# Secure Wi-Fi

## Our Wi-Fi + Your Business = Endless Possibilities

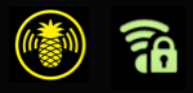
Ryan Orsi


watchguard.com/wifi

#securewifi

# Wi-Fi radios today = 8 billion
# Human population ~ 7.5 billion

## Wi-Fi Security



- Attacking is cheap and commoditized
- Extremely popular but consumers don't understand the risks
- Every Wi-Fi device is vulnerable to attacks typically not even detected
- Rampant stolen passwords, credit cards, email, PII…

WatchGuard

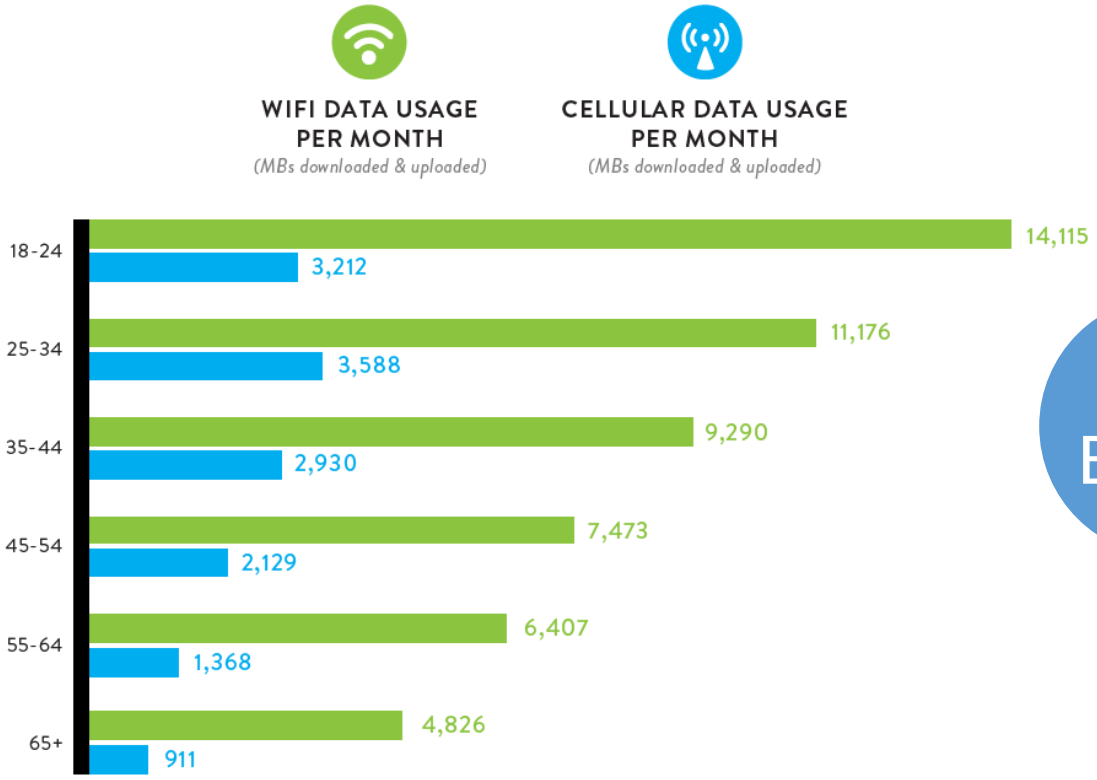
SECURE.
CLOUD.
WIFI.

**Change the Wi-Fi conversation**

W

# The Connected Generation & The Growth of Wi-Fi

## CELLULAR NETWORK USAGE BY AGE




**Cellular** Data used while connected to your carrier's wireless data network. This data counts against a consumer's mobile data plan.
**Wi-Fi:** Data used while connected to a public or private Wireless Hotspot/Network. This data does not count against a consumer's mobile data plan.

Read as: On average, people 18-24 used 14,115 MBs of WiFi data and 3,212 MBs of cellular data during the month of August 2016.

Source: Nielsen



542 Million

Number of public hotspots by 2021

12 Billion

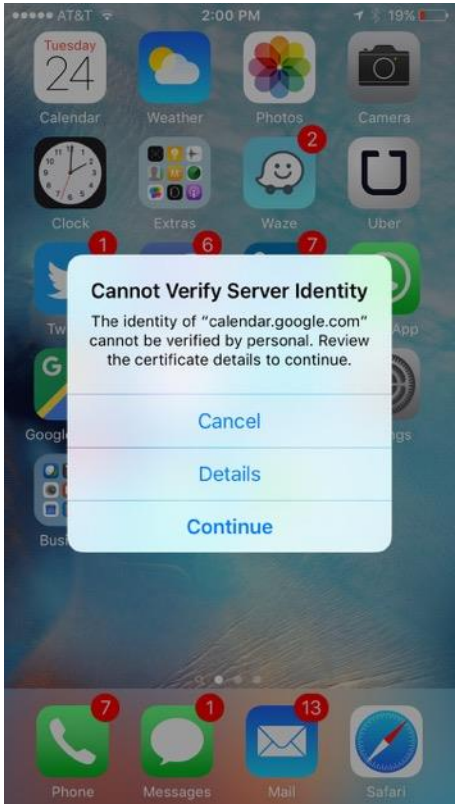
Number of Wi-Fi devices on the planet by 2025

888%

Growth of Wi-Fi since 2013

# Ignorance is Bliss

- 92% of people click “Continue” when the “Cannot Verify Server Identity” warning appears
- Wi-Fi in public places can be unsecure, letting malicious actors view everything you do while connected




91% of users are aware of public Wi-Fi security risks

89% ignore them and use it anyway

# Attack Surfaces

# Wi-Fi Hacking Glossary

- **Man-in-the-middle attack (MiTM) -** where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other
- **WIPS** – Wireless Intrusion Prevention System
- **WIDS** – Wireless Intrusion Detection System
- **Rogue AP** – An access point that is connected to a secured network without authorization
- **Evil Twin** – An access point that is mirroring a Wi-Fi network
- **Honey Pot** – An access point that is presenting an open Wi-Fi network

# So How Easy is it to Hack Wi-Fi?



Starting: $99

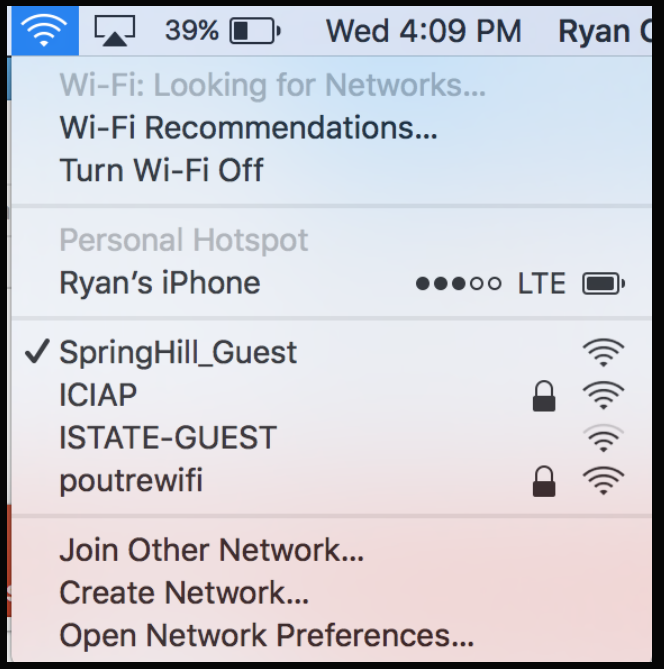
YouTube

> 28,000 videos

Read the blog post:
secplicity.org/2017/07/05/silicon-valley-wi-fi-man-middle-pineapple-attacks/

# Beacon

- Access points send beacon frames periodically to announce it's presence
- Your "Wi-Fi networks in range" list behind the Wi-Fi icon is built by listening for beacon frames



# Probe Request

- Your client devices send probe requests for networks they joined at some point in the past to see if they are nearby.
- For example, your phone might constantly ask for the “Coffee” Wi-Fi network in the hope that it’s nearby and to connect to it

