Low Cost Wireless Surveillance System

Problem Statement

Many physical intrusion prevention technologies can be defeated relatively easy, are costly to implement and monitor, and generally fail to actually detect attacks in progress rather than retroactively.

Project Goal

Develop an affordable system for businesses and individuals to monitor and log nearby devices for later analysis and processing.

Technologies Used

NodeRed

- NodeJS based framework for managing and interfacing between IoT devices and services.

Raspberry Pi Model B (Server)

- Management interface to monitor and configure alerts for unknown devices. Cost: $35

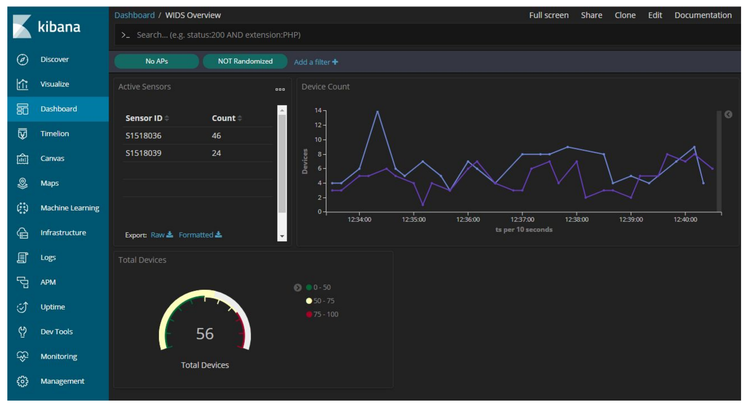
ESP8266 (Sensor Client)

- Low cost WiFi enabled microcontroller.
- Cost: $1-3 per sensor

Sensor Reporting Firmware (C++)

- Constantly monitors nearby WiFi traffic, periodically connecting to the server to report all devices seen since in that period.

Discussion



Ultimately, this project implements various use cases of broad WiFi surveillance, most specifically, it shows how low cost wireless surveillance can be used to monitor and alert administrators when an unknown device comes into contact with company assets or facilities, allowing them to respond in an appropriate and timely manner.

For under $50 in hardware, this project could be developed and tuned to suit a variety of implementation needs, such as an active intrusion detection system (demonstrated in the custom Web UI) or for long term surveillance and analysis with tools such as ElasticSearch and Kibana (as shown above).

Implications

- Home automation/Indoor positioning
- Automated Identity management system (by individual or collection of devices)
- Rf Spectrum Scans/Processing
- Surveillance
  - WiFi Radar
  - Gait/Device/Person tracking
  - Lip Reading…
  - Ect

Server Hardware

CHAMPLAIN COLLEGE

Asher McCauley
Asher@AsherMcCauley.com
Cyber security BS (Specializations in Network Admin and Cyber sec), Criminal Justice Minor.