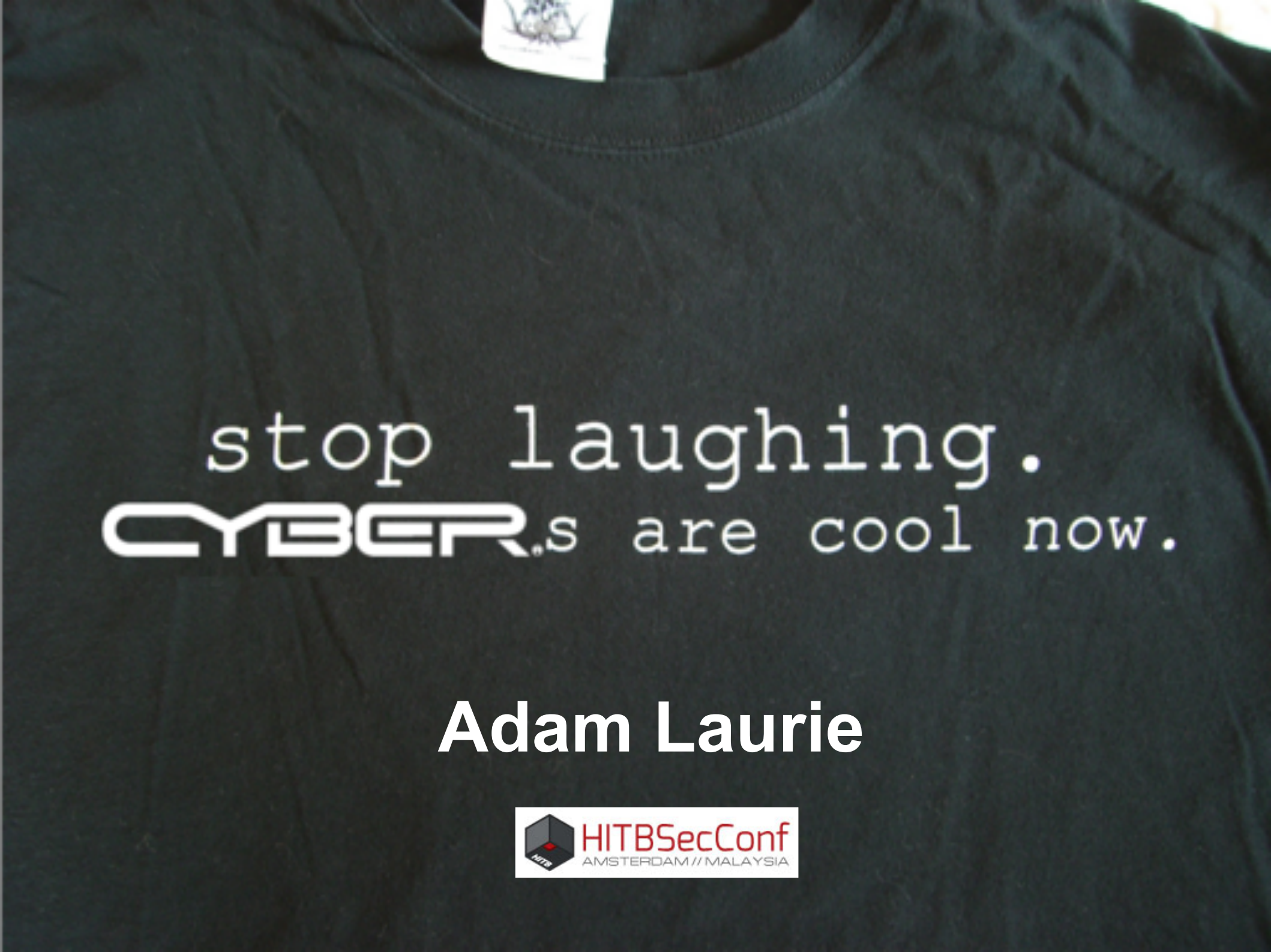
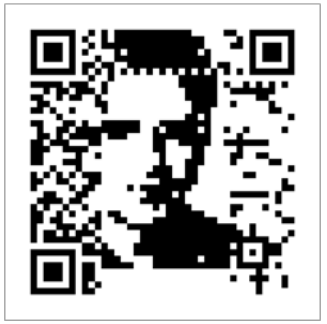


Adam Laurie

HITBSecConf
AMSTERDAM // MALAYSIA



Who Am I?

