Mobile NFC 101

Presenter: Nick von Dadelszen
Date: 31st August 2012
Company: Lateral Security (IT) Services Limited

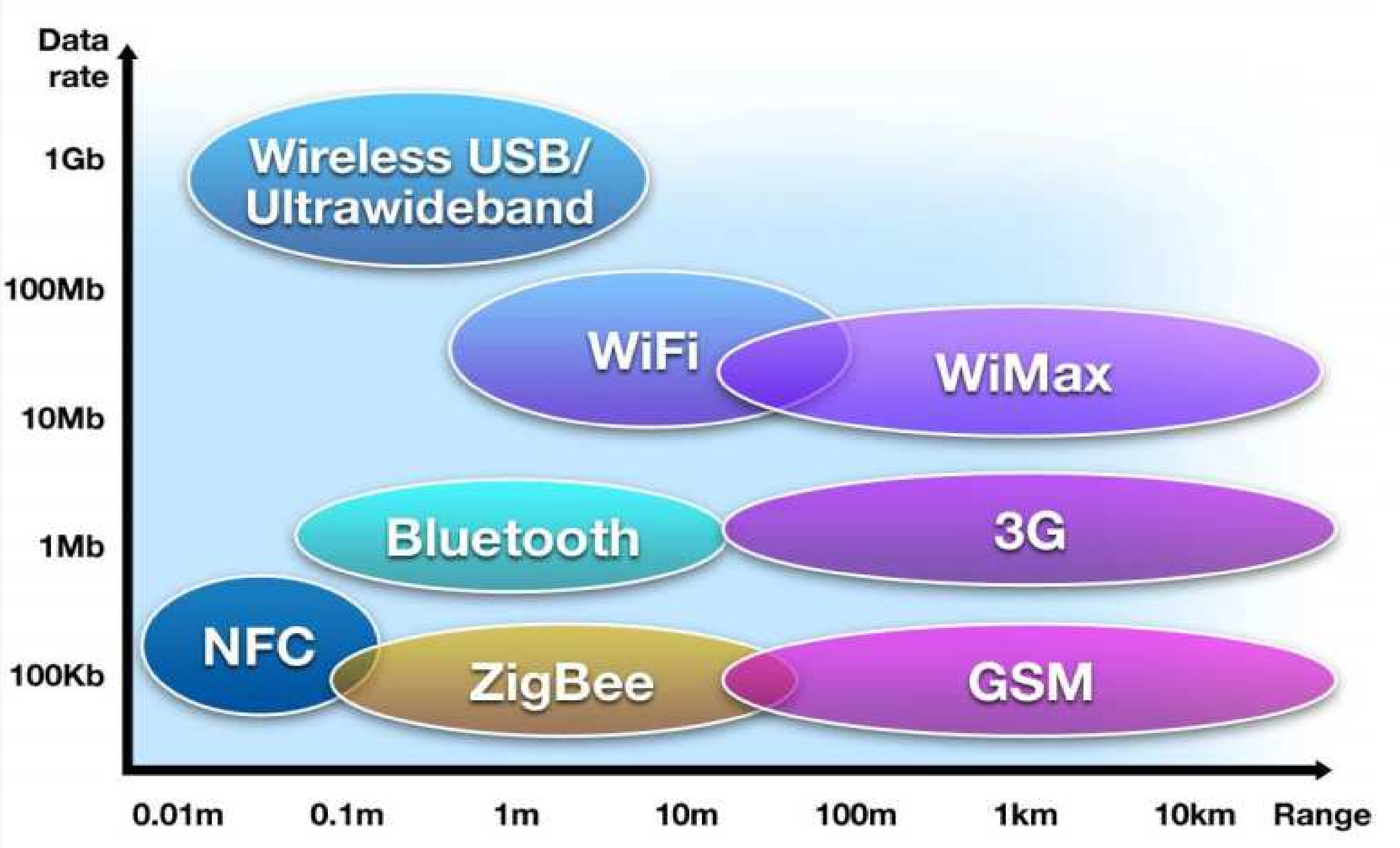
Company Overview

- **Company**
  - Lateral Security (IT) Services Limited
  - Founded in April 2008 by Nick von Dadelszen and Ratu Mason (both directors)
  - Staff - AKL - 6 people, WGTN - 7 people, Hong Kong - 1 person
- **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

