Security: The Internet of Things (IoT)

Internet of Things:

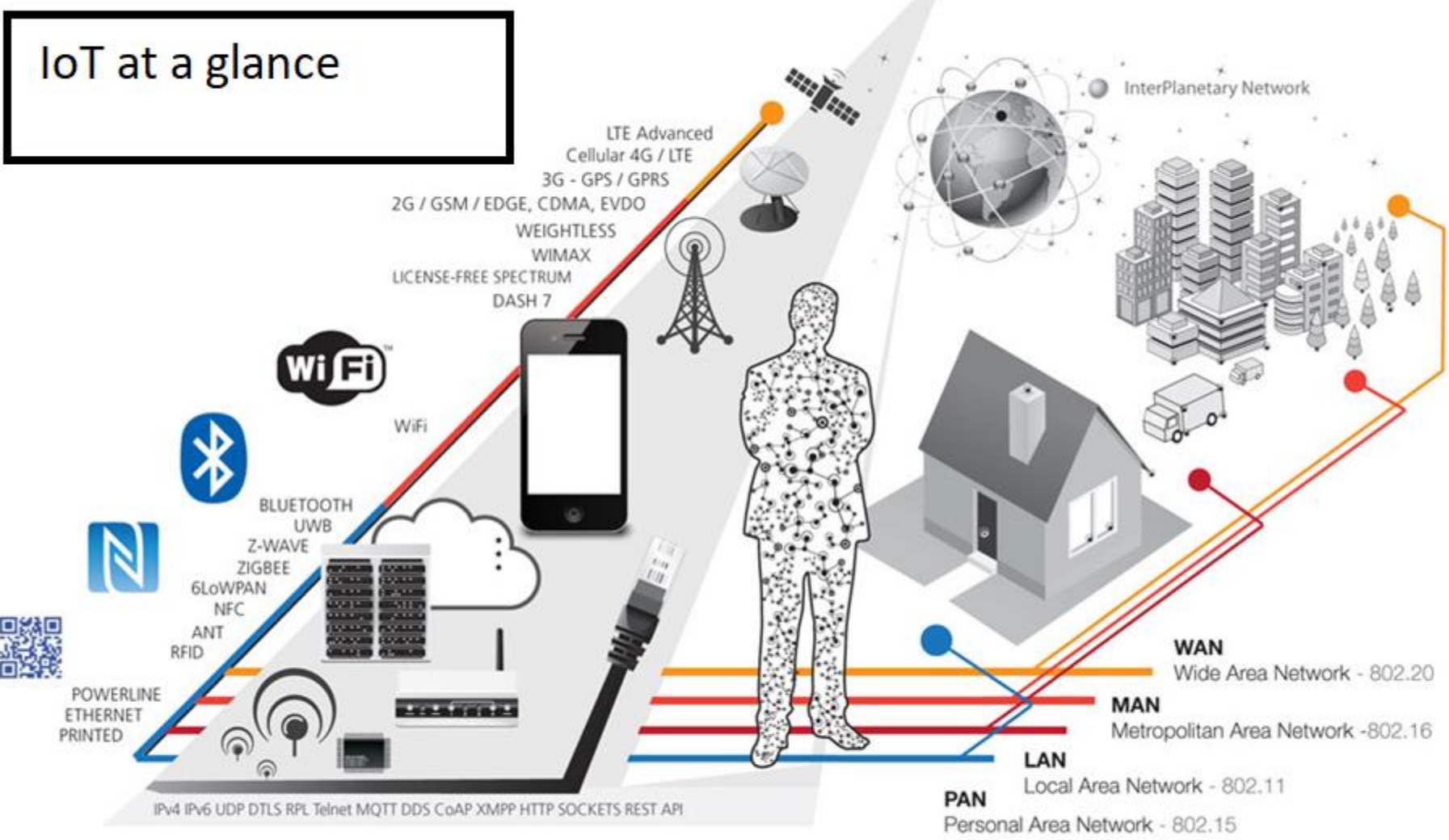
A network of internet-connected objects able to collect and exchange data using embedded sensors.

As the number of connected devices grows to more than 50 billion by 2020, the IoT will provide an unprecedented expansion of exposure to new threat vectors and increased attack surfaces.

IoT threats gain access through the broader Radio Frequency (RF) spectrum.

It’s not just corporate WiFi that presents a threat;
it’s any device enabled by Bluetooth, NFC, RFID, Z-Wave, ZigBee, 2G/3G/4G cellular protocols and a rapidly growing list of others.

IoT at a glance



Problem 1: Many IoT devices connected to the RF spectrum are using protocols not on the wired network which means enterprises can’t detect, inspect and fix vulnerabilities that arise in their unique IoT ecosystem.

Problem 2: Many of these protocols were meant for a single use including IoT-enabled light bulbs, wireless keyboards, mice, and industrial controls like pressure sensors and
water gauges.

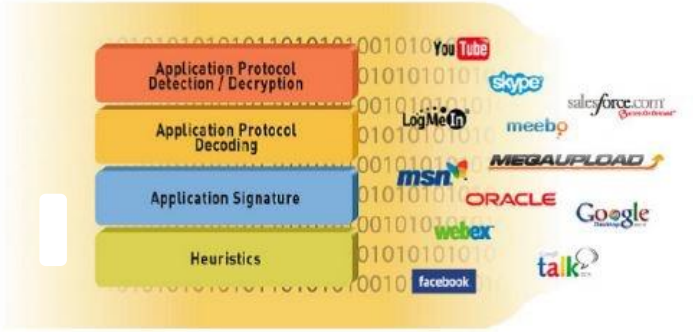
Problem 3: In most instances, IoT devices and the way they implement IoT protocols don’t support security patches – even when a manufacturer discovers a vulnerability.

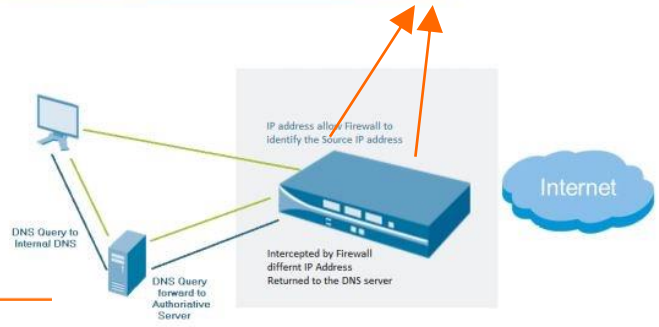
Port	20	22	23	25	53	69	80	…	443	…	994	…	47808	..
Protocol	TCP	TCP	TCP	TCP	UDP TCP	UDP	TCP	…	TCP	…	TCP	…	TCP	..
Application	FTP	SSH	Telnet	SMTP	DNS	DHCP	HTTP	…	SSL	…	IRCS	…	BacNet	..

Pretty simple diagram, but by now most security experts can secure these ports and protocols !

(Wired) Security

100 Mbps





Huge Dollars Spent to Monitor Internet Connections

- Intrusion detection
- Exfiltration detection
- APT detection
- Next gen firewalls
- SIEMs

Wireless Security

NOBODY IS WATCHING THE RADIO SIGNALS!

Meanwhile:

Multiple Gbps are
Leaving via Radio Signals

- Government phones
- Personal phones
- Hotspots
- Rogue cell towers
- Thermostats
- Sensors
- IoT
- ….

What are the Threats?

Example 1: Inexpensive Wireless Bugs use various protocols to steal corporate information

1545 listings for “GSM bug” on eBay

Voice Activated Spy Wall C
GPS Tracker Audio Ear Bu
Device

$20.24 From C

Was: ~~$26.99~~

Buy It Now

Free shipping

299 sold

25% off

1227 listings for “GSM bug” on Amazon

SPONSORED

Portable New USB Spy GSM

$24.49

Buy It Now

Free shipping

Only 1 left!

19 watching

1189 listings for “GSM bug” on Alibaba

SPONSORED

X009 Mini GSM SIM Card Audi
CameraBB

$17.89

Buy It Now

*Example 2: Rogue Cell Towers **2014***

- Rogue Cell Tower:
  - Impersonates Telco carrier tower
  - Cell phones are often promiscuous with their connections and pair with rogue cell towers without checking
  - **THREAT: Enables traffic sniffing and man-in-the middle attacks**

- BUT in 2014 “Rogue Cell Towers”:
  - Confined to **“Stingray”** devices used by Law Enforcement, Military and Intelligence
  - OR a Science Project

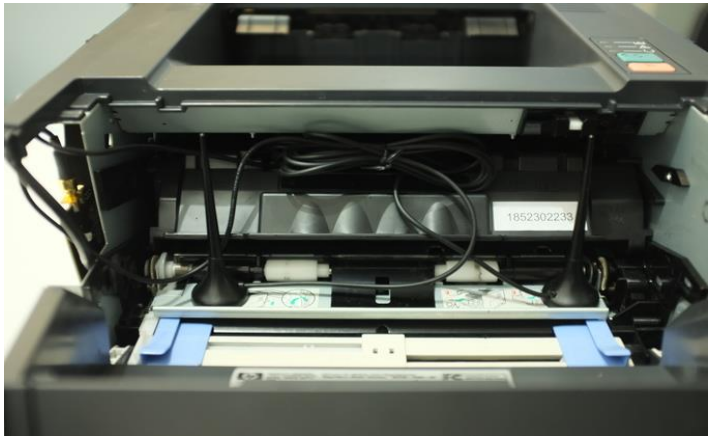
The **StingRay** is an IMSI-catcher, a controversial cellular phone surveillance device

Example 3: Rogue Cell Towers 2016

- Commoditized, commercial units on sale
- Can be hidden in plain sight, e.g. inside an office printer
- Improved Technologies Enable:

  - DIY cell tower w/Open Source + Software Defined Radios

  - Range Networks sells Cell Tower hardware unit w/software installed for under $5k



View from printer cartridge bay, modified to host 2 omnidirectional antennae (TX and RX) fed by SMA cable to BladeRF

Threat Context

- Adversaries will only use wireless threats when there is a specific Return-On-Investment (ROI) compared to other methods
- Scenarios where the ROI is lower than other options will inhibit its selection in any given case

Threat Context

Areas of Utility for advanced wireless attacks include:

- Sustaining access to a target
- Re-establishing access to a target
- Circumventing established security choke-points
- * Degree of repeatability *
- Invisible pivoting from one device to another via wireless interfaces

Threat Context

Risk Areas for the attacker

- Physical Access
- Upfront investment in new tactics
- Time required to execute
- Inconsistency in target environment
- Repeatability

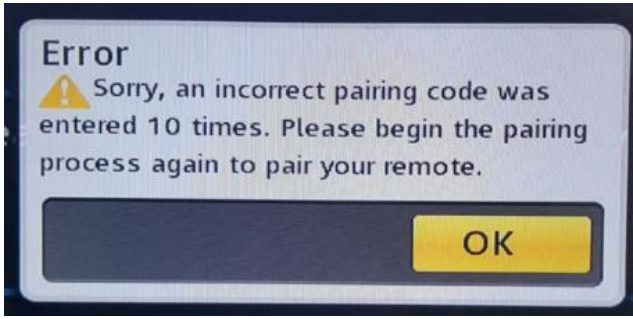
Example 4: From DefCon 2017

Control your STB with your voice!

