I KNOW WHAT YOU DID LAST SUMMER 3
some call me a one trick pony, others call me passionate

- mad scientist hacker who likes to meddle with hardware and software.
- particularly obsessed with wireless.
- degree in computer science from Southern Utah University
- loves include:
  - web application pentesting
  - wireless monitoring and tracking
  - reverse engineering
- creator of the #WiFiCactus
- Kismet cultist
- Runner
Wardriving got popular in the early 2000’s as a way for people to find open networks to piggyback on [1]. Equipment was pretty expensive and limited.

The number of devices that are connected over wireless has increased exponentially since the early 2000’s and make Wardriving, Netstumbling and Wireless Monitoring more exciting than ever.

2000

2015
Backpack Test Project
Warwalking with a single-board computer in my backpack for Defcon 23. Collected data on 2 channels at a time.

2016
Project Lana
Planted 12 monitoring boxes around the conference for Defcon 24. 48 total wireless radios scanning at the same time.

2017+
#WiFiCactus
25 Hak5 Pineapple Tetras that cover 50 total channels in 2.4 and 5 GHz. Over 3 hours of battery life. Weighs ~35 lbs.

Understand the FUD
Nearly every person has heard that DEFCON's network is the most dangerous in the world. I wanted to know why and how it is so dangerous. Understanding is the first step to protecting yourself.

The Connected World
Everything is connected now and usually with more than 1 radio. This makes for amazing data. Whether it’s your phone’s mobile hotspot to the ‘SMART’ THINGS (IoT) need to be connected and we gotta catch them all!

Verify Then Trust
Do you trust that security, software and API’s are being done correctly when communicating over a network? Do you know if your favorite app uses encryption? By scanning yourself you can verify how secure things are.
data captured

got data?

1. DEFCON
   Year by year captured data at DEFCON

2. BLACKHAT
   Year by year captured data at Blackhat

3. Other Places
   Captures at DC China, DefCamp, SaintCon, CactusCon, Shmoocon and more

1.1 TB
how’d you do analysis?
sometimes you have a tool and sometimes you build a tool

Traditional Network Tools

Wireshark and Networkminer were instrumental in providing summery information from the PCAP data. Great for spot checking the data.

Kismet WebUI and KismetDB

Awesome for real-time analytics about what is happening. Additionally helpful to reload KismetDB files after the fact to relive the fun. KismetDB’s are SQLITE DBs which enables easy querying.

PCAPinator

Built a custom Python 3 tool that leverages Wireshark’s command line tools like tshark by using parallel processing on very large PCAP file datasets. Has a lot of custom output types like CSV, HCCX, etc.
 pcapinator

PCAPs or it didn't happen?

JUDGEMENT DAY

Design by: @elkentaro
pcapinator
a tool to run a lot of tsharks

https://github.com/mspicer/pcapinator
pcapinator

a tool to run a lot of tsharks

https://github.com/mspicer/pcapinator
DEMO VIDEO
SO WHAT DID YA’LL DO LAST SUMMER?
getting to know you
where are you from?

Probes and WIGLE.net
This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.

KEY
- WPA 2
- Unknown
- WEP
- WPA
- NONE
getting to **know you**

where are you from?

Probes and WIGLE.net

This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.
getting to **know you**

where are you from?

**Probes and WIGLE.net**

This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.
getting to **know you**

where are you from?

**Probes and WIGLE.net**

This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.
getting to **know you**

*where are you from?*

Probes and WIGLE.net

This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.
getting to **know you**

where are you from?

Probes and WIGLE.net

This info is based on probe requests captured during DEFCON and then searching those using the Wigle API.
getting to know you

where have you been?

MAC Addresses and Where
This graph uses unique MAC addresses and knowing where the MAC address was seen at.
wireless attacks
its not all just pineapples

