HACKING EXPOSED EMBEDDED – THE DARK WORLD OF TINY SYSTEMS AND BIG HACKS

Stuart McClure
McAfee
An Intel Company

Session ID: EXP-302
Session Classification: Intermediate

RSA CONFERENCE 2012

Embedded

- Chips are Everywhere
  - Full OS
- Mobile Payments
- Smart Phones

The Hacks

- NFC
- Android zero shell
- iJacking
- Rogue mouse

Near Field Communications (NFC)

NFC hijacking

- NFC is a technology built into modern phones
- Active (Phone)/Passive(tag)
  - Similar to RFID
- Active (Phone)/Active(POS)
  - Visa and Mastercard touch payment systems
- A/P used in Europe for donations and other simple payments
  - Real world attack that is happening today

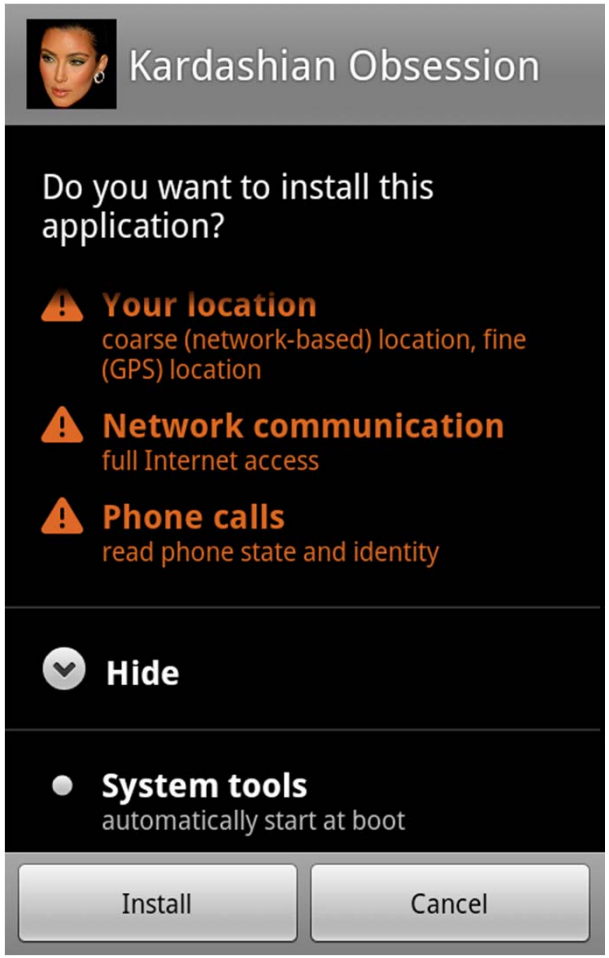
NFC

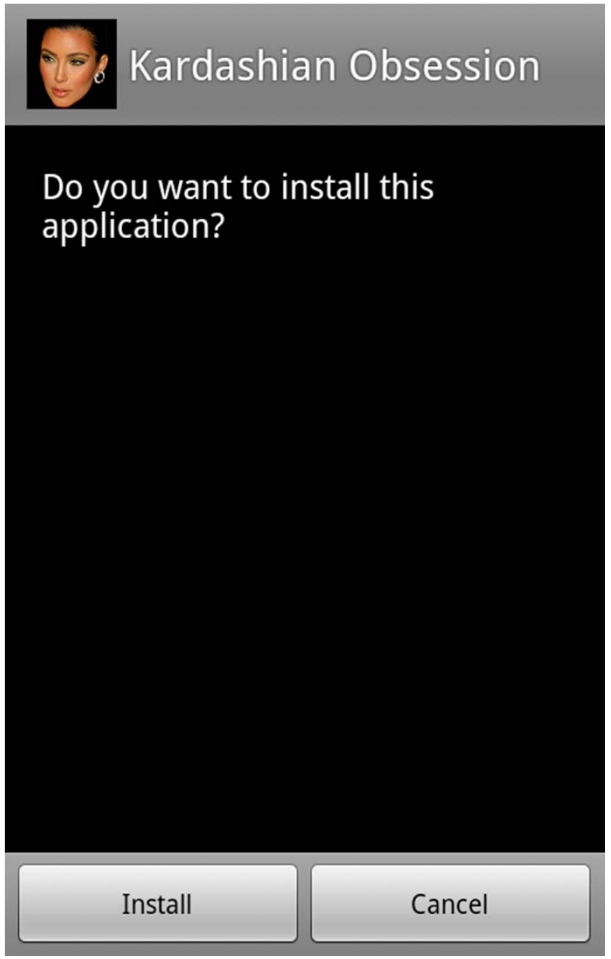
- Explain Donation Poster
- Use Poster to donate
- Hijack Poster
- Steal Donation/Credit Card

Android Zero Shell

Android Zero Shell

Which App is more Safe?



