BLACKWINGINTELLIGENCE

DEFCON 20

NFC Hacking: The Easy Way

Eddie Lee
eddie{at}blackwinghq.com

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!

Introduction // RFID Primer

- 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

Introduction // RFID Primer

- 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)

Introduction // Motivation

- 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

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/
- Kristen 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 (~$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/)

- 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

BLACKWINGINTELLIGENCE

github

Signup and Pricing | Explore GitHub | Features | Blog | Sign in

PUBLIC **CyanogenMod / android_frameworks_base**

forked from KellyMahan/android_frameworks_base

Watch 717 | Fork 645

Code | Network | Pull Requests 24 | Graphs

branch: **ics** | Files | Commits | Branches 12 | Tags 5 | Downloads

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 … …

koush authored 4 months ago

7839cba014

Browse code

Jan 20, 2012

Added NFC Reader support for two new tag types: ISO PCD type A and IS… …

doug yeager authored 6 months ago

c80c15bed5

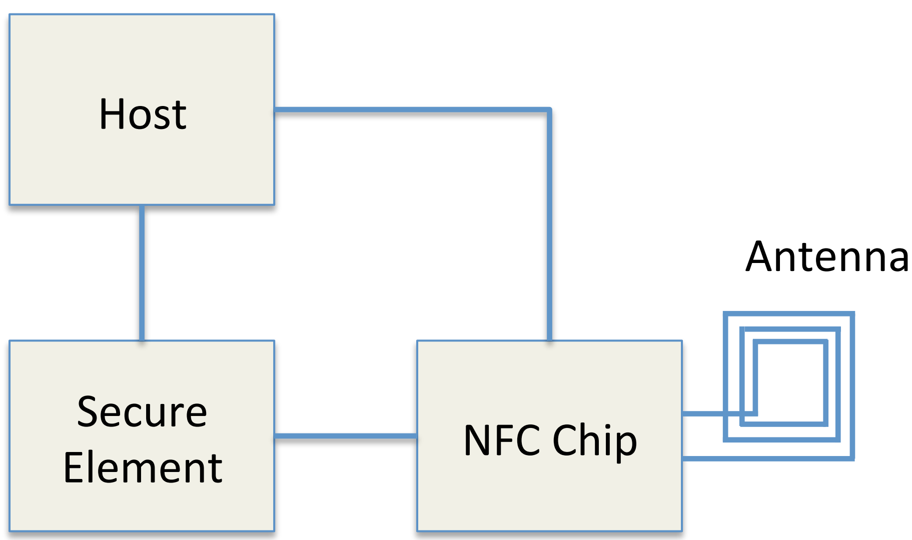
Browse code

Cyanogen Card Emulation

- android_frameworks_base (Java API)
  - https://github.com/CyanogenMod/android_frameworks_base/commit/c80c15bed5b5edffb61eb543e31f0b90eddcdadf
- 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/d41edfd794d4d0fedd91d561114308f0d5f83878
- NFC Reader code disabled because it interferes with Google Wallet
  - https://github.com/CyanogenMod/android_packages_apps_Nfc/commit/75ad85b06935cfe2cc556ea1fe5ccb9b54467695

