

Dessert Deity

A Recipe for Splunk, Raspberry Pi, Kali, Wi-Fi

Ryan Adler (TRex in IRC/Slack) | Security Engineer, SplunkTrust, Defense Point Security, Accenture Federal Services

September 26, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Background

- ▶ This idea was born out of a conversation with DPS Co-worker:
 - I wish there was a way to alert when someone leaves work

So naturally we came up with an idea that centered around Splunk. This was my take.



Sources of Information

A little bit of column A, a little bit of column B

Access Events

- ▶ Log on and Log Off events
- ▶ Successful email access
- ▶ Web Portal activity

Networking Events

- ▶ DHCP leases
- ▶ Static IP traffic
- ▶ DNS queries, or firewall sessions

Timecard Events

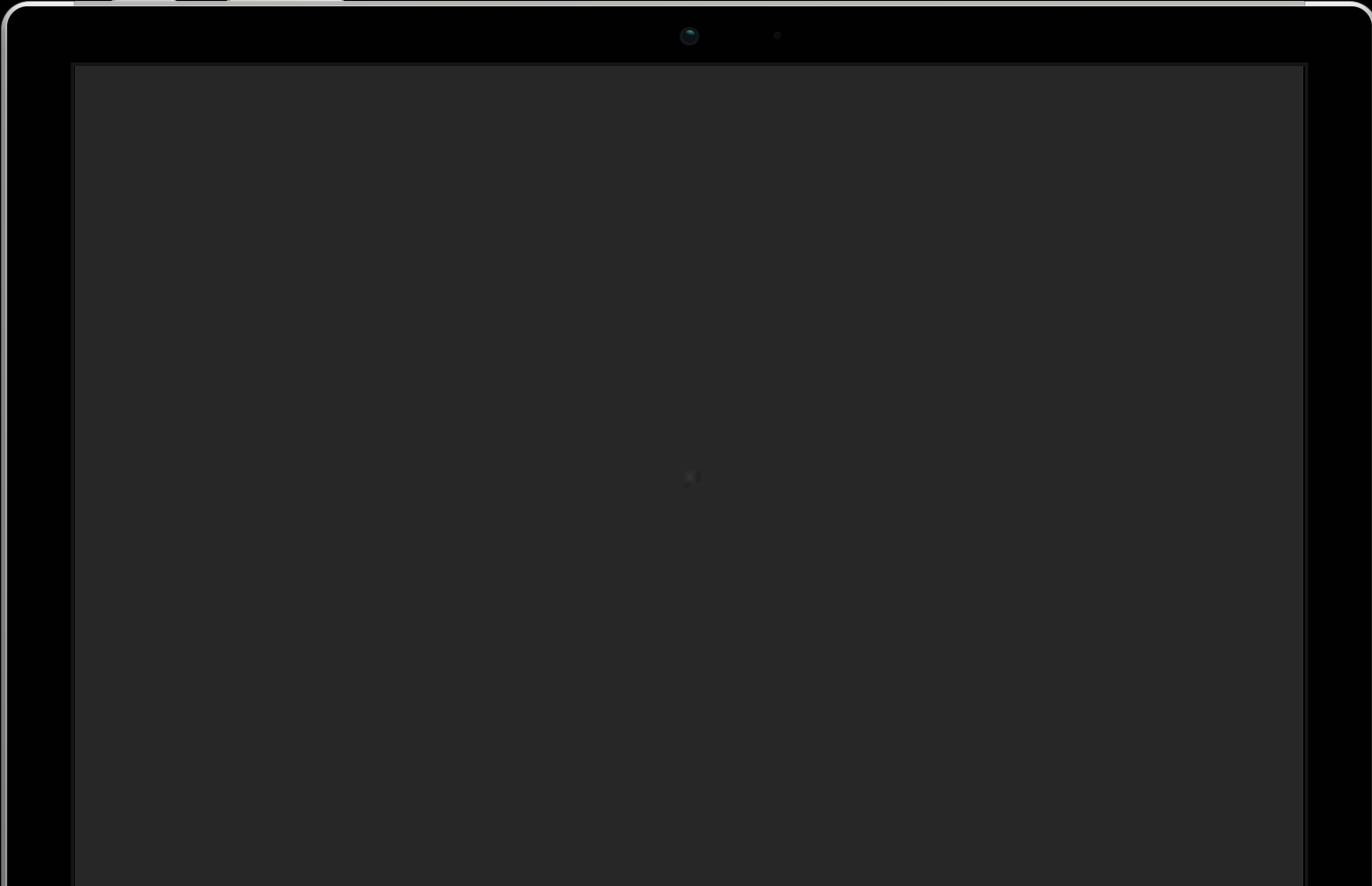
- ▶ Clocking in
- ▶ Clocking out
- ▶ I'm not even supposed to be working today

