ProCheckUp

Don’t judge hardware…

by it’s cover

Can you tell which is the bug?

ProCheckUp

Bug Sweeping Like A Boss

Richard Brain

Technical Director Procheckup

ProCheckUp

This session

1. Bug Sweeping Gear: a quick intro
2. Bugs in the wild: real cases
3. Play time: try it out!

ProCheckUp

. 1 .

Bug Sweeping Gear: a quick intro

ProCheckUp

Commercial-RF & GSM bugs

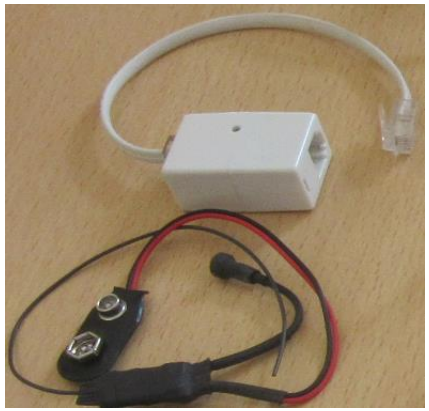
- Come in all shapes & sizes
- Stand alone vs embedded
- Detected by
  - Material
  - Signal
  - Sight

ProCheckUp

Broadband detector

- **Broadband nearfield detector**

Detects RF transmissions to 12GHz



- **USAGE**

  Detect and locate transmitted signals from RF devices

Left: RF bugs with microphones

ProCheckUp

Non Linear Junction Detector (NLJD)

- **MAIN FUNCTION**

Detects electronic devices (regardless if on or off)

Above: bugs embedded

- **USAGE**
  - Illuminates area with hi-frequency RF, semi conductor devices with transistor p-n junction due to nature of junction, energy retransmitted at 2nd harmonic

ProCheckUp

Spectrum Analyser

- **MAIN FUNCTION**

Looks for misuse of the RF spectrum

Above: Video/GSM bugs

- **USAGE**
  - Store signal and trace databases, compares spectrum (including RF mapping)
  - Automatic Threat Correlation– correlates the demodulated audio of a received signal to the ambient noises of an environment

ProCheckUp

Physical search

- Most important, though time consuming!

- **Video Pole Camera**
  - Inspect drop ceilings
  - behind immovable objects
  - Around corners
  - Difficult to reach areas

- **X-Ray Machine**
  - Check inside objects & walls
  - Most thorough method
  - Highly dangerous!

ProCheckUp

. 2 .

Bugs in the Wild: Real Stories

ProCheckUp

Bugs in the… communication

Man in the middle attacks (MITM) – intercepts communication between 2 systems

LINKS

https://www.owasp.org/index.php/Man-in-the-middle_attack

http://www.scmagazine.com/advisory-warns-preinstalled-lenovo-app-could-lead-to-mitm-attacks/article/500553/

ProCheckUp

Bugs in the… ATM

By Laura Northrup May 30, 2014

Did you think that tiny Bluetooth ATM skimmers were a terrifying prospect? Two men in Macau are accused of using long strips that look like circuit boards to infect ATMs and digitally extract customers' card numbers and PINs.

Krebs on Security is the place to learn about scams like these, explaining both the crimes and how they work. In this case, police say that the two suspects aren't from Macau (a Chinese territory west of Hong Kong) but are from Ukraine. They stole $100,000 by corrupting the automatic tellers.

They allegedly used these green objects, which were connected to a laptop, then inserted them in the card slot. This is the best picture that we have of them so far, but the strips are about as wide as a credit card and maybe five times as long. They resemble a circuit board, but no details on exactly how they were constructed have been made public yet. Obviously.

