Security Compass

Geoffrey Vaughan

NFC THREAT LANDSCAPE

Let’s Hack NFC

- How does NFC work?
- How could we hack it?
- Where are the weaknesses?
- What are the security implications?

Security Compass and NFC

- Currently we are devoting a lot of energy towards NFC research.
- Nearly everyone in our company is involved in some form of NFC research.
- This presentation represents some initial discoveries in the space.
- Stay tuned for more in the future.

Who am I?

- Security Consultant @ Security Compass
- MITS
- Ex-Teacher turned Hacker
- Sessional Lecturer at UOIT
- @MrVaughan

About NFC

- Near Field Communication (1-10cm)
- 13.56MHz
- Data rate: 424kilobits/second
- Four modes of operation:
  - Read
  - Write
  - Card Emulation
  - P2P

Compared to RFID

- 125 – 134kHz
- Typically only used for read only.

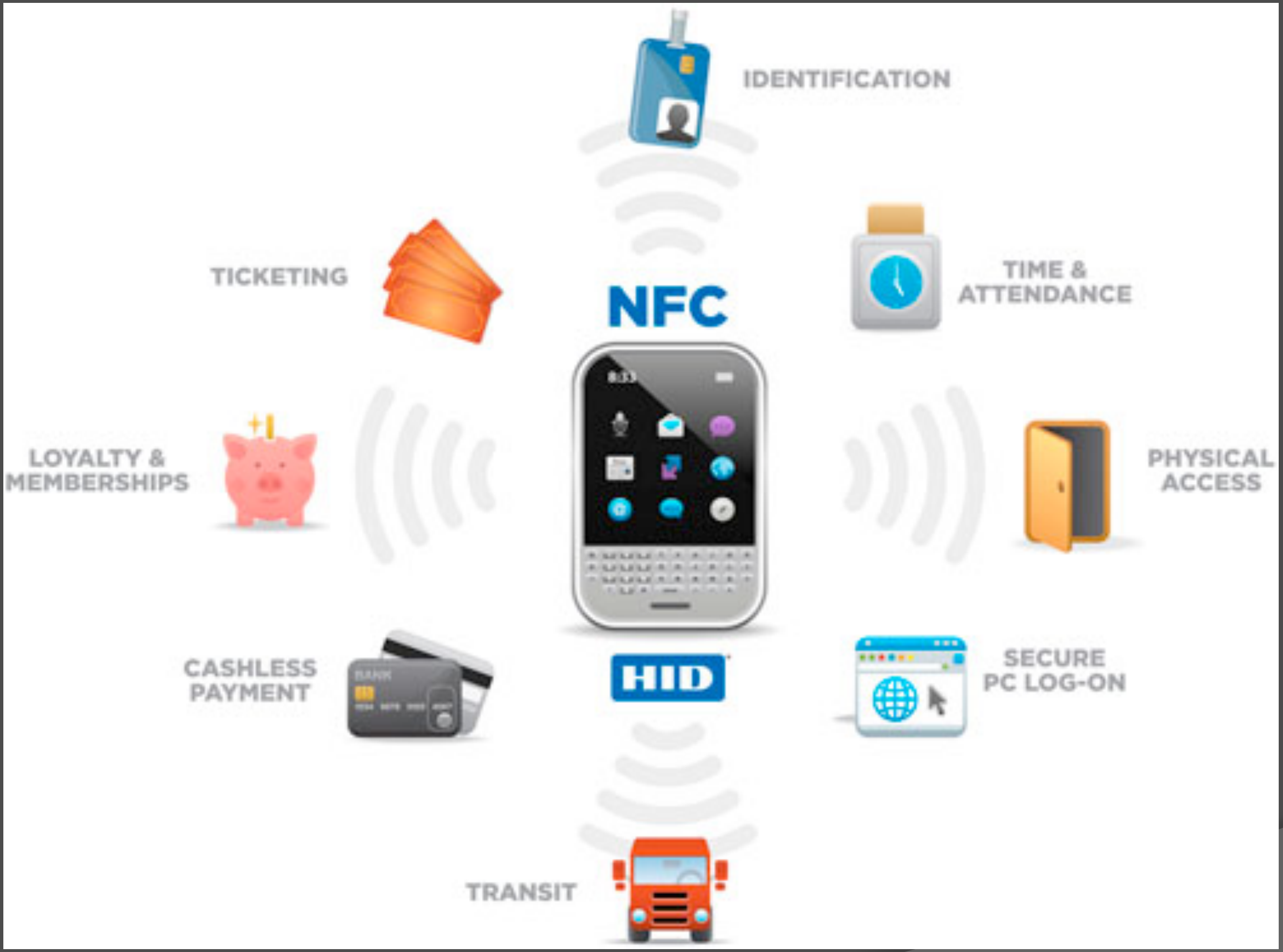
Types of Devices

- Tags
- Card Readers
- NFC Phones (most new phones)
- Readers are being put in many other household devices
- Payment Terminals / Credit Cards

Libraries / Resources

- LibNFC
- Eclipse Plugin - https://code.google.com/p/nfc-eclipse-plugin/
- Proxmark3 Python API - http://proxmark3.com/downloads.html
- ACR122U (USB Reader) - http://www.acs.com.hk/index.php?pid=product&id=ACR122U
- Mercury / ADB – Android debugging tools

Applications



Late to the Party?