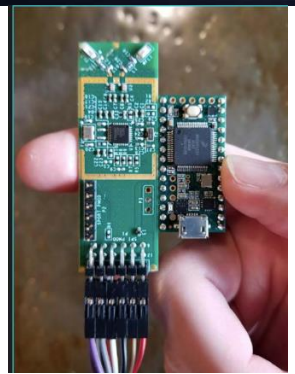
Wireless instead of IR!

Motion activated lights!

TI CC2530 with RF4CE stack



- Everyday devices like TV remote controls can be turned into listening devices that can exfiltrate data



Example 5: Wireless Keyboards & Mice

MouseJack, KeySniffer, KeyJack

MOUSEJACK
- Inject keystrokes from **500ft** away
- Microsoft, Dell, Logitech, Lenovo, Toshiba ….essentially all wireless mice with dongles
- More than 1 billion dongles vulnerable

KEYSNIFFER
- Record ALL your keystrokes as you type them
- Reveals credit cards, username and passwords and all your sensitive, private and confidential information

MouseJack

KeySniffer

THE WALL STREET JOURNAL.

WIRED

A Word of Warning:

section 191(1)

Possession, etc.

191(1) Every one who possesses, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

RF Hacks in the News

NETWORKWORLD

Researchers hack GSM mobile calls using $9 handsets Researchers have demonstrated an alarmingly simple technique for eavesdropping on individual GSM mobile calls without the need to use expensive equipment – *January 3, 2011*

WIRED

Researchers Hack Air-Gapped Computer With Simple Cell Phone Researchers have devised a new method for stealing data—using the GSM network, electromagnetic waves and a basic low-end mobile phone – *July 27, 2015*

---

engadget

Some SIM cards can be hacked in about 2 minutes with a pair of text messages Every GSM phone needs a SIM card, and you'd think such a ubiquitous standard would be immune to any hijack attempts. Evidently not – *July 22, 2015*

WIRED

Big Vulnerability in Hotel Wi-Fi Router Puts Guests at Risk Researchers have discovered a vulnerability in the systems, which would allow an attacker to distribute malware to guests, monitor and record data sent over the network, and even possibly gain access to the hotel's reservation and keycard systems – *March 26, 2015*

PCWorld

Hackers show off long-distance Wi-Fi radio proxy at DEF CON The device uses the 900MHz band, but hides the data in the background radio noise – *August 10, 2015*

ars technica

Hacker Develops Device to Surf the Internet Anonymously ProxyGambit is a $235 device that allows people to access an Internet connection from anywhere in the world without revealing their true location or IP address – *July 15, 2015*

ZDNet

Android smartwatches vulnerable to snooping Bluetooth communications between smartphones and smartwatches running Android are vulnerable to brute-force attacks that can decipher messages sent between the devices into plaintext– *December 11, 2014*

SANS

Bluetooth and its Inherent Security Issues Bluetooth flaw in native security can subject a user to threat vectors: default configuration, theft and loss, eavesdropping and impersonation, person-in-the-middle attack, piconet/service mapping, and denial-of-service attacks

The Register®

Bluetooth privacy is mostly ignored, so you're beaming yourself to the world The popular BLE beacon protocol isn't just a privacy risk up close – it can spy on your phone's or wearable's movements and make you trackable – *July 15, 2014*

engadget

Researchers find major security flaw with ZigBee smart home devices. By making it easier to have smart home devices talk to each other, many companies also open up a major vulnerability with ZigBee that could allow hackers to control your smart devices - *August 7, 2015*

GIZMODO

Philips Hue Light Bulbs Are Highly Hackable. If you're the proud owner of some smart Philips Hue light bulbs, watch out for blackouts—because the bulbs seem to be susceptible to malicious attacks according to new research - *August 14, 2013*

NETWORKWORLD

Researchers exploit ZigBee security flaws that compromise security of smart homes. Researchers at Black Hat and Def Con warned about security flaws in Internet of Things devices using the ZigBee protocol *-August 11, 2015*

The Register®

Simple 'open sesame' to unlock your HOME by radiowave replay attacks are the most basic of penetrative techniques and any modern system should be immune to them, but for some reason the tested Z-Wave sensor wasn't.

Forbes

How Your Security System Could Be Hacked To Spy On You Hacker could track when people were opening and closing windows and doors using cheap SDR and interfere with transmissions (our researcher)

---

black hat®

Honey I'm Home - Hacking Z-Wave Home Automation Systems
Z-Wave protocol is gaining momentum against the Zigbee protocol. This is partly due to a faster, and somewhat simpler, development process – *August 2013*

INTERNATIONAL BUSINESS TIMES

'Extremely chatty' Samsung smart TVs pose major security risk to government, healthcare and energy companies Samsung smart TVs "incessantly" communicate with a server which uses an untrusted security certificate, opening up the potential for hackers to target these devices

---

black hat®

Hacking, Surveilling, and Deceiving Victims on Smart TV Smart TVs have many hardware devices which, if remotely controlled, means bad guys can spy without you knowing. It is possible to make Smart TVs monitor you 24/7 even though users turn off their TV – *August 2013*

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Alarm bells ring for Internet of Things after smart TV hack Two researchers from Colombia University in the US have found that millions of internet-connected TVs could be taken over in a man-in the-middle attack - *June 10, 2014*

The New York Times

The August Smart Lock Shows Why You Should Stick With Dumb Keys So what explains the tech industry's infatuation with smart locks that can unlock your home using a smartphone? A spate of smart locks have hit crowdfunding sites like Kickstarter – *October 14, 2014*

WIRED

Millions of Kwikset Smartkey Locks Vulnerable to Hacking Researchers have been cracking locks at Def Con for years, demonstrating the ability to defeat high-security electronic locks used at the White House and other government offices – *August 3, 2013*

---

tom's GUIDE
TECH FOR REAL LIFE

This 'Smart' Lock May Have Dangerously Dumb Security Some of Sesame's features are perfect examples of how brilliant ideas can fail to take security into account. Of all the dumb ideas coming out of the Internet of Things, these features may be the dumbest yet – *March 4, 2015*

InformationWeek DARKReading

Five Ways To (Physically) Hack A Data Center Many data centers contain easy-to-exploit physical vulnerabilities that don't require hacking into the network – *May 17, 2010*

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Recent Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet The majority of the banking attack traffic does not appear to have been generated by client bots, but rather from compromised servers in data centers – *October 5, 2012*

COMPUTERWORLD

Hackers exploit SCADA holes to take full control of critical infrastructure According to three different reports from experts, it appears that critical infrastructure is a ripe target that is pretty sweet for attackers – *January 15, 2014*

NETWORKWORLD

Hacks to turn your wireless IP surveillance cameras against you researchers showed how to exploit the devices in "To Watch or Be Watched: Turning Your Surveillance Camera Against You" and released a tool to automate attacks – *April 14, 2013*

GIZMODO

A Creepy Website Is Streaming From 73,000 Private Security Cameras A website has collected the streaming footage from over 73,000 IP cameras whose owners haven't changed their default passwords – *November 6, 2014*

WIRED

Popular Surveillance Cameras Open to Hackers, Researchers Say Three of the most popular brands of closed-circuit surveillance cameras are sold with remote internet access enabled by default, and with weak password security – *May 12, 2012*

The Register®

DECT wireless eavesdropping made easy A new attack against phones based on DECT can be carried out cheaply using off-the-shelf kit, together with a little know-how – *December 31, 2008*