# Wiphishing Clients

- Client devices that have saved SSIDs are constantly beaconing to see if those access points are in range

**Karma attack**

**EST. 2005**


/ˈkärmə əˈtak/

*verb*

**1**. listen for SSID beacon requests and pwn people


Starting: $99

YouTube

> 28,000 videos

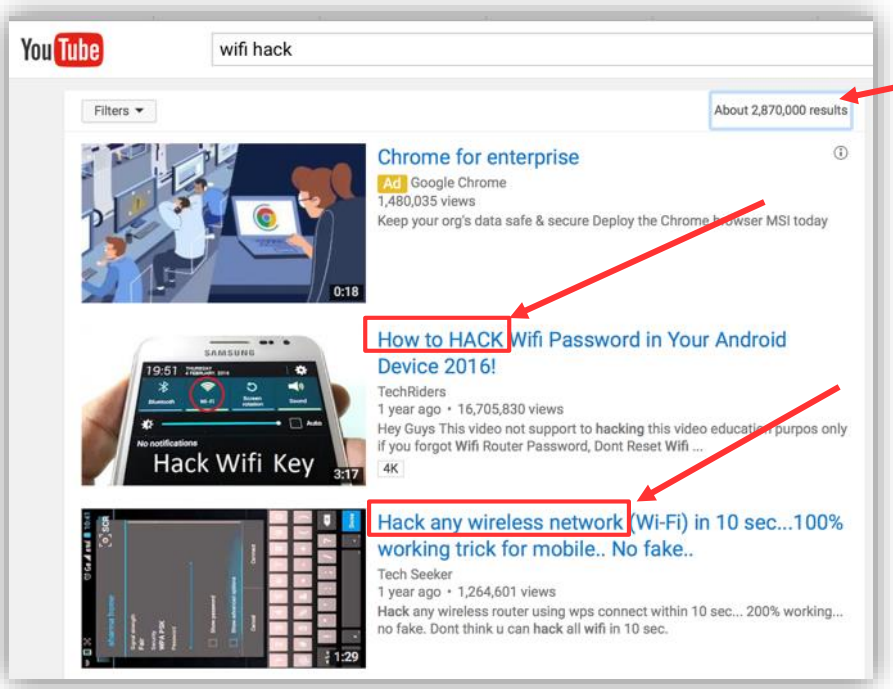
| Name | Version | Author | Description |
|---|---|---|---|
| DWall | 1.1 | sebkinne | Display's HTTP URLs, Cookies, POST DATA, and images from browsing clients as a stream. Wall of Sheep style. |
| Deauth | 1.4 | whistlemaster | Deauthentication attacks of all devices connected to APs nearby |
| EvilPortal | 2.1 | newbi3 | An Evil Captive Portal. |
| SSLsplit | 1.0 | whistlemaster | Perform man-in-the-middle attacks using SSLsplit |
| SiteSurvey | 1.2 | whistlemaster | WiFi site survey |
| ettercap | 1.4 | whistlemaster | Perform man-in-the-middle attacks using ettercap |
| Status | 1.1 | whistlemaster | Display status information of the device |
| nmap | 1.4 | whistlemaster | GUI for security scanner nmap |
| urlsnarf | 1.4 | whistlemaster | Output all requested URLs sniffed from http traffic using urlsnarf |

Intuitive GUI, ready packaged modules

# Who are These Wi-Fi Hackers?

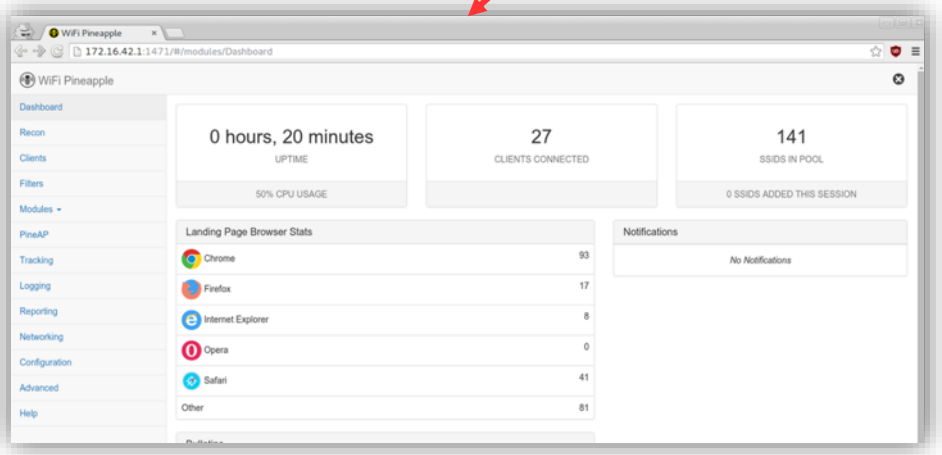
- Hardcore coders, deep dark hackers right?

- Today: **we have youtube**. In less than a weekend, anyone can become a wifi MiTM and launch attacks to steal information across wifi networks




2,870,000 results for “wifi hack”

Hacking tools with easy to use GUIs



# Anatomy of a Man-in-the-middle Wi-Fi Attack


Get in at low layer…

To launch higher layer attacks and gain remote access

SSL Strip

KRACK

PAC File Exploits

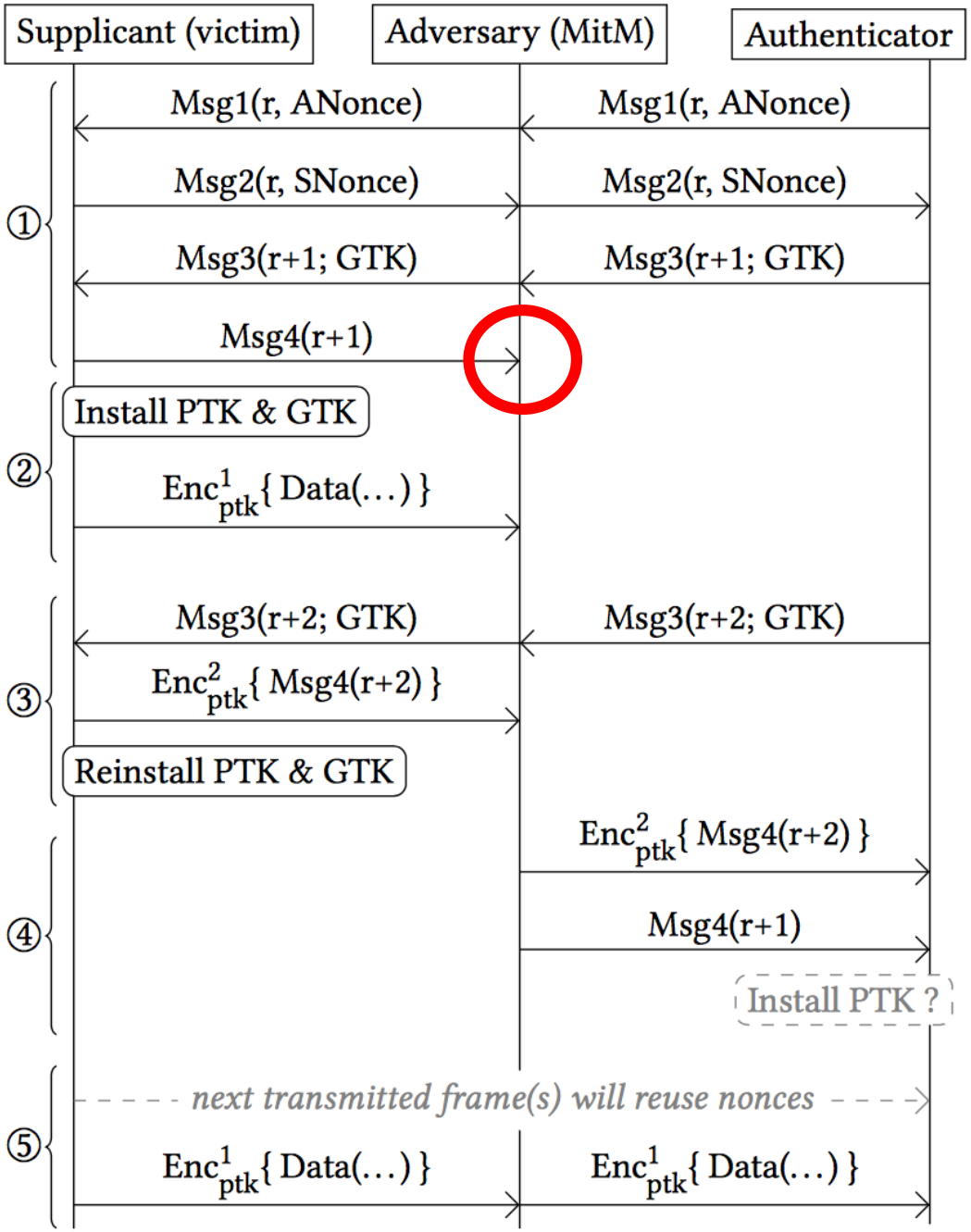
Browser Exploitation Framework (BEEF)