- NFC has been reasonably quickly adopted in Canada
- The US is way behind…. Many haven't even implemented chip and pin
- In other areas its common place and used quite regularly

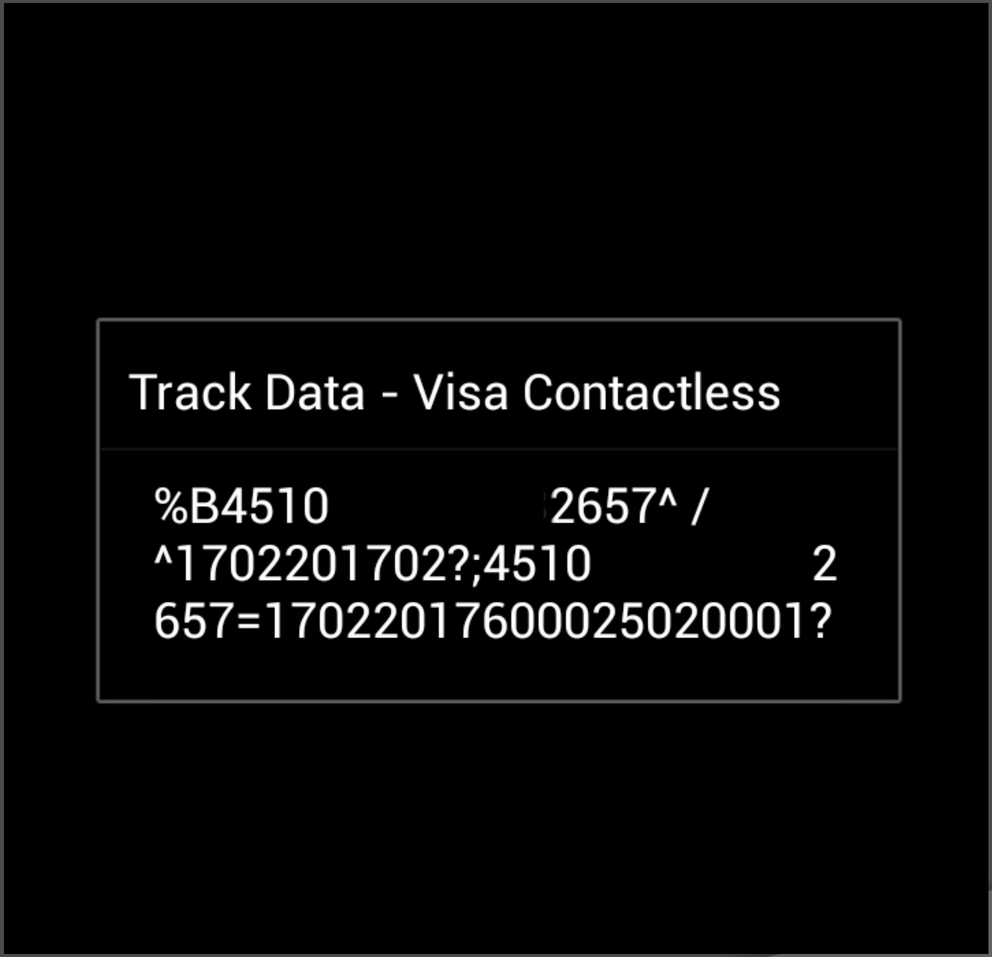
Case 1 –What's really in your wallet?

- NFC is coming in every new Credit Card in Canada
- Makes it quick and easy to make payments just tap and pay.
- Payment amount is usually capped at $50 however that amount is set by the merchant.

Problems?

- Now you have an antenna that you carry around with you everywhere.
- All an attacker needs to do is get within NFC range to steal your CC data (1-10cm)
- See SquareLess for Android

Is this your card?



Track Data - Visa Contactless

```
%B4510 [redacted] 2657^ /
^1702201702?;4510 [redacted] 2
657=17022017600025020001?
```