Wi-fi And Your Data Plan

- ▶ While Data plans are common, so are Wireless hotspots
- ▶ From airports, and coffee shops, to libraries, and even the zoo
- ▶ Wi-Fi is a fire and forget technology to the customer. Enable once, and it'll likely stay enabled. It makes it easier to connect to hot spots, at work and home, and sometimes it'll even inform you when a wireless signal is available.

A Recipe for Information

Wi-Fi, data plans, and ease of use



- ▶ The recipe isn't new, but we've thrown in a couple of twists.
 - Image 1 part Kali Linux for ARM onto a MicroSD
 - Fully bake into a Raspberry Pi
 - Season properly with Scripts
 - Serve with Universal Forwarder

Raw Data

```
<wireless-network number="397" type="infrastructure" first-time="Sun Aug 13 16:27:59 2017" last-time="Sun Aug 13 16:26:27 2017">
<SSID first-time="Sun Aug 13 16:27:59 2017" last-time="Sun Aug 13 16:26:27 2017">
<type>Beacon</type>
<max-rate>54.000000</max-rate>
<packets>7</packets>
<beaconrate>10</beaconrate>
<encryption>WPA+TKIP</encryption>
<encryption>WPA+PSK</encryption>
<encryption>WPA+AES-CCM</encryption>
<essid cloaked="false">0AC4A6</essid>
</SSID>
<BSSID>2C:30:33:0A:C4:A6</BSSID>
<manuf>NETGEAR</manuf>
<channel>1</channel>
<freqmhz>2412 35
<maxseenrate>540
<carrier>IEEE 80
<encoding>CCK</e
<packets>
<LLC>28</LLC>
<data>28</data>
<crypt>0</crypt>
<total>35</total>
<fragments>0</fr
<retries>0</retr
</packets>
<data size>0</dat
```

Time	Event
8/13/17 9:27:12.000 AM	<pre><wireless-client number="1" type="tods" first-time="Sun Aug 13 16:09:11 2017" last-time="Sun Aug 13 16:27:12 2017"> <client-mac>B8:27:EB:E6:3D:94</client-mac> <client-manuf>Raspberry Pi Foundation</client-manuf> <SSID first-time="Sun Aug 13 16:09:11 2017" last-time="Sun Aug 13 16:27:12 2017"> <type>Probe Request</type> <max-rate>54.000000</max-rate> <packets>1</packets> <encryption>None</encryption> </SSID> <channel>5</channel> <maxseenrate>1.000000</maxseenrate> <carrier>IEEE 802.11b+</carrier> <encoding>CCK</encoding></pre>