Evil Portals

Toxic Proxies

Back doors

# WPA2 KRACK



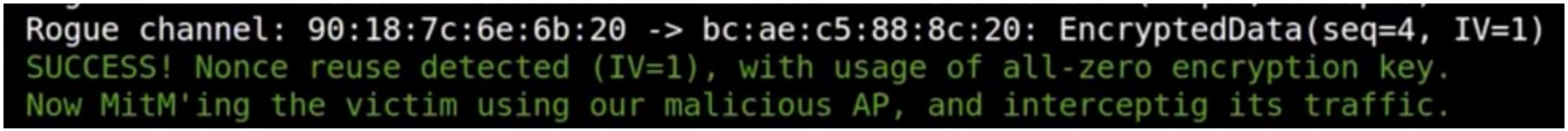

- MiTM blocks AP from receiving handshake message #4
- Client begins sending encrypted traffic after receiving message #3
- Attacker forces re-use of a number that is only meant to be used once "nonce", thereby cracking the encryption



https://papers.mathyvanhoef.com/ccs2017.pdf

# KRACK WPA/WPA2 Vulnerability Overview

## On October 16, 2017 Worse ”crack in the code” in over 10 years for Wi-Fi




- SSIDs using WPA/WPA2 can have the data transmitted over the air intercepted and decrypted
- Affects nearly all Wi-Fi devices globally, primarily a client-side vulnerability
  - 1 vulnerability for APs
  - 9 vulnerabilities for clients

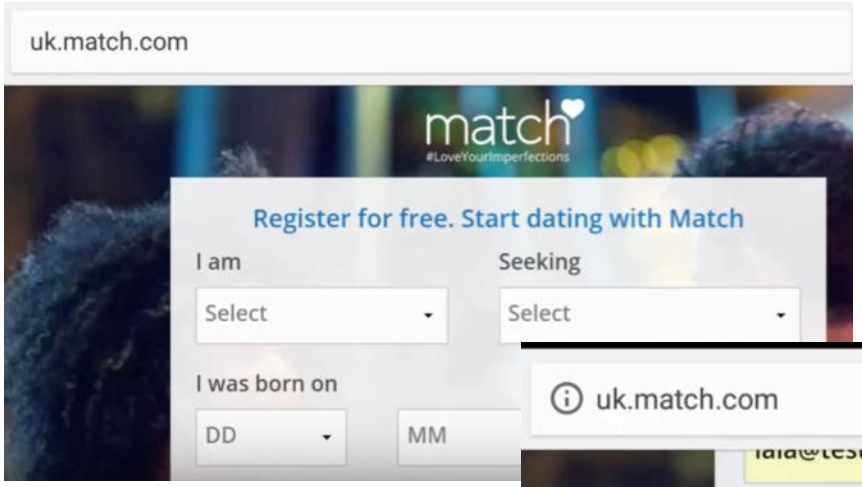
| Resources |
| --- |
| WatchGuard Blog Post: watchguard.com/wgrd-blog/krack-update-protecting-unpatched-devices |
| Researchers’ website: Krackattacks.com |
| CERT List of Patched Vendors |

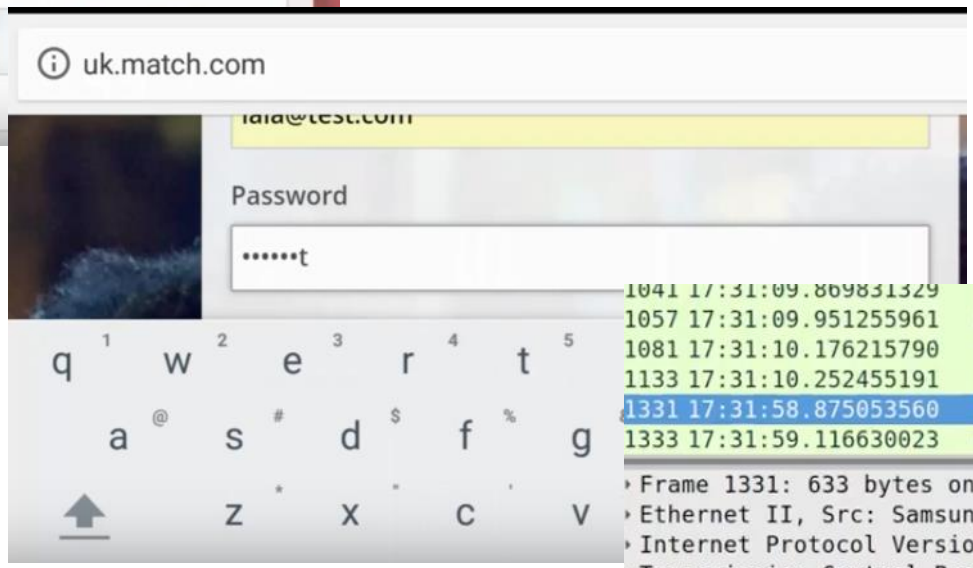
# Can Data Really Be Stolen?

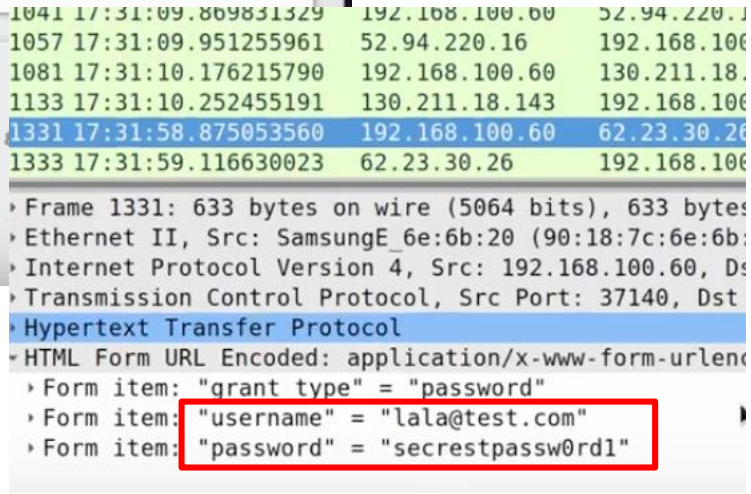
1. Establish MiTM position
2. KRACK WPA2 encryption

3. Beat website encryption with SSL Strip

4. Intercept plain text user name/password



# Vulnerable Clients

"We're probably still going to find vulnerable devices 20 years from now,"

*- HD Moore, network security researcher, Atredis Partners*[1]

