Realtime Bluetooth Device Detection with Blue Hydra

Granolocks
Zero_Chaos
Granolocks Narcissus

- Experimenter
- Developer
- Long walks in the woods
- Travel to exotic locations
- Hacking the planet
- Give great back rubs
Zero_Chaos Narcissus

- Eagle Scout
- Open{Zaurus,Embedded,wrt} Maintainer
- Aircrack-ng Developer
  - Injection/Drivers, airmon-zc
- Pentoo Linux Developer
- Gentoo Linux Developer
- Random Hacker of ARMs
- Husband
- Father
- Random Association of Wireless Researchers (RAWR)
  - Defcon/Shmoocon/etc Wireless CTF
- Far too easily entertained
- Not a lawyer
Bluetooth Waterfall

- Fft screenshot
airmon-ng

- airmon-ng start hci0 fake screenshot
airodump-ng

- Airodump-ng fake screenshot
Our normal approach is useless...

- airmon-ng and airodump-ng errors
Bluetooth Proliferation

- Random IoT and wearables stats
What is Bluetooth

- Cheap
- Cable replacement
- FHSS
- No monitor mode :-(
- Class
  - Class 1 100mW (high power devices, Sena dongle)
  - Class 2 10mW (phone / most laptops)
  - Class 3 1mW
Bluetooth Classic

- Discoverable
- Non-discoverable
Bluetooth Low Energy

- General Discoverability
- Limited Discoverability
- Non-discoverable
  - Yet somehow still advertises?
Basic Bluetooth Security

- PIN
- Etc
- something
Prior Art - cracking

- Redfang
- Btcrack
- Crackle
  - Le pin cracker
- Bluesnarfer
  - Phonebook dumping from old phones
Prior Art - discovery

• Bluelog
  - Discoverable classic only
  - No le support
  - Mostly a logger

• Btscanner
  - Discoverable classic only
  - No le support
  - Unmaintained
  - Neat gui
Prior Art – getting closer

- Bluez
  - Useful documentation and examples
- hciconfig
- hcitool
  - Only discoverable classic devices
  - Lescan works but hard to parse
  - Outdated
- Test-scripts bluez-test discovery
  - Easy to modify
  - Shows classic and le
  - Teaches us how to talk to the bluetooth card
  - Hides some le devices
Prior Art - Ubertooth

- Ubertooth-scan
- Ubertooth-rx
  - Ubertooth-rx -z
Goals

- Like airodump-ng and btscanner
- Support btle
- Find as many extant devices as possible
- Database backend
- Not interesting in cracking/brute forcing
Blue Hydra design logic

- Build on top of existing tools
  - Modify as needed
- Run threads for each discrete task
- Unify into a processing thread
Prior Art – the keystone

- Bluez btmon
- Raw hci info
- Monitor one or many bluetooth dongles
- Reasonably easy to parse
Blue Hydra Architecture

• One thread to monitor btmon
• One thread for handling bluetooth dongle
  – Run classic discovery
  – Listen for le advertisements
  – Support for multiple dongles planned
• One thread to handle ubertooth dongle
  – Support for multiple dongles planned
• One thread for handling sqlite
  – Three chickens for appeasing the sqlite gods
DEMO

• Doing it live!
DEMO backup

- Screenshot 1
DEMO backup

- Screenshot 2
DEMO backup

- Screenshot 3
Conclusions

- Bluetooth hasn’t been looked at much in years
- Simple idea, harder than expected
- Surprising to see just how much is there
THANKS

- DEF CON for letting us present
- Coconut Picard for letting us build and open source blue hydra
- Pwnie Express for paying us to build blue hydra then turning around and letting us open source it
- Ubertooth team for being awesome
- Bluez team for our first solid beating
Q & A

• Q&A will be in room <fill in the blank>