Time Series Results

Busiest Hour Today

7

Busiest Hour over 7 Days

17

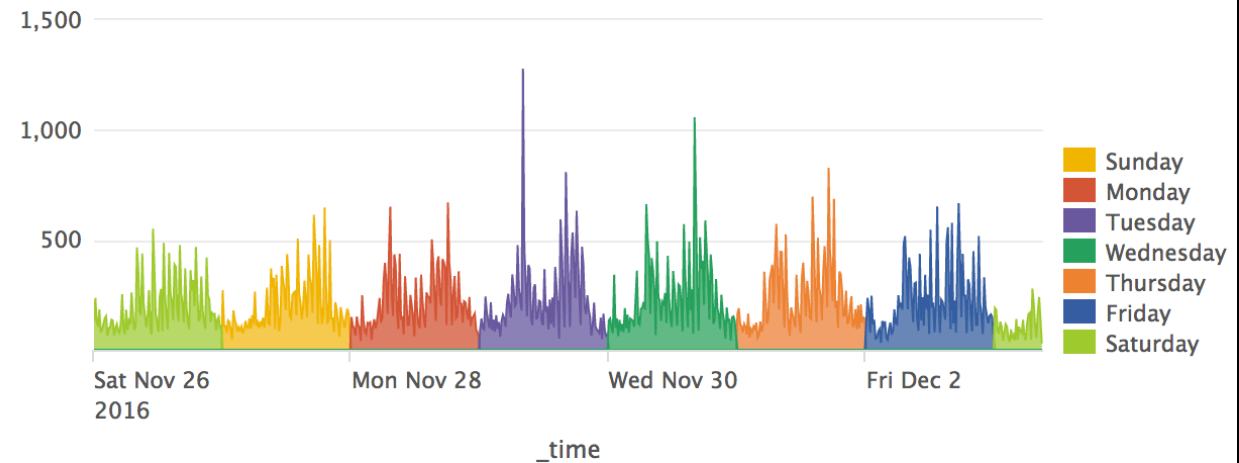
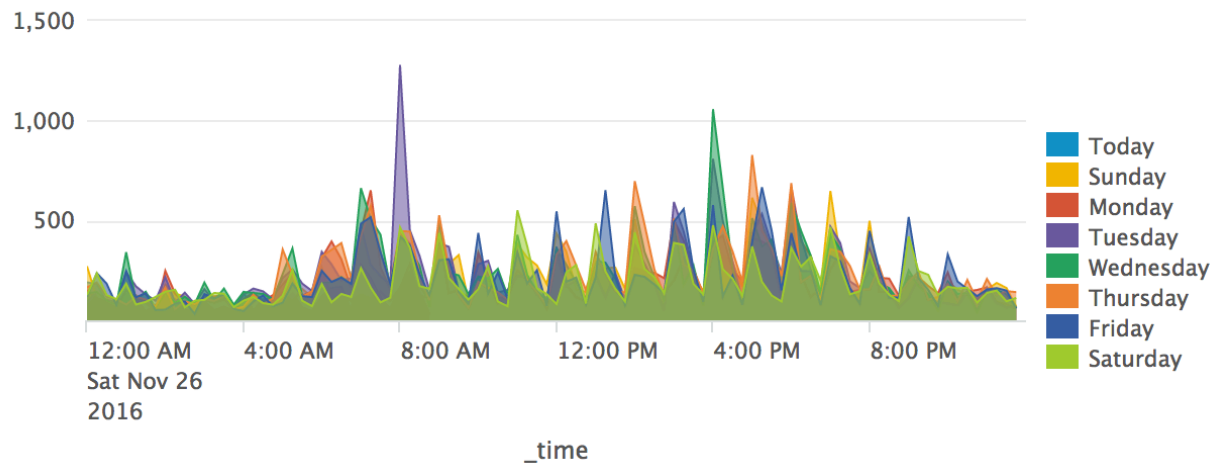
Busiest Minute Today