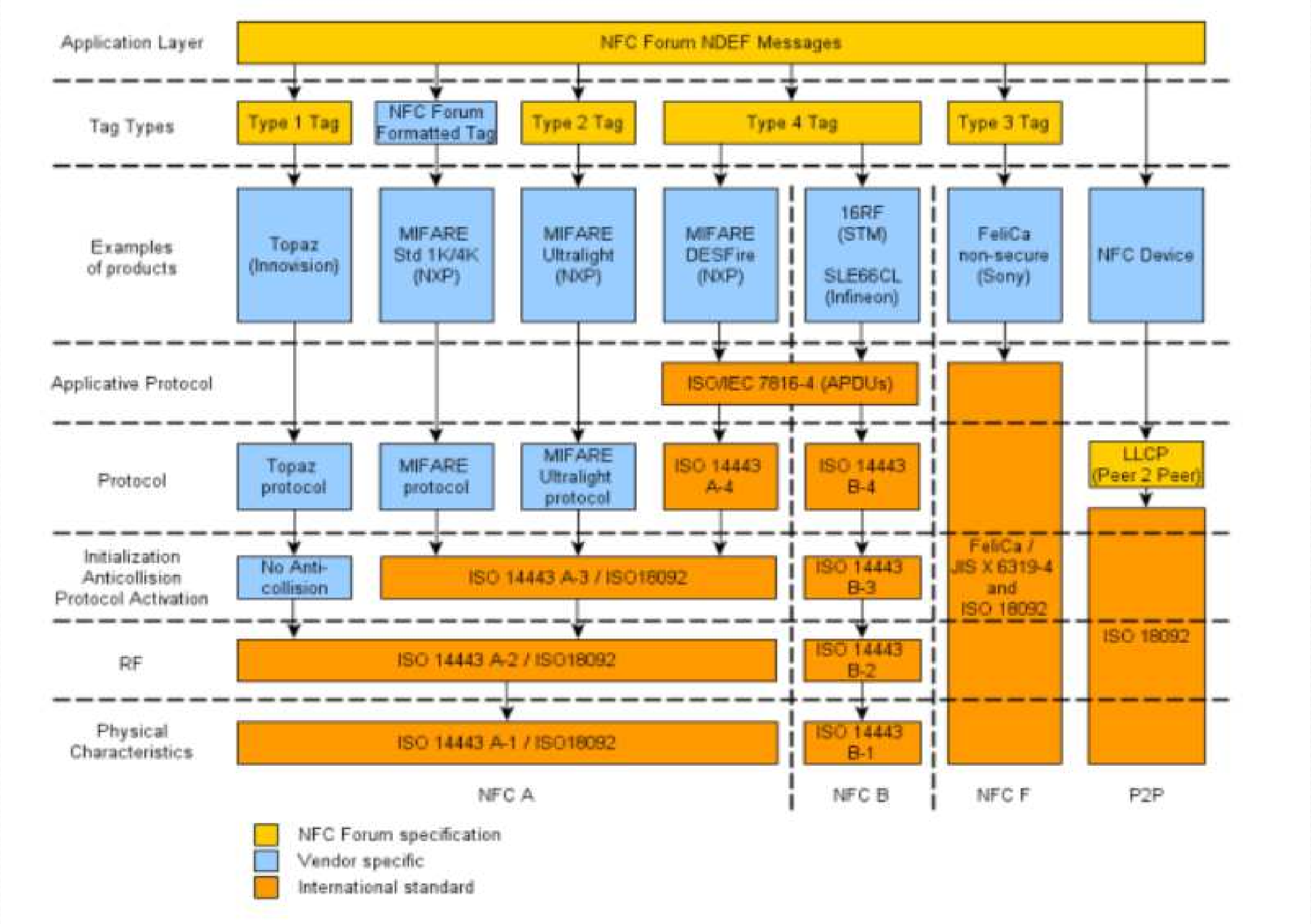
Objectives

- This talk has the following goals:
  - Provide you with an understanding of the technology behind NFC on mobile phones
  - How it integrates with the hardware and application layers
  - Discuss the security considerations for NFC on Mobile and how it differs from standard NFC implementations

How NFC Fits


Data rate
1Gb
100Mb
10Mb
1Mb
100Kb
Wireless USB/ Ultrawideband
WiFi
WiMax
Bluetooth
3G
NFC
ZigBee
GSM
0.01m
0.1m
1m
10m
100m
1km
10km
Range

