Weaponizing your Pets

The War Kitteh and the Denial of Service Dog

DefCon
10 August 2014
Introductions

- Gene Bransfield @gbransfield
- Principle Security Engineer @ Tenacity
- I Love My Job
- They want my job
- They can’t have it
What is This About?

• Having a humorous idea
• Bringing Ideas to Fruition
• Stories of Triumph and Woe
• Valuable Lessons Learned
Weaponize your PETS!?!?!

OH GOD, WHY WOULD YOU DO THAT?
Background:

• 15% of the world’s Internet traffic is dedicated to Cats

• I find most tech briefings boring, so I use pics of cats to help keep people awake
The pic that started it all:
Just Finished a Presentation…

• Someone told me they were going to give me this tracking collar that they won
  – GPS
  – Cellular
  – Told you where the Kitteh was at all times

• …add a little wifi sniffer and we’d have a WAR KITTEH!!!!
What about the DoS Dog?

• AT Outerz0ne

• LadyMerlin walked in with a dog wearing a harness that said Denial of Service Dog

• I said “Is there a Pineapple in there?”
  – No, the dog is a pain, but that’s a great idea!
Working Animals
Badder Ass Working Animals
Real Navy Seal
Flipper Pic
Other Research Efforts

• Accoustic Kitty
MY STUFF -- Requirements

• War Kitteh Requirements:

• CONOP: Put a collar/harness on a cat and allow said feline to roam the neighborhood normally. The collar/harness shall contain a GPS tracking device and a wireless sniffer/scanner. We'll be looking to map WiFi Access points similar to war driving.
  – 0.) CAT SHALL NOT BE HARMED
  – 1.) Cat shall be able to comfortably wear stuff and should not be harmed by said stuff or by wearing said stuff
  – 2.) GPS shall record waypoints with associated date/time stamp for collection post-walkabout (e.g. when the cat returns).
    • a.) optionally, solution to provide on-demand locational data as well so we can find a lost kitteh or kitteh harness
  – 3.) WiFi sniffer scanner shall sync time with GPS device and collect wifi SSIDs and other WiFi-related signals for later Analysis
Other Products

• Mr Lee Cat Cam
  – http://www.mr-lee-catcam.de

• Pet Tracker
  – http://www.pettracker.com

• Garmin
  – https://buy.garmin.com/
GumStix
Cotton Candy
RockChip 3066
Thinking about it…

- Small form factor
- GPS
- Wifi
- Cellular
How ‘bout a Cell Phone?
Now make an APK!?!?

• Need to code a wifi war driving

• Let’s do some android coding…?

• They already thought of that…
WiGLE WiFi
Volunteer Cat
Cat Coat?
“Cat” Coat
Plan:

• Put Tech in Coat
• Put Coat on Cat
• Send cat on walkabout
• Recover data when cat returns
• Profit!
Step 1
Step 2
Step 2 cont
Step 3
Step... 4?
...yeah...
Trying this again....
Ummm....
Last Known GPS...?
Lessons Learned

• Cats are damn hard to work with

• Always test before you send out ‘spensive stuff

• Amazon Prime account

• Worried about cat, so no more coat

• Smaller form factor with same capability
Talked to my Friend Bill...

- **Hobbiest & Technologist**

- **What about Arduino**
  - Small form factor
  - Low power consumption
  - Does what you need it to do and no more
  - Many chips, variety of solutions
What is Arduino?

• Arduino is an open-source electronics platform based on easy-to-use hardware and software. It's intended for anyone making interactive projects.

• Lots of expansion boards of “Shields”

• Make robots, remote control cars, home security products, etc.
Freezer check
Robotic Hand
Video Games
Small Form Factor...

- Arduino Mini...
Good News… Bad News…

• **Good News!**
  – Open Source
  – Inexpensive

• **Bad News!**
  – Poorly Documented
  – Takes forever to get to you
  – Questionable performance…
Well I Never…

• Done Anything with Arduino

• Worked with firmware/small chip sets

• Not a professional coder…

• Soldered
Don’t Worry

It's Easy!
Plan...

1.) Learn about Arduino
   -- Get some basic stuff

2.) Decide on most accommodating form factor for WarKitteh

3.) Put it all together in a collar FTW

4.) Do some stuff with DoS Dog…
Basic Stuff…

- Arduino Uno
Flashy Things…
Cooler Stuff!

• I need software libraries for WiFi  
  – They got it!

• I need software libraries for GPS  
  – They got it!

• I need software libraries for SD card stuff  
  – They got it!!
Shout Out…

- Jeremy Blum Videos
  – Jeremyblum.com
I r a Expert!

WHY YES

I AM THE EXPERT!
So I got...