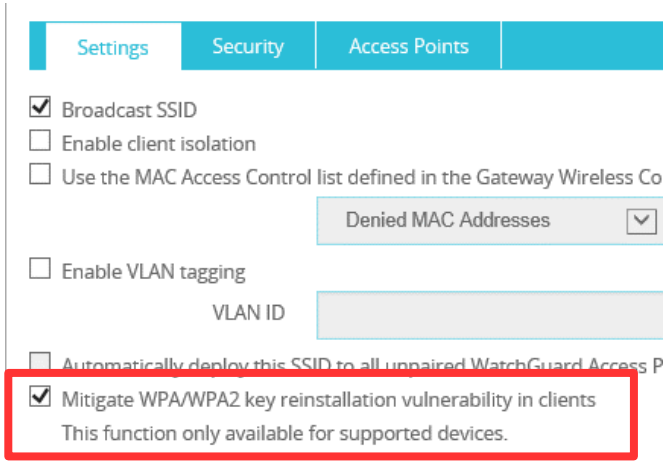
- Patching all clients in a business' environment is very difficult if not impossible
- Major manufacturers for laptops, phones, tablets are easier to coordinate
- Printers, web cameras, projectors, TVs, wearables, and other IoT devices may not have patches available in a timely manner, or possibly ever

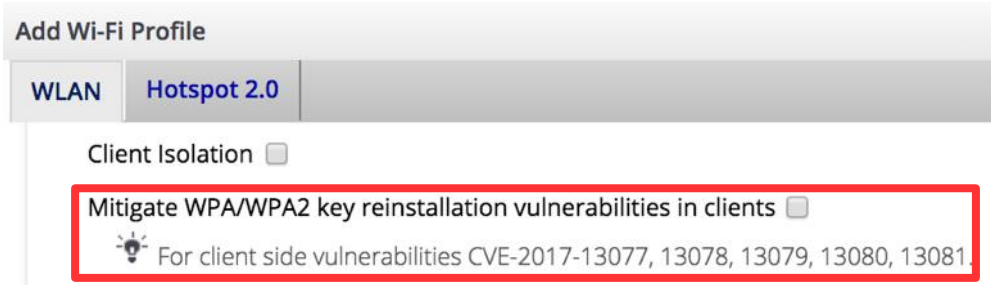
[1] https://www.wired.com/story/krack-wi-fi-iot-security-broken/

# Client Vulnerability Mitigation

For unpatched clients, look for Wi-Fi vendors that offer protection for unpatched clients by mitigating the attack

Example KRACK mitigation feature:



# WIPS for Zero Day Protection

Use dedicated WIPS sensors with **MAC Spoofing Prevention** enabled to provide zero-day protection against unknown future vulnerabilities.

From researchers' website[1]:

**So you expect to find other Wi-Fi vulnerabilities?**

*"I think we're just getting started."* — Master Chief, Halo 1


| Resources |
| --- |
| Learn more about WIPS:<br>watchguard.com/wips |

[1] https://www.krackattacks.com/#faq

# KRACK Summary

- Changing your Wi-Fi password(s) won't help
- Patch
  - APs: SSIDs using 802.11r are vulnerable
  - Clients: see vendor websites for patches
- Ways to protect unpatched clients from KRACK:
  - Use APs with mitigation features for KRACK
  - Utilize dedicated WIPS sensors for zero day protection

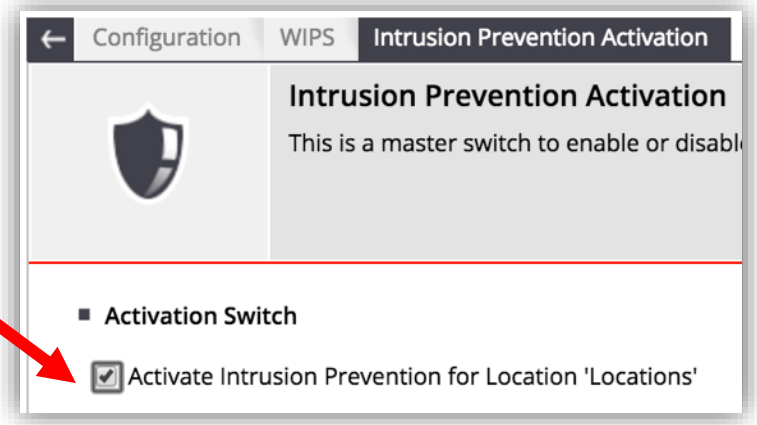


[1] https://www.krackattacks.com/#faq

# Protection

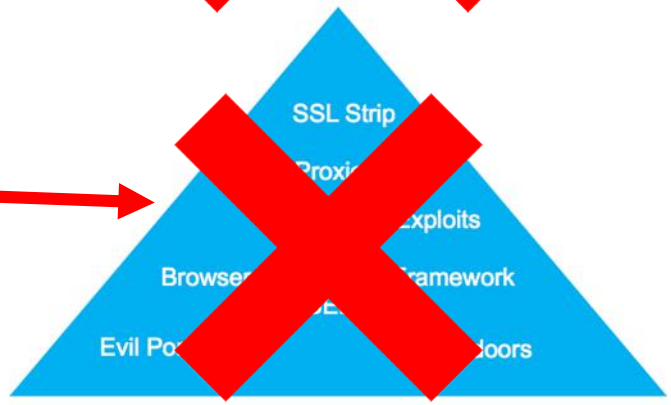
# Stop the MiTM, Stop The Hacks

**#1**
Turn on WIPS




**#2**
Take out the MiTM


**#3**
Stop the hacks



# Failed Attempts at Wi-Fi Security

Relied on correlating MAC addresses to find rogue APs

- Leads to high false positives
- Leads to illegally taking down neighboring authorized APs
- Can cost hundreds of thousands of dollars in fines

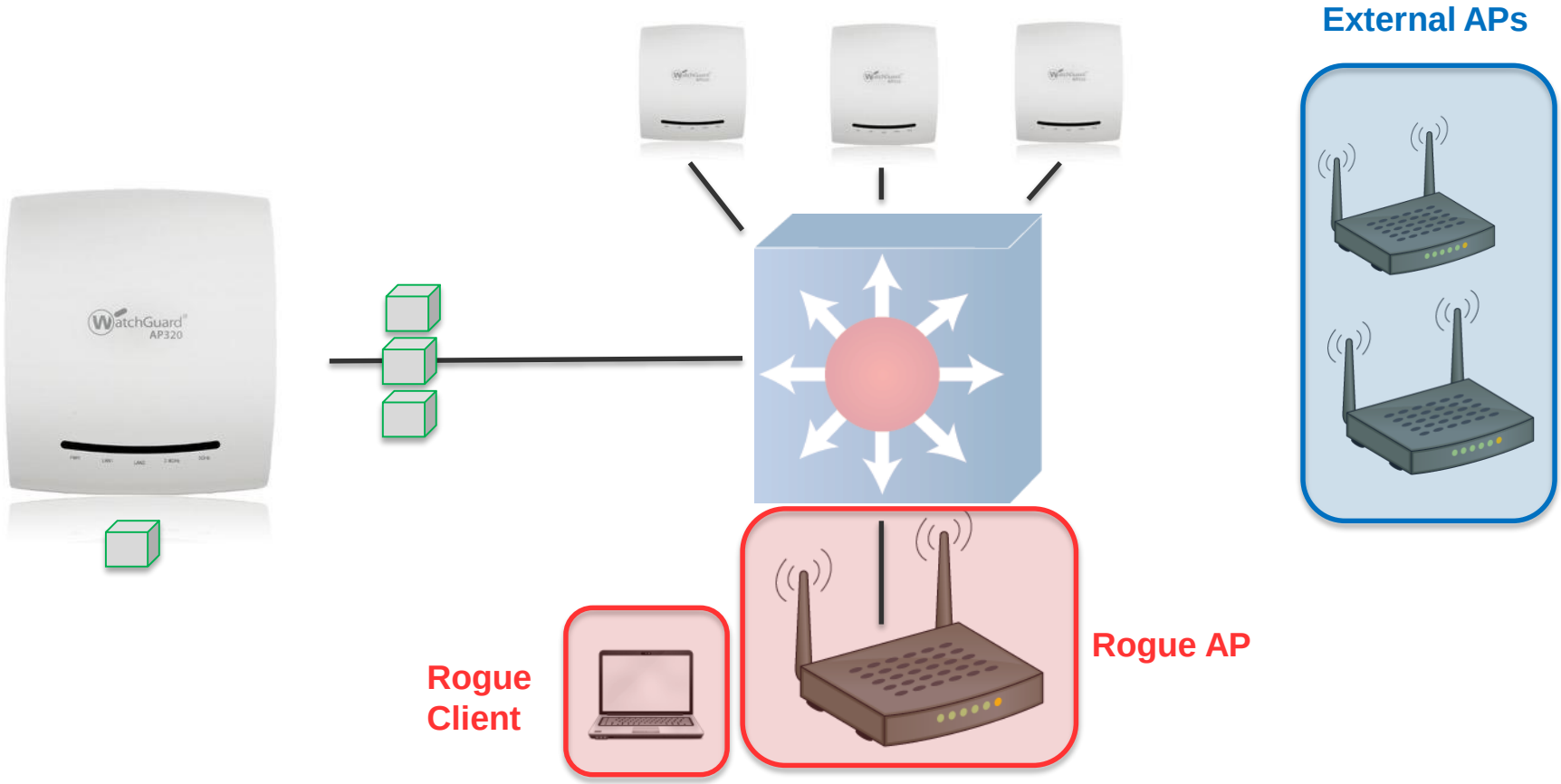
**$718,000 in FCC fines!**


From major WLAN vendor documentation:

| |
|---|
| “extreme caution” |
| “may impact neighboring networks” |
| “can impact the normal operation of valid APs belonging to a nearby business” |

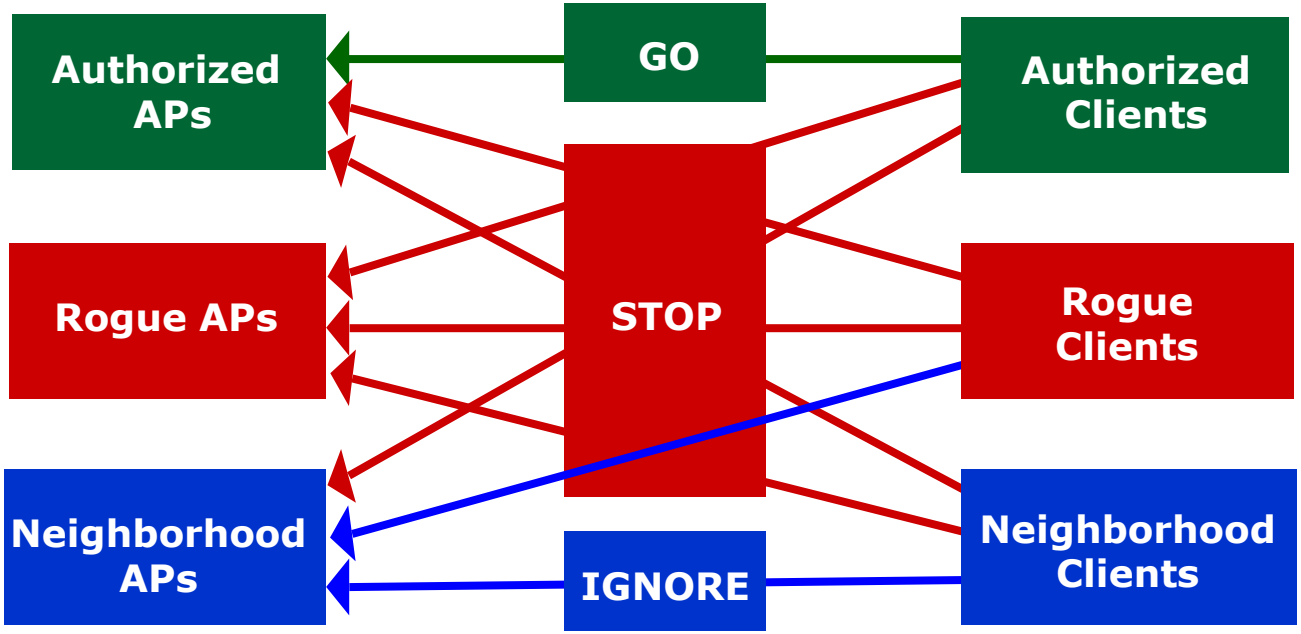
# *Accurate Classification of “good“ vs “bad“*

- Wired-Side Injection
- Wireless-Side Injection

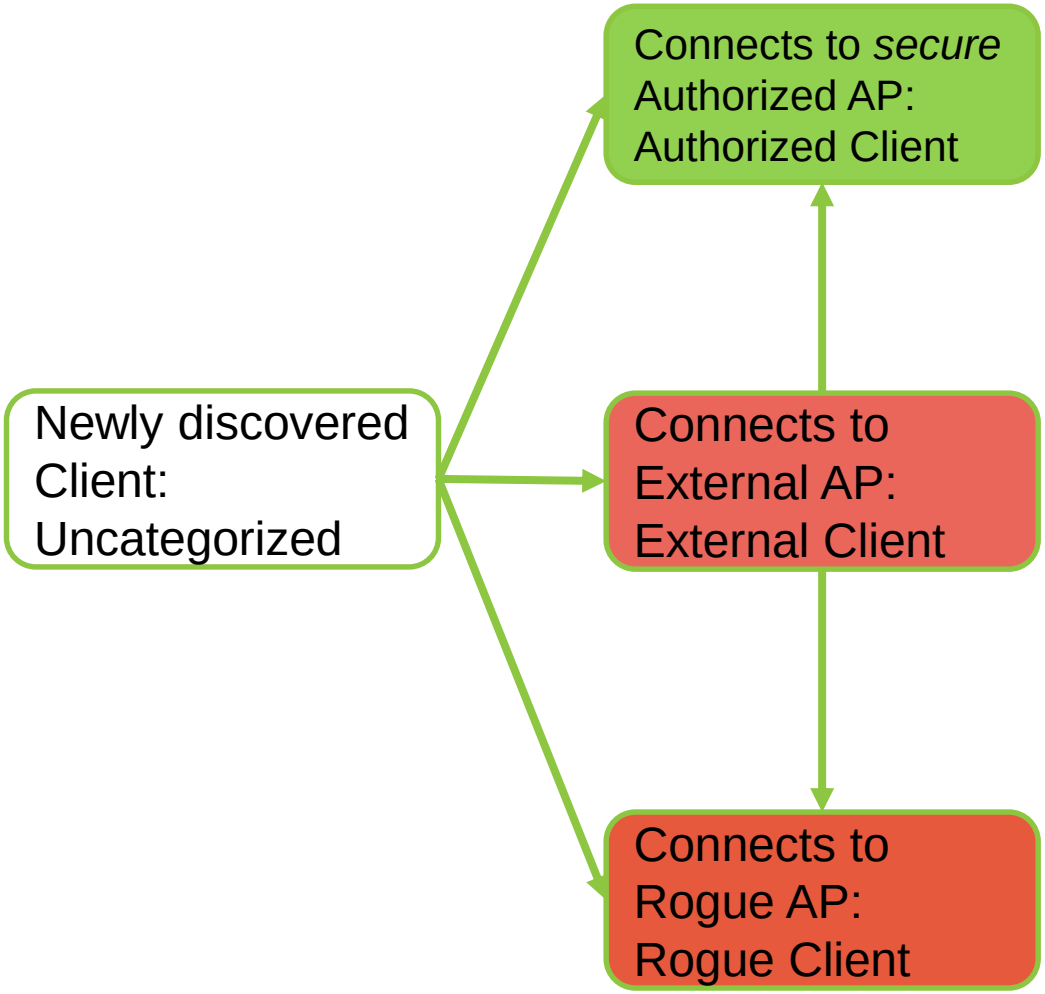


# WIPS Security Policy Basics

Accurate classification of **APs** and **Clients** is crucial



# Client Auto-classification




Additional ways to auto-classify Clients:

Integration APIs with leading WLAN controllers to fetch Authorized Clients list.

Import MAC addresses of Authorized Clients from file.