BLACKWINGINTELLIGENCE

NFC Hardware Architecture

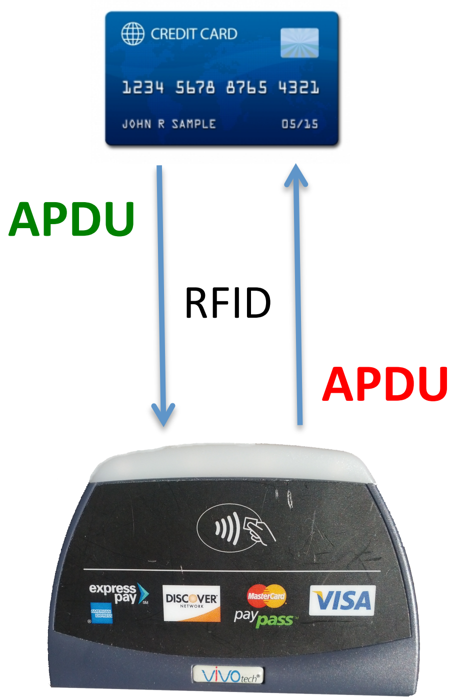


Tool Features

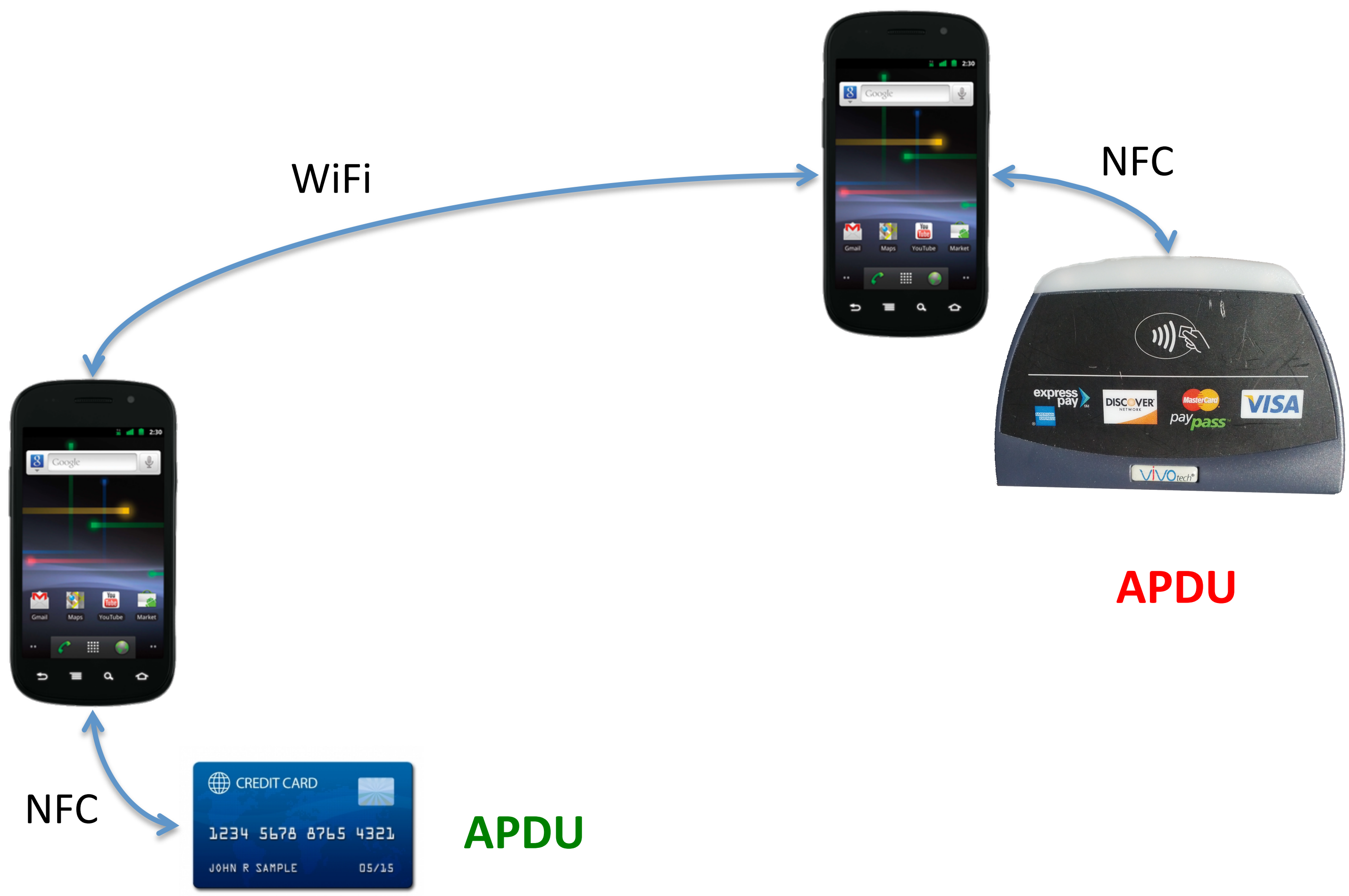
- Proxy transactions
- Save transactions
- Export transactions
- Tag replay (on Cyanogen side)
- PCD replay

