PacSec
November 2015

Blue-Toot

or

”My Android Had a Little Accident...”

Adam “Major Malfunction” Laurie

Who are we?

- Aperture labs: www.aperturelabs.com

Who are we?

- Aperture labs: www.aperturelabs.com

Who are we?

- Aperture labs: www.aperturelabs.com

Who are we?

- Aperture labs: www.aperturelabs.com

Who are we?

- Zac Franken
  - Chip Monkey
    - Scary Chemicals
    - Bad Smells

Who are we?

- Adam Laurie
  - Code Monkey
    - Convert scary analogue Magic Moonbeams to lovely Digital Bits & Bytes

Aperture Labs

www.aperturelabs.com

What?

What?

- Bounty programs
  - Pwn2own
    - Mobile Pwn2own
- Android NFC
- Android Bluetooth

Android + NFC = Blue-toot

Android + NFC = Blue-toot

Android + NFC = Blue-toot

Android + NFC = Blue-toot

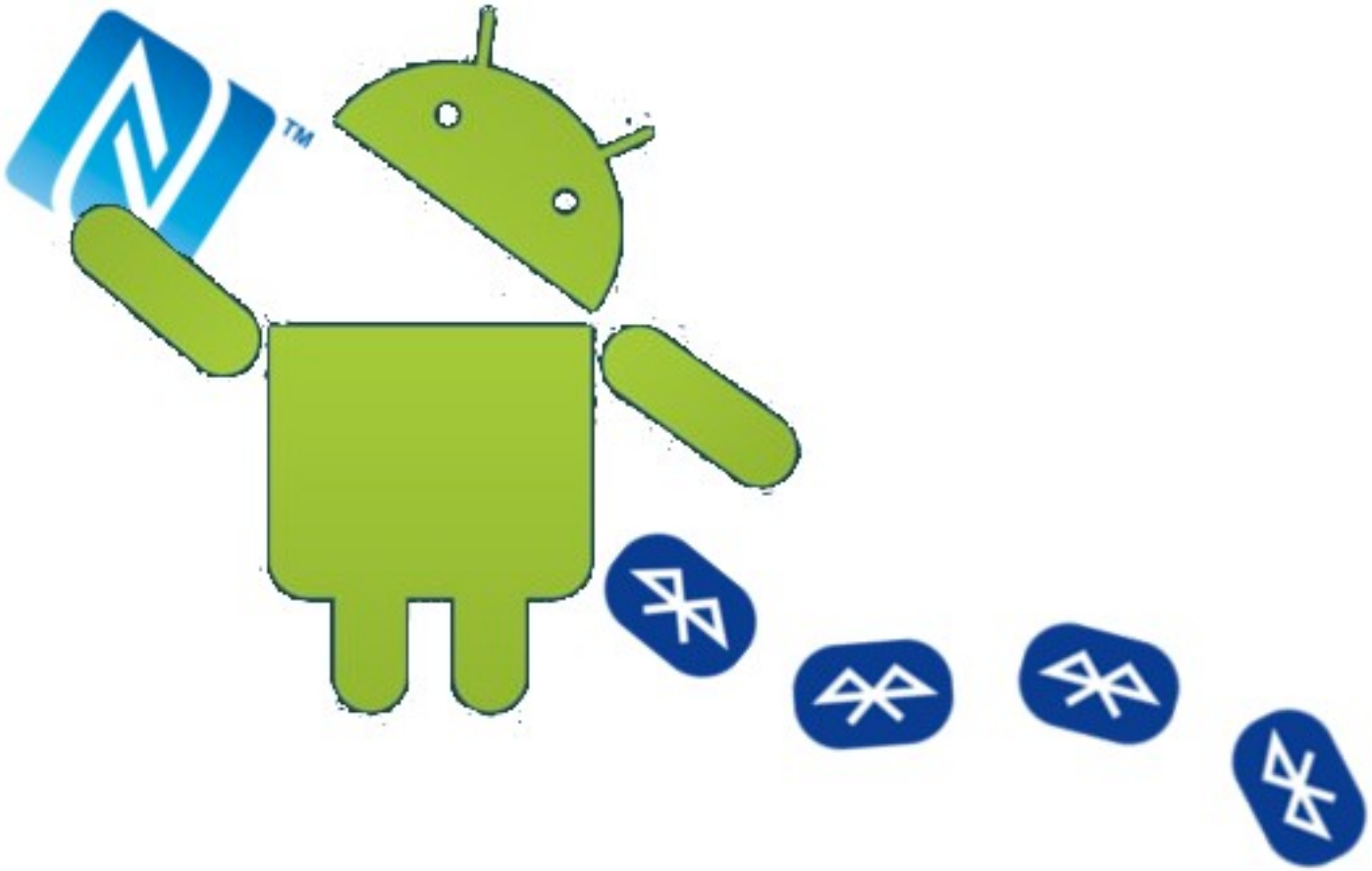
Android + NFC = Blue-toot

Android + NFC = Blue-toot

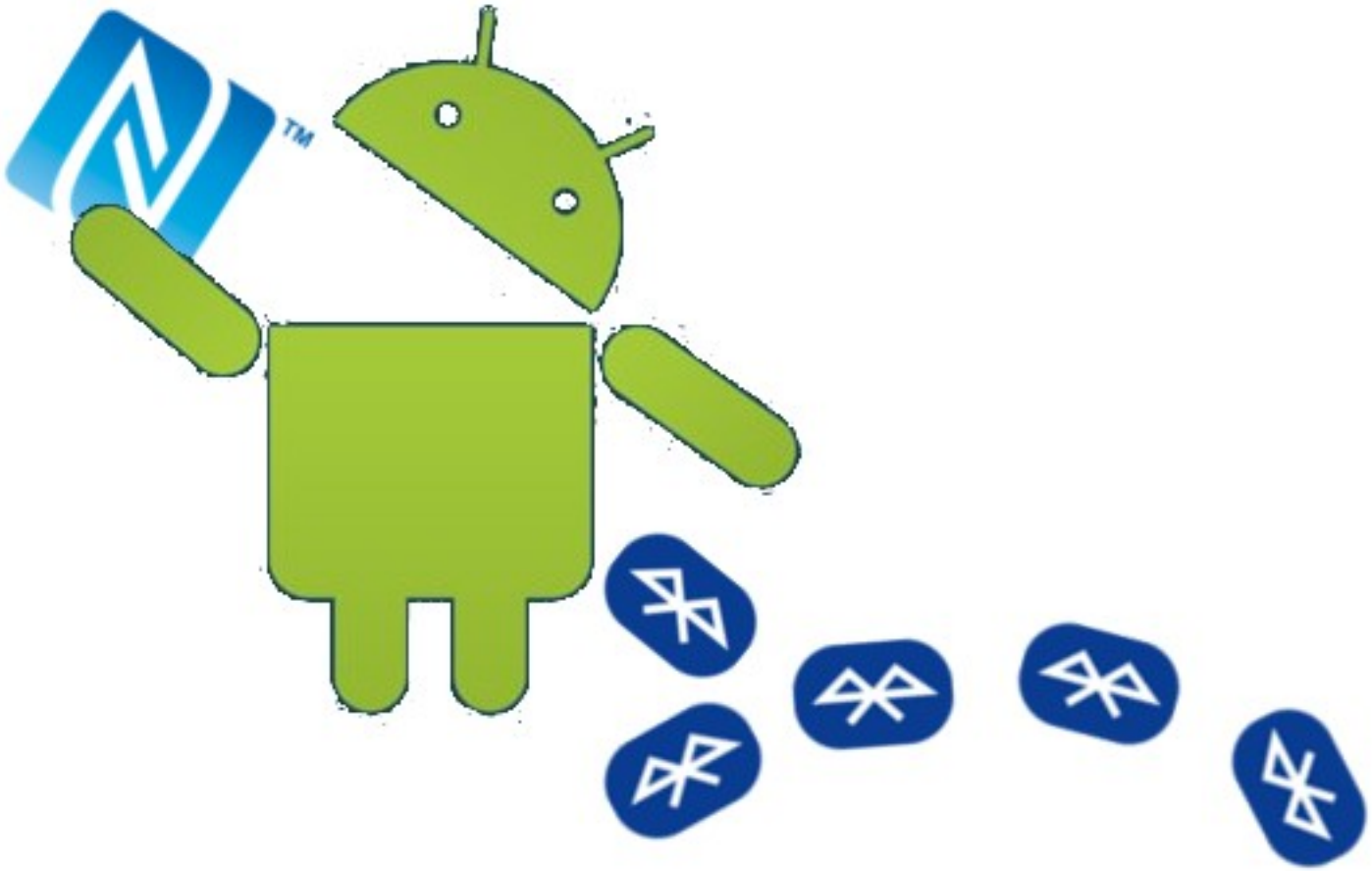
Android + NFC = Blue-toot

Android + NFC = Blue-toot

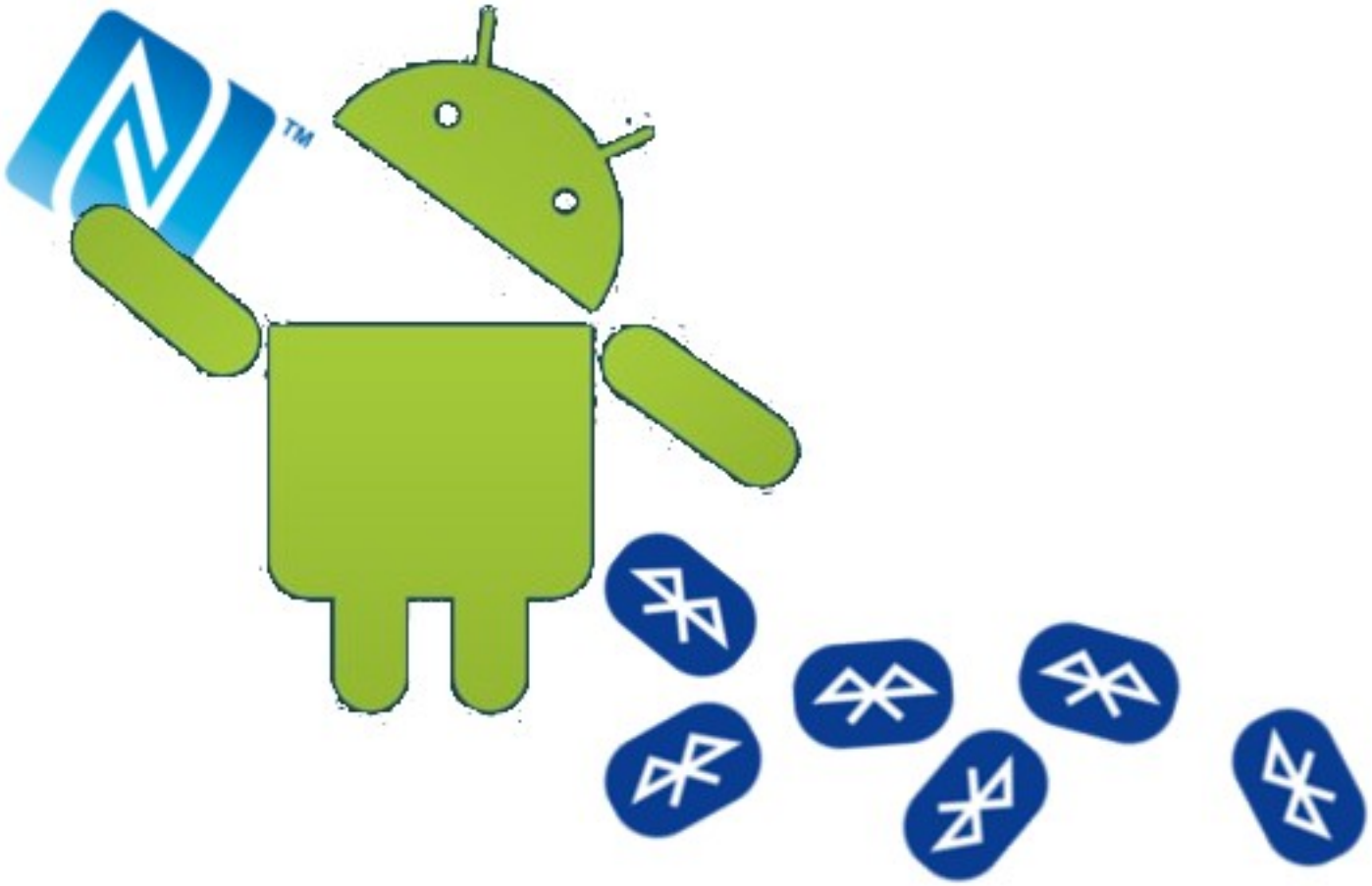
Android + NFC = Blue-toot



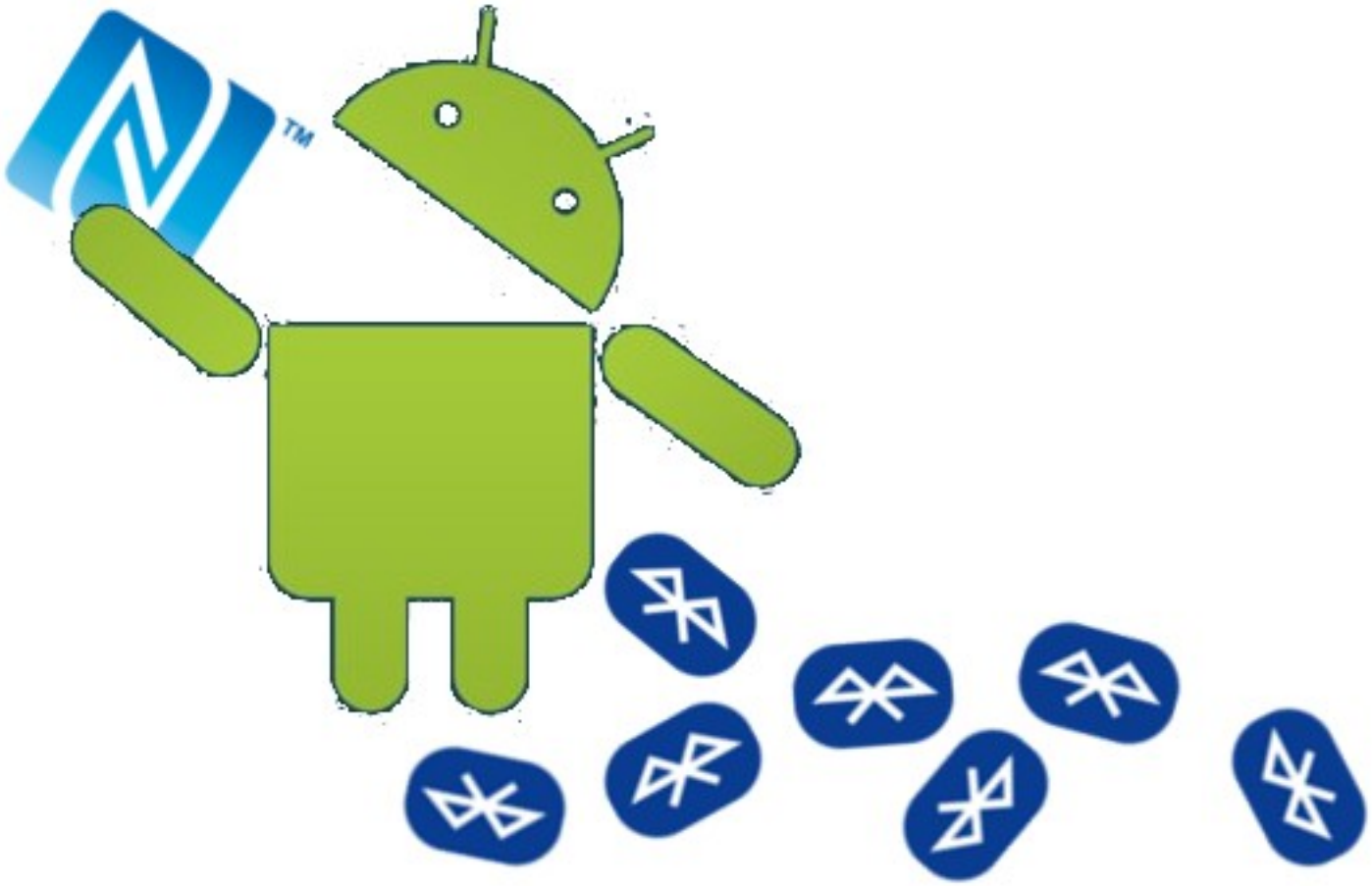
Android + NFC = Blue-toot



