
# IOT Platform Vulnerabilities & Remedies

Presented at the OpenIOT Summit - April 6, 2016

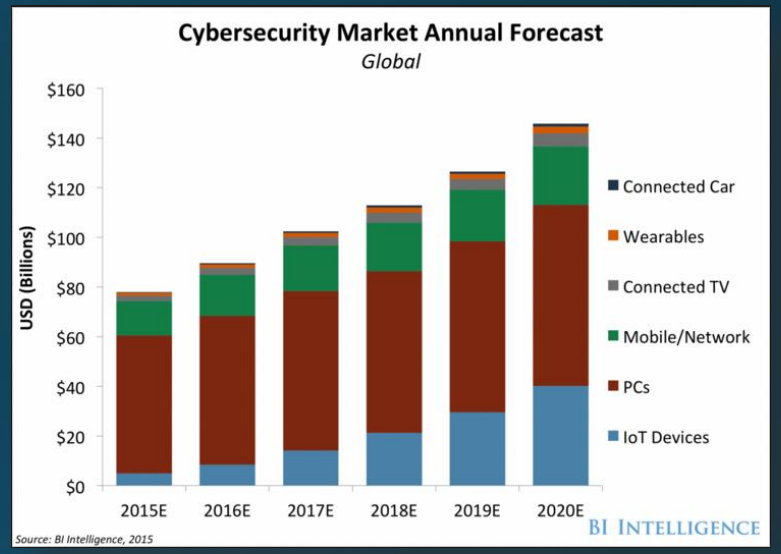
Chris Kocks - Director, IOT Practice

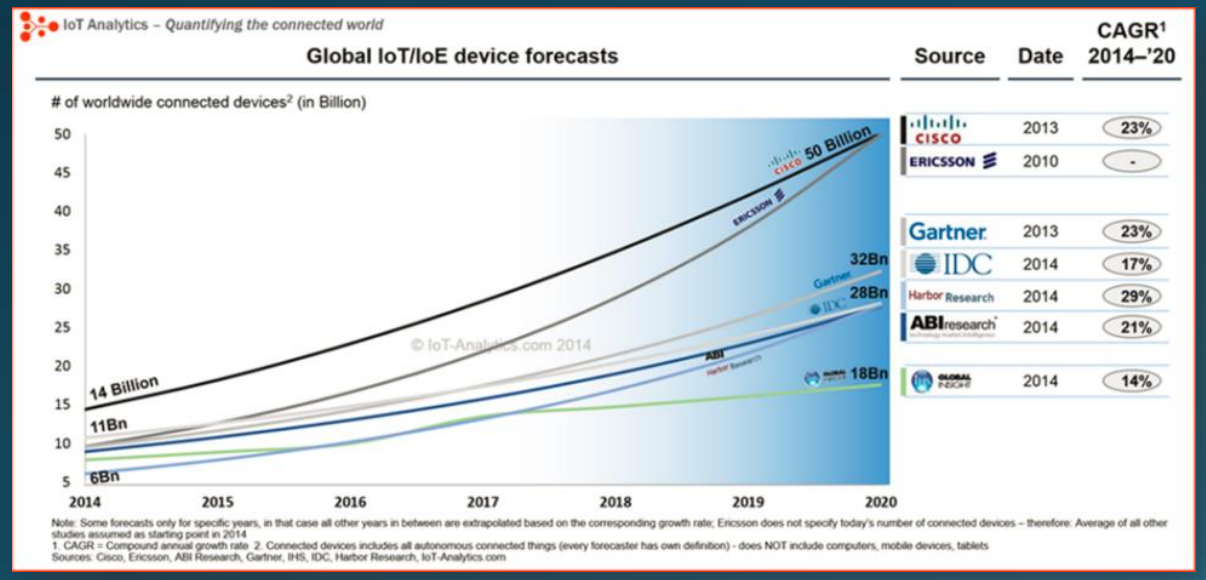
pureIntegration

# Growth of IOT Increases Vulnerabilities

2020 Forecast:

- 25 – 50 billion devices (Cisco, Ericsson, IDC, ABI, Gartner)
- 26 objects/person (Intel)
- Economic impact: $2 - $5 trillion (Cisco, McKinsey Global Institute, IDC, GSMA & Machina Research, Gartner, Harbor Research)