HELP NET SECURITY

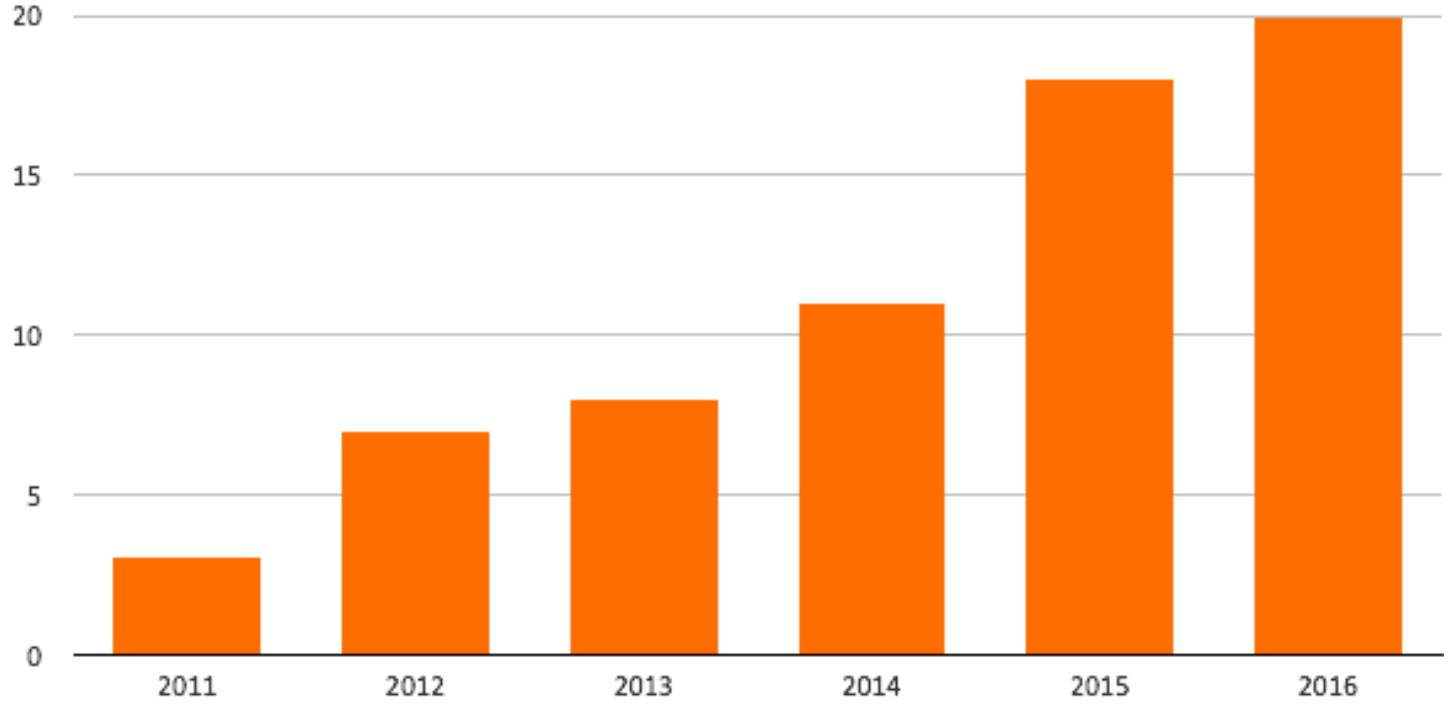
Is Your Cordless Phone Being Hacked? If you still have an early analog cordless phone, then your conversations can potentially be easily intercepted by anyone with a radio scanner available at most local hobby stores – *March 20, 2014*

NETWORKWORLD

DECT phones and POS terminals are vulnerable security experts have built a cheap laptop-based sniffer that can break into cordless phones, debit card terminals and security door mechanisms – *January 5, 2009*

Attacks Are Moving to Radio Frequency

DEFCON RF-Based Hack Presentations



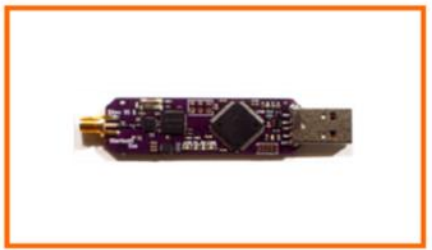
Attack Technologies for Modern Threat Agents

Software Defined Radio 10 Years Ago

$100K+ for an SDR (Software Defined Radio)

Today's Software Defined Radios (Receivers and Transmitters)

Providing Threat Agents an RF Platform for Attack

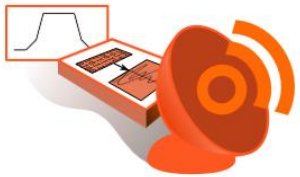


$20 SDRs
put basic radio hacking in the hands of every teenager

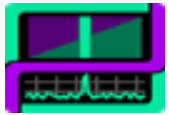
$1000 SDRs
put a precise weapon in the hands of every professional Threat Agent

Software For Software Defined Radios

Enabling Threat Agents to Develop Attack Applications



GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM



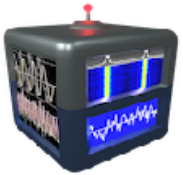
SDR# (SDRSharp)

Baudline

Inspectrum

SDR-Radio

Communications System Toolbox



CubicSDR

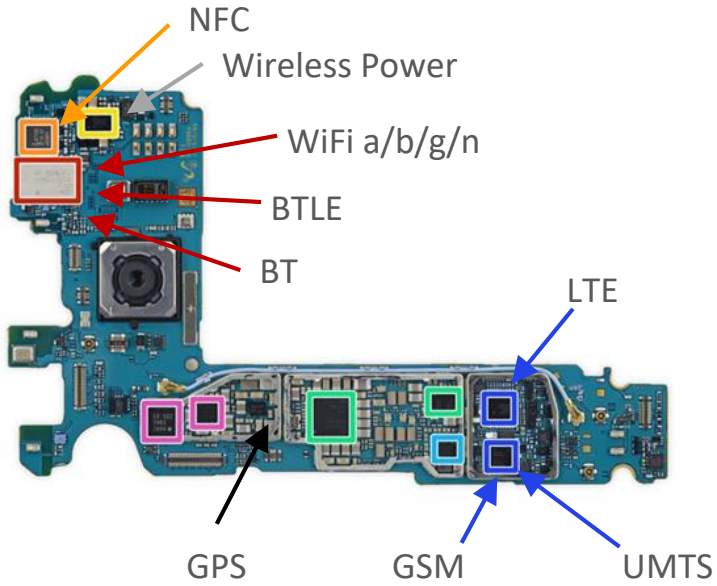
THE BIG SECRET

For the Security of Internet of Things:

It's not about the **"Things",** it's about the **Radios!**

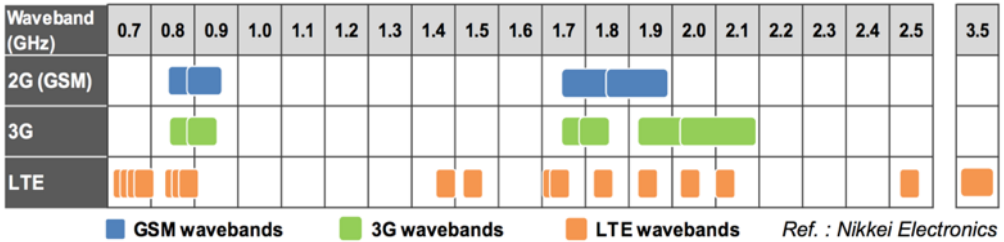
Example: Cell Phones

Samsung S7 has 9 Radios



Avago AFEM-9040 multiband multimode module
EPCOS D5275 antenna switch module
EPCOS D5287 antenna switch module
Murata FAJ15 front end module
Murata KM5D18098 Wi-Fi module
Qorvo QM78064 high band RF fusion module
Qorvo TQF6260 PA duplexer
Qorvo QM63001A diversity receive module
Qualcomm QFE3100 envelope tracker
Qualcomm QFE2550 digital tuner
Qualcomm WTR4905 transceiver
Qualcomm WTR3925 transceiver

RF bands



NFC = 13MHz

GPS = 1575MHz

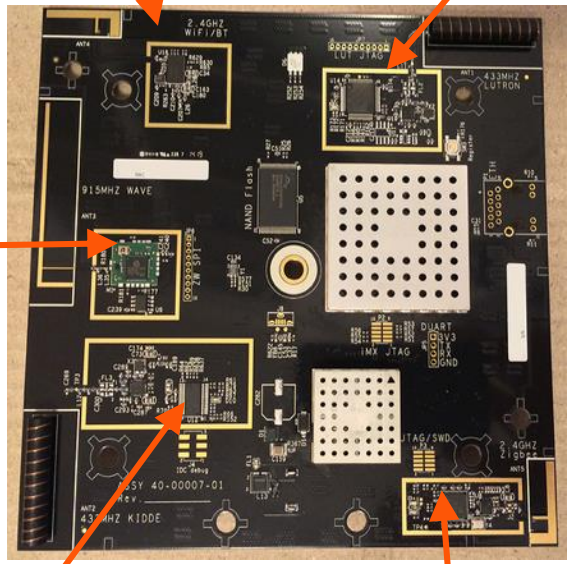
BT/Wifi = 2400MHz

Example: Home Automation

This $70 home automation hub has 6 radios!

BT/Wifi (2400/ 5800 MHz)

Lutron (433MHz)

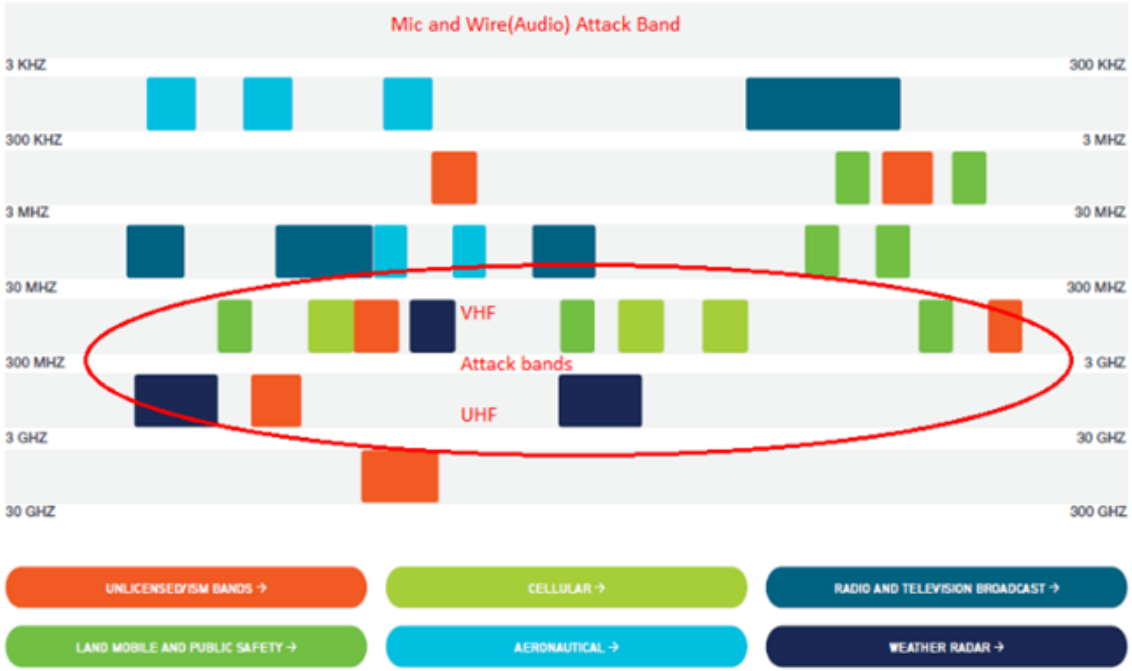


Z-Wave (915MHz)