Case - 2

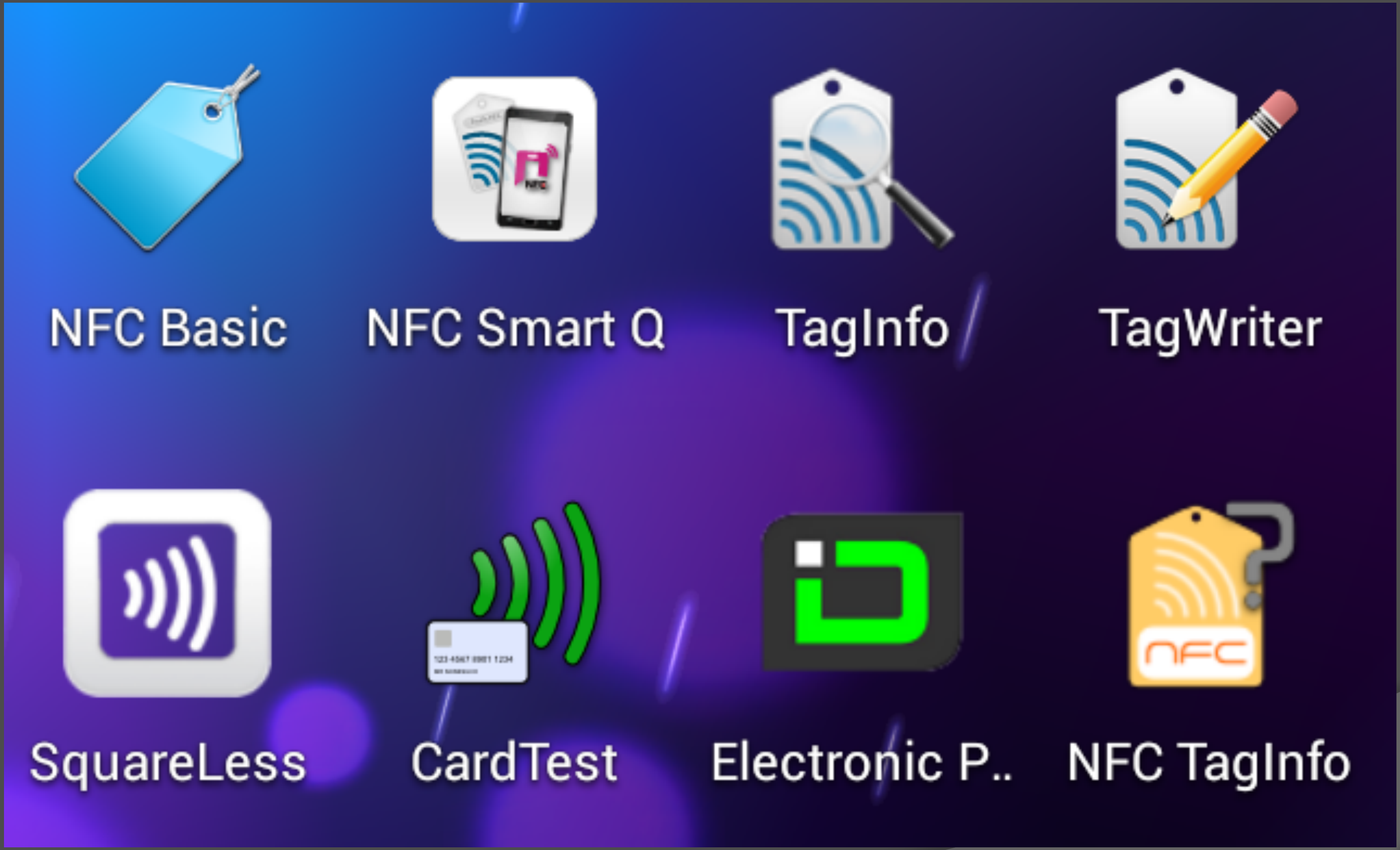
- Sally is drawn in to a clever poster about an upcoming concert.
- With NFC enabled on a phone a user she makes contact with the NFC Smart Poster.
- The poster will direct the user to a webpage. Where she can purchase tickets to attend the concert.

What could go wrong?

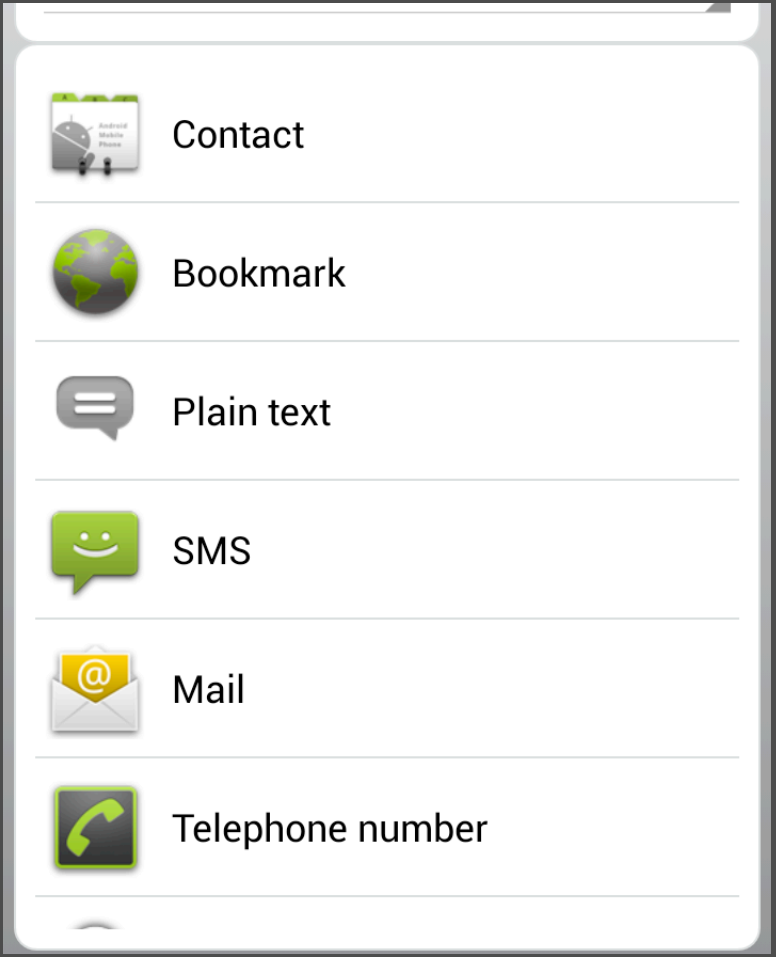
NFC enabled, now what?

