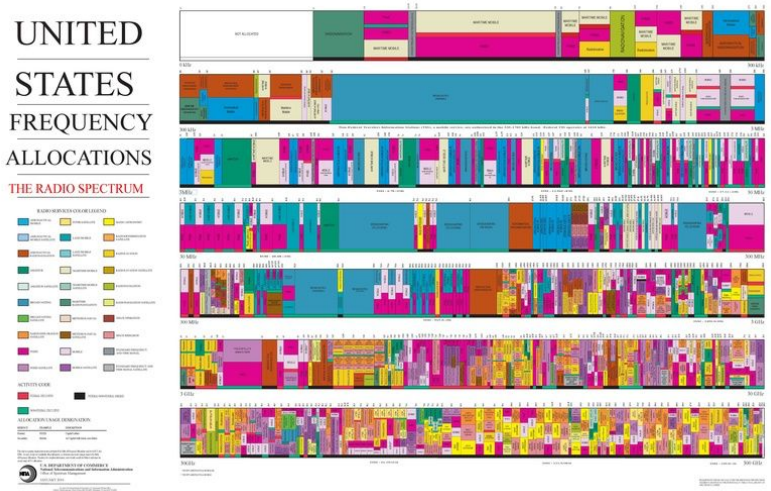
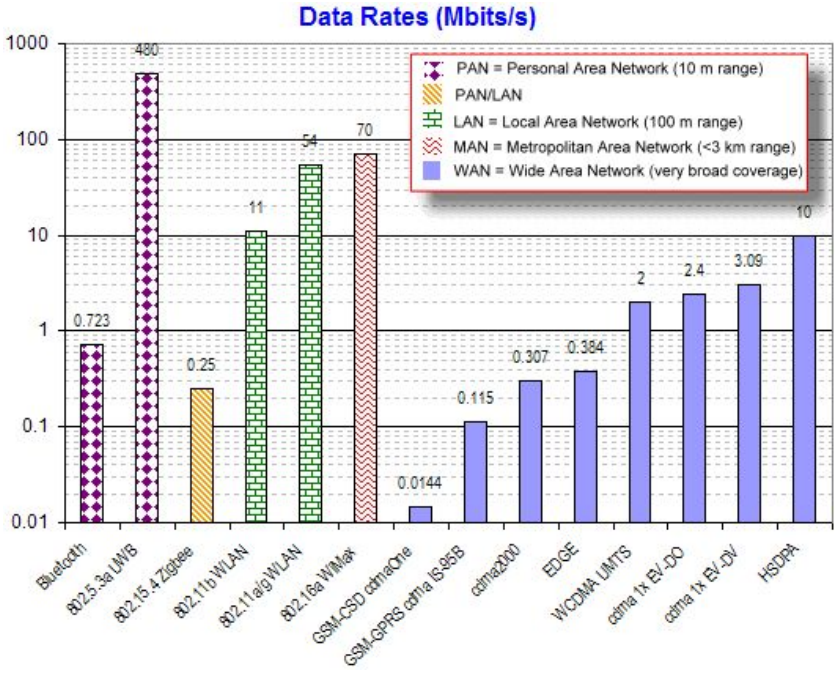
Lightweight Physical Intrusion Detection System

Designing a lightweight and easy to deploy wireless intrusion detection system.

Why RF?


UNITED
STATES
FREQUENCY
ALLOCATIONS
THE RADIO SPECTRUM


Data Rates (Mbits/s)
PAN = Personal Area Network (10 m range)
PAN/LAN
LAN = Local Area Network (100 m range)
MAN = Metropolitan Area Network (<3 km range)
WAN = Wide Area Network (very broad coverage)
1000
100
10
1
0.1
0.01
480
54
70
11
10
0.723
0.25
0.0144
0.115
0.307
0.384
2
2.4
3.09
Bluetooth
802.15.3a UWB
802.15.4 Zigbee
802.11b WLAN
802.11a/g WLAN
802.16a WiMax
GSM-CSD cdmaOne
GSM-GPRS cdma IS-95B
cdma2000
EDGE
WCDMA UMTS
cdma 1x EV-DO
cdma 1x EV-DV
HSDPA