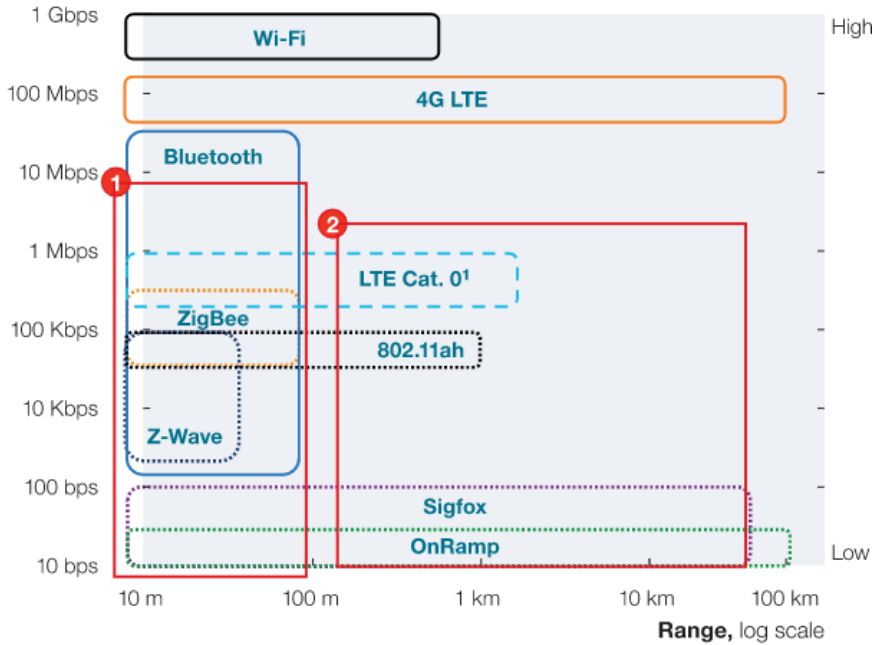
Kidde (433MHz)

ZigBee (2400MHz)

An Attackers Guide to the Radio Spectrum



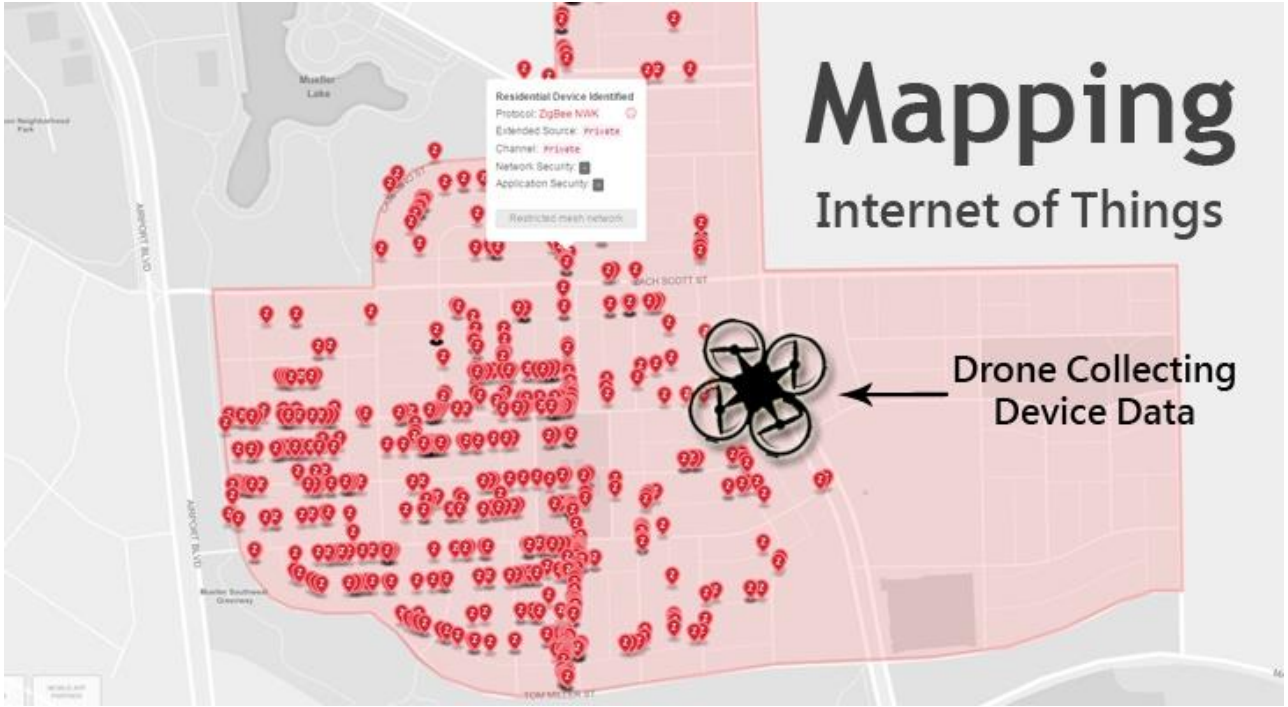
Current IoT Attack Focus.



1 Many competing standards for low-range, medium-low data rate hinder growth for many IoT applications
- Interoperability missing
- Consortia wars might be emerging
- Additional incompatibilities in higher communication layers, eg, 6LoWPAN vs ZigBee

2 Standard white space for low-data-rate, low-power, high-range applications such as smart grid
- Wi-Fi and LTE have high power consumption
- Alternatives with low power and wide range (eg, LTE Cat. 0, 802.11ah, Sigfox, and OnRamp) are in very early stages and compete against each other

Using a Drone to Locate ZigBee Protocol – based IoT Devices



The First Step Of the APT is Always Reconnaissance!

Today's Connected Device Threat

The "Ready for Radio" Problem

RF-enabled devices are pervasive, do not seek permission to enter

Example

Not yet configured ZigBee Network

ZigBee®

Bluetooth keyboard with a vulnerability

Bluetooth®

We Need a Security Methodology for IoT:

Proposal:

- **Detect**
- **Analyze**
- **Respond**

Who Are the Radio Experts?

KEY TECHNOLOGIES

Detect, Analyze, Locate, Respond

- **DETECT: Use Collaborative SDR-based Sensors** to quickly and accurately scan the spectrum for emitters. Utilizing sophisticated algorithms and techniques to intelligently make distributed decisions about whether to observe a known signal versus scanning another part of the spectrum to find unknown signals.

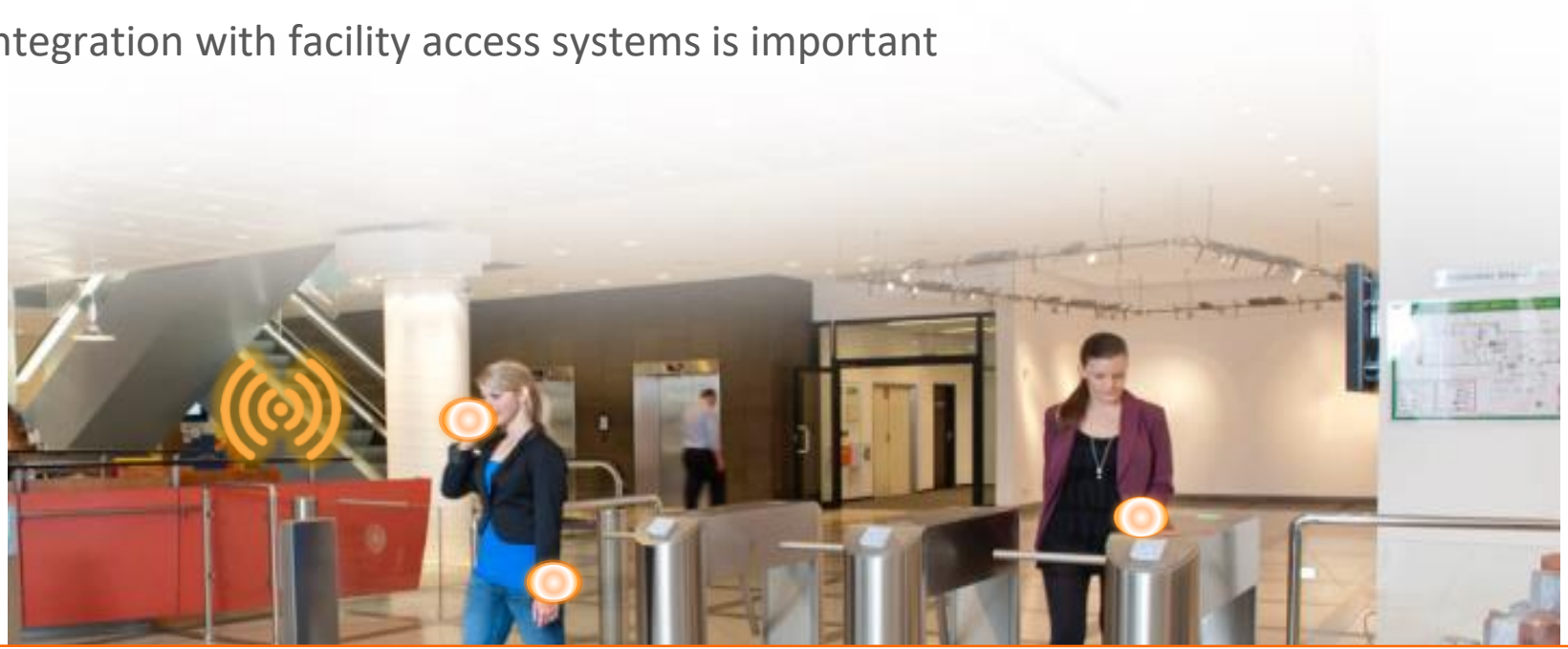
- **ANALYZE: Use Device Fingerprinting** to detect and identify Friend/Foe/Unknown in an enterprise's airspace. Leverage detected information to resolve and produce situational awareness of RF emitters and RF Personas.