- How the phone handles the NFC tag depends on the type of data on the card and the phone/OS you are using.
- Some phones will perform NFC actions without prompting the user.
- Some phones require the phone to be active.
- Some require the phone to be logged in.

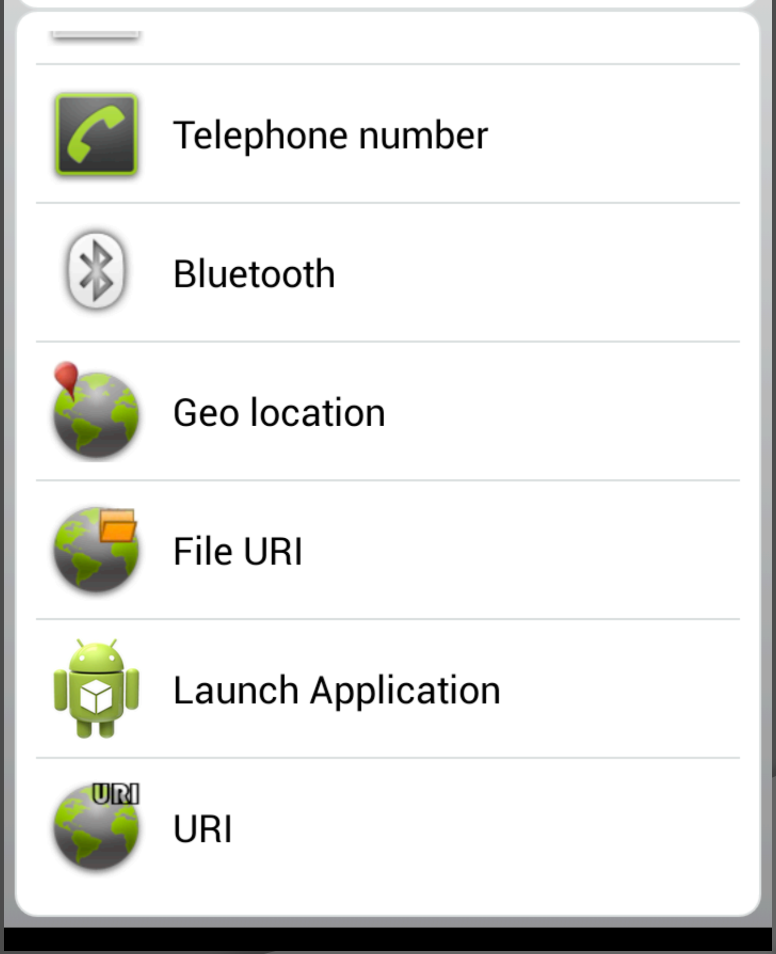