NFC Protocols



Application Layer	NFC Forum NDEF Messages						
Tag Types	Type 1 Tag	NFC Forum Formatted Tag	Type 2 Tag	Type 4 Tag		Type 3 Tag	
Examples of products	Topaz (Innovision)	MIFARE Std 1K/4K (NXP)	MIFARE Ultralight (NXP)	MIFARE DESFire (NXP)	16RF (STM) SLE66CL (Infineon)	FeliCa non-secure (Sony)	NFC Device
Applicative Protocol				ISO/IEC 7816-4 (APDUs)		FeliCa / JIS X 6319-4 and ISO 18092	
Protocol	Topaz protocol	MIFARE protocol	MIFARE Ultralight protocol	ISO 14443 A-4	ISO 14443 B-4		LLCP (Peer 2 Peer)
Initialization Anticollision Protocol Activation	No Anti-collision	ISO 14443 A-3 / ISO18092			ISO 14443 B-3		ISO 18092
RF	ISO 14443 A-2 / ISO18092				ISO 14443 B-2		
Physical Characteristics	ISO 14443 A-1 / ISO18092				ISO 14443 B-1		
	NFC A				NFC B	NFC F	P2P

🟨 NFC Forum specification

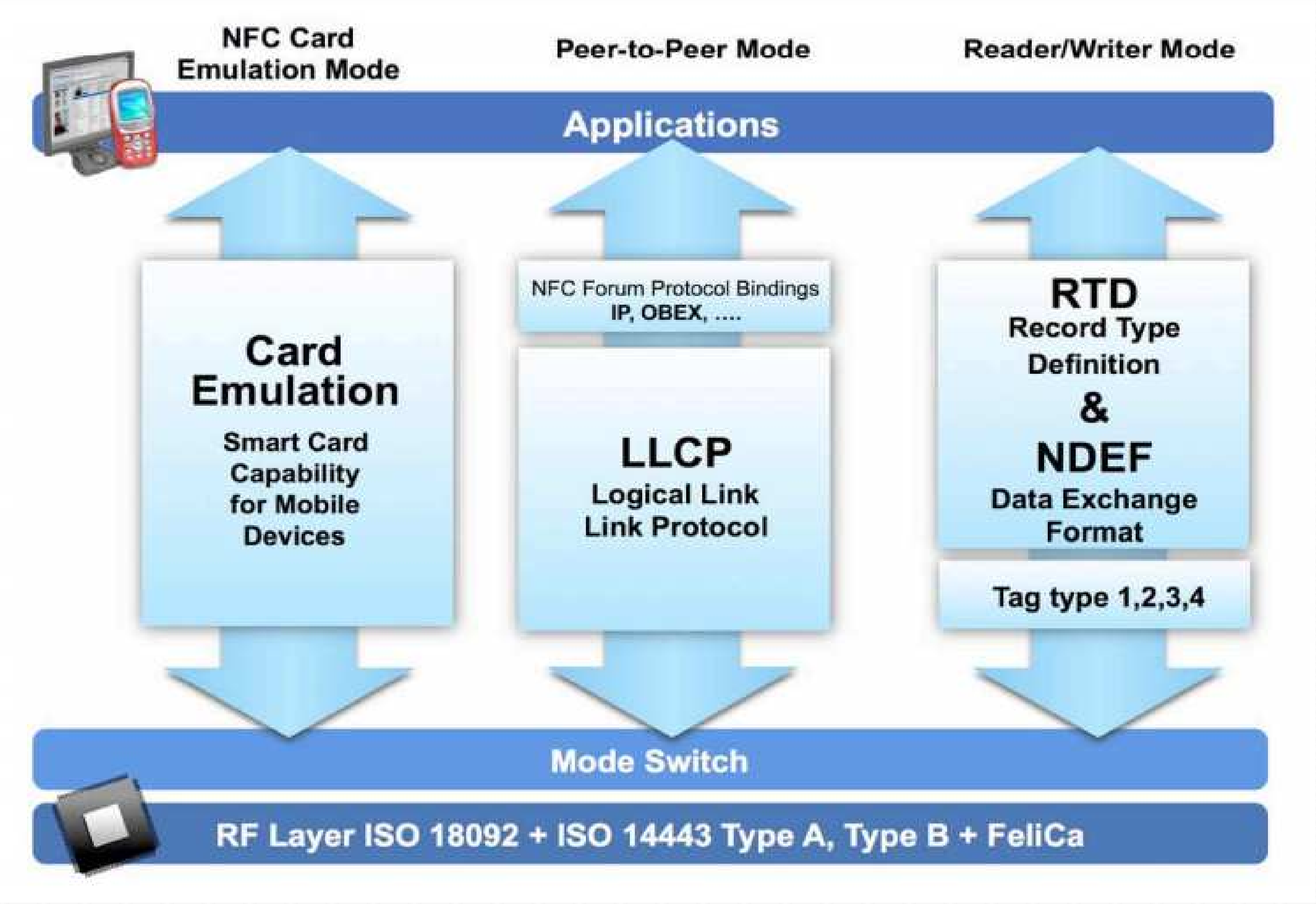
🟦 Vendor specific

🟧 International standard

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 the iPhone 5
- Huge increase in distribution from last year

Mobile Architecture



NFC Card Emulation Mode

Peer-to-Peer Mode

Reader/Writer Mode

Applications

Card Emulation

Smart Card Capability for Mobile Devices

NFC Forum Protocol Bindings
IP, OBEX, ….

LLCP
Logical Link Link Protocol

RTD
Record Type Definition
&
NDEF
Data Exchange Format

Tag type 1,2,3,4

Mode Switch

RF Layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

NFC Types In Mobiles

- Reader/Writer mode
  - Phone can read passive tags
  - Default on Android with NFC
  - Android APIs available for easy use
  - Many apps in the market
  - My own RFIDiot app is an example of this

Reader/Writer Sample Code

```
if (NfcAdapter.ACTION_TECH_DISCOVERED.equals(action)) {

    Parcelable nfcTag = intent.getParcelableExtra("android.nfc.extra.TAG");
    Tag t = (Tag)nfcTag;
    IsoDep myTag = IsoDep.get(t);

    if( !myTag.isConnected() )
     {
     myTag.connect();

     byte[] hexAPDU = HexToList(APDU);
     byte[] response = myTag.transceive(hexAPDU);