- **LOCATE: Localize** all emitters in the corporate airspace. Passively localize any emitter within 'several meters' of accuracy, enabling geofencing of emitters to produce localization-based alerts for sensitive areas.

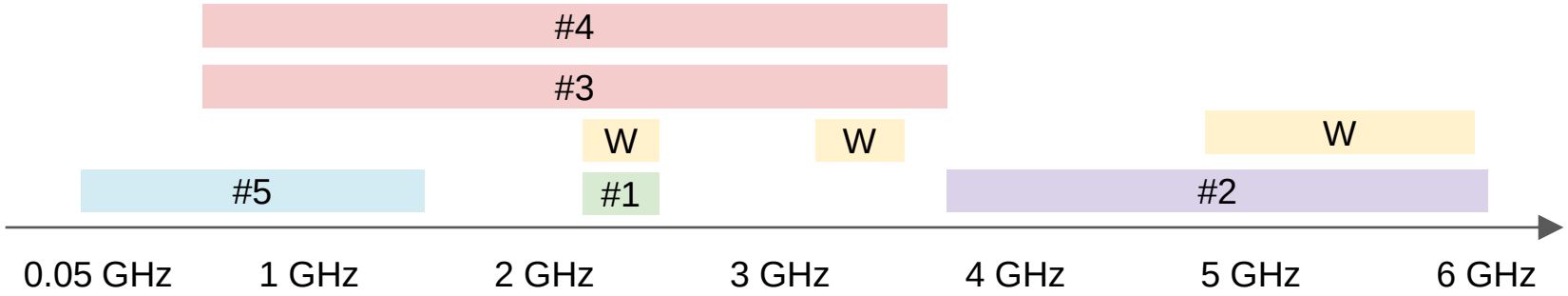
- **RESPOND**: Provide **Human readable** alerts and reports to SOC for appropriate response. Might want to consider enhanced tools for first responders

About the RF Persona

- Convergence of physical and cyber security
- Device identification and linking to personnel
- Integration with facility access systems is important



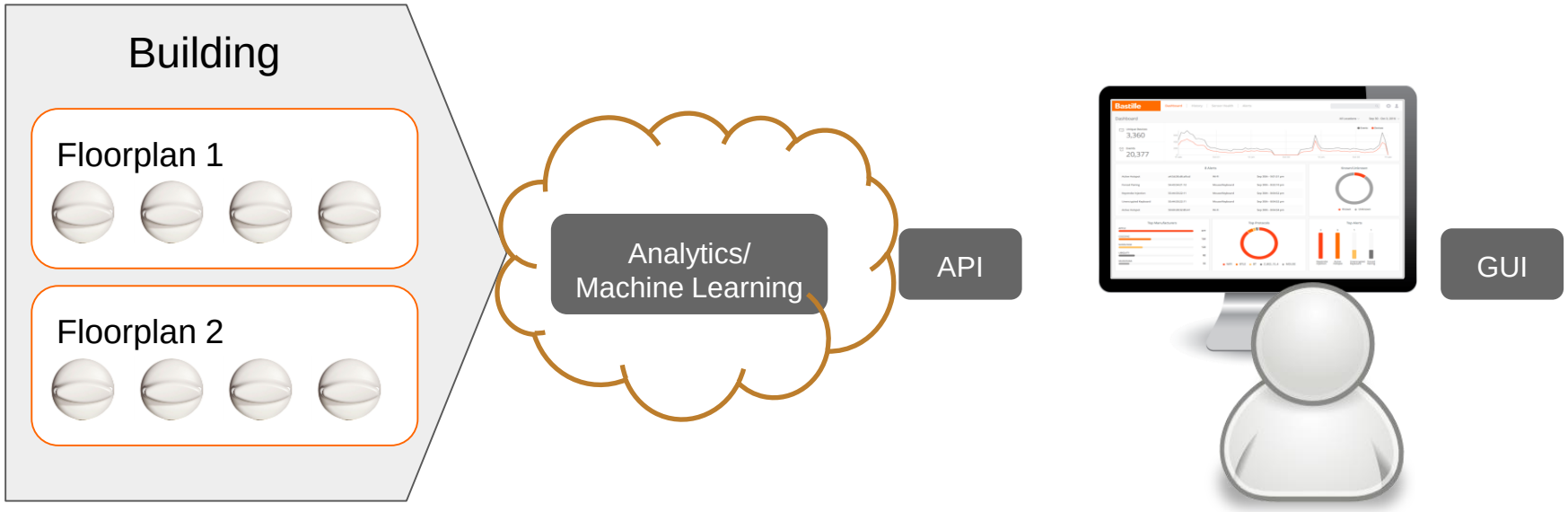
Detect:
The Necessary Essential Frequency Bands Only



Top Protocols by Front End

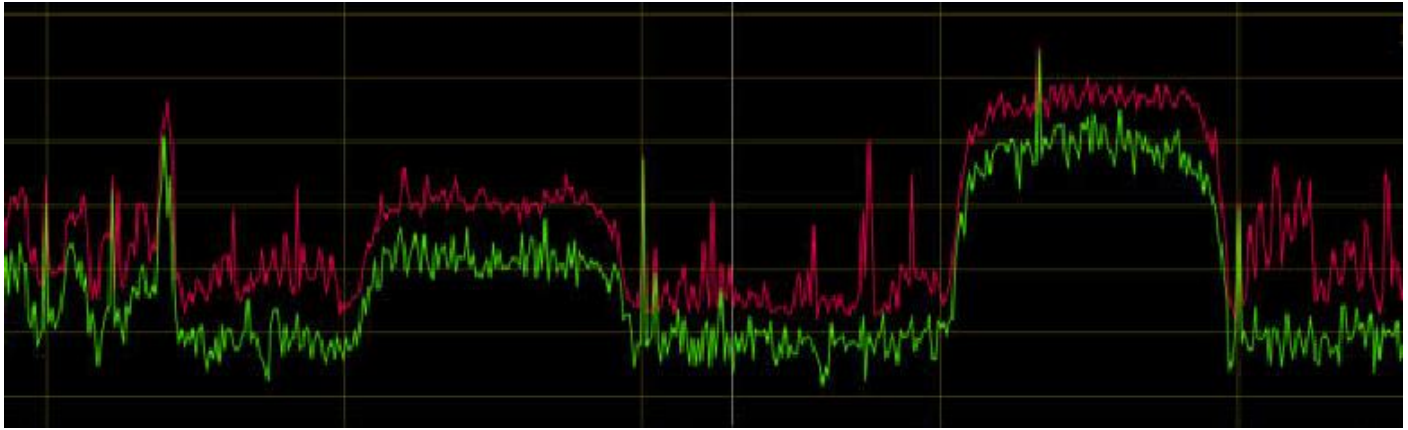
#1	BT, BTLE, Mouse/Keyboard, Zigbee
#2	White Space Protocols
#3	Cellular (LTE-GSM)
#4	DECT
#5	Push-to-Talk, Z-Wave, 900MHz phones, Cellular, Key Fobs, Alarm Systems
W	WiFi (802.11abgn/ac); 2.4GHz, 3.6GHz, 5GHz

Scalable Detection – For ‘Enterprise’ Deployments



Analyze: The Multi Protocol IoT environment

Analyze:



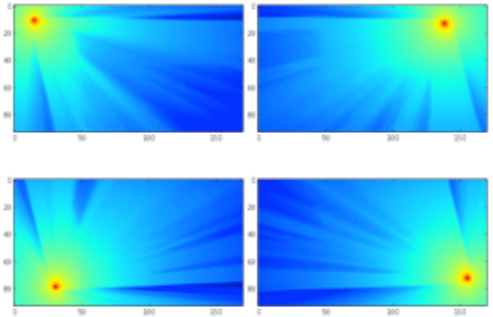
- Canada (mcc=302)
  - Rogers Wireless (mnc=720)
    - Lac=17500 (445C hex)
      - CellID=3891 (F33 hex)
        - Sector=2, [full CellID 38912, 9800 hex] 870.
          - TCH channels
            - 872.8 MHz, 146 channel
            - 873.6 MHz, 150 channel
            - 890.2 MHz, 233 channel
          - Neighboring BCCH channels
            - 869.4 MHz, 129 channel
            - 869.6 MHz, 130 channel
            - 869.8 MHz, 131 channel
            - 870.0 MHz, 132 channel
            - 870.2 MHz, 133 channel
            - 870.6 MHz, 135 channel
            - 870.8 MHz, 136 channel
            - 871.0 MHz, 137 channel
            - 871.2 MHz, 138 channel
            - 871.4 MHz, 139 channel
            - 871.6 MHz, 140 channel
            - 872.2 MHz, 143 channel
            - 872.4 MHz, 144 channel
            - 872.6 MHz, 145 channel
            - 872.8 MHz, 146 channel
            - 1970.4 MHz, 713 channel
            - 1970.8 MHz, 715 channel

