NFC Hacking: The Easy Way
About Me

★ Security Researcher for Blackwing Intelligence (formerly Praetorian Global)

★ We’re always looking for cool 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

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 / 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)
- Make it easier to analyze protocols
- Make it easier for other people to get involved

- Contribute to reasons why this standard should be fixed
★★ Adam Laurie (Major Malfunction)
★ RFIDIOt
★ [http://rfidiot.org](http://rfidiot.org)

★★ Pablos Holman
★ Skimming RFID credit cards with ebay reader
★ [http://www.youtube.com/watch?v=vmajlKjLT3U](http://www.youtube.com/watch?v=vmajlKjLT3U)

★★ 3ric Johanson
★ Pwnpass

★★ Kristen Paget
★ Cloning RFID credit cards to mag strip

★★ 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)
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 (~$60 - $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/](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:
  - Cyanogen 9 nightly build from: Jan 20 - Feb 24 2012
  - Or Custom build of Cyanogen
History for androidFrameworks_base/core/java/android/nfc/tech/IsaPcdA.java

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

Jan 20, 2012
Added NFC Reader support for two new tag types: ISO PCD type A and ISA... Doug Yeager authored 6 months ago
- android_frameworks_base (Java API)
  - https://github.com/CyanogenMod/android_frameworks_base/commit/c80c15bed5b5edff61eb543e31f0b90edcdad3

- android_external_libnfc-nxp (native library)
  - 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/d41edfd794d4d0f6dd91d561114308f0d5f83878

- NFC Reader code disabled because it interferes with Google Wallet
  - https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/75ad85b06935cfe2cc556ea1fe54cb9b54467695
Tool Features

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

- Don’t need to know the correct APDUs for a real transactions
  - Use the tool to learn about the protocol (APDUs)
Standard Transaction

APDU

RFID

APDU
How It Works // Proxy Mode

- NFC
- WiFi
- APDU

NFC → WiFi → APDU → NFC
How It Works // Modes

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

⭐ 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
Replay Reader (Skimming mode*)
- Put phone near credit card
- Nothing special going on here
- Know the right APDUs

Replay Card (Spending mode)
- Swipe phone across reader
- Phone needs to be able to detect reader – Card Emulation mode
- Requires CyanogenMod tweaks
- Virtual wallet
Antennas

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
★ EMV Book 3  

★ See RFIDIOt (ChAP.py) and pwnpass for APDUs used for skimming

★ Proxy not needed for skimming and spending  
★★ Just for protocol analysis
### 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 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x6f 0x2d 0x84 0x0e 0x32 0x50 0x41 0x59 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x00 0xa4 0x04 0x00 0x07 0xa0 0x00 0x00 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x6f 0x1e 0x84 0x07 0xa0 0x00 0x00 0x00 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x80 0xa8 0x00 0x00 0x04 0x83 0x02 0x00 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x80 0x06 0x00 0x80 0x08 0x01 0x01 0x00 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCD: 0x00 0xb2 0x01 0x0c 0x00 0x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAG: 0x70 0x45 0x57 0x13 0x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name: CARDHOLDER/VALUED
Card Number: ****
Expiration Date: ****
Service Code: 0101
iCVV: 14044 57 (0x00 0x44 0x14 0x57)
Let’s see it in action!
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