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

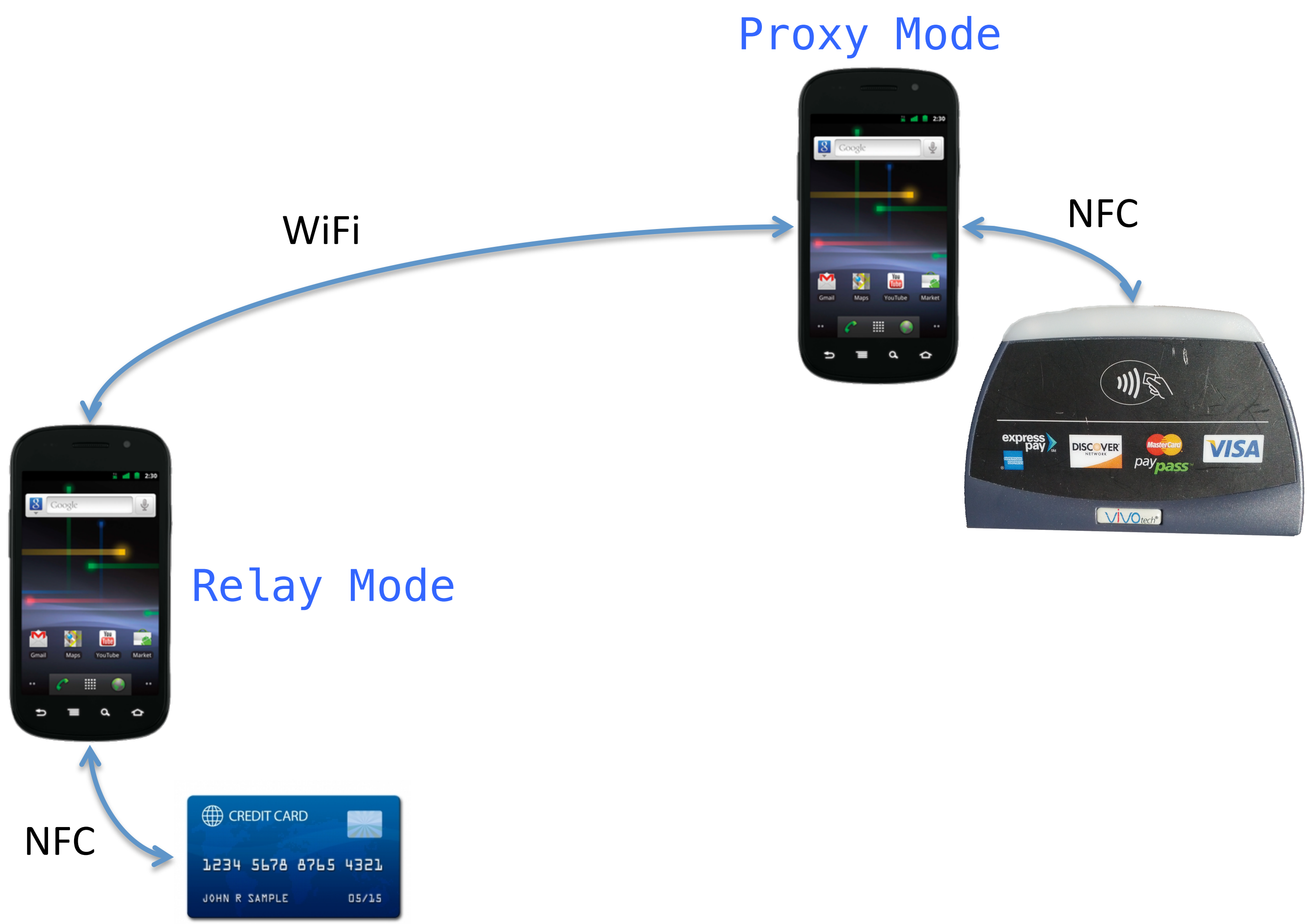
Standard Transaction



How It Works // Proxy Mode



How It Works // Terminology



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

How It works // Replay Mode

- 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

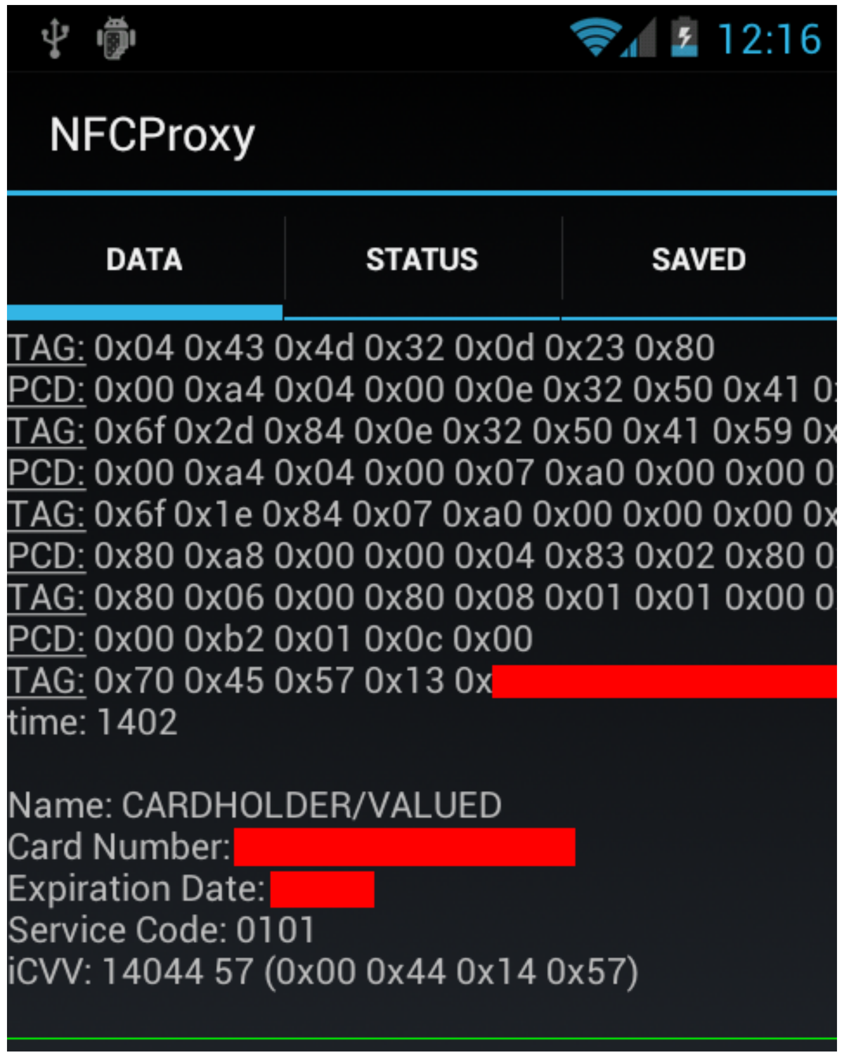
Antennas

- 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

APDU-Speak

- EMV Book 3
  - http://www.emvco.com/download_agreement.aspx?id=654
- See RFIDIOt (ChAP.py) and pwnpass for APDUs used for skimming
- Proxy not needed for skimming and spending
  - Just for protocol analysis

Sample Output



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

Source Code

- Now available for download and contribution!
- http://sourceforge.net/projects/nfcproxy/

Q & A

- Questions?
- Contact: eddie{at}blackwinghq.com