Frequency /	Operator	la/ci/sector/pov	Frequency /	Operator	la/ci/sector/pov	Frequency /	Operator	la/ci/sector/power (dBm)	Frequency /	Operator	la/ci/sector/po
1805.2/ 512			1824.0/ 606			1842.8/ 700			1861.6/ 794		
1805.4/ 513			1824.2/ 607			1843.0/ 701			1861.8/ 795		
1805.6/ 514			1824.4/ 608			1843.2/ 702			1862.0/ 796		
1805.8/ 515			1824.6/ 609			1843.4/ 703			1862.2/ 797		
1806.0/ 516			1824.8/ 610			1843.6/ 704			1862.4/ 798		
1806.2/ 517			1825.0/ 611			1843.8/ 705			1862.6/ 799		
1806.4/ 518			1825.2/ 612			1844.0/ 706			1862.8/ 800		
1806.6/ 519			1825.4/ 613			1844.2/ 707			1863.0/ 801		
1806.8/ 520			1825.6/ 614			1844.4/ 708			1863.2/ 802		
1807.0/ 521			1825.8/ 615			1844.6/ 709			1863.4/ 803		
1807.2/ 522			1826.0/ 616			1844.8/ 710			1863.6/ 804		
1807.4/ 523			1826.2/ 617			1845.0/ 711			1863.8/ 805		
1807.6/ 524			1826.4/ 618			1845.2/ 712			1864.0/ 806		
1807.8/ 525			1826.6/ 619			1845.4/ 713	Canada, Rogers Wireless;	BCCH 17500/ / /;	1864.2/ 807		
1808.0/ 526			1826.8/ 620			1845.6/ 714			1864.4/ 808		
1808.2/ 527			1827.0/ 621			1845.8/ 715	Canada, Rogers Wireless;	BCCH 17500/ / /;	1864.6/ 809		
1808.4/ 528			1827.2/ 622			1846.0/ 716			1864.8/ 810		
1808.6/ 529			1827.4/ 623			1846.2/ 717	Canada, Rogers Wireless;	BCCH 17500/ / /;	1865.0/ 811		
1808.8/ 530			1827.6/ 624			1846.4/ 718	Canada, Rogers Wireless;	BCCH 17500/ / /;	1865.2/ 812		
1809.0/ 531			1827.8/ 625			1846.6/ 719	Canada, Rogers Wireless;	BCCH 17500/ / /;	1865.4/ 813		
1809.2/ 532			1828.0/ 626			1846.8/ 720			1865.6/ 814		
1809.4/ 533			1828.2/ 627			1847.0/ 721	Canada, Rogers Wireless;	BCCH 17500/ / /;	1865.8/ 815		
1809.6/ 534			1828.4/ 628			1847.2/ 722	Canada, Rogers Wireless;	BCCH 17500/ / /;	1866.0/ 816		
1809.8/ 535			1828.6/ 629			1847.4/ 723			1866.2/ 817		
1810.0/ 536			1828.8/ 630			1847.6/ 724	Canada, Rogers Wireless;	BCCH 17500/ / /;	1866.4/ 818		
1810.2/ 537			1829.0/ 631			1847.8/ 725			1866.6/ 819		
1810.4/ 538			1829.2/ 632			1848.0/ 726	Canada, Rogers Wireless;	BCCH 17500/ / /;	1866.8/ 820		
1810.6/ 539			1829.4/ 633			1848.2/ 727	Canada, Rogers Wireless;	BCCH 17500/ / /;	1867.0/ 821		
1810.8/ 540			1829.6/ 634			1848.4/ 728	Canada, Rogers Wireless;	BCCH 17500/ / /;	1867.2/ 822		
1811.0/ 541			1829.8/ 635			1848.6/ 729	Canada, Rogers Wireless;	BCCH 17500/ / /;	1867.4/ 823		

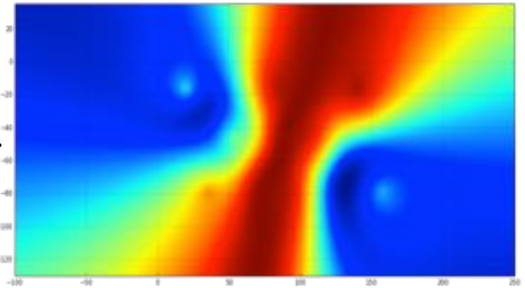
869.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
869.6	Canada, Rogers Wireless;	BCCH 17500/ / /;
869.8	Canada, Rogers Wireless;	BCCH 17500/ / /;
870.0	Canada, Rogers Wireless;	BCCH 17500/ / /;
870.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
870.6	Canada, Rogers Wireless;	!BCCH 17500/ 3891/ 2/ -45.0 dBm;
870.8	Canada, Rogers Wireless;	BCCH 17500/ / /;
871.0	Canada, Rogers Wireless;	BCCH 17500/ / /;
871.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
871.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
871.6	Canada, Rogers Wireless;	BCCH 17500/ / /;
872.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
872.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
872.6	Canada, Rogers Wireless;	BCCH 17500/ / /;
1845.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
1845.8	Canada, Rogers Wireless;	BCCH 17500/ / /;
1846.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
1846.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
1846.6	Canada, Rogers Wireless;	BCCH 17500/ / /;
1847.0	Canada, Rogers Wireless;	BCCH 17500/ / /;
1847.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
1847.6	Canada, Rogers Wireless;	BCCH 17500/ / /;
1848.0	Canada, Rogers Wireless;	BCCH 17500/ / /;
1848.2	Canada, Rogers Wireless;	BCCH 17500/ / /;
1848.4	Canada, Rogers Wireless;	BCCH 17500/ / /;
1848.6	Canada, Rogers Wireless;	BCCH 17500/ / /;

Analyze: Localization of Radios Inside the Environment

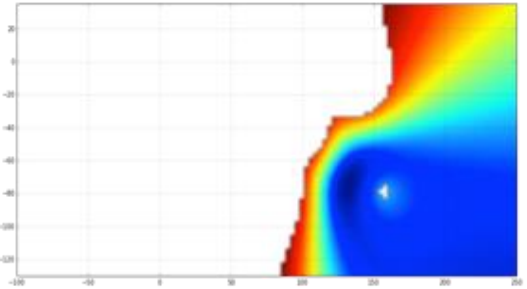
Facility Propagation Inference



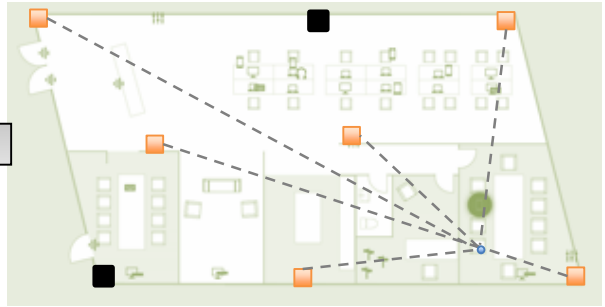
Error Analysis



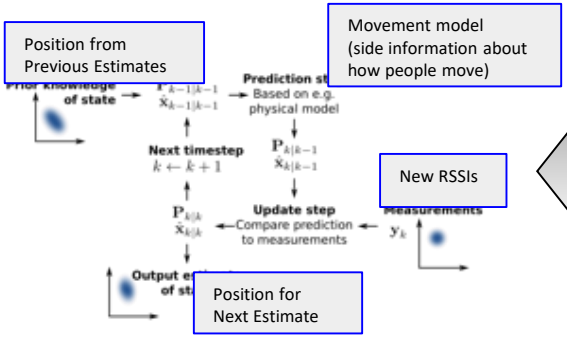
Error Filtering/Smoothing



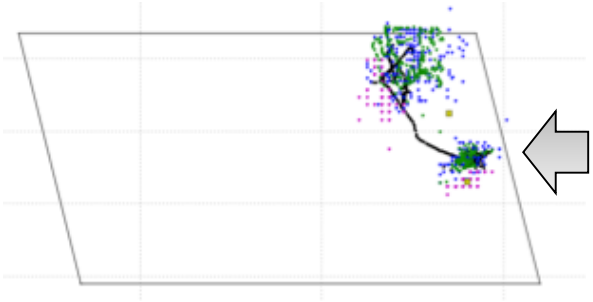
Cross Validation



Algorithms and Logic



Emitter Location Estimates



Emitter Location Technologies

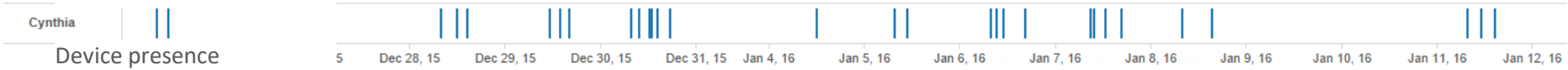
1. AoA and TDOA are not suitable for inside a facility.

2. PoA works well, can be highly accurate, but is extremely complex, requires highly precise instrumentation and timing. Demands complex installation requirements. Very expensive for enterprise deployments due to needed additional infrastructure.

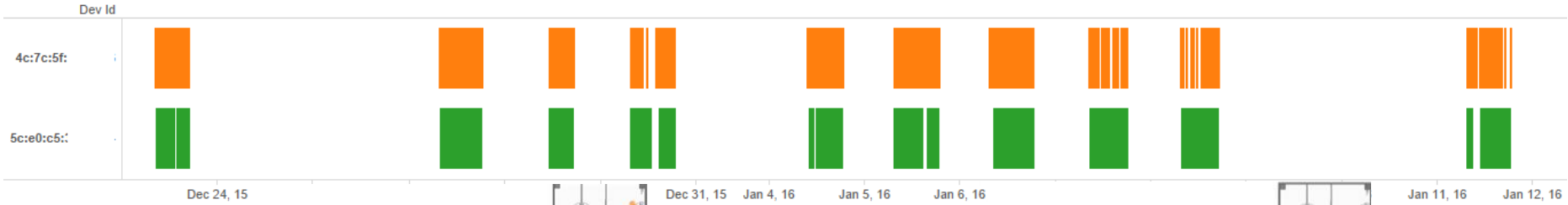
3. 'Localization' is not as precise as PoA, but is 'good enough' and provides reasonable repeated results, every time, all the time, with a 'plug and play deployment' process.

