Network Analysis 101 For IoT

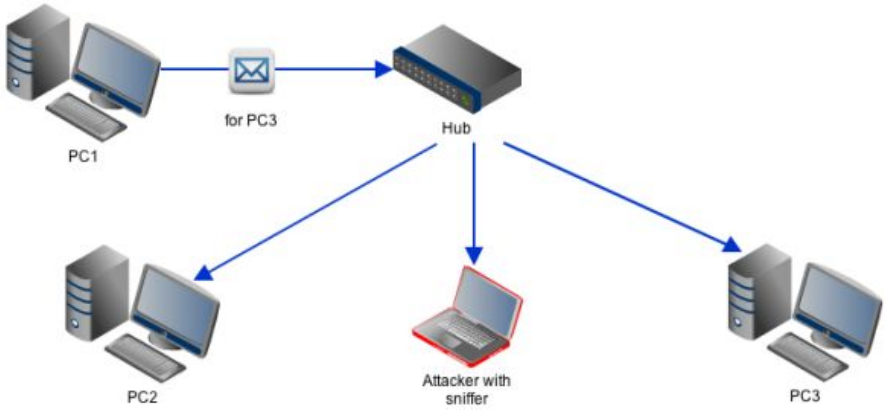
Because Sniffing Packets is No Longer Something We Should Hide

Protocol Analysis? Wassat?

- Networking? Like the social network?
- Simple introduction to packet inspection using Wireshark
- Not going to work through individual setup.
- Why do we sniff packets and why would this be important for IoT projects?

Packet Inspection Methods

- Network perspective
- Wireless network inspection
- Corporate networks and deep packet inspection
- ARP spoofing

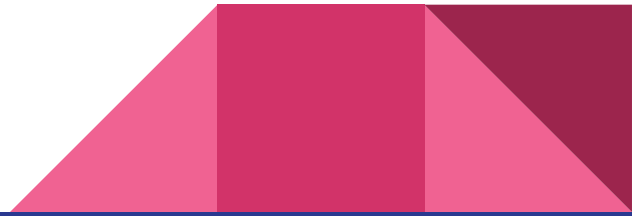


Our Setup

- Open wireless access point (ssid: “StrabucksFreeWifi” join at your own risk)
- Wireshark running on my laptop with two NICs
- Wlan2 is running on external wireless USB device in Monitor mode and promiscuous

Benchmarking

- Why benchmark your network traffic? Why not?
- A lot of work, but pays off (especially if you’re worried about security issues)



Detecting Anomalies

- Using Wireshark’s statistics, you may be able to infer that something isn’t right.
- GeoIP plugins are available to show you where you’re communicating to

Resources

- General Networking Guide (super long though, find sections you want to read)
  - http://www.tcpipguide.com/
- Wireshark/tshark
  - https://www.wireshark.org/
  - http://wiresharkbook.com/
- Using Raspberry Pi as Intrusion Detection Device (shows network packets) http://www.tripwire.com/state-of-security/security-data-protection/sweet-security-part-2-creating-a-defensible-raspberry-pi/
- For Setting Up Your System
  - https://www.google.com -- great search tool!