# WIPS Protects From **Over-the-Wire** Threats

- **Rogue AP** — Unauthorized APs connected to your network that your clients connect to instead of your legitimate APs
- **Client Misassociation** — Authorized clients on your network that associate to external APs in your vicinity
- **Misconfigured AP** — APs connected to your network with a configuration that does not conform to your security policies
- **Unauthorized Association** — Unauthorized external clients that connect to your APs
- **AP MAC Spoofing** — An AP that spoofs the wireless MAC address of a legitimate AP

# WIPS Protects From **Over-the-Air** Threats

- **Honeypot /Evil Twin AP** — Rogue APs from nearby networks that broadcast the same SSID as one of your APs to appear as a legitimate AP on your network
- **Denial of Service (DoS) Attack** — DoS attacks degrade and disrupt the performance of your wireless network
- **Rogue Client** — Rogue clients are unauthorized clients that connect to your wireless network.
- **Ad hoc Connection** — An ad hoc connection is a peer-to-peer connection between clients that can circumvent security
- **Bridging Client** — A client with packet forwarding enabled between wired and wireless interfaces can result in authorized access to your wired network

# Be Informed When Selecting a WIPS Technology

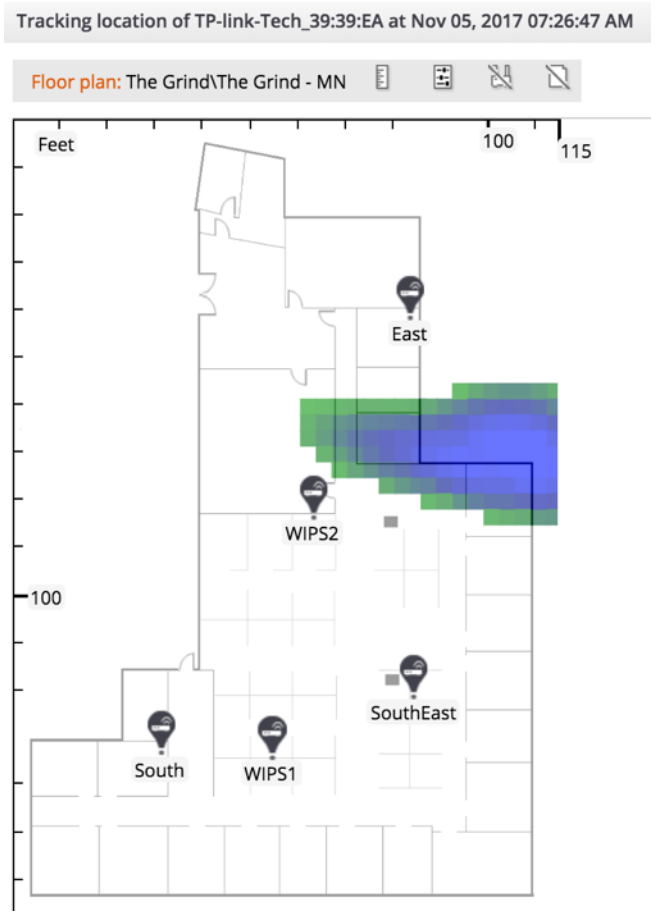

**Signature Matching On Packet Contents:**

- All attack tools don't have signatures
- Signature fields in tools are modifiable
- Signatures lag attack tools
- Signatures matching approach creates abundant false positives & negatives

**Packet Anomaly Detection On *Unknown* Thresholds**

- Common Thresholds: signal strength, probe request intervals…
- It doesn't help to give threshold comparators, when users don't know the right thresholds
- Inaccurate stats based on partial observation
  - Right threshold to catch real threats, while avoiding false alarms

# WIPS Tip: Accurate Location Tracking



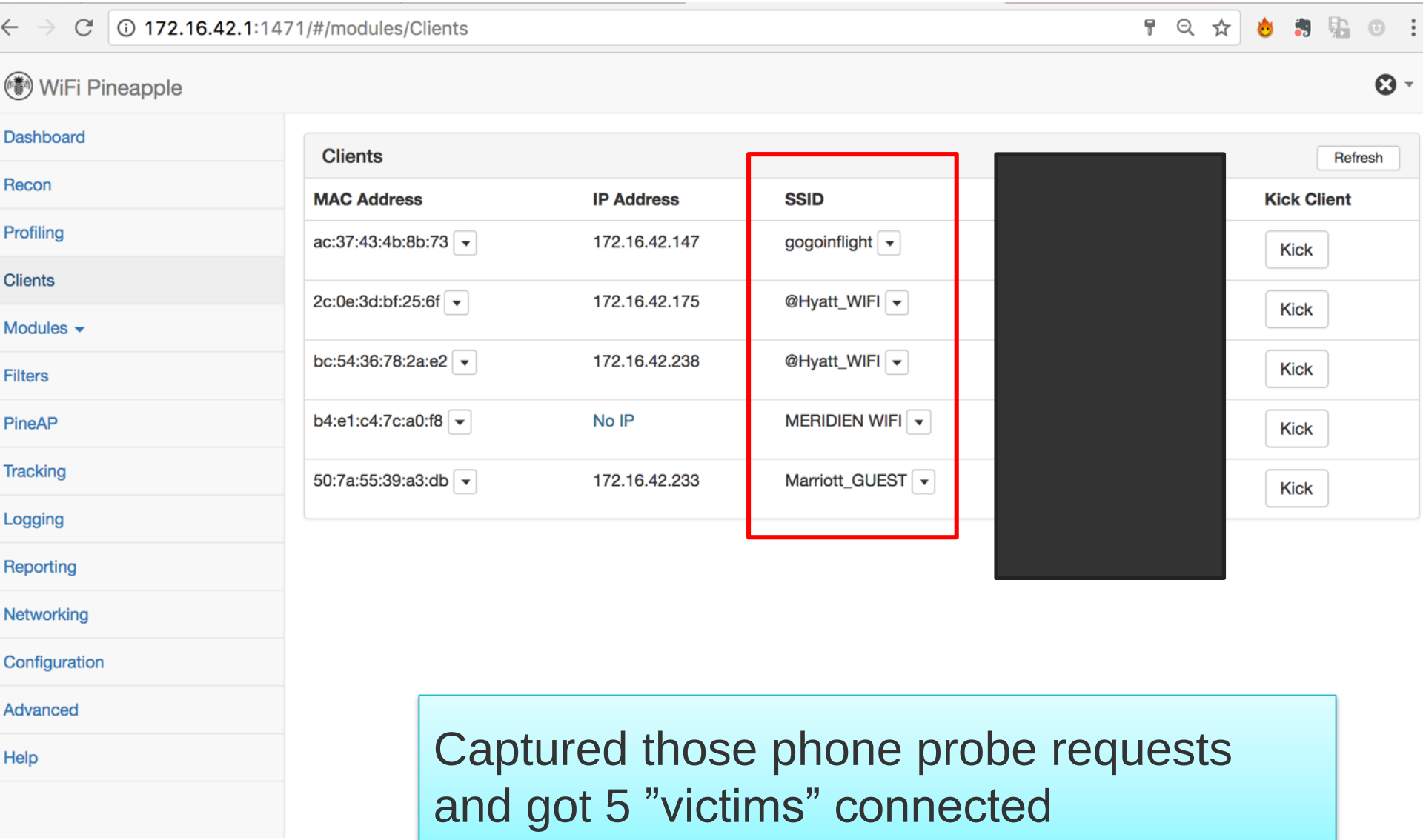

Look for WIPS technologies that can triangulate the location of attackers:

- No need for RF site survey
- 15 ft. accuracy in most environments

No search squads to locate Wi-Fi devices

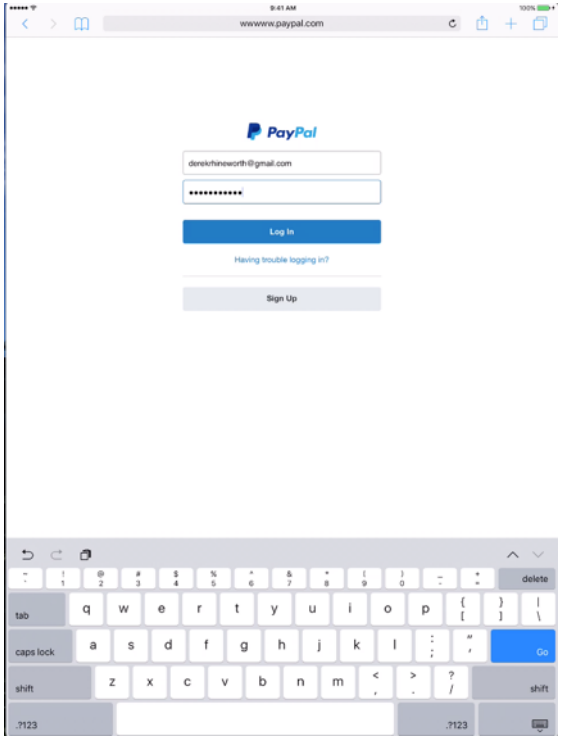
# Real-life example

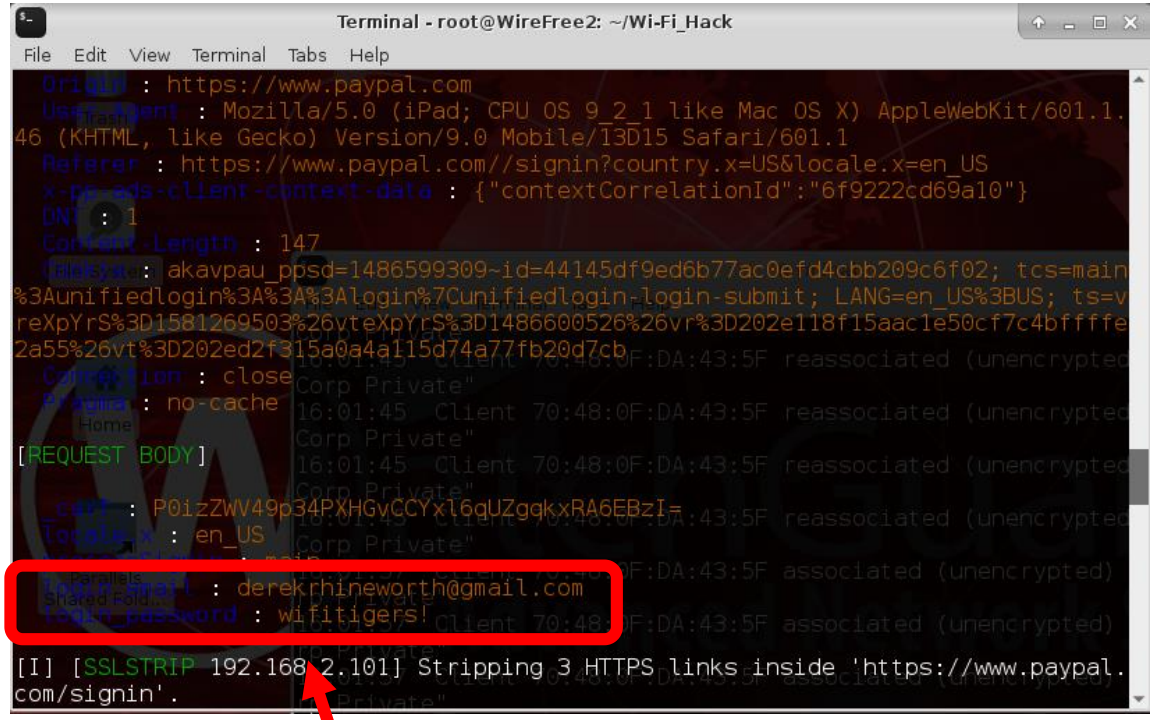
Don’t take any pictures or you’ll get me in trouble




Captured those phone probe requests and got 5 ”victims” connected

# Stealing PayPal Credentials

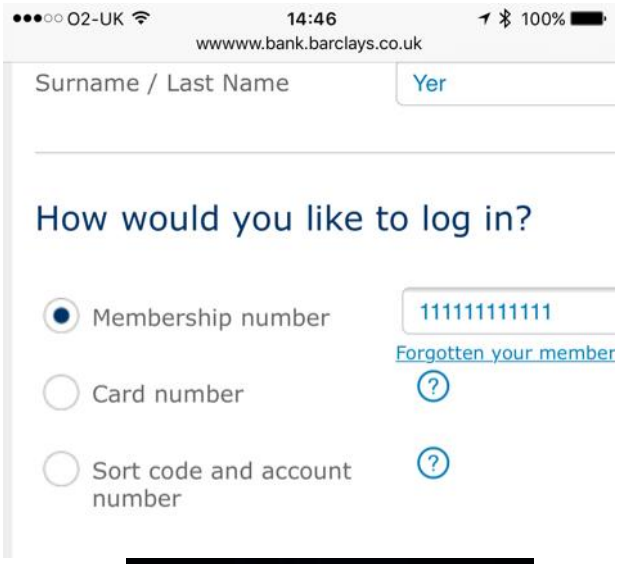


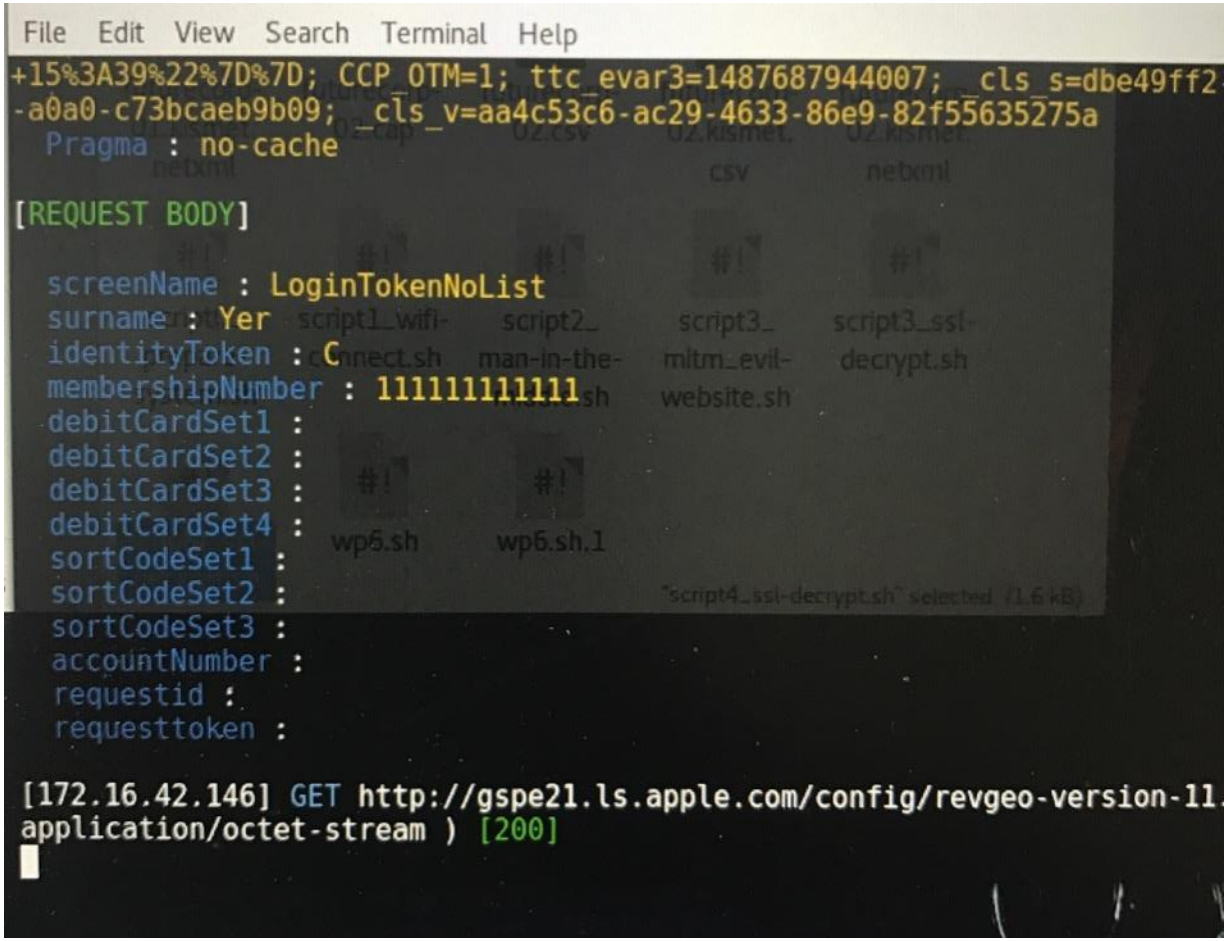

Victim logs in not realizing this is a HTTP site and sends username, password in plain text to the attacker

Login credentials!