- White Hat Hacker
- Open Source Advocate
- DEFCON Goon
  - Major Malfunction
- RFIDIOt

Old Skool

- I’ve been doing this for 20 years now…
- WiFi, Bluetooth, Magstripe, Satellite, RKE (Remote Key Entry), Chip & PIN, RFID/NFC, DVB-T, Zigbee

Back in the day...

- What has changed
  - Not all hackers are the bad guy
  - Support - somewhere to report problems
  - Not getting arrested for reporting
  - Not getting sacked for going to “hacker” conferences

Suspect Nation 2006 – passports, bluetooth and RFID chips

The Hack

- Passport
- Cloning now trivial
- Download international standard
- Some Python code
- Full data recovery from MRTD
- Certificates
- Signing data
- Self-sign FTW!
- PKD – Public Key Directory
(Not all countries signed up)

The Hack

- RFID
- Multiple tools now available
- RFIDler
- RFIDIOt
- Proxmark3
- libnfc
- Multi-personality blanks
- Q5
- T55x7
- Hitag2

The Hack

- Bluetooth
- Open RFCOM channel
- Allows full access to:
- SMS
- Phonebook
- Calendar
- AT Commands
-

The Hack

- Bluetooth
- Open RFCOM channel
- Allows full access to:
- SMS
- Intercept and reply to confirmation message for tracking service signup
-

The Hack

- Bluetooth
- Open RFCOM channel
- Allows full access to:
- Calendar
- Learn about meetings / movements

The Hack

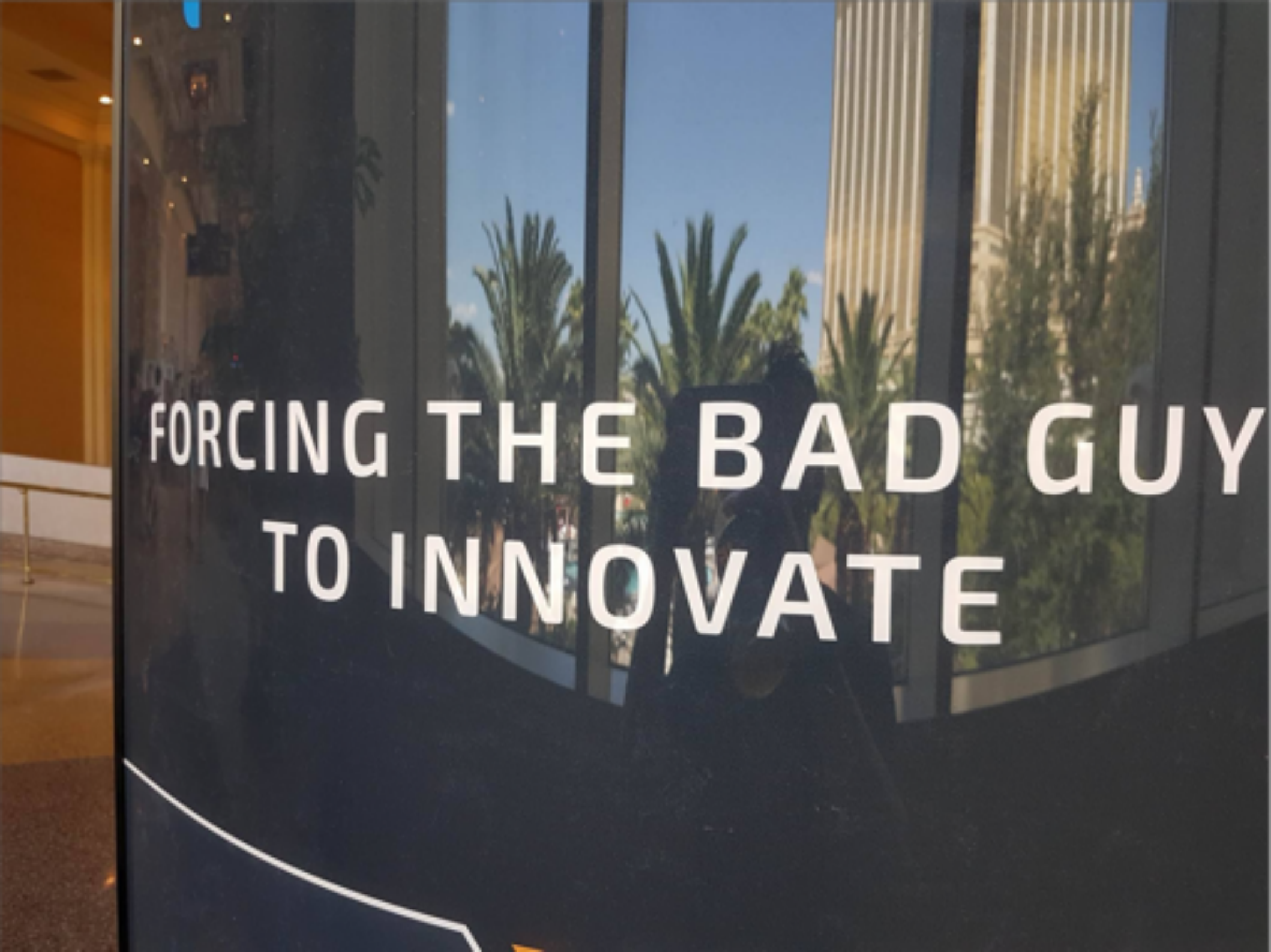
- Bluetooth
- Open RFCOM channel
- Allows full access to:
- Phonebook
- Learn contact details of 3rd parties
-