Analyze: RF Persona Creation, Localization

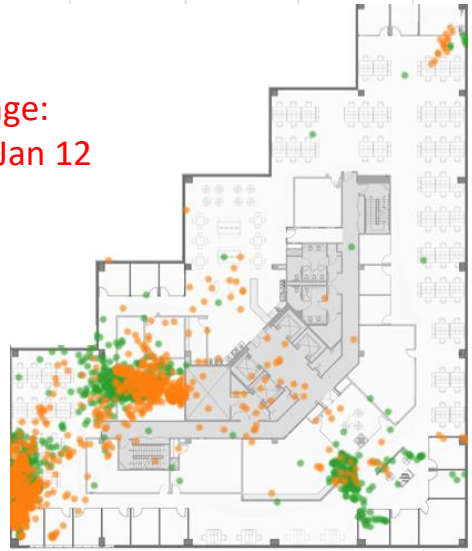
Badge Swipes



Device presence

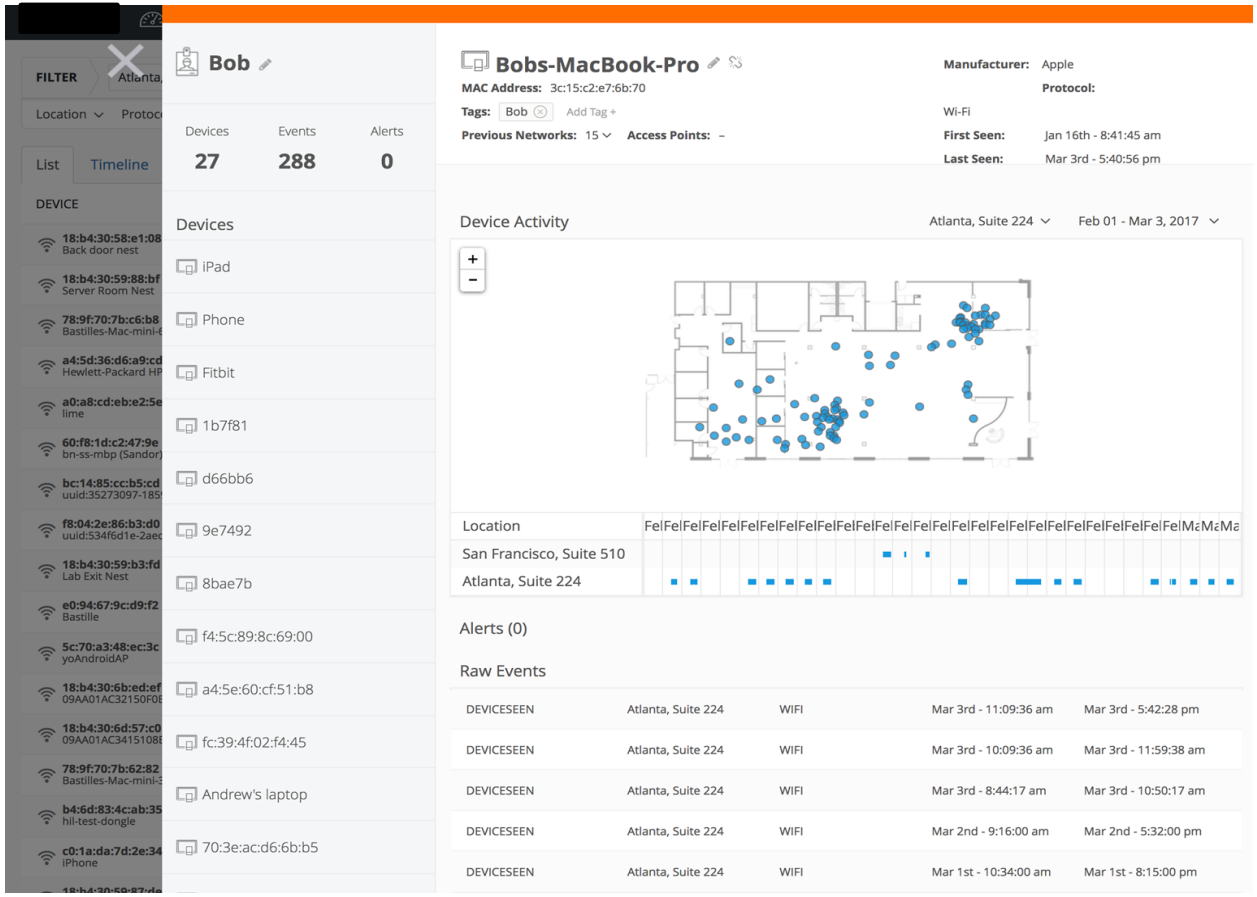


Date Range:
Dec 23 - Jan 12

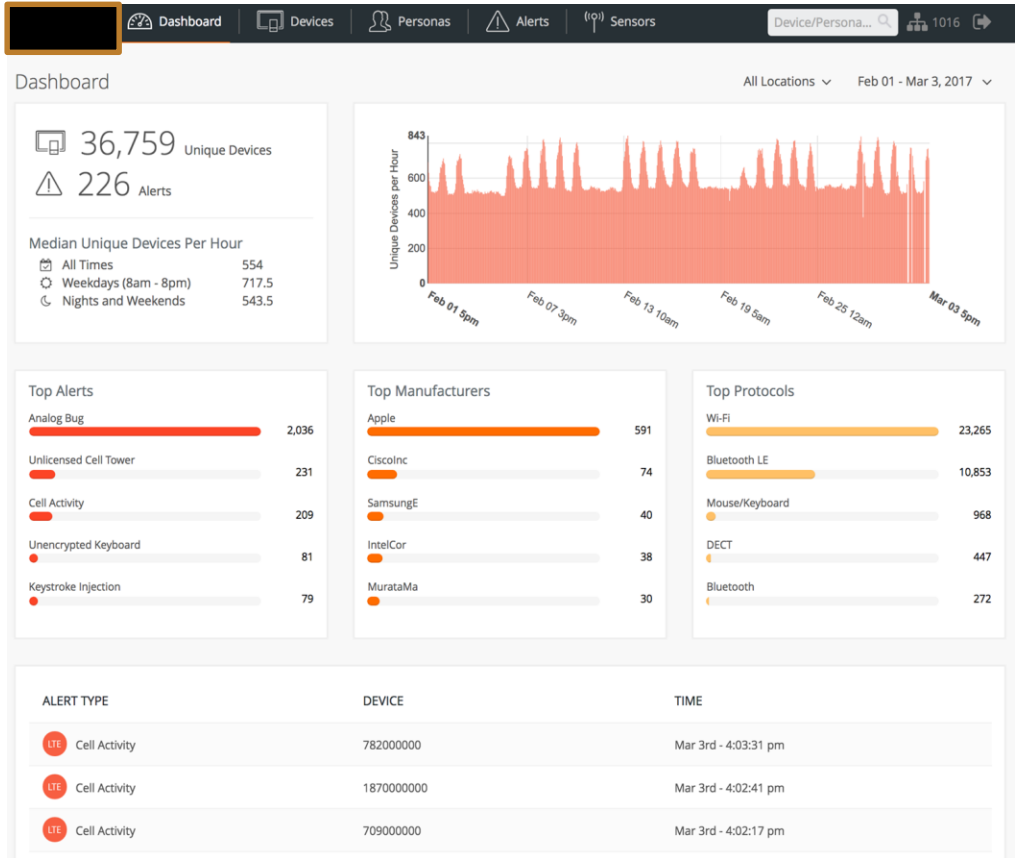


Single Day,
Specific Time:
Dec 28, 12pm

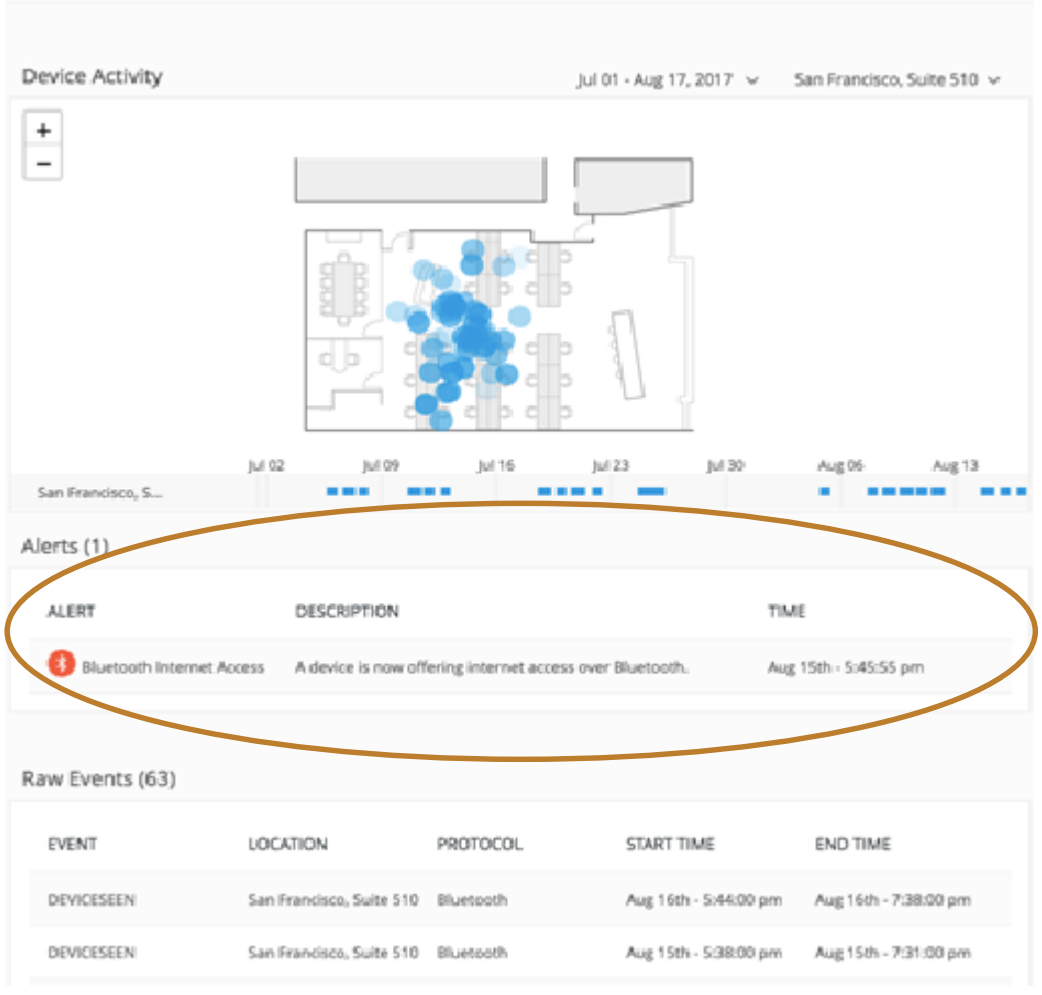
Analyze: A Single Persona and Associated Devices