08:09

Busiest Minute over 7 Days

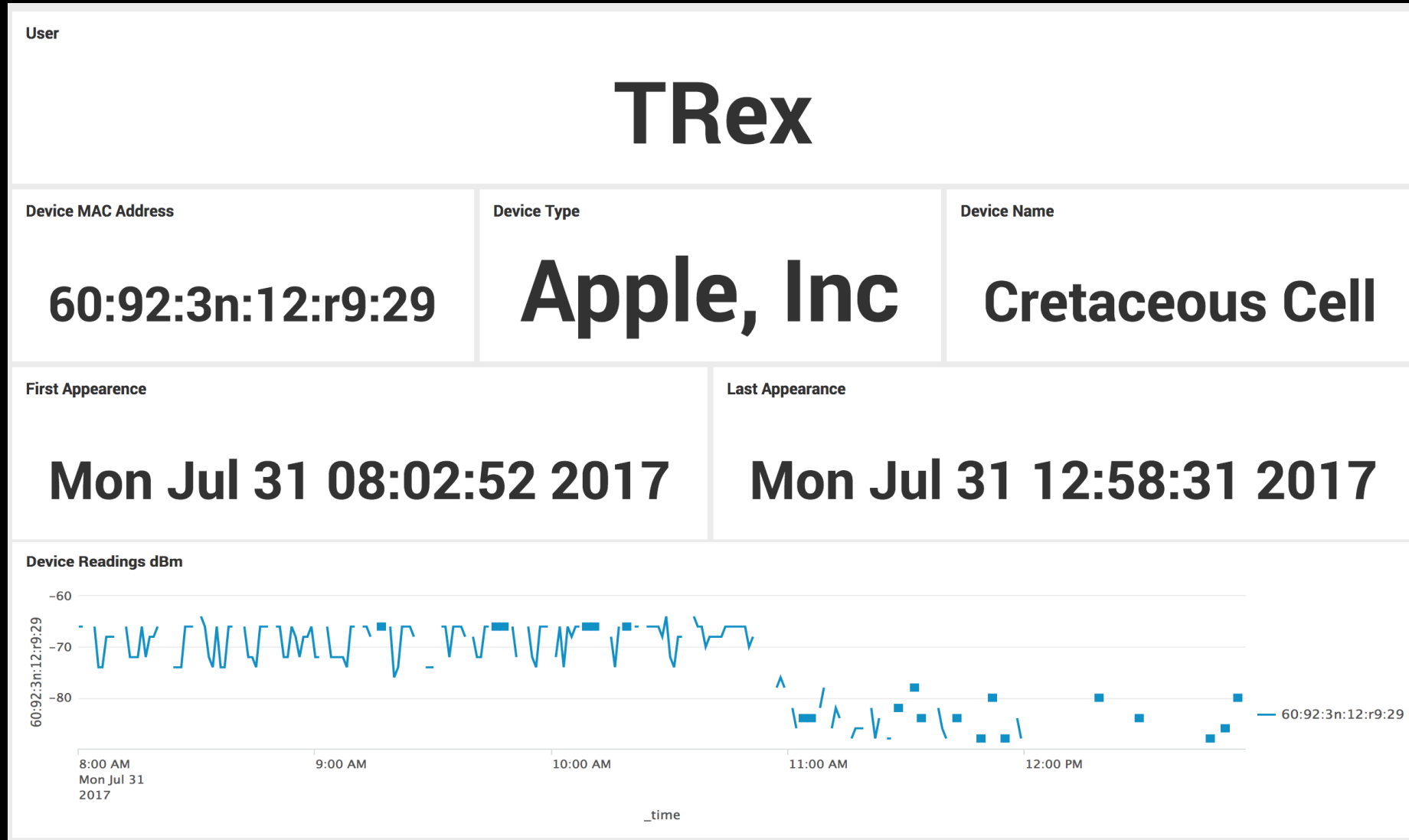
11/30/2016 16:02

Day by Day



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2016.12.0 (Windows NT 6.0; WOW64; rv:51.0) like Gecko" 128.241.220.02 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MEX11A74-0" 317.27.160.00 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2016.12.0 (Windows NT 6.0; WOW64; rv:51.0) like Gecko" 128.241.220.02 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MEX11A74-0" 317.27.160.00 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1" 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2016.12.0 (Windows NT 6.0; WOW64; rv:51.0) like Gecko" 128.241.220.02 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MEX11A74-0" 317.27.160.00 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