## ComputerWorld Survey

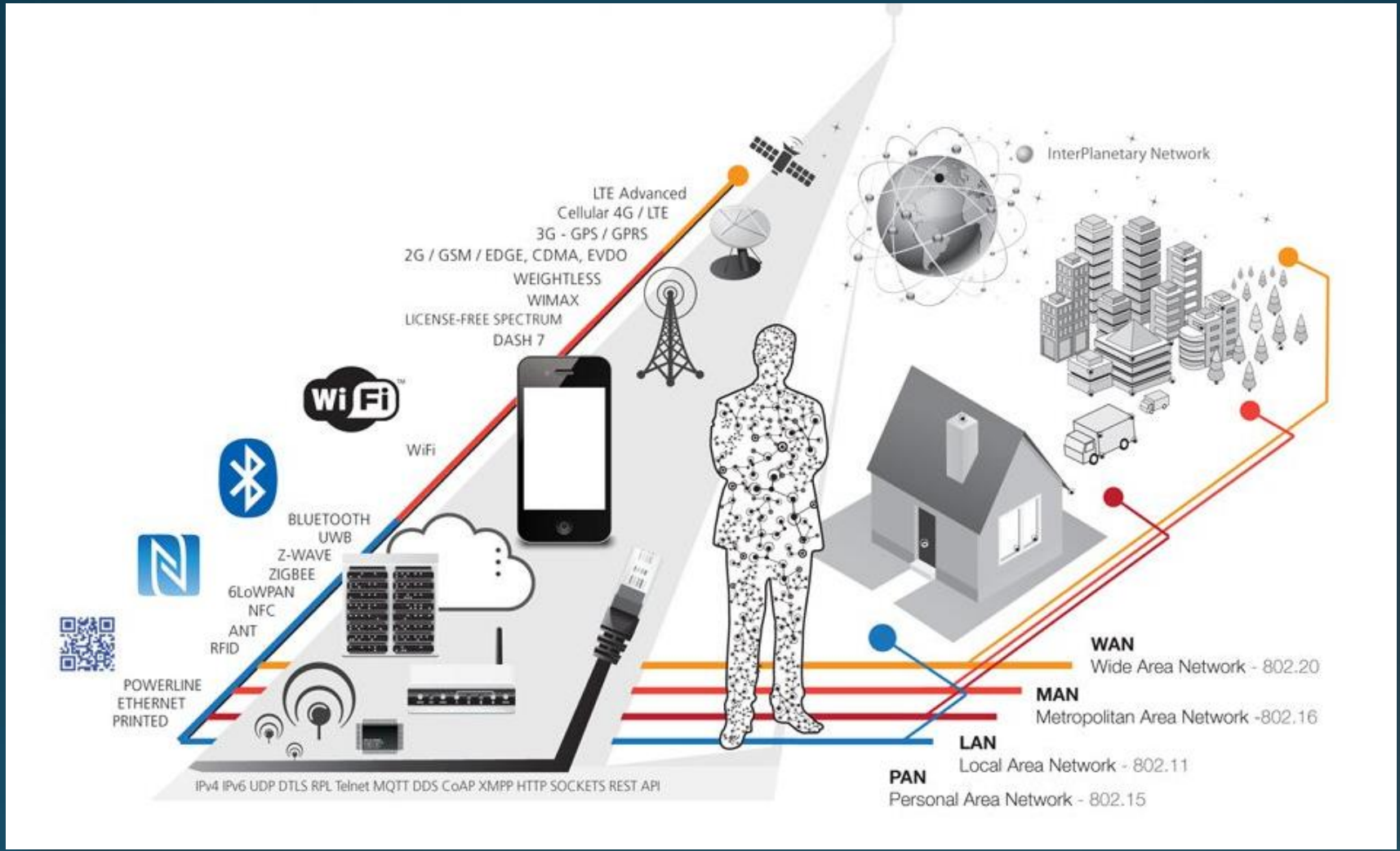
**Nearly half (46%) of IT Leaders said they will invest more next year in:**

- Access control
- Intrusion prevention
- Filter MAC addresses
- Identity management
- Virus and malware protection

"IOT is our single biggest **threat** AND **opportunity** over the next 10 years."