According to a source at the bank in question, inserting the circuit board card thingy caused the machines to crash and restart, then run normally while slurping up card number and PIN data f… customers. The government says that the two suspects returned to the ATM… loot, extracting it from the machine using the same green st…

LINKS

http://krebsonsecurity.com/2014/05/thieves-planted-malware-to-hack-atms/

IMPACT: $100,000

ProCheckUp

Bugs in the… USB

- Installs malware to enable spying or MITM attacks

LINKS

http://arstechnica.com/information-technology/2015/01/playing-nsa-hardware-hackers-build-usb-cable-that-can-attack/

http://motherboard.vice.com/read/michael-ossmann-and-the-nsa-playset

http://www.dailymail.co.uk/sciencetech/article-2920419/When-USBs-attack-Hackers-create-covert-spy-plug-inspired-NSA-s-Cottonmouth-surveillance-kit.html

Above: USB Bug

ProCheckUp

Bugs in the… Products

LINKS

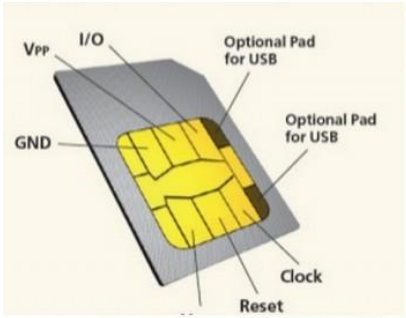
http://www.popsci.com/article/gadgets/china-spying-russia-bugged-clothing-irons

http://gizmodo.com/5897493/all-chinese-made-electronics-could-be-bugged-says-former-head-of-us-counterterrorism

ProCheckUp

Bugs in the… SIM

- Software and SIM can both be bugged



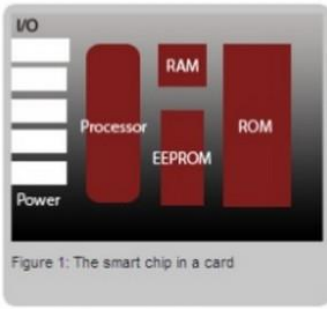
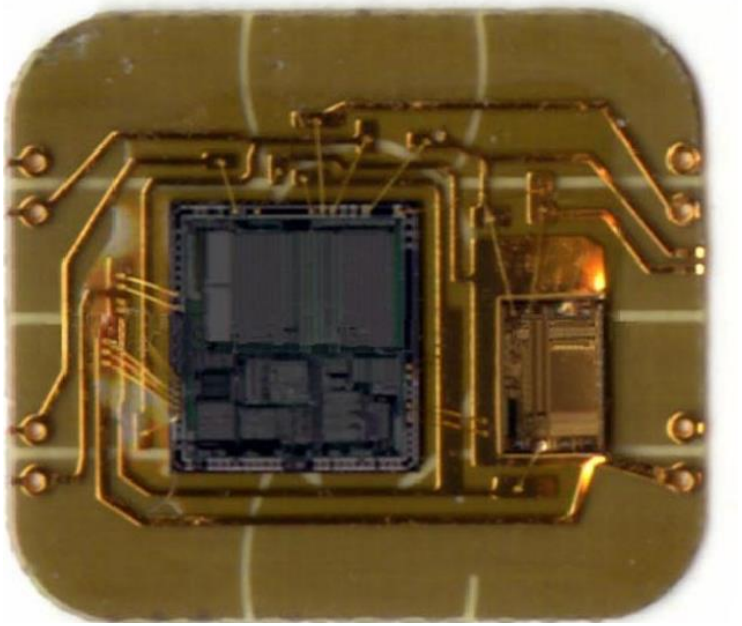