• Arduino WiFi Shield
And Finally…

• Itead Studio GPS Shield
The plan...

• Get a WiFi collection function
  – Write to SD Card

• Get a GPS tracker
  – Write to SD card

• Combine
WiFi Shield

• Set up was easy

• Drivers worked

• Messing around with parameters and variables and

• VICTORY!!!
EASY!!!
A bit about GPS

• **NMEA string**
  – National Maritime Electronics Association
    
    $GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47

• **Boot process**
  – Start up
    • Where am I…?
  – Listen to SPACE
  – Get a lock (at least 3 satellites)
    • 2-15 minutes!!! (depending on conditions)
• Poorly Documented

• No docs in kit

• Searched forever to find baudrate of 34800

• Now I can’t NOT find it
Put all the components together!
So weird error…

• Something about 80% of memory utilized…

• Libraries and variables were too much…

• Arduino Uno – 32K

• Arduino Mega2560 – 256K
Purchased the Mega...
Put THAT all together
It WORKS!!!

WOOHOO!!!
Arduino Mega2560

- Mo Memory
  - Mo betta
  - Mo betta

- Mo Ports
  - Mo betta

- Mo Size
  - Not Mo betta
Tiny Arduino2560?

- Arduino MegaMini from JK Devices

- DON’T DO IT!!!!! more later...
Spark Core

• Spark.io
GPS chip

- GP-635T
Micro SD Card

- SparkFun MicroSD Breakout Board
So it works, but...

- MegaMini says it’s going to be 4 weeks to ship at least...

- Other solutions are too big (size) or too small (memory)

- Spark.io Spark Core
  – Shipping problem, had to borrow one
Real Tech on Spark

- ARM 32-bit M3 CPU ✓
- 128KB Memory (wooHOO!!!) ✓
- SPI and I2C compliant ✓
- TI CC3000 WiFi chip ✓
- “Arduino Compatible” ✗
  - Worked with external components
  - Coding wouldn’t work
OMG

Oh God

not again...
Start-up Product

• Starting everything from scratch
  – Didn’t have libraries for the stuff I needed

• To spite that, VERY COOL

• Dedicated core group of developers
  – Shout out to peekay123

• Lets see what happens…
Libraries

• Someone Posted SD Card Libraries to the forums
  – They Compiled!

• Someone posted GPS libraries to the forums…
  – They Compiled & Worked with GPS Shield!
WiFi Libraries

• …no readily available stuff for what I wanted to do

• Spark is an “Internet of Things” device

• WiFi as a service – not to mess with
Adafruit FTW!

• Adafruit CC3000 Breakout board

• Libraries available on the Adafruit website for Download

• Messed with it earlier… let’s see if it works!
It WORKS!!!

WOOHOO!!!
So now…

• Got GPS working on Spark

• Got SD compiled on Spark

• Got SSID collection working on Spark

• Now to work with tiny components
Now, onto soldering
Rule 1

grab this part.

noooooo not this part!
Rule 2
First attempts went very well...
• At home everything went Great!

• Took it out for a walk around the yard and it was great!

• Took it for a ride in the car and FAIL!!!

• What happened…?
Spark Concept

• Internet of Things device

• Never meant to be disconnected from the Internet

• Encased in a “If status == WIFI_ON” clause
  – Must be connected to a known WAP to return true
What to do

- Noticed that I could scan SSID’s before I associated with the AP
- Removed code from clause
- That’s all I need anyway!
More testing…

• Took it for a drive

• Got Data back!!!!

• Looked at the GPS cords… they were off by about half a mile…

• GPS Libraries were wrong
TinyGPS++

• LOVE to use TinyGPS++
  – Everything I need
  – Didn’t work in Spark

• How to Port Libraries? Talk to Bill

• Rocket Science
  – Replace Arduino with Spark and fix what blows up
It WORKS!!!

WOOHOO!!!
Next Problem

• **Power Consumption**
  – How to do it best…?

• **Eflite 3.7v 500mAh batteries**
Testing for Power Consumption

• Originally tried cycling everything on and off
  – That really didn’t work well

• Put main chip in Deep sleep to save juice
  – Keep GPS chip on

• Collections every 30 sec lasted 4 hours

• Collections every 10 minutes lasted 8 hours
Time to Make Collar
Form Factor

• DeSoldering is TWICE as much fun as soldering
  – NOT

• Internet again NOT helpful

• YouTube makes it look TOO easy
NOVALabs Shout Out

• Reston, VA

• Ted
  – Mad Scientist/Evil Genius
  – Helped me learn EAGLE

• Brian
  – Soldering Tutor
  – Right Iron, Right Solder
Now... where my Maker’s at?