- Brand Name Fortune 500 Board of Directors

# IOT: Multiple Wireless Technologies

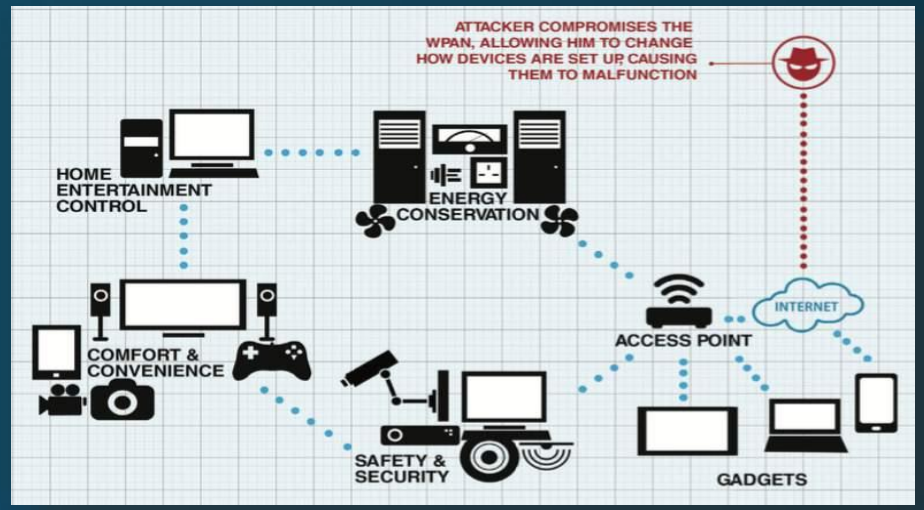



Source: http://postscapes.com

# IOT Security Issues


- Insecure web interface
- Insufficient authentication
- Insecure network services
- Lack of transport encryptions
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software
- Poor physical security

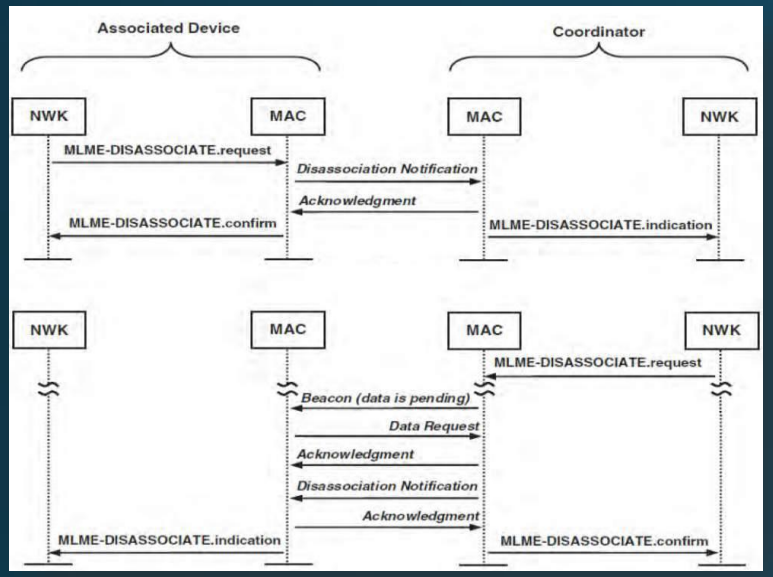
**Recent IOT Hacks:**
Fitbit
Samsung Smart TV
Nest
Jeep
Comcast




## Wireless Network Threats

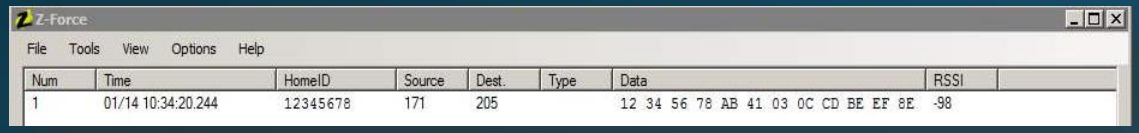
- Traffic Analysis
- Passive Eavesdropping
- Active Eavesdropping
- Unauthorized Access - Ransomware
- Man-in-the-Middle Attacks
- Session Hi-Jacking
- Replay Transactions
- Denial of Service (DoS)