Figure 1: The smart chip in a card

LINKS

http://www.slideshare.net/silpol/us-13nohlrootingsimcardsslides

http://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/#7506f6c74e39



ProCheckUp

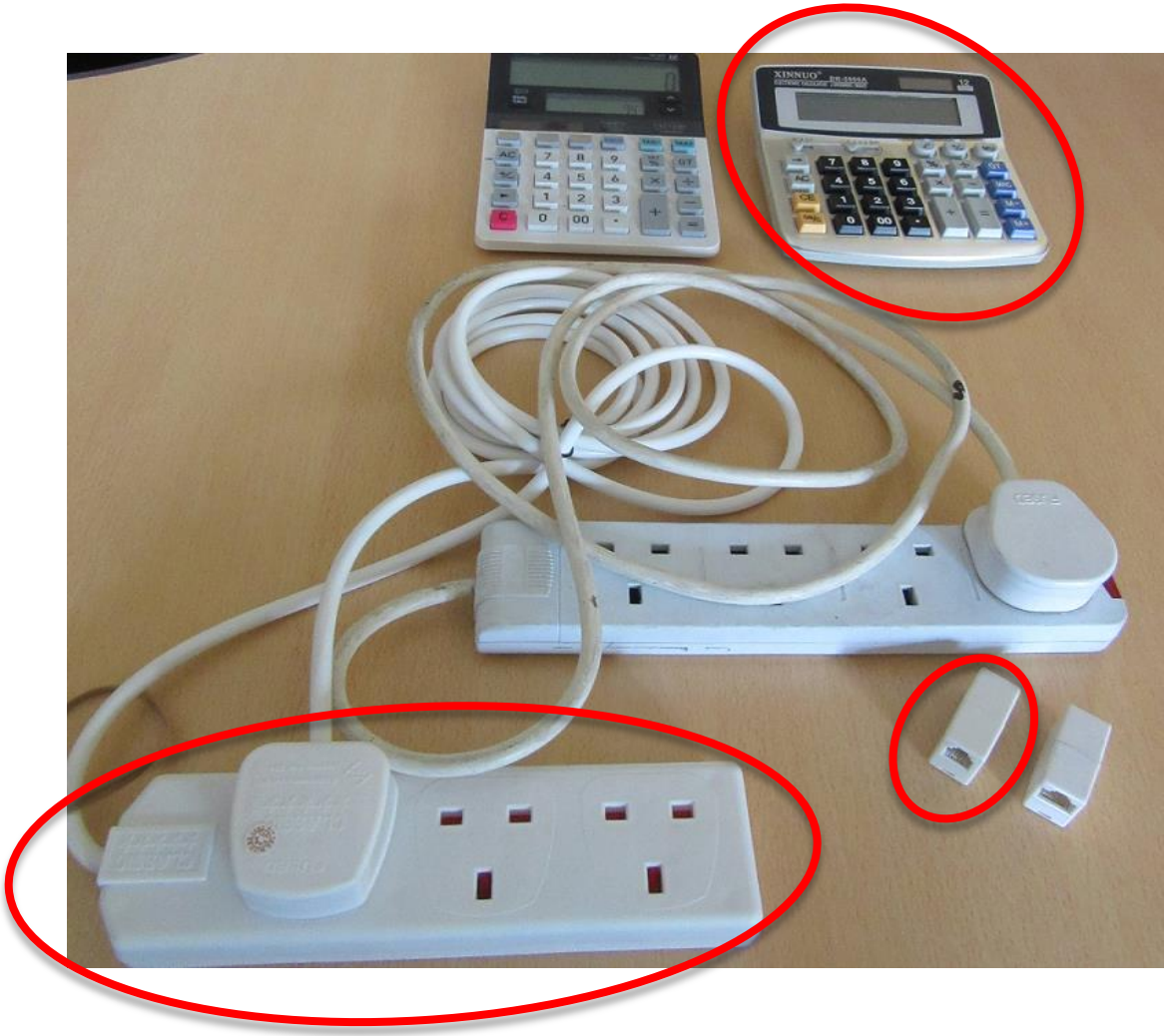
. 3 .

Bug Sweeping Gear: your turn!

ProCheckUp

Did you get it right?

- Don’t get fooled by quality
- Look for holes (most likely microphone)
- Screened bugs can evade tools



ProCheckUp

www.procheckup.com

ProCheckUp are a CHECK, CREST, PCI and Cyber Essentials Plus accredited company with vast wealth of experience in security testing and consulting. Our bespoke services are delivered to the world's leading finance, banking and insurance organisations, UK Central and Local Government authorities and FTSE 100 companies.