Kismet IDS Provided These Alerts

Thanks to the built in Intrusion Detection System in Kismet, it is able to identify these threats and log them to the Kismet database. This is a small sampling of common wireless threats in the environment.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Attack Type</th>
<th>OUI/Manufacturer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>92:16:F9:9F:4D:08</td>
<td>Deauthentication</td>
<td>Unknown</td>
<td>Likely random MAC address, trying to DDOS or gather handshakes</td>
</tr>
<tr>
<td>07:7D:FD:FF:A1:A1</td>
<td>Deauthentication</td>
<td>Unknown</td>
<td>Likely random MAC address, trying to DDOS or gather handshakes</td>
</tr>
<tr>
<td>00:FF:A4:9F:FB:98</td>
<td>Deauthentication</td>
<td>Unknown</td>
<td>Likely random MAC address, trying to DDOS or gather handshakes</td>
</tr>
<tr>
<td>02:C0:CA:8D:A3:F4</td>
<td>KRACKS Attack</td>
<td>Unknown</td>
<td>Likely random MAC address, trying to break encryption</td>
</tr>
<tr>
<td>00:13:37:A6:16:8B</td>
<td>MiTM/Karma</td>
<td>Hak5</td>
<td>Pineapple doing pineapple things. At least 50 other Pineapples were seen as well.</td>
</tr>
<tr>
<td>AE:5F:3E:64:7F:0A</td>
<td>SSID bigger than 32 bytes</td>
<td>Unknown</td>
<td>Something fishy is going on here with the SSID</td>
</tr>
</tbody>
</table>
Wall of sheep?  
Not really, but here's some probably fake creds

<table>
<thead>
<tr>
<th>Server</th>
<th>Protocol</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.97.160.12 (hotdog.net)</td>
<td>HTTP</td>
<td>bomb</td>
<td>8=* ***</td>
</tr>
<tr>
<td>136.160.88.139 (usna.edu)</td>
<td>HTTP</td>
<td>dadmin010</td>
<td>PS2YS65***********</td>
</tr>
<tr>
<td>23.56.119.46 (samsung.com)</td>
<td>HTTP</td>
<td>highspeed2</td>
<td>HCMRX2***********</td>
</tr>
<tr>
<td>161.170.244.20 (walmart.com)</td>
<td>HTTP</td>
<td>leviton4</td>
<td>XOAELJU***********</td>
</tr>
<tr>
<td>70.120.194.95 (austin.0x.no)</td>
<td>HTTP</td>
<td>NationalShitpostingAgency</td>
<td>NSA********</td>
</tr>
<tr>
<td>133.242.149.131 (perorist.win)</td>
<td>HTTP</td>
<td>peropero</td>
<td>perop***********</td>
</tr>
<tr>
<td>23.38.226.56 (xfinity.com)</td>
<td>HTTP</td>
<td>surt8</td>
<td>U0Z69L8Y***********</td>
</tr>
<tr>
<td>64.137.180.143</td>
<td>HTTP</td>
<td>******* will help build Trump’s wall</td>
<td>F87ef***********</td>
</tr>
<tr>
<td>211.251.140.134</td>
<td>SNMPv1</td>
<td>SNMP Community</td>
<td>public</td>
</tr>
</tbody>
</table>
data leaks
sharing is caring!

App API’s using HTTP

Found in the DEFCON 25 dataset this API leaks location information potentially from a weather app showing sunrise info on a mobile device. The app could have trusted access to location data and shares it with anyone listening.

Host: www.met.no

API Call:
http://api.met.no/weatherapi/sunrise/1.1/?lat=36.1164&lon=-115.1785&date=2018-08-11

Lat/Lon: 36.1164,-115.1785

API still accepts HTTP requests today but was updated a little:
http://api.met.no/weatherapi/sunrise/2.0/?lat=36.1164&lon=-115.1785&date=2018-08-11&offset=-08:00
data leaks
sharing is caring!

App API’s using HTTP
Found in the DEFCON 26 dataset this API leaks location information from a ZTE Desktop Widget using Accu-Weather which likely has privileged access to location data on your phone.

Host: accu.weather.com
Device: Android


Lat/Lon: 36.11675439,-115.1785

Currently still using HTTP for the API.
Alienware Bloatware

Found in the DEFCON 26 dataset this API call leaks your Alienware laptop serial number and OS version.

Host: content.dellsupportcenter.com

Device: Windows 10 Build 6.0.6992.1236

API Call:
http://content.dellsupportcenter.com/mstr/pd.txt?pr=Alienware%2017%20R3&os=Win%2010%20%2817134.165%29&build=6.0.6992.1236&up=true&serial=9RN1462&id=4997f137-e883-45e2-9714-50d5f2c4c45b&dl=true&saaver=2.2.3.2&wr=1%2F20%2F2017%2012%3A00%3A00%20AM

Warranty Status: Expired Jan 20, 2017
DNS is typically unencrypted

The listed domains had DNS queries that were passed in the clear. If the website is using encryption no other information beyond DNS was gathered.