# Executed Attack: Network Auth Key Establishment



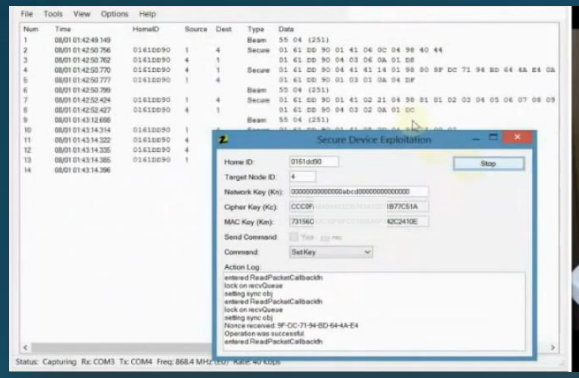

*Disassociation/ De-authorization*

- Pre-installed keys managed by the controller via OTA commands
- Each node has copy of keys (32 being standard) with a key manipulation algorithm
- Controller sends the key manipulation data to each device in a simultaneous command
- Controller checks value produced by node against its own to authorize communication
- This key scheme can be easily manipulated by use of a De-Authorization attack
- The node being detached is programmed to accept network key established by the gateway




*Node attempting to connect with a host/ controller*

- Once disconnected, node attempts to reestablish connection with host (but in many cases will default to the first host it finds)
- Although encryption is in place, it's possible to record the key set message and extract the key (but ineffective due to timing constraints and the use of low power transmissions)
- It is also possible and feasible to calculate all necessary keys from captured packets




*Spoofing the controller*

- Once connected to the host (spoofing the controller) it will accept the key and subsequent commands from its new host
- In the screenshot, the attacker uses this to send both a "SetKey" and "Unlock" command to the door

Contribution Source: R.J. Brownlow, Security Researcher

# Executed Attack: Physical Key Extraction Via Firmware

*Thermostat with debug access*

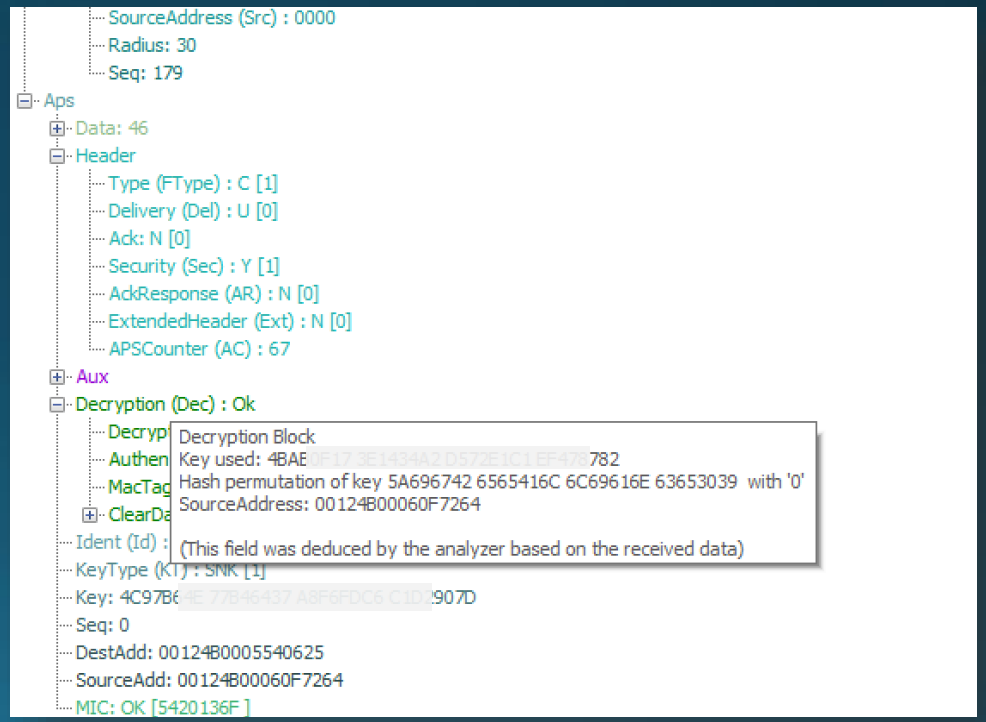
- Keys are stored in every node of the network and can be extracted from the factory firmware by way of the debugger interface
- In this example, a Z-Wave thermostat (manufacturer withheld), COTS flash programmer, factory development kit software tools and jumper wires are used to dump the firmware with a Serial to USB interface