Some NFC Apps



Standard NFC Functions

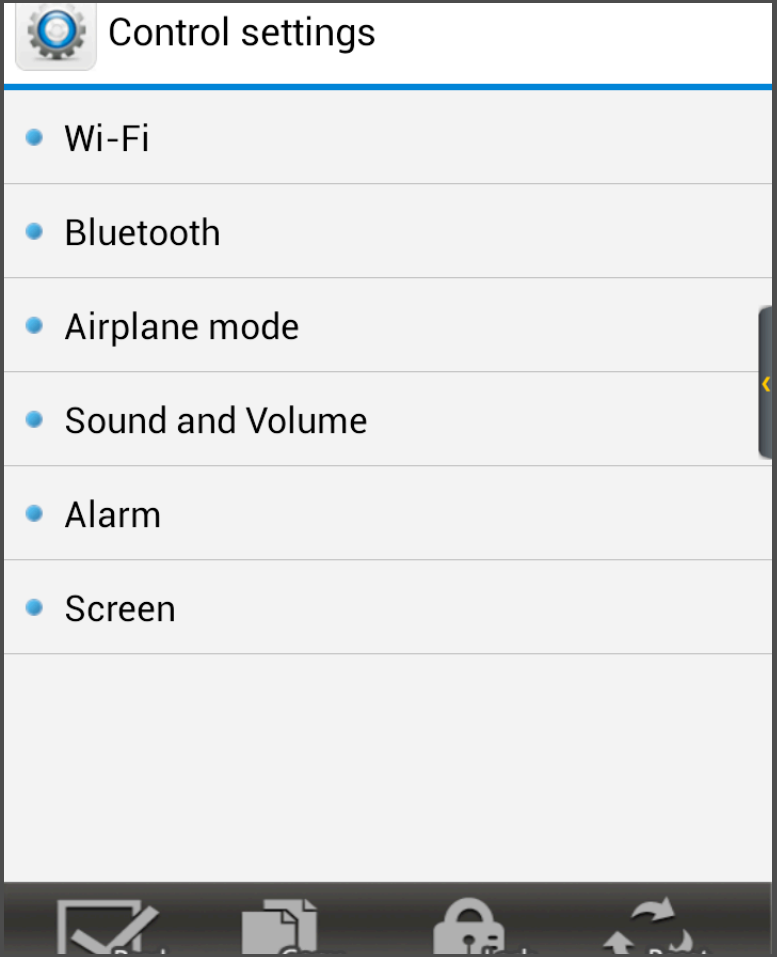


- Contact
- Bookmark
- Plain text
- SMS
- Mail
- Telephone number



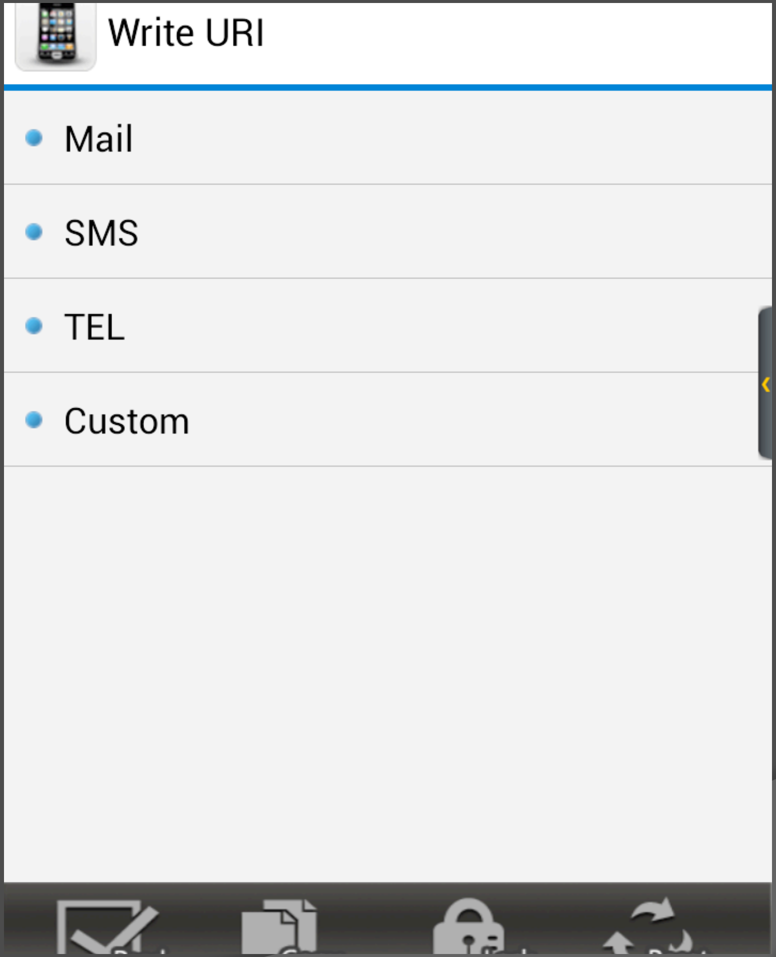
- Telephone number
- Bluetooth
- Geo location
- File URI
- Launch Application
- URI

