nfc

Commit History

Mar 28, 2012
Merge branch 'ics-mr1-release' of https://android.googlesource.com/pl... 26ee6ed3f2
cyanogen authored 4 months ago

Mar 22, 2012
enable gwallet SE emulation 75ad85b69
doug yeager authored 4 months ago
★ Cyanogen Card Emulation

★ Git commits that add ISO PCD reader support

★ android_frameworks_base (Java API)
  ★ [https://github.com/CyanogenMod/android_frameworks_base/commit/c80c15bed5b5edfbb61eb543e31f0b90eddcad6](https://github.com/CyanogenMod/android_frameworks_base/commit/c80c15bed5b5edfbb61eb543e31f0b90eddcad6)

★ android_external_libnfc-nxp (native library)
  ★ [https://github.com/CyanogenMod/android_external_libnfc-nxp/commit/34f13082c2e78d1770e98b4ed61f446beeb03d88](https://github.com/CyanogenMod/android_external_libnfc-nxp/commit/34f13082c2e78d1770e98b4ed61f446beeb03d88)

★ android_packages_apps_Nfc (Nfc.apk – NFC Service)
  ★ [https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/d41edfd794d4dofedd91d561114308f0d5f83878](https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/d41edfd794d4dofedd91d561114308f0d5f83878)
Cyanogen Card Emulation

- NFC Reader code disabled because it interferes with Google Wallet
  - [https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/75ad85b06935cfe2cc556ea1fe5cc9b54467695](https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/75ad85b06935cfe2cc556ea1fe5cc9b54467695)
  - Revert this commit to get reader support back

- Nexus S nightly build (3/22/2012)
  - [http://goo.im/cm/crespo4g/nightly/update-cm-9-20120322-NIGHTLY-crespo4g-signed.zip](http://goo.im/cm/crespo4g/nightly/update-cm-9-20120322-NIGHTLY-crespo4g-signed.zip)
NFC Hardware Architecture

- **Host**
- **Secure Element**
- **NFC Chip**
- **Reader/PCD**

Connections:
- Host to Secure Element
- Secure Element to NFC Chip
- Reader/PCD to Antenna
- Antenna to Antenna
Standard Transaction

APDU

RFID

APDU
Tool Features

★ Proxy transactions
★ Save transactions
★ Export transactions
★ PCD replay
★ Tag replay (on Cyanogen side)

★ Don’t need to know the right APDUs to query RFID tags
  ★ Replaying is easy!
  ★ Use the tool to learn about the protocol (APDUs)
How It Works // Proxy Mode

- Protocol Analysis
- Immediate Skim and Use

NFC

WiFi (IP)

NFC

APDU

APDU
How It Works // Terminology

NFC

WiFi

Proxy Mode (Cyanogen)

NFC

Relay Mode
How It Works // Startup Modes

★ Relay Mode
★ Place Relay on card/tag
★ Opens port and waits for connection from proxy

★ Proxy Mode
★ Swipe across reader
★ Forwards APDUs from reader to card
★ Transactions displayed on screen
★ Long clicking allows you to Save, Export, Replay or Delete

★ Encrypted Communication
★ Requires password (both sides)
★ Slower transactions
★ Can disable
★ Faster
★ No Auth
Proxy not required for replay

Replay PCD (Skimming mode*)
★ Put phone near credit card
★ Different types of cards -> Different Requests
★ Nothing special going on here

Replay Tag (Spending mode)
★ Swipe phone across reader
★ Requires CyanogenMod tweaks
★ Virtual wallet
★ Pitfalls
★ Don’t’ replay the same saved transaction twice at a real POS terminal
★ Replay in the right order
★ Haven’t test Discover or Amex at live POS
A word about android NFC antennas
- Galaxy Nexus: CRAP!
- Nexus S: Good
- Optimus Elite: Good

NFC communication is often incomplete
- Need to reengage/re-swipe the phone with a card/reader
- Check the “Status” tab in NFCProxy
<table>
<thead>
<tr>
<th>DATA</th>
<th>STATUS</th>
<th>SAVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAG: 0x04 0x43 0x4d 0x32 0x0d 0x23 0x80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x00 0xa4 0x04 0x00 0x0e 0x32 0x50 0x41 0x70 0x32 0x04 0x70 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x6f 0x2d 0x84 0x0e 0x32 0x50 0x41 0x59 0x70 0x32 0x04 0x70 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x6f 0x1e 0x84 0x07 0xa0 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x80 0x06 0x00 0x80 0x08 0x01 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x00 0xb2 0x01 0x0c 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x70 0x45 0x57 0x13 0x00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time: 1402</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name: CARDHOLDER/VALUED
Card Number: [REDACTED]
Expiration Date: [REDACTED]
Service Code: 0101
iCVV: 14044 57 (0x00 0x44 0x14 0x57)
- EMV Book 3

- See RFIDIoT (ChAP.py) and pwnpass for APDUs used for skimming

- More info on service code and iCVV
  - ISO/IEC 7813:2006
  - http://blog.opensecurityresearch.com/2012/02/deconstructing-credit-cards-data.html
Demo!

Let’s see it in action!
Future Work

☆ What’s next?
☆ Generic framework that works with multiple technologies
  ☆ Requires better reader detection
☆ Pluggable modules
  ☆ MITM
  ☆ Protocol Fuzzing
Now available for download and contribution!

http://sourceforge.net/projects/nfcproxy/
Questions?

Contact: eddie{at}blackwinghq.com
How It Works

★ High level overview
   ★ Proxy
      ★ One end on card, one end on PCD
      ★ One end is a standard nfc enabled android phone
      ★ One end needs to be able to detect a reader
         ★ Go into card emulation
   ★ Communicates over wifi
   ★ After you capture the transactions you only need one phone

★ And why it works this way
   ★ Proxy is used so that the protocol(?) can be analyzed
   ★ Quick way to learn APDUs without needing to read documentation
      ★ Just replay
Walkthrough

★ Pick Mode
★ Relay Mode
  ★ Opens port and waits for proxy
  ★ Settings
  ★ Place Relay on card/tag
★ Proxy Mode
  ★ Note connection finickiness
    ★ Gnex aweful anntenna
    ★ Optimus Elite/Nexus S good
  ★ Swipe across reader
  ★ Transaction is automatically proxied
  ★ Slight lag
  ★ Data on screen is temporary. Must manually save
  ★ Describe data
  ★ Long Clicking allows you to save, export, replay, delete
  ★ Watch status tab for errors
  ★ Save tab contains built-in PCD and saved transactions
I. Introduction
   a. Brief primer on NFC/RFID
   b. Motivation
      i. Why create this tool?
II. Other/Previous work
   a. Scanning and reading RFID credit card from POS
      i. Pablos Holman
      ii. 3ric - Pwnpass
   b. Converting RFID to swipe-able card
      i. K. Paget
   c. Tag reading apps
III. How it works
   a. High level overview
   b. Standard hardware
      i. Custom Rom features
IV. Tool features
   a. Proxy mode
      i. Capture PCD requests and Tag responses
      ii. Don’t really need to understand protocol for replay
   b. Replay Tags
   c. Replay PCDs
V. Walkthrough (via slides)
   a. Show proxy transaction of CC and POS terminal
      i. Show physical setup
      ii. Show data output
   b. Show replay of credit card
   c. Show replay of PCD/POS
VI. Future work/Hopes
   a. Make tool into a generic framework that supports multiple