<table>
<thead>
<tr>
<th>ALL YOUR DNS...</th>
<th>ALL YOUR DNS...</th>
<th>ALL YOUR DNS...</th>
</tr>
</thead>
<tbody>
<tr>
<td>voyzwhpwt.coxhn.net (x1k)</td>
<td>tracker-api.my.com</td>
<td>tracking.optimatic.com</td>
</tr>
<tr>
<td>track.eyewitnessads.com</td>
<td>digitaltarget.ru</td>
<td>pixel.*.com (x50)</td>
</tr>
<tr>
<td>splunkoxygen.com</td>
<td>eb3dba18c25854f62ed2c3b5e73cd97a.0001abf0.iot.dc.org</td>
<td>cdn.*.com (x5k)</td>
</tr>
<tr>
<td><a href="http://www.pornhub.com">www.pornhub.com</a></td>
<td>wifiprotect.mcafee.com</td>
<td>api.*.com (x5k)</td>
</tr>
<tr>
<td><a href="http://www.pjrc.com">www.pjrc.com</a></td>
<td><a href="http://www.wifipineapple.com">www.wifipineapple.com</a></td>
<td>f*ckinghomepage.com</td>
</tr>
<tr>
<td>teamviewer.com</td>
<td>abercrombie.com</td>
<td>ads.*.com</td>
</tr>
</tbody>
</table>
DNS is typically unencrypted
Thanks to Slack using subdomains we can find out about all of the secret slacks people are using at DEFCON.

<table>
<thead>
<tr>
<th>SLACK FTW</th>
<th>0xproject.slack.com</th>
<th>def0x.slack.com</th>
<th>operationona.slack.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018defconwork.slack.com</td>
<td>files.slack.com</td>
<td>rbs-interns.slack.com</td>
<td></td>
</tr>
<tr>
<td>avtokyo.slack.com</td>
<td>ic3ethereum.slack.com</td>
<td>redballoonsecurity.slack.com</td>
<td></td>
</tr>
<tr>
<td>blockchainedu.slack.com</td>
<td>infosecboston.slack.com</td>
<td>seccon2016noc.slack.com</td>
<td></td>
</tr>
<tr>
<td>cohort-x-corp.slack.com</td>
<td>mohikan.slack.com</td>
<td>sfs-csusb.slack.com</td>
<td></td>
</tr>
<tr>
<td>consensys.slack.com</td>
<td>muckrock.slack.com</td>
<td>spamandhex.slack.com</td>
<td></td>
</tr>
<tr>
<td>darksite26.slack.com</td>
<td>openzeppelin.slack.com</td>
<td>status-im.slack.com</td>
<td></td>
</tr>
</tbody>
</table>
DEFCON is truly a global community

DEAUTH’s will happen

PINEAPPLES are a thing

API’s will leak

IT WAS DNS (MYSPACE?????)

Hackers like Slack for some reason

Don’t believe the HYPE, looking at you broadpwn
countermeasures protection

knowing is half the battle!

DO NOT AUTO-CONNECT
Do not enable auto-connect when connecting to an open Wireless Network! Delete networks from your devices that you are not going to continue to connect to!

USE A VPN
VPN services are cheaper and easier to use now than ever. You can get one that has an app on your device that will enable you to easily enable it when you are on an untrusted network.

USE 4G*/5G INSTEAD
Using data over cell networks should reduce your risk and coupling it with a VPN on top will make it even better.

*New research about 4G vulnerabilities is due to be released stay tuned for updates and panic.
thank you
this project could have not been possible without so many of you!

DEF CON
thank you for giving me the inspiration to keep being curious!

HAK 5
huge thank you to everyone at hak5 who’ve been supportive from the beginning!

KISMET
huge thank you to dragorn! without kismet this project wouldn’t have been possible!

SAINTCON
the conference that gave me the confidence to keep presenting!

DC801
greetz and thank you to all of the supportive utah hackers who have always been there for me!

NETWORK MINER
thank you to Netresec for giving me access to their awesome software!

GRAPHISTRY
thank you for solving big data visualization problems and providing me access to your API!

WIGLE.NET
thank you for creating an awesome war driving app and sharing the data with the world!
thank you
this project could have not been possible without so many of you!

HUGE THANK YOU TO EACH OF YOU HERE AND ONLINE THAT CONTINUALLY SUPPORT ME!

you are the inspiration that keeps me innovating and building late into the night!
the end

@d4rk_m4tter

github.com/mspicer/pcapinator

palshack.org

@d4rk_m4tter_

bit.ly/2OkdYz2