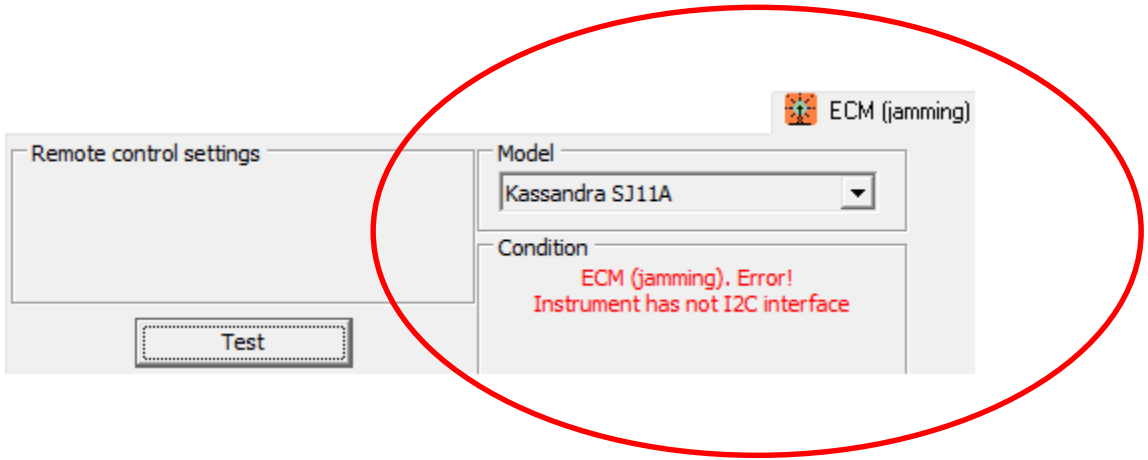


Analyze: Know all the Emitters in Your Environment



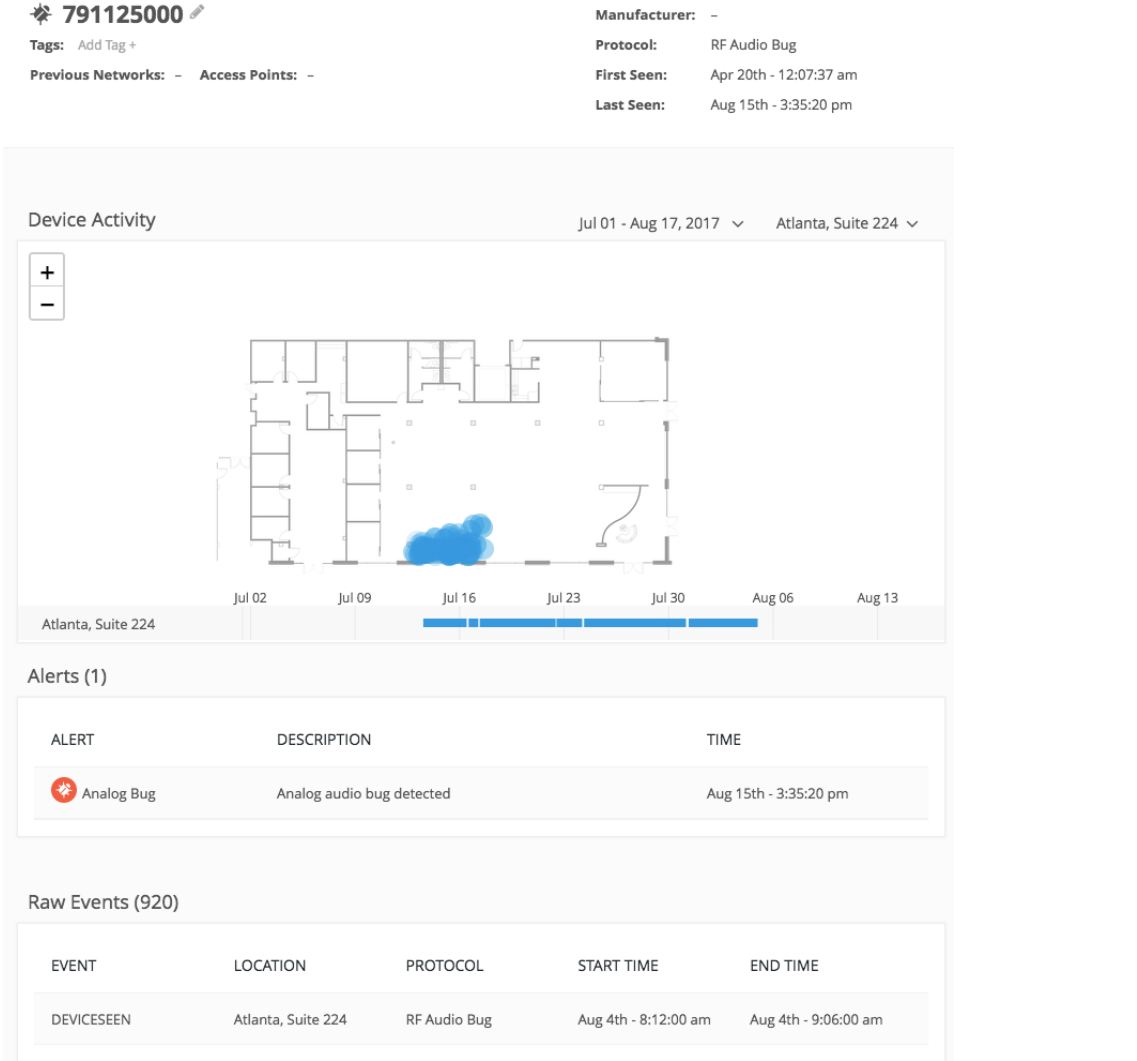
Respond: Automated Alerts for Critical Events




ECM (jamming)
Remote control settings
Model
Kassandra SJ11A
Condition
ECM (jamming). Error!
Instrument has not I2C interface
Test

Respond: Reporting

Its what we can do now (legally). Please don't consider jamming!



Classified Facilities

- Enforce No Cell Phone policy
- Enforce No Wireless Infrastructure policy
  - ZigBee enabled power management systems
  - Z-Wave enable HVAC system
  - Wireless security systems
  - Wireless lighting systems

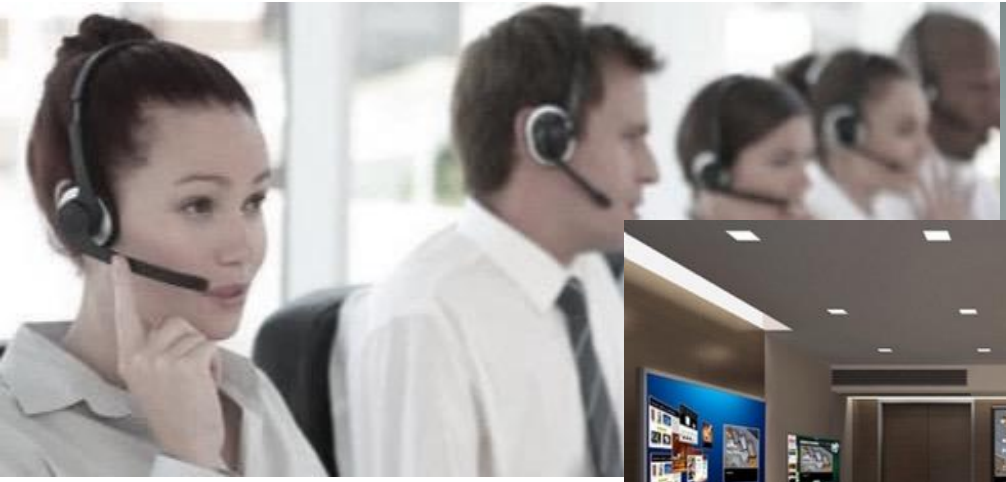
DIGITAL FORCE PROTECTION

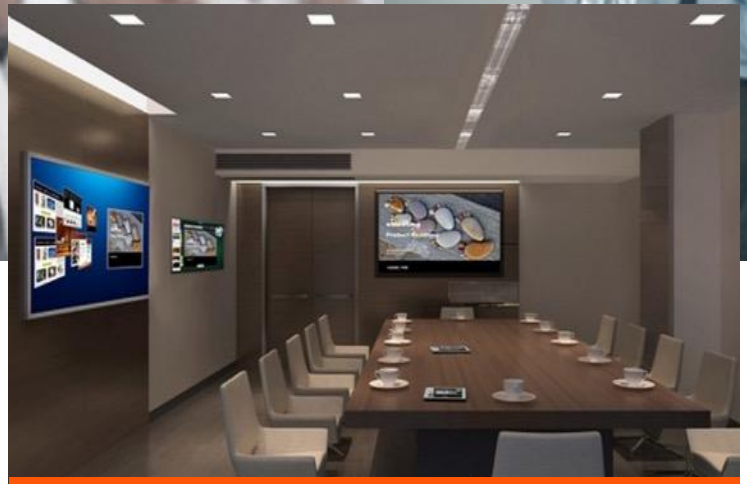
- On-demand low-cost red teaming of an environment to detect unwanted wireless threats and attackers
- Could be deployed to temporary operating facilities like ‘Corporate Retreat’ conference facilities
- Detect wireless devices that enter and leave the room
- Detect wireless vulnerable devices
- Detect wireless surveillance devices

CRITICAL INFRASTRUCTURE DEFENSE

- Detection of vulnerable or compromised critical infrastructure wireless C2 systems
- Detection of active wireless attack on critical infrastructure

IoT Protocols are in and about Every Organization Today





What Vulnerable IoT Devices are in Your Organization?

CONTACT

John Pavelich

Spectral Guard Inc

613-294-1068