Interactive Drilldown For Device History



An Unusual Source Of Information

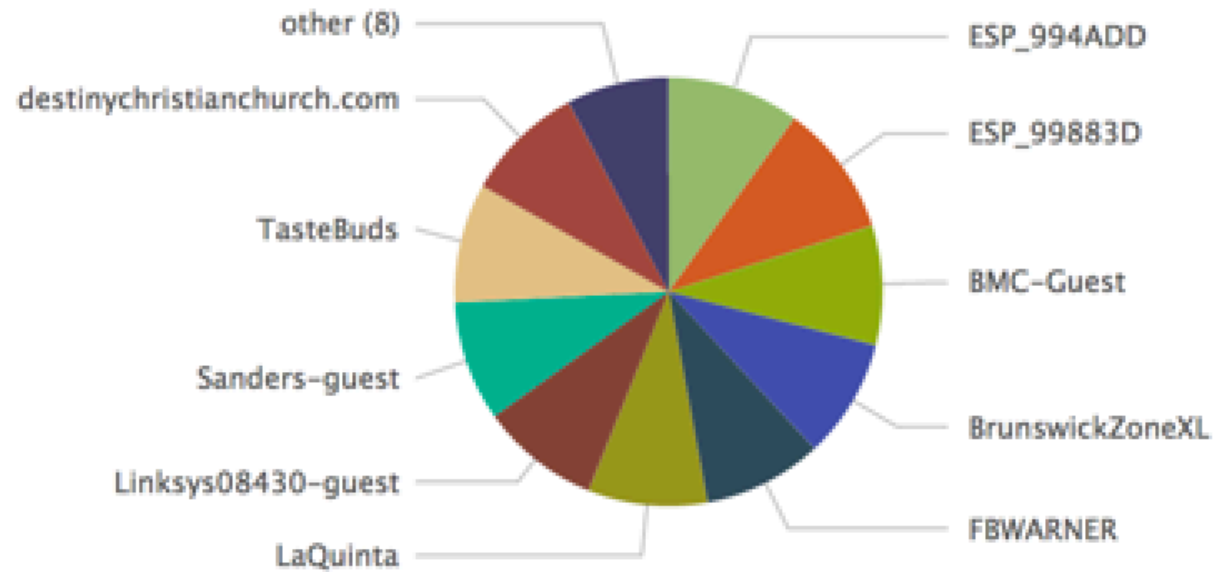
Mobile Devices and Wi-Fi



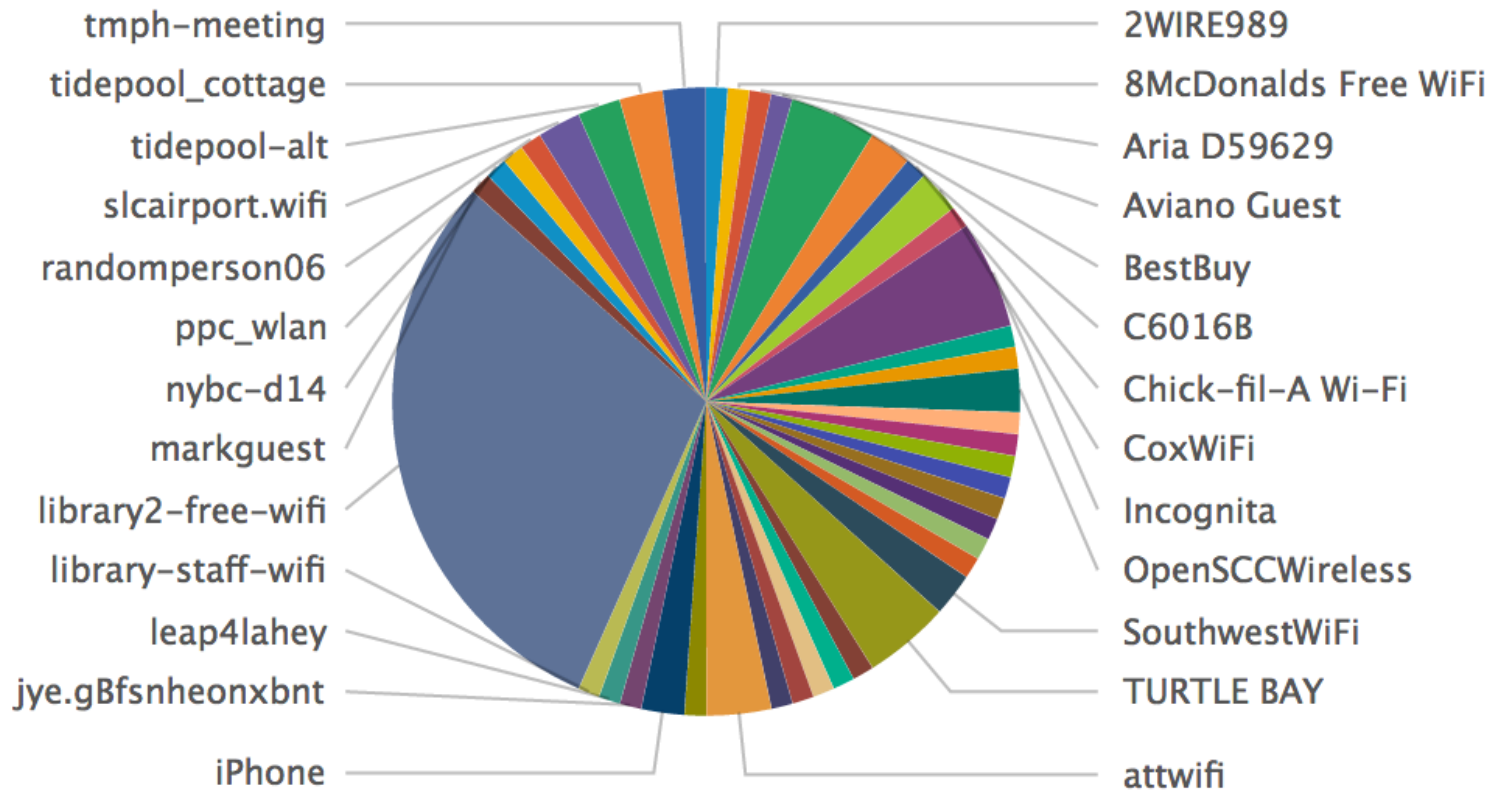
- ▶ Am I connected to a wireless network?
 - Preferred network 1, are you there?
 - Preferred network 2, are you there?
 - Preferred network 9, are you there?
 - Is anybody listening to me?

SSID Results

List of SSIDs from a single, well traveled device.



