ANWI

All New Wireless IDS

SANKET KARPE

LEAD MALWARE RESEARCH ENGINEER

QUALYS

RISHIKESH BHIDE

SENIOR SOFTWARE ENGINEER

QUALYS

Need For Wireless IDS

- Insecure Wi-Fi connections are often misused by users in vicinity
- Evil-Twin APs near Public Wi-Fi are often used to steal user data
- Home users rarely, if ever, update router firmware
- Commercial Wireless Intrusion Detection Systems cause 1000's of $

How hackers are stealing personal data by infiltrating phones through fake hotel Wi-Fi

A NEW investigation reveals how easily hackers are stealing personal information from the phones of unwitting holiday-makers.

James Cox — The Sun — MARCH 12, 2018 1:11PM

Last updated: 08:25 PM ET, Sun July 22 2018

Traveling through These Airports? Don't Connect to Their Public Wi-Fi

AIRLINES & AIRPORTS | MIA TAYLOR | JULY 19, 2018

682 387

Wi-Fi Attack Types

Evil-Twin

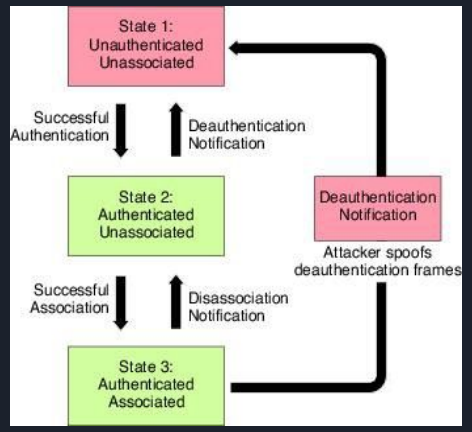
Fraudulent Wi-Fi APs

Host spoofed websites & steal credentials

De-authentication

Denial Of Service

Forces client to connect to Evil-Twin



Wi-Fi Abuse

Wi-Fi misuse in vicinity hotel/home

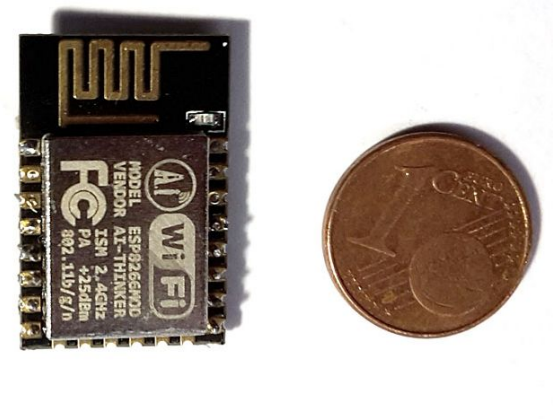
Guest or Open Wi-Fi networks are exposed

ANWI Overview

Sensors

ESP8266 based & costs 5$

Support IEEE 802.11 b/g/n Wi-Fi & Promiscuous mode



Aggregator

Node-RED Server on Raspberry Pi

Receive data via NRF Radio or Wi-Fi Channel

Reporting

Sends alert via IFTTT service

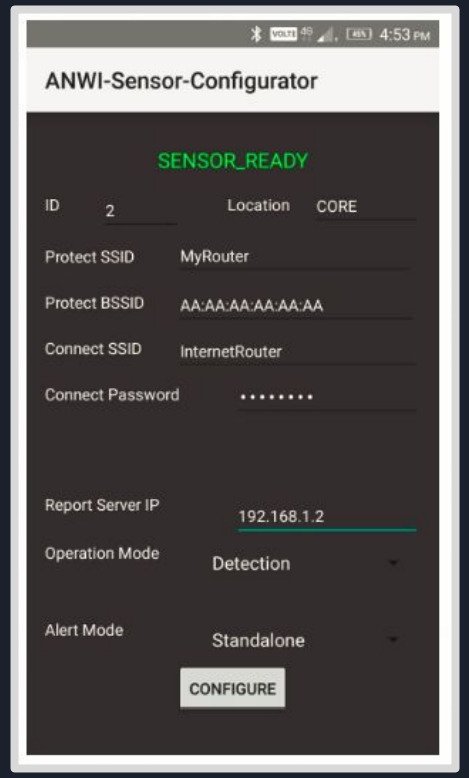
Kibana dashboard for reporting & searching

IFTTT

kibana

ANWI Sensor Configuration

Mobile Application



Web Server

Serial Console

ANWI Key Features

- Small size, Low power consumption
- Easy to setup and deploy
- Supports Standalone and Managed mode
- Alerts if any sensor goes offline
- Easy to add detection for new Wi-Fi attacks
- Fraction of the cost of commercial solutions

Demo

Thank You!

Any Questions?

sanket.karpe@gmail.com

bhide.rishikesh@gmail.com