     String hexResponse = ListToHex(response);
```

NFC Types In Mobiles

- Peer-to-Peer Mode
  - Allows two devices to talk directly to each other
  - Android Beam is an example of this
  - Can send URLs, Contacts, Apps etc between phones
  - Can be used to pair bluetooth devices
- In both reader/writer and Peer-to-peer mode, Android OS has direct access to NFC reader hardware

NFC Types In Mobiles

- Card Emulation
  - Allows a phone to act as a tag
  - Multiple examples available now
    - Google Wallet
    - Snapper Touch2Pay
    - BNZ/Vodafone NFC trial
- This is where things aren’t quite so straightforward

Card Emulation Difficulties

- In order to emulate a card you need a secure element (SE) to hold the applet
- SE can be multiple places:
  - Embedded
  - On a SIM
  - On an SD
- Phone hardware must allow communication between NFC controller and SE
- For SIM cards this is SWP

Card Emulation Difficulties

- ○ To develop using Card Emulation you must have access to the SE to install the applet
  - ○ Google holds the keys to the embedded SE on Nexus phones
  - ○ Mobile Carriers hold the keys to the SIM SE
  - ○ Almost no phones support SD-SE

- Extremely difficult for the average developer to perform card emulation

SWP Card Emulation

- Multiple phones now support SWP
  - Samsung Galaxy SIII
  - Any phone supporting Snapper Touch2Pay
  - Pretty much any other NFC phone except Google branded phones
- SWP enables applet on SIM to access NFC controller
- SWP does not allow the mobile OS to access the applet
- SWP provides access over wireless interface only

To Access Applet From OS

- To access applet from OS app, two options:
  - Use Mobile OTA network to access SIM from carrier and remote call to mobile app
  - Enable access to SIM from OS
    - Access to SIM is through baseband processor, not application processor
    - BB must provide AT commands to enable transparent APDU exchange
    - Only Touch2Pay phones have these modifications