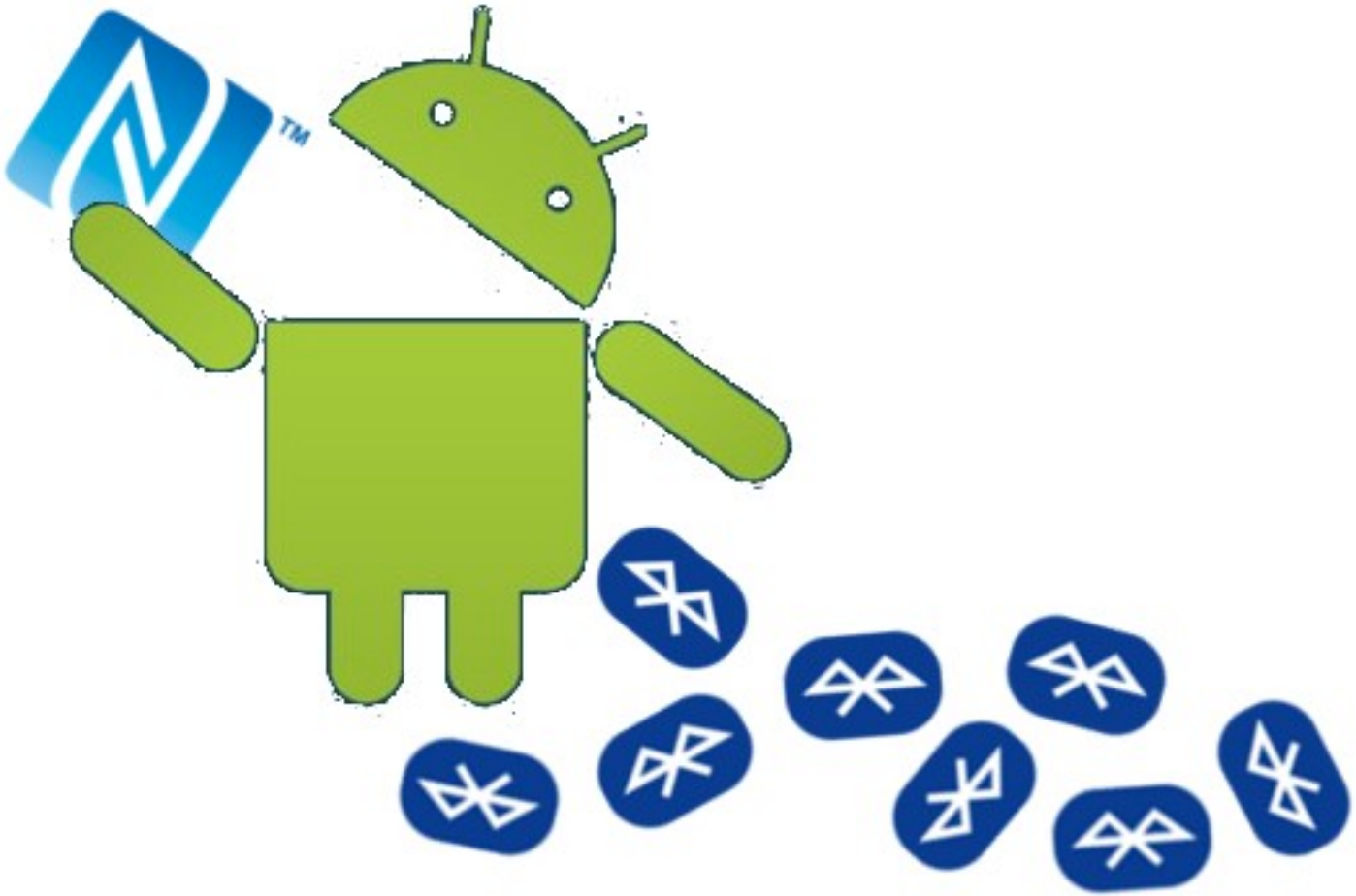
Android + NFC = Blue-toot



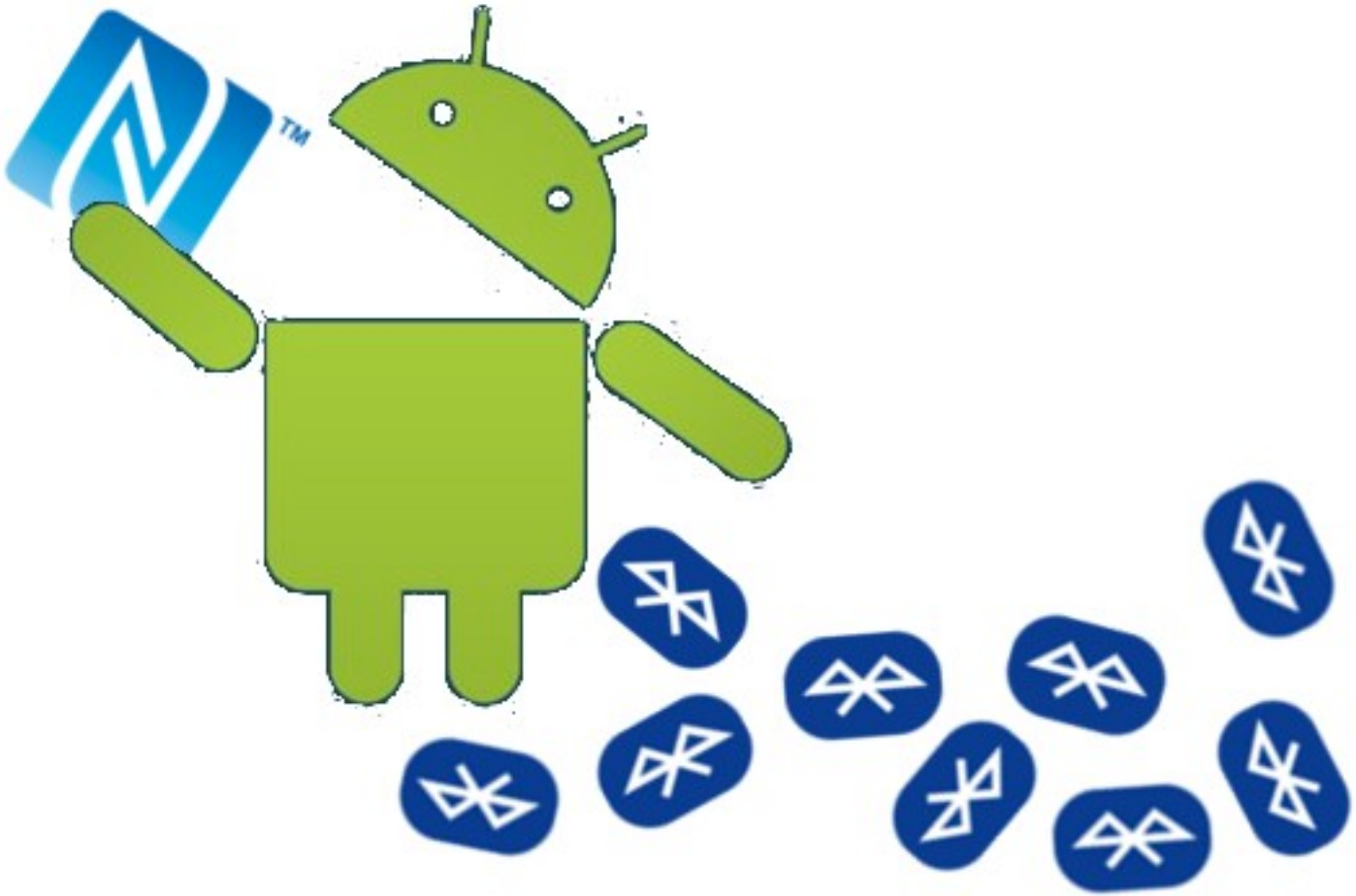
Android + NFC = Blue-toot



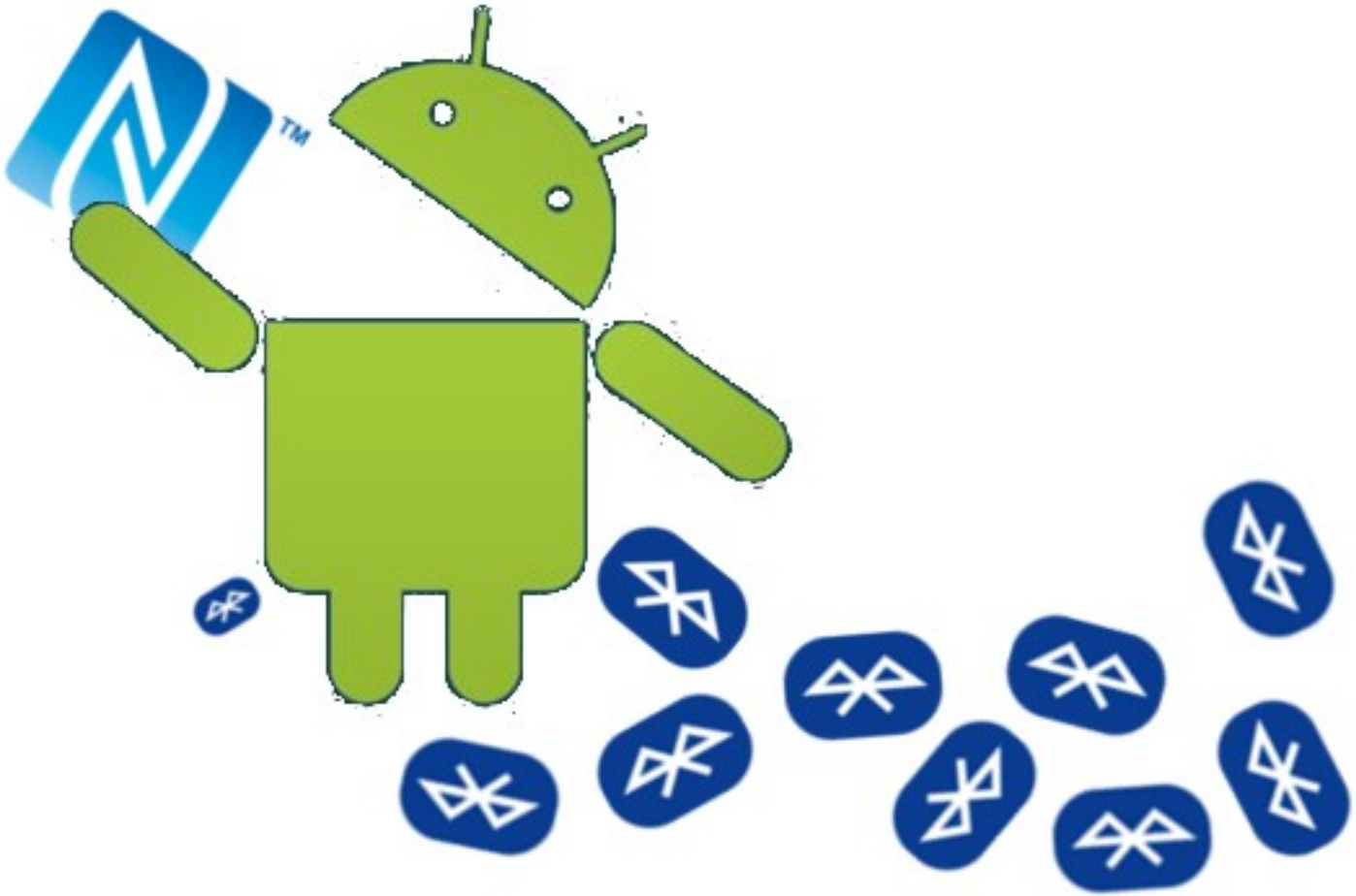
Android + NFC = Blue-toot



Android + NFC = Blue-toot



Android + NFC = Blue-toot



Why?

- Mobile pwn2own 2013
  - Short Distance ($50,000):
    - Bluetooth, or Wi-Fi, or NFC

Why?

- Mobile pwn2own 2013
  - Short Distance ($50,000):
    - Bluetooth, or Wi-Fi, or NFC

- Pwned in departure lounge on the way home...

Why?

- Mobile pwn2own 2013
  - Short Distance ($50,000):
