NFC Redux

Presenter: Nick von Dadelszen
Date: 17th November 2012
Company: Lateral Security (IT) Services Limited
Company Overview

Company

- Lateral Security (IT) Services Limited
- Founded in April 2008 by Nick von Dadelszen and Ratu Mason (both directors)
- Staff - AKL - 7 people, WGTN - 7 people

Services

- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modelling and risk assessment)
- Regular ongoing technical testing and assurance programs

Differentiators

- True vendor independence
- Security testing and advisory are our niche specialties
- Highly experienced and skilled staff
Presentation Objectives

- Provide an update on NFC research and security
- Release my new tool, NFCapture
- Do some crowd-sourcing research
NFC On Mobiles

- Samsung Nexus S first Android phone to get NFC chip
- Android, Blackberry, Nokia phones with NFC available
  - Samsung Galaxy SIII
  - Several Snapper phones
- iPhone cases with NFC
- Rumoured for Not on the iPhone 5
- Huge increase in distribution from last year
Recent Research

- Recent NFC research since last Kiwicon includes:
  - Kristen Paget – Shmoocon 2012
  - Charlie Miller – Blackhat 2012
  - MWR Labs – Pwn2Own EUSecWest 2012
  - Eddie Lee – Defcon 2012
Contactless Credit Card Fraud

- Kristen Paget presented onstage a method of performing credit card fraud using contactless payments
- Get CC number, expiry and rolling CVV from contactless card
- Write data to mag card
- Use mag card in a reader that can’t tell the difference between mag and contactless (Square was used for the demo)
Attacking The NFC Stack

- Charlie Miller presented excellent research at Blackhat 2012
- He fuzzed the NFC stack on a Nexus S using an ACR122U
- Results:
  - Multiple crashes
  - Found a vulnerability that enabled him to gain full control of the phone
Bluetooth Pairing

- Nokia phones can use NFC to automatically pair bluetooth devices
- No requirement to enter a PIN
- No other confirmation by default
- Once paired, can use tools such as obexfs to gain access to the device
Android Beam

- Android Beam can be used to pass info between devices, or from a tag to a device
  - Contacts
  - URLs
  - Apps
- There is no confirmation on the receiving side
- Automatically runs the associated app
- Combined with a browser bug this is pretty dangerous
MWR at Pwn2Own

- Used Android Beam to upload a file to phone
- Phone opened Android document viewer, which contained a memory corruption bug
- Gained full control of phone
- Won $30,000
Card Emulation – Solved!

- Card emulation on Android was very difficult
- Last year I stated this would be solved in 6-12 months
- CynogenMod solved this to enable their SimplyTapp payment app
- First MITM proof of concept released at Defcon (August 2012)
  - NFCProxy - Eddie Lee at Blackwing
My New Tool - NFCapture

- Have written a new tool called NFCapture
- Is an upgrade of my old tool released last year
- Is designed to be a framework to allow researchers to easily review and manipulate NFC systems
- Multiple functions:
  - Card read
  - Card emulation
  - MITM
NFCapture – Card Read

- NFCapture can read ISO-14443 tags
- Gets information to send from a network socket
- Can be remote server or local python
- Still compatible with RFIDIOt
- I am hoping scripts will be shared to read different types of cards
Card Read Script

```python
import sys
import os
import pyandroid
import datetime

Verbose = True

aidlist = [
    ['TESTER', 'a0000000041010'],
]

n = pyandroid.Android()

while(42):
    uid = n.select()
    print('GMT Timestamp: ' + str(datetime.datetime.now()))

    current = 0
    cc_data = False

    while current < len(aidlist):
        if Verbose:
            print('Trying AID: ' + aidlist[current][0] + ':' + aidlist[current][1] + '00')
            apdu = '00A0400007' + aidlist[current][1] + '00'
            r = n.sendAPDU(apdu)

        if r[-4:] == '9600':
            uid = uid[:1]
            n.sendResults("Card found-UID: " + uid + "-Card type: " + aidlist[current][0])
            print("\nCard found-UID: " + uid + "\nCard type: " + aidlist[current][0])
            break

        current += 1

    if not quiet:
        print('Ending now ...')

    n.deconfigure()
    print
```
NFCapture - Card Emulation

- If you run CynogenMod you can put my app into emulation mode
- Takes card responses from network socket
- Can run from remote server or local python
- Now you can write very simple python to emulate a card transaction
Card Emulation Script

```python
import sys
import os
import pyandroid
import datetime

Verbose = True
Quiet = False

n = pyandroid.Emulator()

while(42):
    APDU = n.select()
    print 'GMT Timestamp: ' + str(datetime.datetime.now())

while APDU is not "close":
    if Verbose:
        print 'Received APDU: ' + APDU
        sendData = '0000000000000000'
    if Verbose:
        print 'Sending data: ' + sendData
    APDU = n.sendAPDU(sendData)

if not Quiet:
    print 'Ending now ...'

n.reset()
print
```
Using my tool and two phones you can now do simple MITM

One phone needs CynogenMod to be the emulator

Can run from remote server or local python
import sys
import os
import pyandroid
import datetime

Verbose = True
Quiet = False

p = pyandroid.Android()
e = pyandroid.Emulator()

while(42):
    uid = p.select()
    APDU = e.select()

    print 'GMT Timestamp: ' + str(datetime.datetime.now())

    while APDU:
        if Verbose:
            print 'Received APDU: -' + APDU + '-'
        r = p.sendAPDU(APDU)
        if Verbose:
            print 'Response from proxy is: ' + r
        APDU = e.sendAPDU(r)
        if Verbose:
            print 'Sent response to emulator, new APDU is: -' + APDU + '-'
        if not Quiet:
            print 'Ending now ...'
p.reset()
e.reset()
print
Let's Do Some Research!

- I want to see how realistic it is to get someone else's tag
- I am going to use you guys to do it
- I have written a “kiwicon mode” for my tool for this
- Posts the info to a website

- PLEASE ONLY USE ON FRIENDS AT KIWICON!!
Please Download And Use This Weekend!

https://www.lateralsecurity.com/downloads/NFCapture-v1-0.apk
Questions & Contacts

Lateral Security (IT) Services Limited

Wellington
38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone: +64 4 4999 756
Email: sas@lateralsecurity.com

Auckland
187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com

Presentation Download
www.lateralsecurity.com/presentations