



# 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

 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





# Wi-Fi Attack Types

## Evil-Twin

Fraudulent Wi-Fi APs

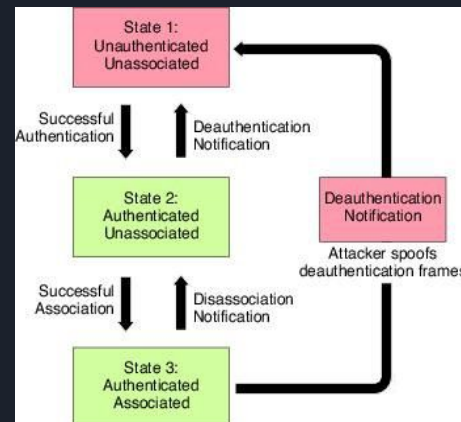
Host spoofed websites & steal credentials



## 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



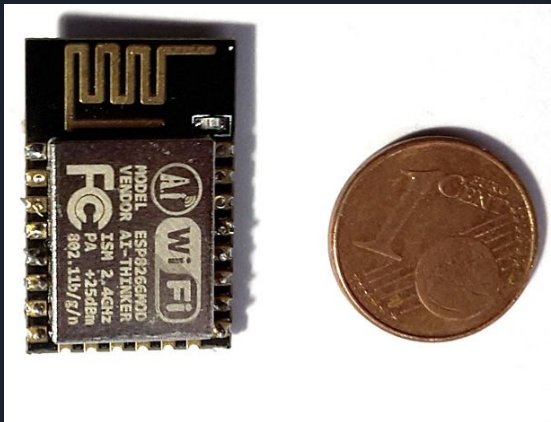


# ANWI Overview

## Sensors

ESP8266 based & costs 5\$

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



## Aggregator

Node-RED Server on  
Raspberry Pi

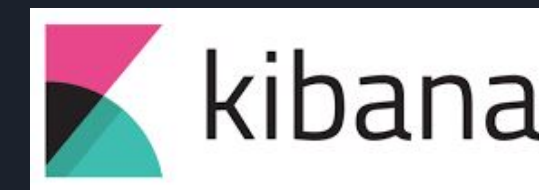
Receive data via NRF Radio  
or Wi-Fi Channel



## Reporting

Sends alert via IFTTT service

Kibana dashboard for  
reporting & searching





# ANWI Sensor Configuration

## Mobile Application

ANWI-Sensor-Configurator

**SENSOR\_READY**

ID	2	Location	CORE
Protect SSID	MyRouter		
Protect BSSID	AA:AA:AA:AA:AA:AA		
Connect SSID	InternetRouter		
Connect Password	*****		
Report Server IP	192.168.1.2		
Operation Mode	Detection		
Alert Mode	Standalone		

**CONFIGURE**

## Web Server

**ANWI ( All New Wireless IDS) -  
Sensor Configuration**

Sensor ID: 1

BSSID To Protect: 00:11:22:33:44:55

SSID To Protect: Protect\_SSID

Connection SSID: Connect\_SSID

Connection SSID Password: Connect\_PASSWORD

Alert Mode: ☒ Standalone Mode (IFTTT) ☐ Server Mode

Alert Server IP: 192.168.243.23

**Save Settings**

## Serial Console

```
> Executing task: platformio.exe device monitor

--- Miniterm on COM4 115200,8,N,1 ---
--- Quit: Ctrl+C | Menu: Ctrl+T | Help: Ctrl+T

Sensor ID : 2
Sensor Location : NORTH
SSID To Protect : ANWI
BSSID To Protect : 00:11:22:33:44:55
Connection SSID : SSID
Operation Mode : Detection Mode
Alert Mode : Standalone Radio Mode
JUST_CONFIGURED

ets Jan 8 2013,rst cause:2, boot mode:(3,6)

load 0x4010f000, len 1384, room 16
tail 8
chksum 0x2d
csum 0x2d
v614f7c32
~ld
```



# 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](mailto:sanket.karpe@gmail.com)

[bhide.rishikesh@gmail.com](mailto:bhide.rishikesh@gmail.com)