• Need to make a cat collar...

• How do I make a cat collar???
  – Lots of Ways

• Friend Joe suggested ribbons
  – Sew them together
Ribbon
Get a Grandma
Volunteer Cat
So let’s PRACTICE first..

- Let cat out with no-tech collar and see if he tolerated it…

- HE DID!
Old Way…
Weight...
So... New plan

• Tech goes in the Collar

• Collar goes on the cat...

• Cat goes on a walk about...

• Profit
Initial results

• ...Nothing....!?!?!?!?

• Put collar on cat

• Cat walked under a bush

• Hung out and licked himself for 20 minutes
New Deployment procedures

• Let collar sit outside for 5-10 min

• Bring cat to collar, put it on cat

• Let cat go for a walk about...

• …profit…!?!?!???????
SUCCESS!!!!
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Lat</th>
<th>Lon</th>
<th>SSID</th>
<th>Signal</th>
<th>Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/4/2014</td>
<td>11:46:31</td>
<td>39.09994</td>
<td>-76.******</td>
<td>8NBN8</td>
<td>-93</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:51:38</td>
<td>39.09986</td>
<td>-76.******</td>
<td>KNPI1</td>
<td>-95</td>
<td>WEP</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:51:38</td>
<td>39.09986</td>
<td>-76.******</td>
<td>NOTyourWiFi</td>
<td>-94</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:56:46</td>
<td>39.09987</td>
<td>-76.******</td>
<td>UDRK2</td>
<td>-98</td>
<td>WEP</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:56:46</td>
<td>39.09987</td>
<td>-76.******</td>
<td>8NBN8</td>
<td>-96</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:56:46</td>
<td>39.09987</td>
<td>-76.******</td>
<td>P41R1</td>
<td>-95</td>
<td>WEP</td>
</tr>
<tr>
<td>7/4/2014</td>
<td>11:56:46</td>
<td>39.09987</td>
<td>-76.******</td>
<td>NOTyourWiFi</td>
<td>-96</td>
<td>WPA2</td>
</tr>
</tbody>
</table>
Coco
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Lat</th>
<th>Lon</th>
<th>SSID</th>
<th>Signal</th>
<th>Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>6WWV8</td>
<td>-94</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>CROWLEY</td>
<td>-93</td>
<td>WEP</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>DIRECT-roku-09C2C5</td>
<td>-88</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>xfinitywifi</td>
<td>-82</td>
<td>OPEN</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>CoxWiFi</td>
<td>-80</td>
<td>OPEN</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>16:59:07</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>CableWiFi</td>
<td>-80</td>
<td>OPEN</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:04:16</td>
<td>38.94365</td>
<td>-77.*****</td>
<td>Apple Network 6b7973</td>
<td>-89</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:04:16</td>
<td>38.94365</td>
<td>-77.*****</td>
<td>6WWV8</td>
<td>-92</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:04:16</td>
<td>38.94365</td>
<td>-77.*****</td>
<td>CQXPP</td>
<td>-76</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:04:16</td>
<td>38.94365</td>
<td>-77.*****</td>
<td>P6829</td>
<td>-96</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:09:25</td>
<td>38.94386</td>
<td>-77.*****</td>
<td>NETGEAR</td>
<td>-94</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:09:25</td>
<td>38.94386</td>
<td>-77.*****</td>
<td>DIRECT-roku-409</td>
<td>-93</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:14:34</td>
<td>38.9435</td>
<td>-77.*****</td>
<td>7LXJ3</td>
<td>-83</td>
<td>WEP</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:14:34</td>
<td>38.9435</td>
<td>-77.*****</td>
<td>peri</td>
<td>-93</td>
<td>WPA</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:14:34</td>
<td>38.9435</td>
<td>-77.*****</td>
<td>Ward3DC</td>
<td>-88</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:14:34</td>
<td>38.9435</td>
<td>-77.*****</td>
<td>MYI14</td>
<td>-96</td>
<td>WEP</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:19:43</td>
<td>38.94323</td>
<td>-77.*****</td>
<td>7LXJ3</td>
<td>-94</td>
<td>WEP</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:19:43</td>
<td>38.94323</td>
<td>-77.*****</td>
<td>LuckyWhale_2GEXT</td>
<td>-93</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:24:52</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>LKMY4</td>
<td>-96</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:24:52</td>
<td>38.94373</td>
<td>-77.*****</td>
<td>MYI14</td>
<td>-94</td>
<td>WEP</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:40:19</td>
<td>38.94316</td>
<td>-77.*****</td>
<td>LuckyWhale_2GEXT</td>
<td>-92</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:40:19</td>
<td>38.94316</td>
<td>-77.*****</td>
<td>Motyka Wireless</td>
<td>-88</td>
<td>WPA</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:40:19</td>
<td>38.94316</td>
<td>-77.*****</td>
<td>Ward3DC</td>
<td>-90</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:40:19</td>
<td>38.94316</td>
<td>-77.*****</td>
<td>SXJ32</td>
<td>-94</td>
<td>WPA2</td>
</tr>
<tr>
<td>7/19/2014</td>
<td>17:40:19</td>
<td>38.94316</td>
<td>-77.*****</td>
<td>Q8ZS7</td>
<td>-96</td>
<td>WEP</td>
</tr>
</tbody>
</table>
That’s the WarKitteh!