The Hack

- Bluetooth
- Open RFCOM channel
- Allows full access to:
- AT Commands
- Initiate callback (start ‘bug’)
-

Industry response

- Initial scepticism - ‘experts’ refuting our findings
- Nokia & Sony Ericsson took 18 months to release firmware fix.
- Bluetooth SIG
  - Unplugfests
    - All problems ‘solved’ (!)

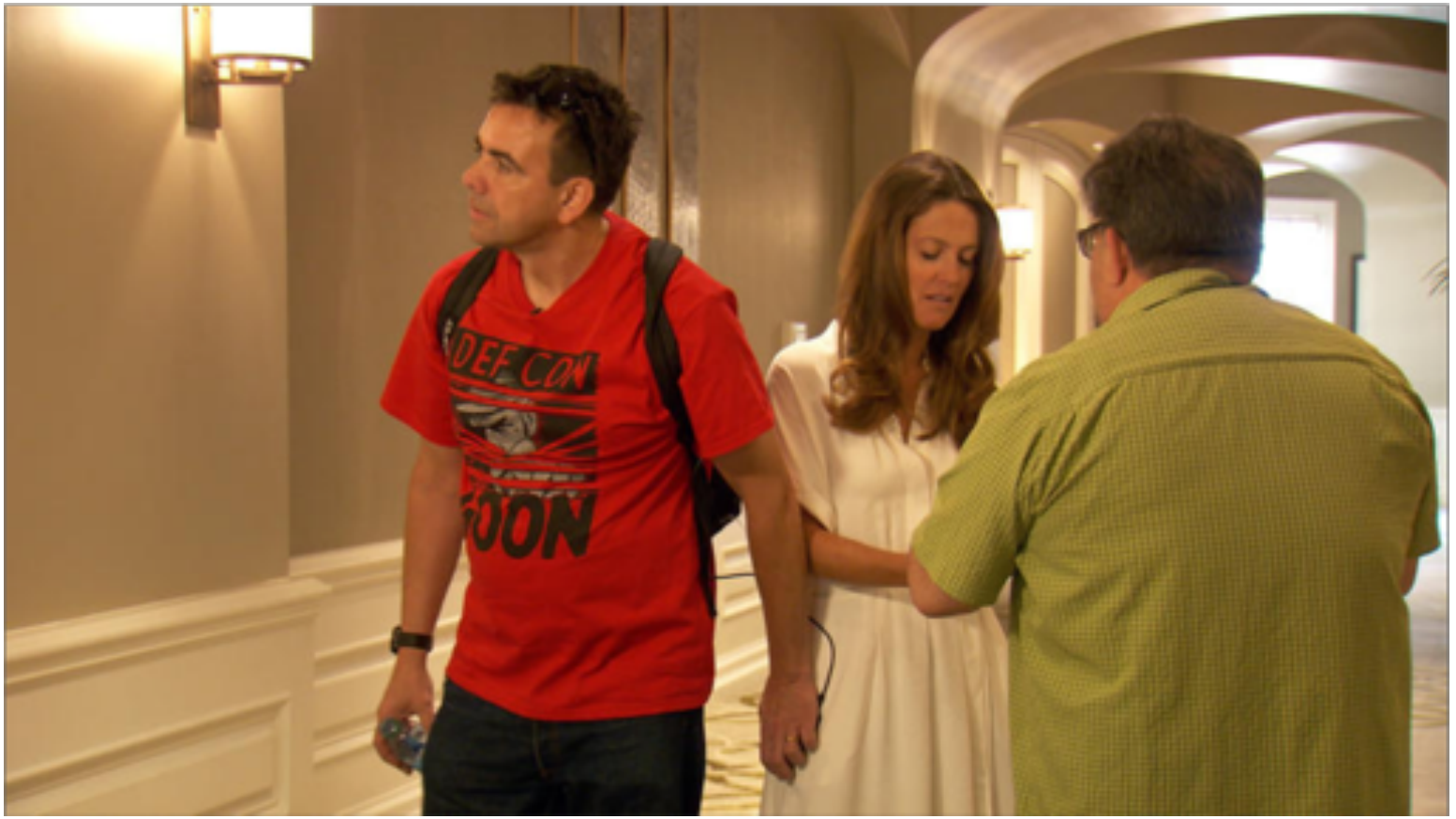

FORCING THE BAD GUY
TO INNOVATE

TV vs Reality

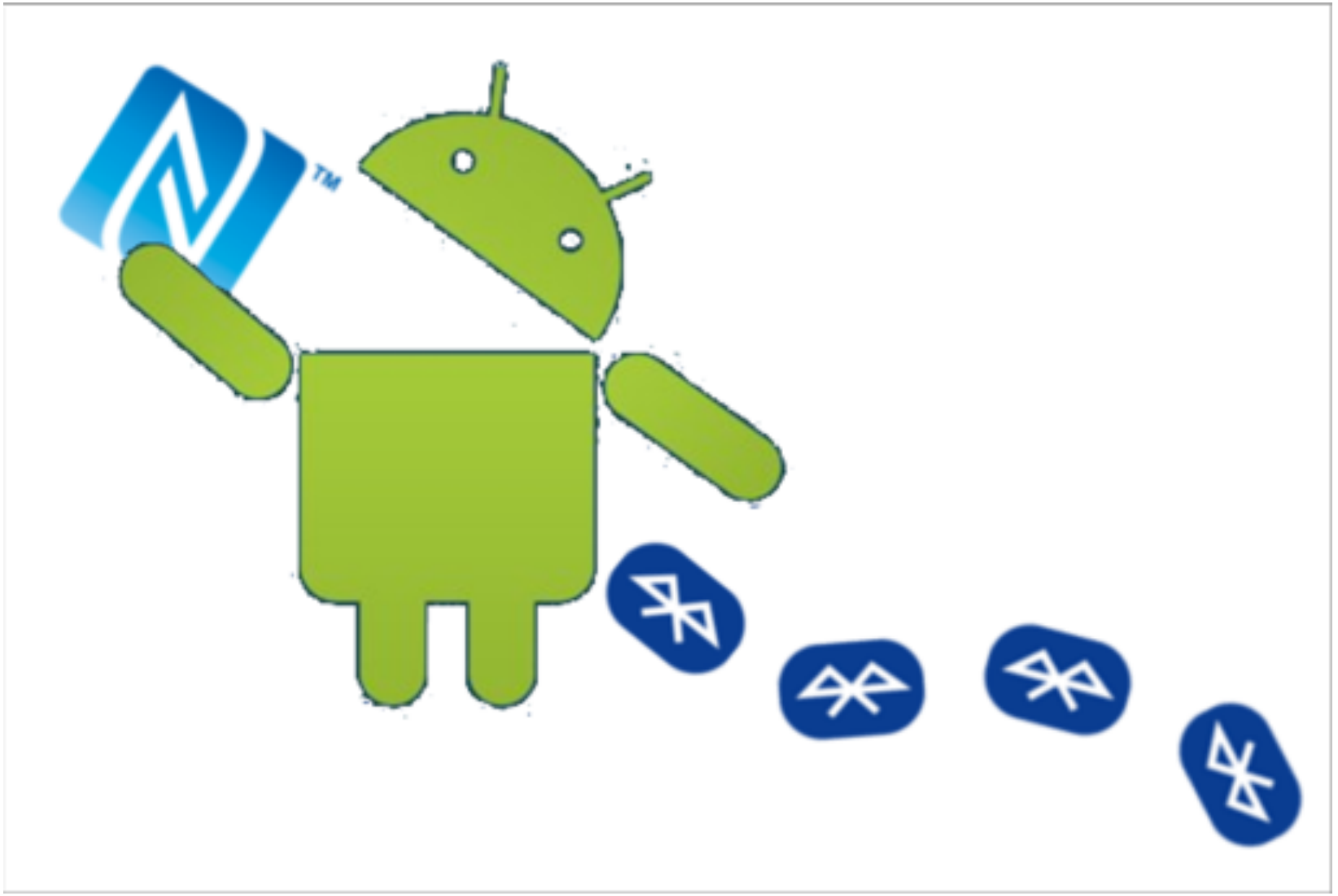
- Same problem, 14 years later...