SSID Results



Drive-Fi: Dessert Delivery

On the Rocky Road

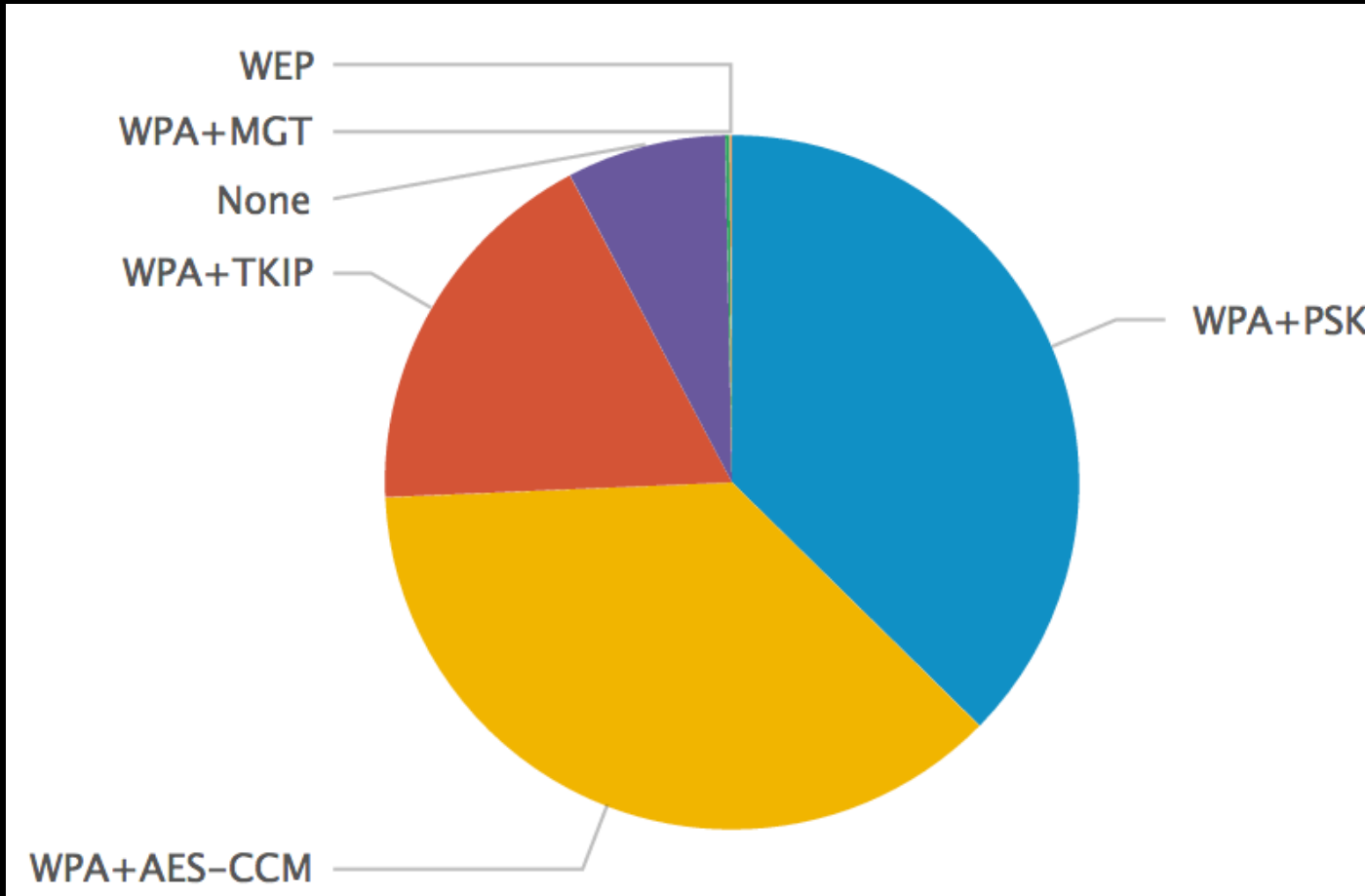
► Objectives

- See how the system operates while driving
- Survey the neighborhood security posture (WPA vs WEP)
- Try it out on the freeway
- Don't look suspicious



“PSA: Please do not **Splunk** and Drive”

Wireless Wanderer



► Encryption Stats

- 450 Unique access point MAC addresses
- 80%+ use WPA based encryption
- 16% use no security at all
- 0.25% use WEP...
- That's 1 WEP signal in 10 minutes of driving

Wireless Printers

ssid 	encryption 
HP-Print-6E-Officejet Pro 8600	None
HP-Print-D6-ENVY 5530 series	None
HP-Print-4A-ENVY 4500 series	None
HP-Print-08-Officejet 4630	WPA+PSK WPA+AES-CCM
DIRECT-EC-HP OfficeJet 4650	WPA+PSK WPA+AES-CCM
HP-Print-99-ENVY 4500 series	WPA+PSK WPA+AES-CCM

Possible Applications

- ▶ Municipalities measuring live reactions to road closures
- ▶ Live custom heat maps showing non-joined but still present mobile devices
- ▶ Vector and velocity of an anonymous device between two probes
- ▶ Measuring the effectiveness of a physical advertisement campaign
- ▶ Evaluation of security education on protecting mobile devices outside of the corporate environment
- ▶ Getting to know your employees, customers, and the habits of those in your general area
- ▶ Real Estate advertisement evaluation: How many people are driving by, and how many actually see the property?
- ▶ Red team activities, specifically social engineering

Thank You!

And don't forget about the search party!



► Documentation/Links

- <http://bit.ly/2x6sVKQ>

► Contact Info

- Ryan.Adler@defpoint.com
- Or just talk to me. I'll be wandering around .conf17 too!

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017