*USB Debugging Tool*

- There are numerous USB dongles available from leading manufacturers
- Dongles traditionally only supported a single radio type (Wi-Fi, ZigBee, Z-Wave, BLE, etc.); however, several manufacturers are now beginning to manufacture multi-radio chips available in USB dongle form factors

*IDE displaying the encryption key in plaintext*

- Once accessed and dumped, the manufacturer's development kit can be used to decode the firmware code into plaintext as seen below




Contribution Source: R.J. Brownlow, Security Researcher

# Executed Attack: OTA Key Transport Interception

*Debugger Tool Capturing Wireless Packets*

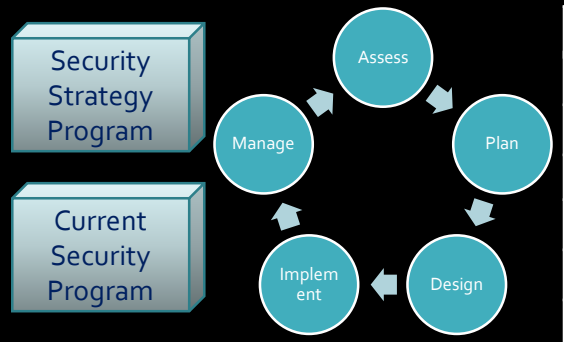
- In this authorization scheme, keys are transported directly to devices requesting to access the controller
- The node sends a beacon broadcast to all devices in range (seen in red below), essentially looking for any network to join
- The responding controller sends an acknowledgement and confirmation of availability (green)
- The node acknowledges receipt and requests a key to access the controller as a network resource (yellow)
- The controller responds with the network key and the node is added to the network (white-cropped out intentionally)
- This entire transaction is sent in clear text and can easily be extracted by wireless sniffing methods

| P.nbr. | Time (ms) | Length | Dest. Address | Source Address | Port | Device Info | Transaction ID | Applicaton payload | | RSSI (dBm) | LQI | FCS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | +0 | | | | Encryption Number | Rec.Type / Send.Type / HCount | | | | | | |
| 1 | =0 | 17 | 0x00000001 | 0x00000002 | NO 0x01 | ALWAYS_LISTEN END_DEVICE 01 | 0x02 | 03 BB CC DD | Ping: Length Data 03 BB CC DD | -64 | 1 | OK |
| 2 | =0 | 21 | 0x000000FF | 0x00000002 | NO 0x02 | SLEEPS/POLLS RANGE_EXTENDER 02 | 0x42 | 00 AA BB CC DD 33 55 02 | Link: App.Info Token Local_Port Link_numb. RX_Type 0x00 0xDDCCBBAA 0x33 0x55 SLEEPS/LISTENS | -64 | | |
| 3 | =0 | 16 | 0x00000001 | 0x00000002 | NO 0x02 | NEVER_LISTENS ACCESS_POINT 02 | 0x42 | 00 3F 01 | Link: App.Info Acc.Token RX_Type 0x00 0x3F SLEEPS/POLLS | -64 | 1 | OK |
| 4 | =0 | 19 | 0x000000FF | 0x00000002 | SW 0x03 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | 01 DD CC BB AA 11 | Join: App.Info Token Nbr_Conn. 0x01 0xAABBCCDD 0x11 | -64 | 1 | OK |
| 5 | =0 | 19 | 0x00000001 | 0x00000002 | HW 0x03 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | 01 55 66 77 88 00 | Join: App.Info Token Encryption Key 0x01 0x88776655 NO | -64 | 1 | OK |
| 6 | =0 | 22 | 0x00000001 | 0x00000002 | HW 0x03 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | 01 55 66 77 88 A3 01 02 03 | Join: App.Info Token Encryption Key 0x01 0x88776655 SW 01 02 03 | -64 | 1 | OK |
| 7 | =0 | 14 | 0x00000001 | 0x00000002 | NO 0x04 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | 00 | Security: Encryption Key NO | -64 | 1 | OK |
| 8 | =0 | 17 | 0x00000001 | 0x00000002 | NO 0x04 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | C3 01 02 03 | Security: Encryption Key HW 01 02 03 | -64 | 1 | OK |
| 9 | =0 | 15 | 0x00000002 | 0x00000001 | NO 0x05 | ALWAYS_LISTEN END_DEVICE 07 | 0x42 | 01 02 | Frequency: App.Info Freq.Index 0x01 0x02 | -64 | 1 | OK |
| | Time (ms) | | Dest. | Source | Port | Device Info | Transaction | Applicaton payload | Management | RSSI | LQI | FCS |