# Stealing Banking Credentials



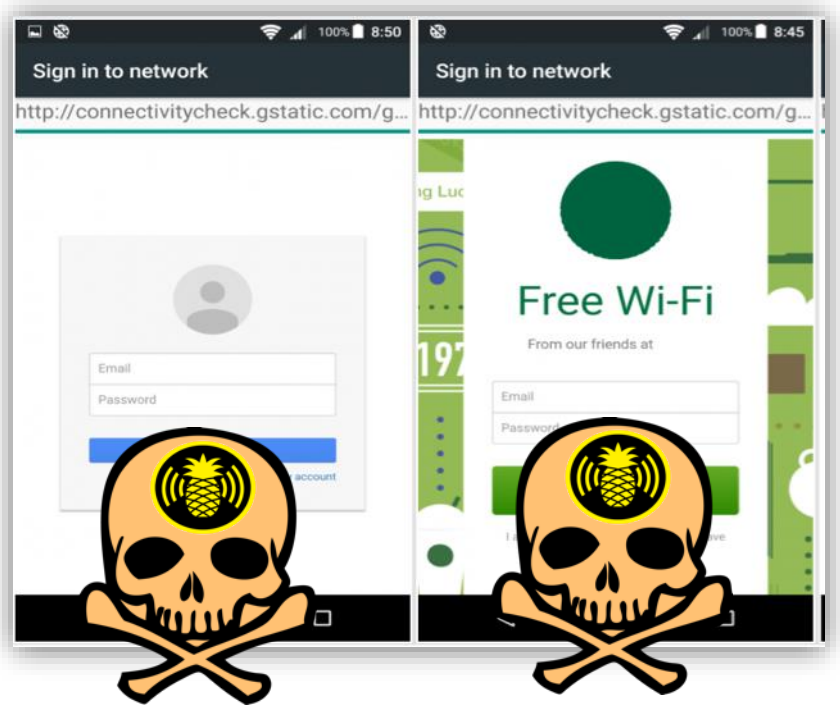




# Other Common Targets

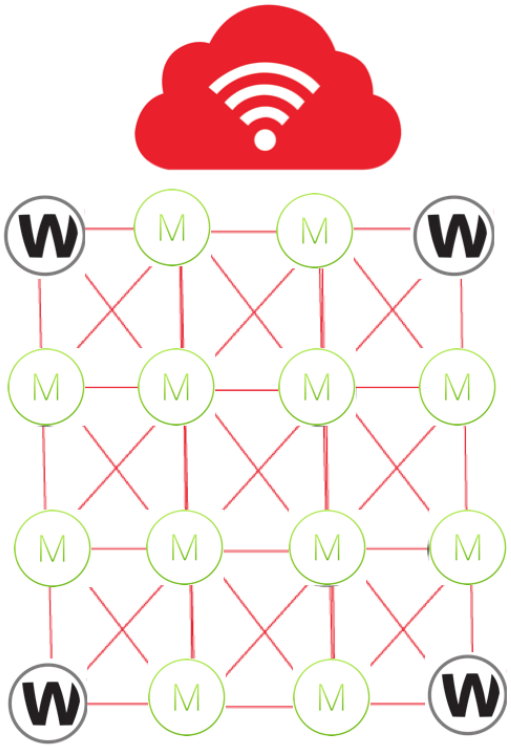

# Evil Portals Running Rampant

- Hackers mimic popular splash pages to create “evil portal”
- Victims unsuspectingly fall right into their trap to
  - Hand over sensitive information
  - Install a browser exploit
  - Allow malware to be dropped to their device



# You Don‘t HAVE to Rip and Replace

*Gain added Wi-Fi security without needing to replace your existing access points.*



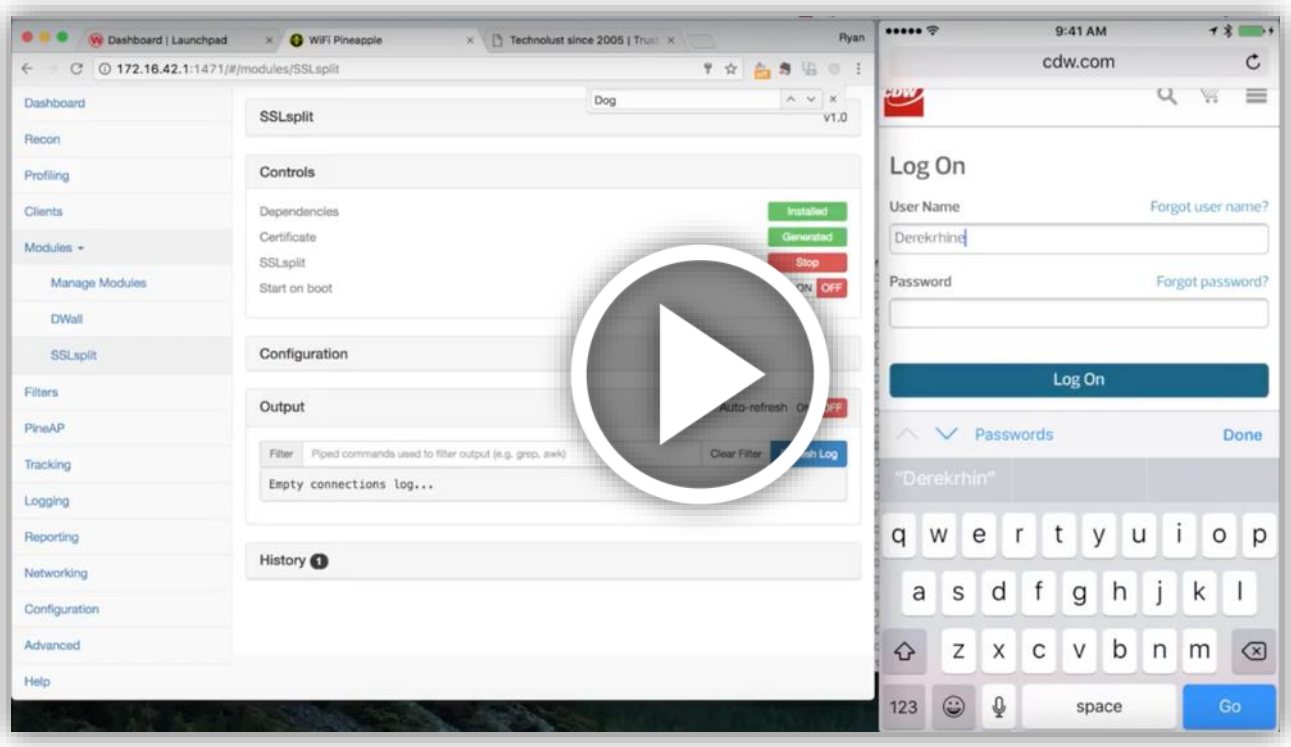


WatchGuard APs as ‘dedicated WIPS sensors’ installed alongside competitor’s APs

WIPS

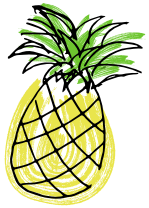
# Video: Wi-Fi Man-in-the-middle attack explained

https://www.youtube.com/watch?v=qQmpKaXFUt4



# Check Out Our Secure Wi-Fi Web Series!

Episode 1:
Anatomy of a Wi-Fi Hack





Episode 2:
Defending Your Airspace



Episode 3:
IoT Current and Future Threats



**watchguard.com/wifi-webinars**

# THANK YOU


Learn more at:

watchguard.com/wifi

#securewifi