Application Specific Card Data



Control settings

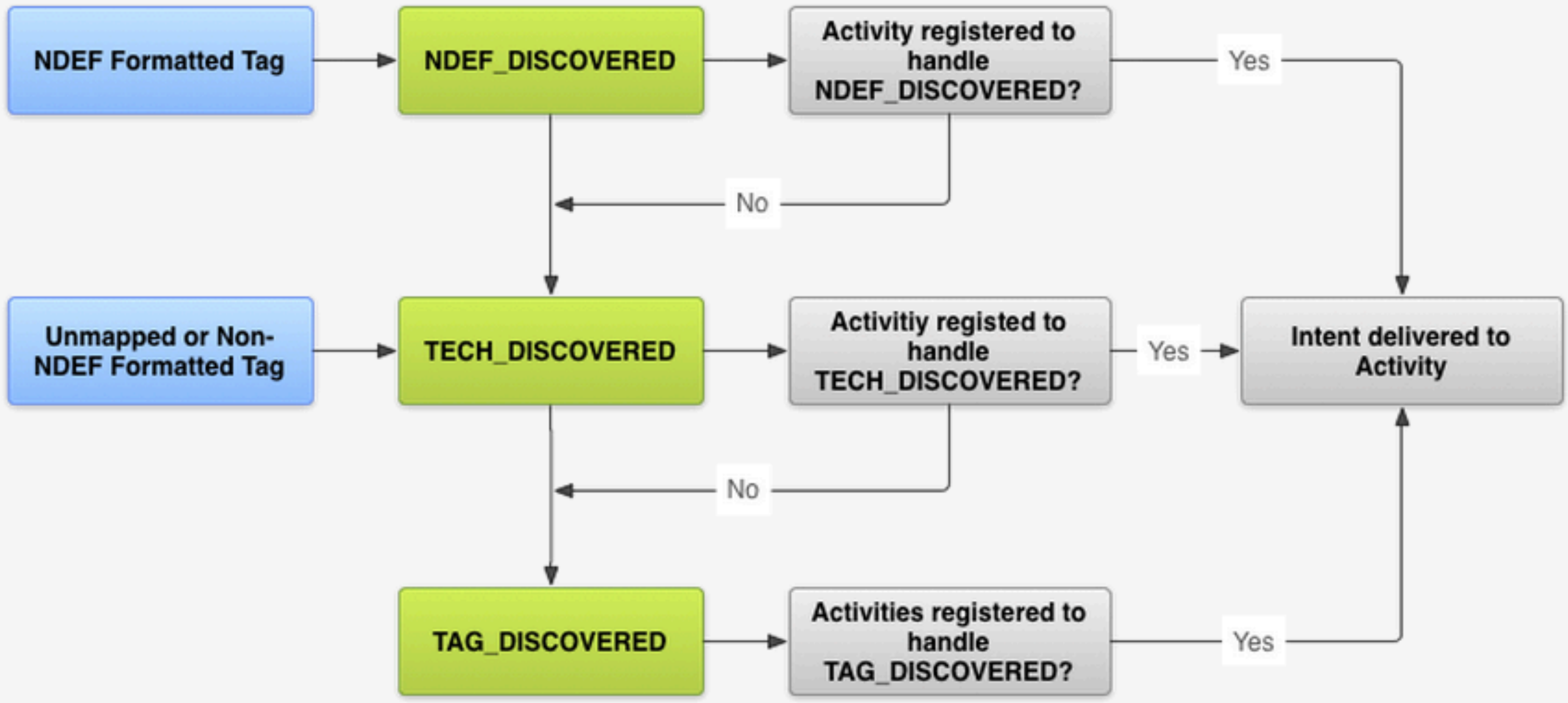
- Wi-Fi
- Bluetooth
- Airplane mode
- Sound and Volume
- Alarm
- Screen



Write URI

- Mail
- SMS
- TEL
- Custom

Android NFC Handler



NDEF Formatted Tag

NDEF_DISCOVERED

Activity registered to handle NDEF_DISCOVERED?

Yes

No

Unmapped or Non-NDEF Formatted Tag

TECH_DISCOVERED

Activitiy registed to handle TECH_DISCOVERED?