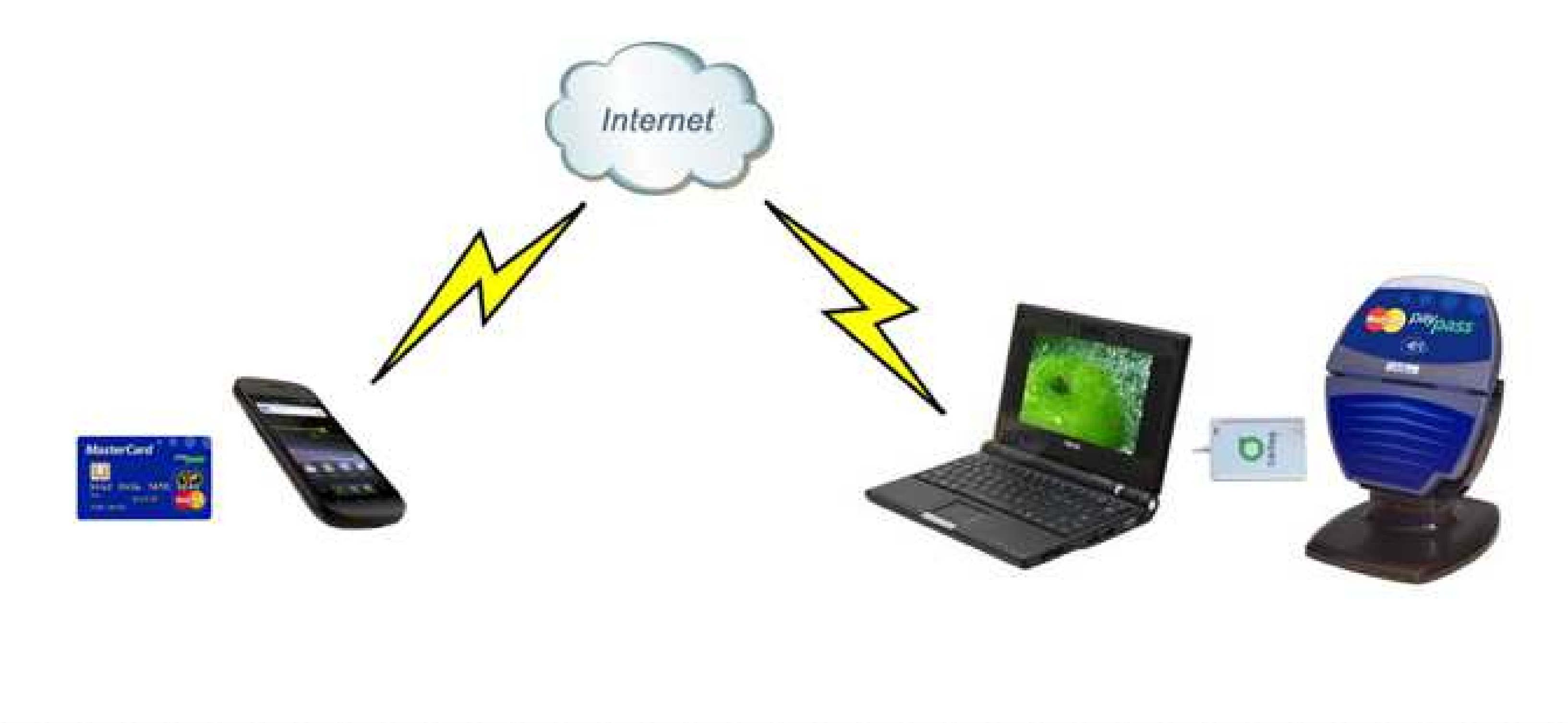
Security Considerations

- Mobile NFC as a delivery platform
  - Mobile RFIDiot
  - MITM
  - Malicious apps
- Mobile NFC as a target
  - Mobile payment apps
  - NFC stack
  - Android Beam

Mobile RFIDiot

- I presented my Mobile RFIDiot code at Kiwicon last year
- Allows you to use a phone as an RFIDiot reader
- Includes ability to read cards such as credit cards and passports
- Can be used to perform MITM
- New version (A “Nick Special”) to be released at Kiwicon this year

MITM Theory



Malicious Apps

- A malicious NFC app could be installed on numerous phones
- The app could read any nearby NFC tag and send the data to the attacker
- Now your phone could be sniffing your credit cards without you knowing

Attacking Payment Apps

- Apps in phones are the same apps as in cards:
  - Credit cards
  - Snapper
- However, now it is connected permanently to a computer with internet access
- Mobile malware etc can now attack payment apps without being in the vicinity

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

Charlie Miller’s Fuzzing Setup

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 could be pretty dangerous

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

Roundup

- Mobile NFC use is increasing significantly
- As with any new tech, there is a security learning curve
- If you are developing NFC apps, make sure you understand the threat model
- If you are attacking NFC apps, go have fun (with the usual disclaimers)

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, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com