LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

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

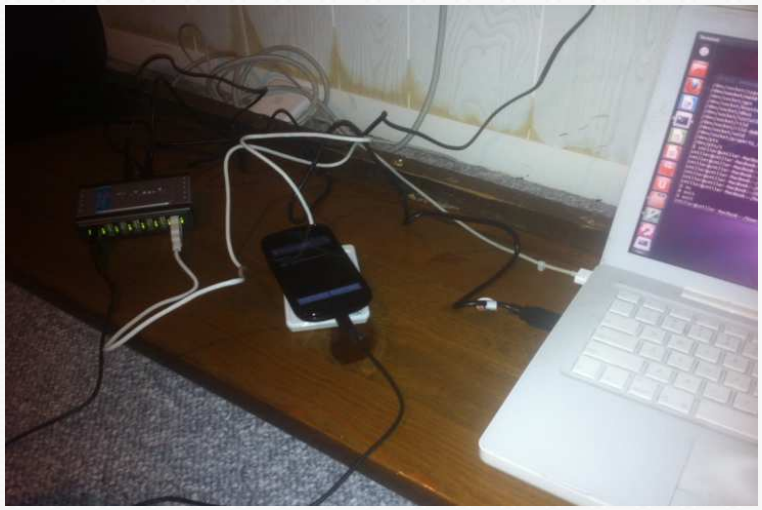
- Recent NFC research since last Kiwicon includes:
  - Kristen Paget – Shmoocon 2012
  - Charlie Miller – Blackhat 2012
  - MWR Labs – Pwn2Own EUSecWest 2012
  - Eddie Lee – Defcon 2012

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

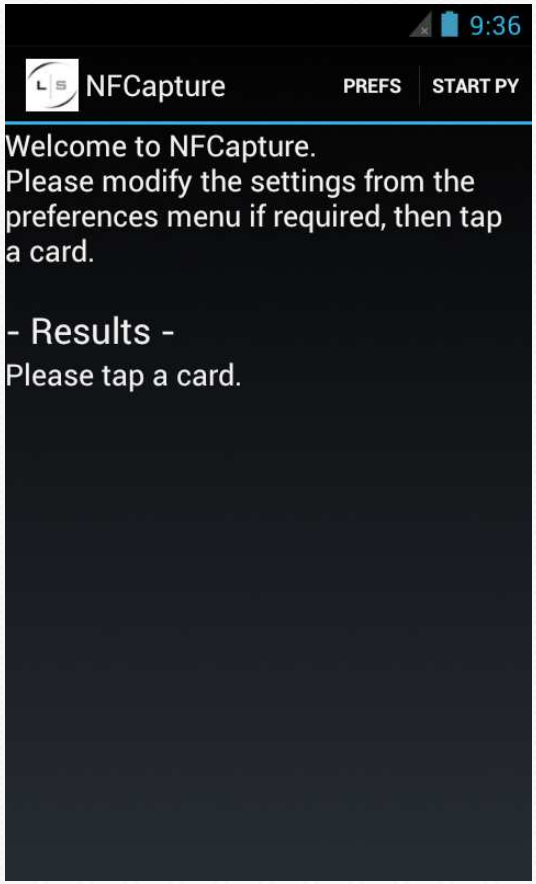
- Used Android Beam to upload a file to phone
- Phone opened Android document viewer, which contained a memory corruption bug
- Gained full control of phone
- Won $30,000

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

```
26  import sys
27  import os
28  import pyandroid
29  import datetime
30
31  Verbose= True
32
33  aidlist=    [
34          ['TESTER',      'a0000000041010'],
35          ]
36
37  n = pyandroid.Android()
38
39  while(42):
40      uid = n.select()
41      print 'GMT Timestamp: ' + str(datetime.datetime.now())
42
43      current = 0
44      cc_data = False
45
46      while current < len(aidlist):
47          if Verbose:
48              print 'Trying AID: '+ aidlist[current][0]  + ':' + aidlist[current][1] + '00'
49          apdu = '00A4040007' + aidlist[current][1] + '00'
50          r = n.sendAPDU(apdu)
51
52          if r[-4:] == '9000':
53              uid = uid[:-1]
54              n.sendResults("Card found-UID: " + uid + "-Card type: " + aidlist[current][0])
55              print "\nCard found-UID: " + uid + "\nCard type: " + aidlist[current][0]
56              break
57
58          current += 1
59
60      if not Quiet:
61          print 'Ending now ...'
62      n.deconfigure()
63      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

```
26  import sys
27  import os
28  import pyandroid
29  import datetime
30
31  Verbose= True
32  Quiet= False
33
34  n = pyandroid.Emulator()
35
36  while(42):
37      APDU = n.select()
38      print 'GMT Timestamp: ' + str(datetime.datetime.now())
39
40      while APDU is not "close":
41          if Verbose:
42              print 'Received APDU: ' + APDU
43          sendData = '000000009000'
44          if Verbose:
45              print 'Sending data: ' + sendData
46          APDU = n.sendAPDU(sendData)
47
48      if not Quiet:
49          print 'Ending now ...'
50      n.reset()
51      print
```

NFCapture - MITM

- 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

MITM Script

```
26  import sys
27  import os
28  import pyandroid
29  import datetime
30
31  Verbose= True
32  Quiet= False
33
34  p = pyandroid.Android()
35  e = pyandroid.Emulator()
36
37
38  while(42):
39      uid = p.select()
40      APDU = e.select()
41
42      print 'GMT Timestamp: ' + str(datetime.datetime.now())
43
44      while APDU:
45          if Verbose:
46              print 'Received APDU: -' + APDU + '-'
47          r = p.sendAPDU(APDU)
48          if Verbose:
49              print 'Response from proxy is: ' + r
50          APDU = e.sendAPDU(r)
51          if Verbose:
52              print 'Sent response to emulator, new APDU is: -' + APDU + '-'
53
54      if not Quiet:
55          print 'Ending now ...'
56      p.reset()
57      e.reset()
58      print
```

Lets 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!!**

LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

Please Download And Use This Weekend!

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

Questions & Contacts

Presentation Download
www.lateralsecurity.com/presentations

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