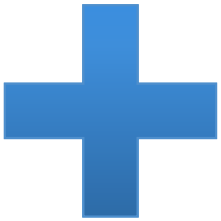


Android Zero Shell

- Install App
- Introduce Command and Control
- Demo the Zero Shell
- Show App Exploitation to get additional Privs

iJacking

iJacking



iPwn your iDevice

iJacking

- Show iPad connecting to Wifi
- Use ipad to log into gmail
- Show exploit on iPad
- Send APT/VNC
- Introduce C&C
  - Show Map
  - Dump Keychain
  - Show Reverse Shell

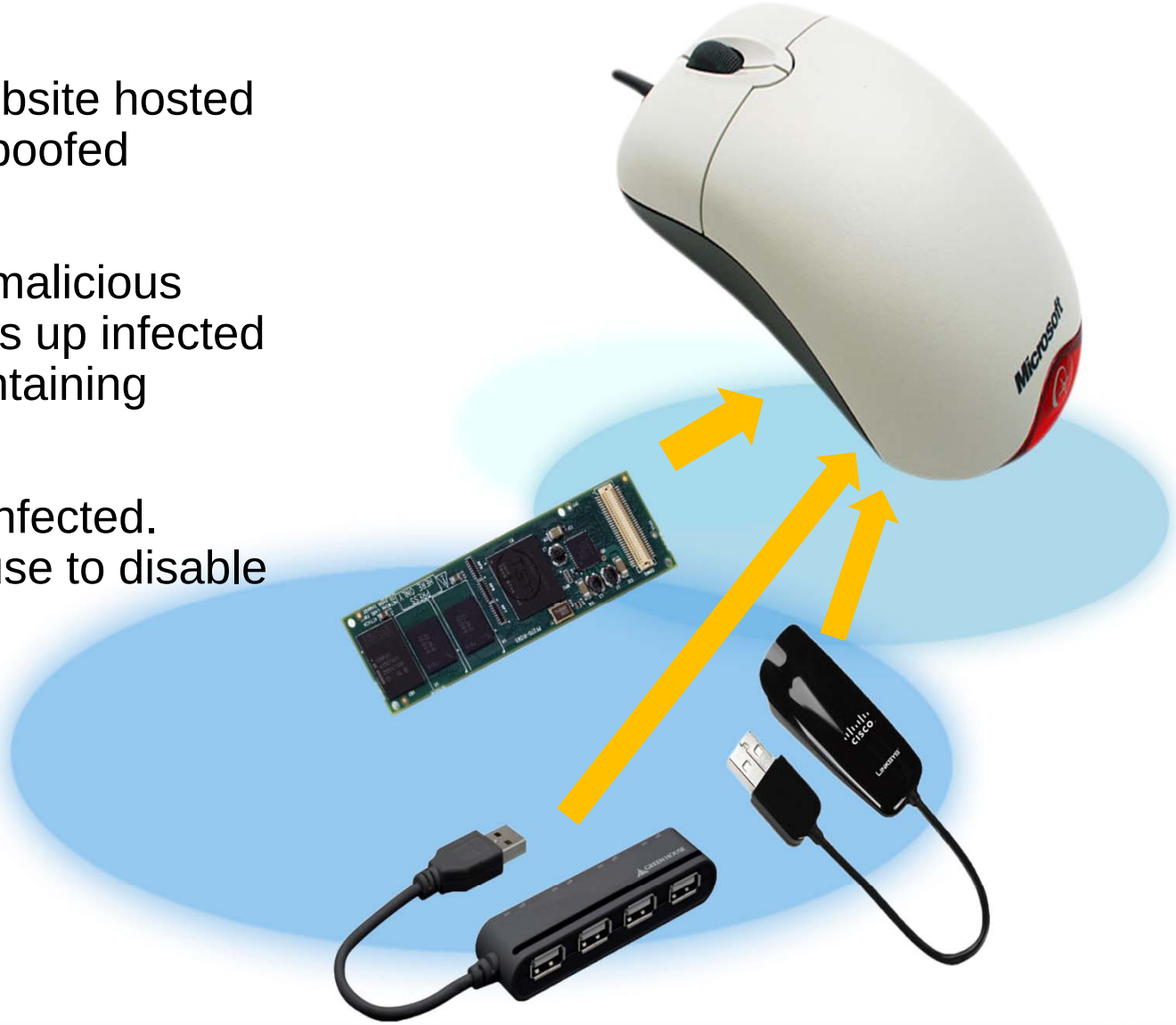
Rogue Mouse

ROGUEMOUSE

- Embed a USB hub and Ethernet Adapter into mouse.
- Embed a miniature ARM computer with running Linux with DHCP and HTTPD.
- Connect the ARM computer to the Ethernet Adapter with a crossover cable.
- Control a virtualized LAN targeting ANY valid IPv4 Network ID via the ARM computer.

MALWAREINJECTION

- User navigates to website hosted somewhere on the spoofed network.
- Trojan mouse hosts malicious webserver and serves up infected software updates containing malware code.
- Host computer now infected. Malware signals mouse to disable internal interface.



Countermeasures

- NFC
  - Active/Active is safer (for now)
- Android zero shell
  - Be careful of apps, get only from legitimate sources
- iJacking
  - Keep up to date on patches, be careful where you connect
- Rogue mouse
  - Block new USB devices, or just don't plug them in

Apply Slide

- NFC
- Android zero shell
- iJacking
- Rogue mouse

Thank you!