Modular Architecture

Capture
Application to listen and record nearby Rf

Sensors:

- **GSM - RTL-SDR**
- **WiFi - RPi WiFi**
- **Bluetooth — RPi bluetooth**

Recorded Metrics

- **Signal strength indicator (SSI)**
- **MAC/IMSI address**
- **Time of scan**

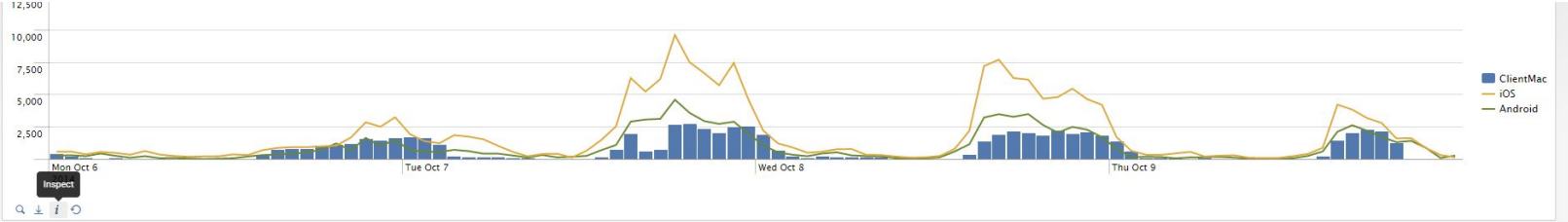
Store — Central location for sensor logs

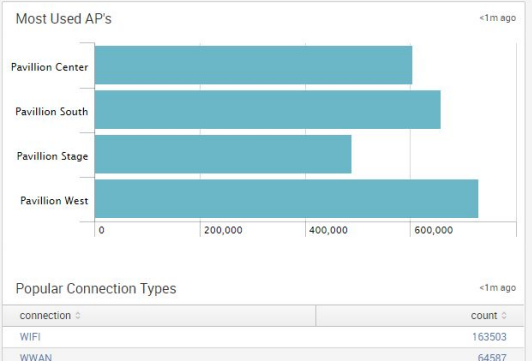
Display/Report data — Custom dashboard querying from data storage application.

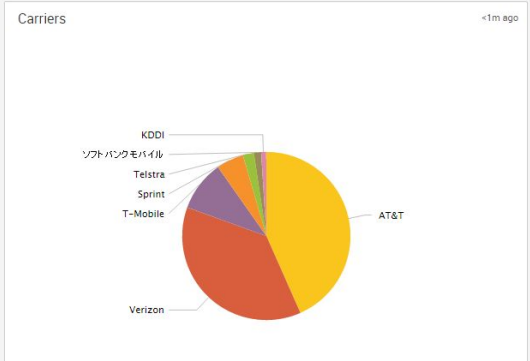
Analyse — Review new logs and trigger intrusion “alerts”

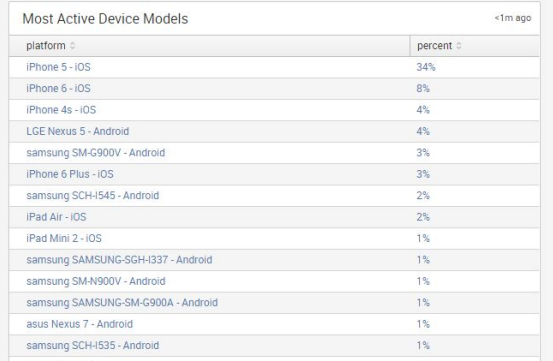
Basic Implementation

Deploying a WIDS allows administrators to know when company assets are exposed and respond accordingly, rather than hopelessly relying on the physical security controls they have in place.









Advanced use cases?

Identity management system (fingerprint individual /collection of devices)

Home automation/Indoor positioning

Spectrum Scans/Processing

Surveillance

- WiFi Radar
- RSSI/CSI
- Gait/Device/Person tracking
- Lip Reading...