    - Bluetooth, or Wi-Fi, or NFC

- Pwned in departure lounge on the way home...

Why?

- Mobile pwn2own 2013
  - Short Distance ($50,000):
    - Bluetooth, or Wi-Fi, or NFC

- Pwned in departure lounge on the way home...
    - Not. Too late...

Why?

- Mobile pwn2own 2014

  "You are welcome to hold your vuln for Mobile Pwn2Own 2014 or to submit now to the ZDI for consideration as a regular case." - ZDI

Bounties

Bounties

- The good:
  - Reward **anyone** for finding bugs
  - Research not driven by company

Bounties

- The good:
  - Reward **anyone** for finding bugs
  - Research not driven by company
  - Big bucks - **$75,000** top prize in 2014

Bounties

- The bad:
  - Research paid only on success
    - Cheaper for vendor
    - More expensive for researcher
  - No free market – vendor sets value
  - Selling vulns feels wrong!
  - Saving vulns for bigger payoff

Bounties

- The ugly:
  - “mobile” pwn2own not so mobile!
    - WiFi / NFC / Bluetooth category must be completed in RF shielded cage
      - No phone network!
        - Jump through hoops to “win”

Bounties

- The ugly:
  - "winning" may be decided by coin toss
    - Competition is over after 1st win
    - 5 entries in 2014

Bounties

- The ugly:
  - "winning" may be decided by coin toss
    - Competition is over after 1st win
    - 5 entries in 2014
      - Subsequent winners given ½ prize

Bounties

- The ugly:
  - Next day vuln “worthless”
    - Unless you sell it on the black market...
      - Errmmm... What's the difference?

Bounties

- The ugly:
  - Less secure by definition:
    - Not all security companies will have access to all vulns
    - You are only as secure as the group covered by your preferred vendor

Bounties

- The ugly:
  - **Wassenaar**

Dragos tweeted on Sept 1st:

"The first bona fide casualty of the Wassenaar changes: HP won't be doing PWN2OWN Mobile in Japan due to new export restirctions."

The Hack

- NFC
  - NDEF
    - SmartPoster
    - WiFi Config
    - Bluetooth handover

The Hack

- NFC
  - NDEF
    - Bluetooth handover
      - Switches on Bluetooth
      - Target “open” service
        - Obex push
      - Send HCI command on established connection

The Hack

- Bluetooth
  - Send HCI command on established connection
    - Connection is always encrypted
    - Either side can request key change
      - Push new key

The Hack

- Bluetooth
  - Push new key
    - New key now in target keysfile
    - Restart Bluetooth stack on target
    - Key found in keysfile at startup == TRUST!

The Hack

- Bluetooth
  - Push new key
    - New key now in target keysfile
    - Restart Bluetooth stack on target
    - Key found in keysfile at startup == TRUST!

The Demo

- This is where it all goes horribly wrong...