Ding!

I'm done
Denial of Service Dog

Whippet

Whippet Good
DoS Dog

• So…. More trolling than anything

• WiFi Pineapple
  – Procured at ShmooCon

• TV B Gone
  – Adafruit/RadioShack

• Doggie Backpack with “Denial of Service Dog” patches
What I’m gonna do is...

• **Karma**
  – Answers Probes

• **DNS Spoof**
  – Redirects all things to Pineapple

• **randomroll**...
  – ‘cause RickRoll makes trolling better
TV B Gone ...in pieces.
TV B Gone
Some minor modifications...
Patches

• WHOLLY Crap! What a pain in the butt!

• Nobody does it anymore

• ‘Cept Irina & Friends at JoAnn’s Fabrics in Sterling, VA
  – Thank Jesus
Victory!
Demo Video
Volunteer Dog
Volunteer Dog
Volunteer Dog Ready to Go!
Putting it on a Doggie Backpack
LEDs...
Dog will Shake

• TV B Gone wasn’t designed to be shaken in the manner in which V-dog was shaking..

• Also set off the TV-B-Gone
Do you mind if we come in?

Sure! Want something to drink?

Why does it say Denial of Service dog?

Love!? Play!??
Sports Bar

QUE?!

BALL!

Never gonna give you up...
Best STORE

Do you mind if We come in?

Sure! Make sure he Doesn’t poop on anything

LOVE YOU!!!
Box Store Cont...

Circus Afro
Circus Afro

Best
STORE

GOAL!!!!

SQUIRREL!

Denial Of Service Dog
Results...

• According to results, several hapless victims connected to Karma/Denial of Service dog
  – Logging Fail

• Only one person asked about “Denial Of” service dog

• Most people said “NICE DOGGY!”
So What Have We Learned???

• A tech hobbyist with no prior firmware experience can create a functional WarKitteh Collar in a short amount of time.

• In 2014 there are STILL unsecured WiFi hotspots

• Lots of devices still probe

• Still no patch for human stupidity

• Cats – AND DOGS – are really hard to work with
Shout out

• Jeremyblum.com
• Adafruit.com
• Sparkfun.com
• Spark.io
• Arduino.cc
Oh BTW

- JK Devices (jkdevices.com)
  - Complete Scam
  - Don’t waste your money

- No emails

- No contact

- No Product
Thanks

- Reeves
- Bill
- Joe
- Joey
- Nancy
- Ricky
- V-dog.owners
- Spark.io Guys
- NoVaLabs Guys
- V-dog
- Skitzy
- Coco
- Tenacity
- DefCon
DefCon WarKitteh

WarKitteh
Walking The Strip
Monuments
Willing Participants
Drunk Participants
# Results

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Lat</th>
<th>Lon</th>
<th>SSID</th>
<th>Signal</th>
<th>Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/9/2014</td>
<td>5:34:42</td>
<td>36.12057</td>
<td>-115.173</td>
<td>AirOne</td>
<td>-90</td>
<td>WPA2</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>Flamingo-Rooms-Cox</td>
<td>-89</td>
<td>OPEN</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>MOTOMESH</td>
<td>-81</td>
<td>OPEN</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>attwifi</td>
<td>-73</td>
<td>OPEN</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>CROMWELL</td>
<td>-88</td>
<td>OPEN</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>GJJ</td>
<td>-93</td>
<td>WPA2</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>GAMMA</td>
<td>-86</td>
<td>WPA2</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>ALPHA</td>
<td>-84</td>
<td>WPA2</td>
</tr>
<tr>
<td>8/9/2014</td>
<td>5:45:01</td>
<td>36.11575</td>
<td>-115.173</td>
<td>DELTA</td>
<td>-86</td>
<td>WPA2</td>
</tr>
</tbody>
</table>
Video... er... PIC!!!
DefCon DoS Dog
CNN Kitteh
Questions?

Thank You For Your Attention Any Questions?
That’s all Folks

Thank You

Kitteh is Pleased