60 minutes – pairing phone

- https://www.cbsnews.com/news/60-minutes-overtime-how-strangers-can-hack-the-phone-in-your-pocket/



Android + NFC = Blue-toot



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
- Cancel Bluetooth handover
- Key found in keysfile at startup == TRUST!
- P0wned!

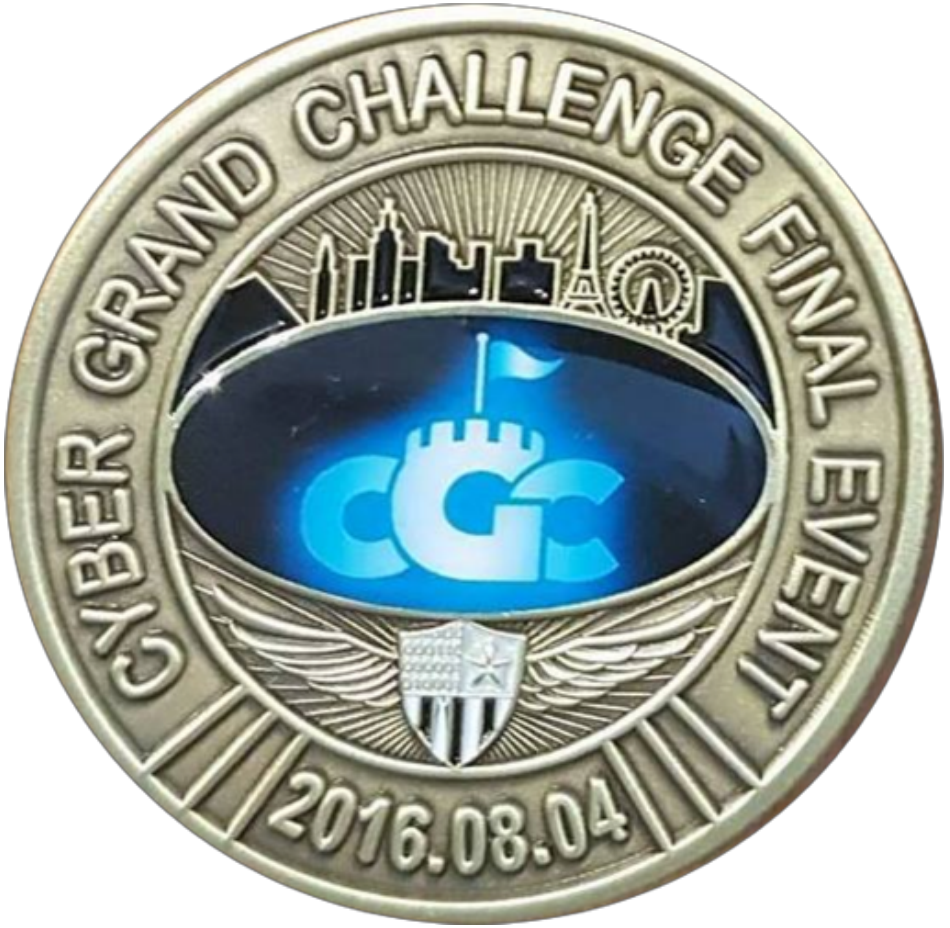
The Hack

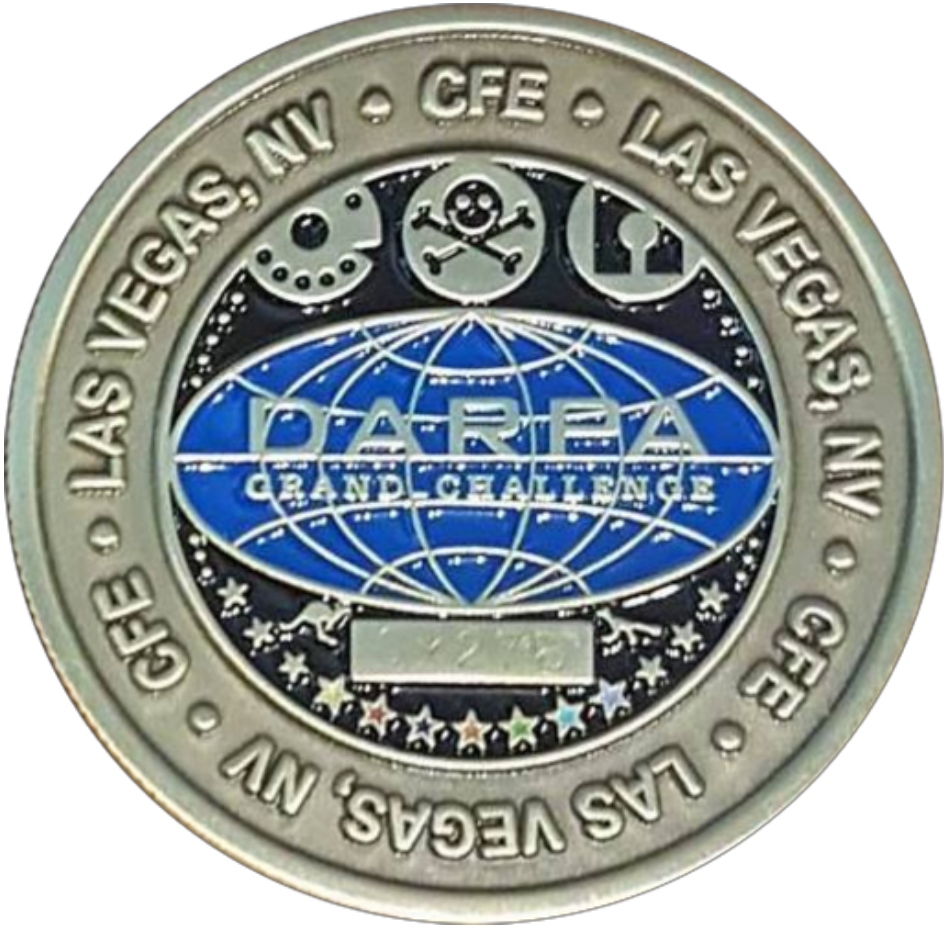
- Bluetooth
- P0wned!
- Access to AT commands

Industry Response

- Encouraged to enter bug bounty competition...
- Come to Tokyo, win big!

Come to Vegas, win big!





The End?

- WiFi, Bluetooth, Magstripe, RKE (Remote Key Entry), Satellite, Chip & PIN, RFID/NFC, DVB-T, Zigbee
- How many of these technologies with published hacks are now considered ‘secure’?