Yes

Intent delivered to Activity

No

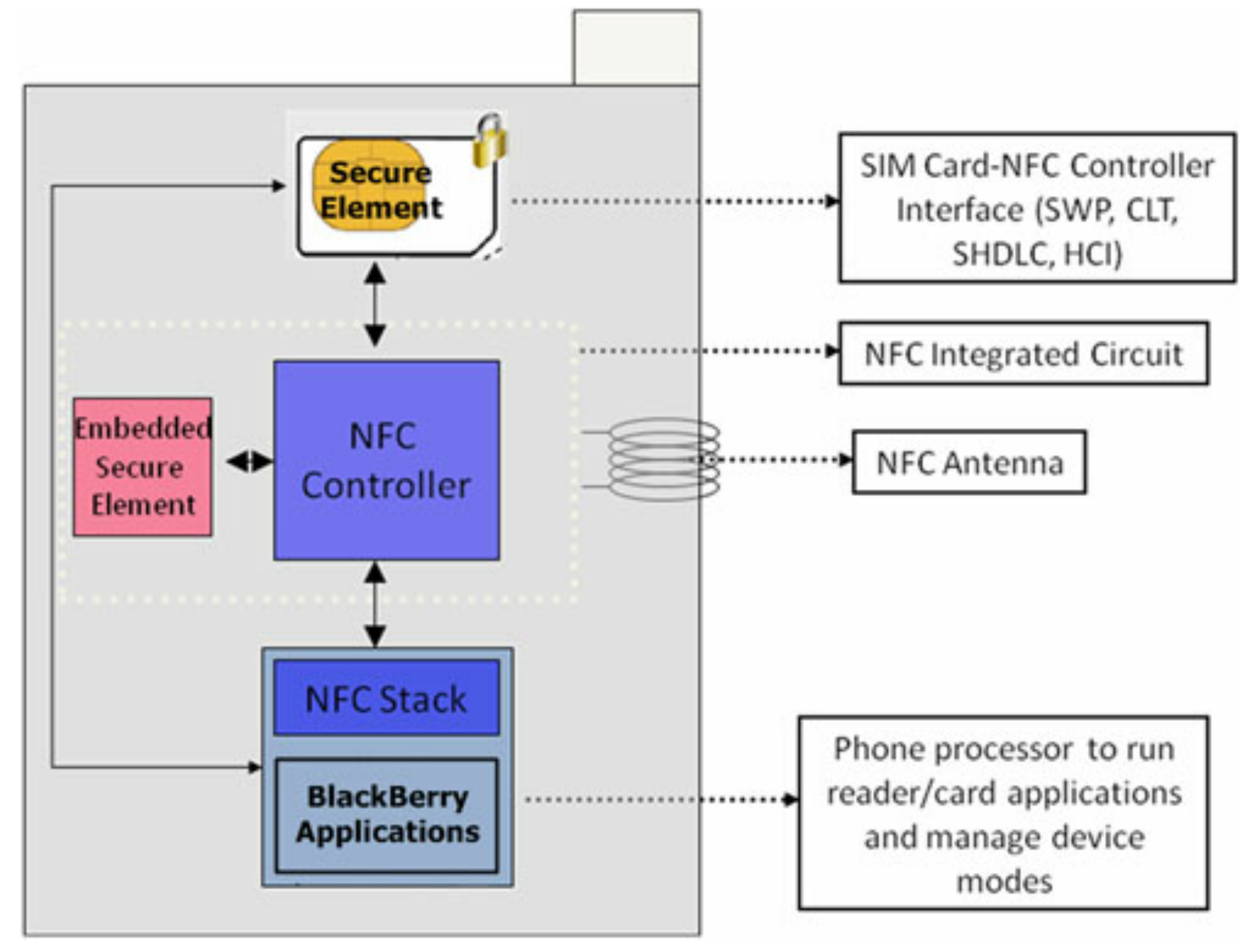
TAG_DISCOVERED

Activities registered to handle TAG_DISCOVERED?

Yes

http://developer.android.com/guide/topics/connectivity/nfc/nfc.html

Blackberry Architecture (Bold 9900)


Secure Element
Embedded Secure Element
NFC Controller
NFC Stack
BlackBerry Applications
SIM Card-NFC Controller Interface (SWP, CLT, SHDLC, HCI)
NFC Integrated Circuit
NFC Antenna
Phone processor to run reader/card applications and manage device modes

Threat Model

- Consider a typical smart phone user with NFC enabled.
- They have a number of popular apps that are commonly running in the background.

Assets – What do they want to protect?

1. Confidentiality - User data and personal information should be protected from disclosure to an attacker.
2. Integrity - An attacker should not be able to use NFC to compromise a victim device or hijack control from it.
3. Availability - An attacker should not be able to use the NFC device to disrupt service to a smart phone user.

Possible Threats?

Threat 1- Browser Launch

Depending on your phone, an NFC tag might direct your phone to a web page without prompt.

Varies by manufacture.

Factors:

- Locked/Unlocked
- Awake/Asleep

Threat 1 - Dangers

- Bandwidth Abuse
- DoS
- Click-jacking
- Browser exploitation
- Privilege escalation
- Remote Code Execution

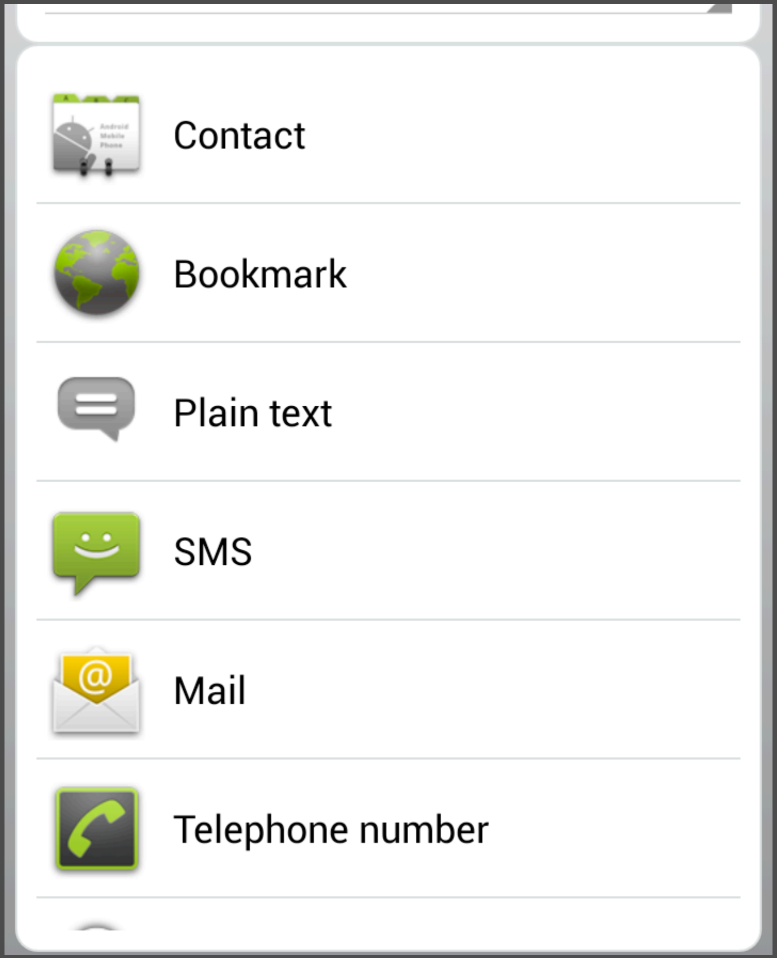
Threat 2 – Bump Attack on Core phone feature

