LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

Mobile Apps and RFID

The Tale Of Two Techs

Presenter: Nick von Dadelszen

Date: 6th November 2011

Company: Lateral Security (IT) Services Limited

LATERAL | SECURITY

Company Overview

- Company
  - Lateral Security (IT) Services Limited
  - Founded in April 2008, HQ in Wellington
  - Directors: Nick von Dadelszen and Ratu Mason
- Information Security Services
  - Technical testing (penetration testing, system configuration, source code)
  - Design and architecture review
  - Advisory (governance, risk, policy and compliance)
  - Incident Response
  - Lifecycle auditing (design, pre prod, post prod)
  - Regular ongoing testing programs
- Differentiators
  - True vendor independence
  - Security testing is our niche specialty
  - Very highly skilled staff

LATERAL | SECURITY

Intro

- Two topics I have previously presented on:
  - OWASP 2011 - Testing mobile applications
  - Kiwicon 2009 - Smart Card Security
- Both feature emerging technologies that interest me
- These technologies are now converging

LATERAL | SECURITY

NFC Phones

- Samsung Nexus S first Android phone to get NFC chip
- Android, Blackberry, Nokia phones with NFC available
- iPhone cases with NFC
- Rumoured for the iPhone 5

LATERAL | SECURITY

NFC In Android

- Interaction available through APIs
- Pushed heavily by Google

- Being used in P2P apps
  - Sharing URLs, contacts, apps

- Starting to be monetised
  - Google wallet (more later)
  - PayPal P2P transfers

LATERAL | SECURITY

NFC Elements

- NFC Reader
  - Available from documented APIs
- NFC Chip
  - No documentation available
  - Embedded SmartMX dual chip
    - Mifare 4k
    - Secure Element

LATERAL | SECURITY

The Good

- We now have an RFID reader with mobile internet access
- Enter Mobile RFIDiot

LATERAL | SECURITY

The Bad

- We now have an RFID reader with mobile internet access which no one will notice
- Enter the worlds first mobile, PCI compliant credit card skimmer

LATERAL | SECURITY

The Ugly

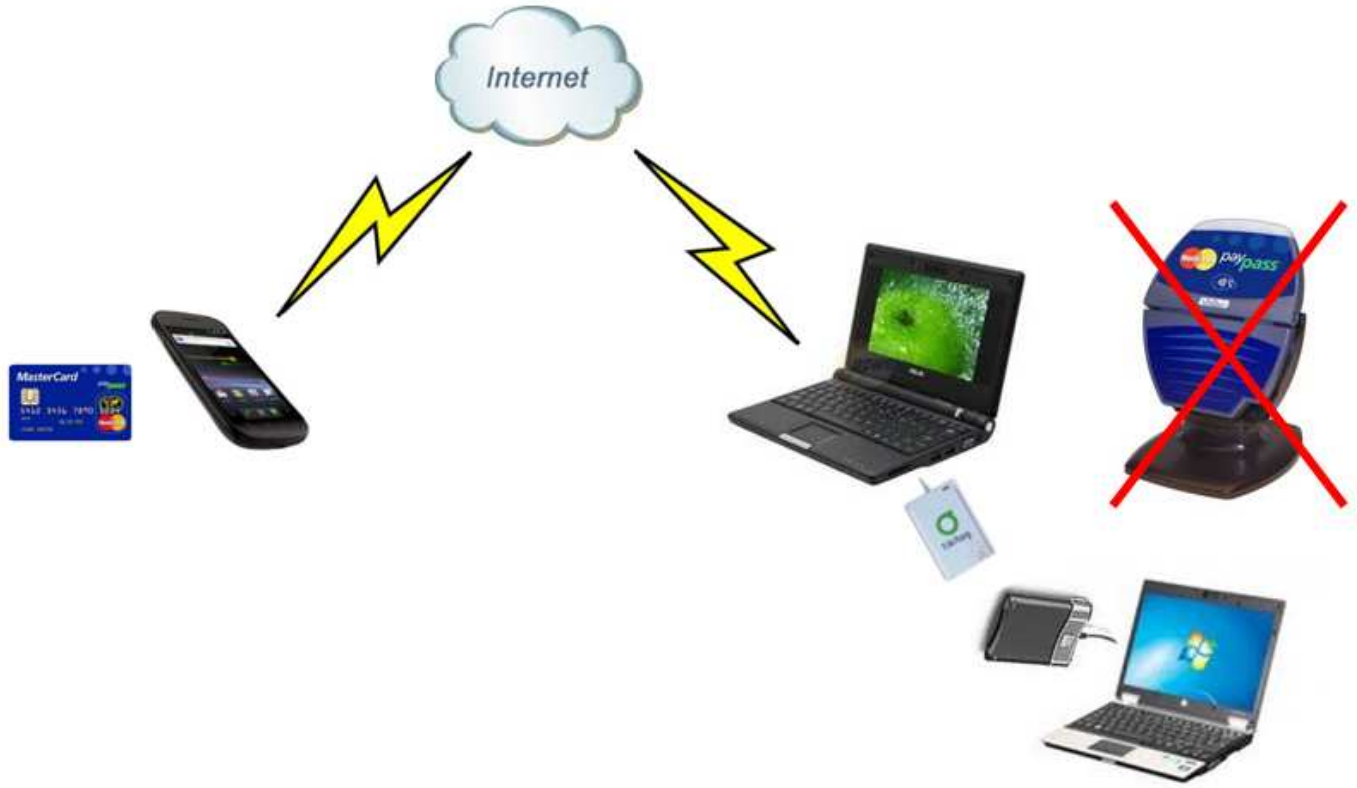
- What about installing malicious sniffing apps on other's phones?
- What about MITM with a mobile phone?

LATERAL | SECURITY

MITM Theory

LATERAL | SECURITY

MITM Implementation



LATERAL | SECURITY

The Future

- Need full card emulation with a mobile phone
- People are working on it
- The more apps that use this, the more likely it will get opened up
  - Google Wallet
  - Kaching
  - …

LATERAL | SECURITY

Future MITM

LATERAL | SECURITY

What About Those Payment Apps?

LATERAL | SECURITY

iCarte

- Exactly like sticking something onto your phone

LATERAL | SECURITY

What You Can Do

- Consider other peoples phone are wirelessly malicious
- Use RFID blocking wallets
- Regularly check bank statements
- Remember that most NZ banks guarantee you against fraudulent credit card payments

LATERAL | SECURITY

Tools

- https://www.lateralsecurity.com/OurTools.html
  - LS-NFC-Client.apk + source
  - Pyandroid.py
  - RFIDIOt patch
- http://www.rfidiot.org

LATERAL | SECURITY

Questions?

LATERAL | SECURITY

Contact Details

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 1010, New Zealand

Phone: +64 9 3770 700

Email: sas@lateralsecurity.com

LATERAL | SECURITY