- NFC is woven into many of the core features of a phone.
- I’m sure all of them are perfectly secure.

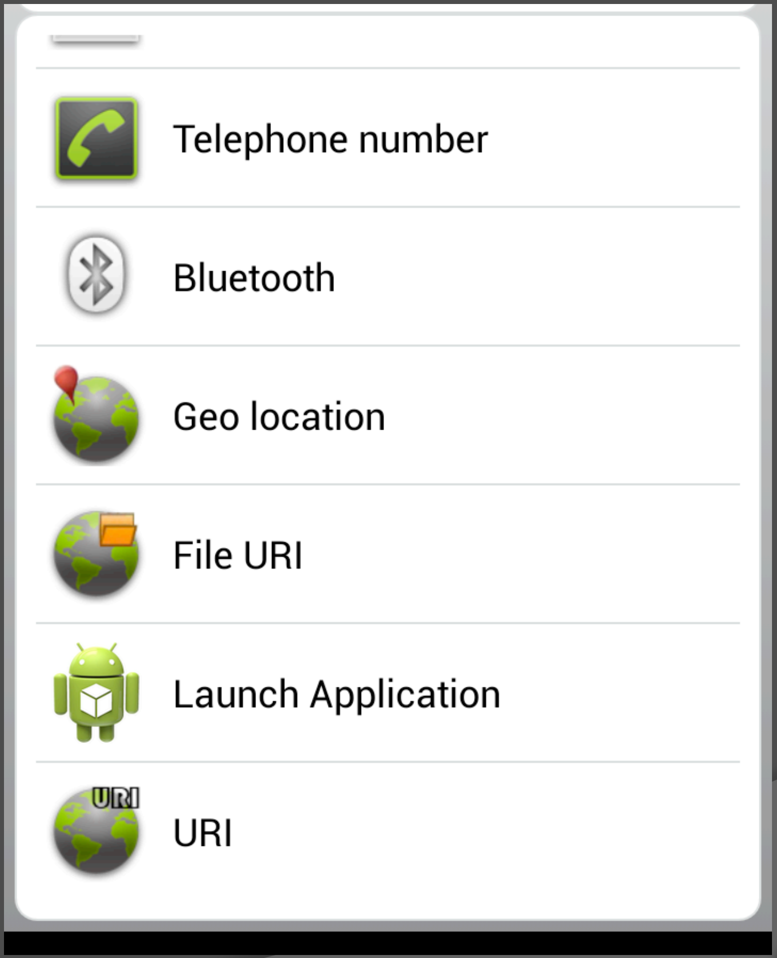
Threat 2 - Dangers

- What we are seeing is that with NFC enabled an attacker has access to a large potential of phone activities.
- NFC is also a relatively new technology that hasn’t had its code hardened by years of attackers finding and fixing weaknesses. Like some of the other code areas.
- In this threat an attacker might exploit potentially weaker code to manipulate the phone into performing some of its primary functions (sending messages, making class, etc)
- How a phone responds to the various tags depends largely on the OS and the manufacturer.

Standard NFC Functions



- Contact
- Bookmark
- Plain text
- SMS
- Mail
- Telephone number



- Telephone number
- Bluetooth
- Geo location
- File URI
- Launch Application
- URI

Threat 3 – App Exploitation

- I’m sure all apps installed on your phone are perfectly secure.
- Consider an NFC bump that launches an app that is already installed on your phone.

Threat 3 – Possible attacks

- Liking / Tweeting / Posting Social Media content on your behalf.
- Launching actions on apps that don’t properly timeout sessions.
- Exploiting an application’s privileges to gain access to other phone features.

Observations

- The NFC Threat Landscape is very very large!
- Device security varies drastically by manufacture and by OS (and version).
- Security vs. ease of use is a very common trade off when pushing a new technology.

Mitigating the Risks

- Turn NFC off when its not in use. “Always on” is not a good strategy.
- Prompt users for actions before they are taken.
- Limit the NFC handler’s reach into core phone features.

Future Work – What we're working on.

- Extending the NFC range
- Exploiting Point of Sale systems
- Remote Code Execution (Holy Grail)
- Browser Exploitation
- Fuzzing / Proxying NFC
- Bypassing Card Level Access Control

Thank you

Security Compass

Geoffrey Vaughan

GeoffV@SecurityCompass.com

@MrVaughan