Contribution Source: R.J. Brownlow, Security Researcher

# Plans For Reducing Risk

## Develop a Comprehensive Security Strategy




| Establish Control Objectives |
| --- |
| Identify security controls your company uses (ISO, NIST, etc.) |
| Develop an effective vulnerability management program |
| Implement strong access controls and security measures |
| Develop testing, scan schedules, & patch management program |
| Develop an info security policy to fit your business model |
| Conduct readiness assessment, risk management and preparation for ISO/IEC 27001 or NIST conformance |

## Vulnerability & Penetration Testing


### Tactical Level

- Change Admin Passwords and Usernames
- Upgrade Wireless Encryption
- Change the Default System ID
- Filter MAC Addresses
- Don't Publicly Broadcast Your Network
- Don't Auto-Connect to Open Public Networks
- Use Built-In Firewalls
- Position Routers, APs, and Controllers Securely
- Turn Off Networks/Devices At Risk

# Tools for Reducing Risk

### Historic Troubleshooting Tools

- Detailed Forensics
- Scope Forensics
- Alarm Forensics

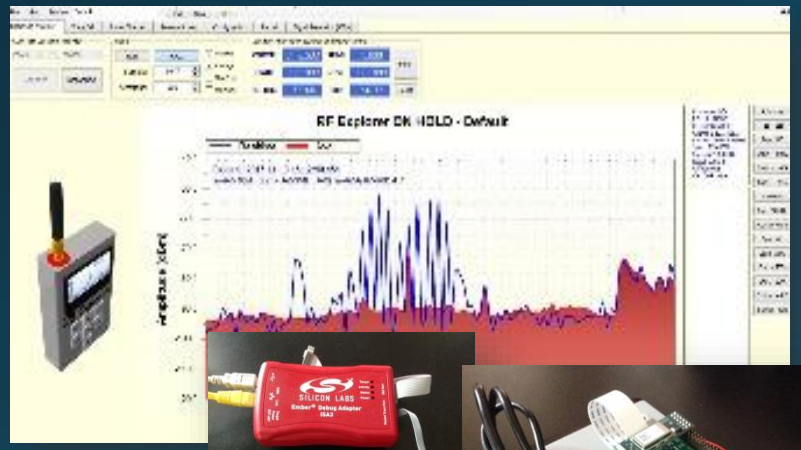
### Real-Time Troubleshooting Tools

- Live Wireless Analysis
- Client Connectivity Test
- AP Connection Test
- Spectrum Analysis
- Live RF Visualization

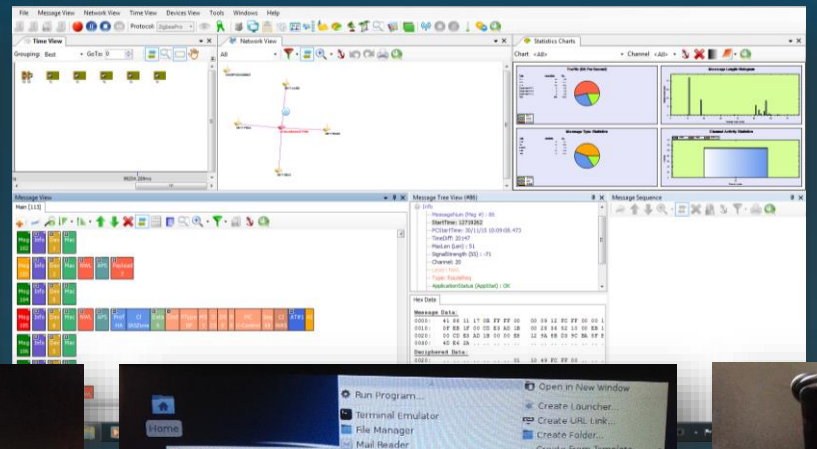
### Proactive Trouble Prevention

- AP Connection Testing
- Monitor Policy Compliance
- Monitor Performance Compliance
- RF Coverage Change Modeling

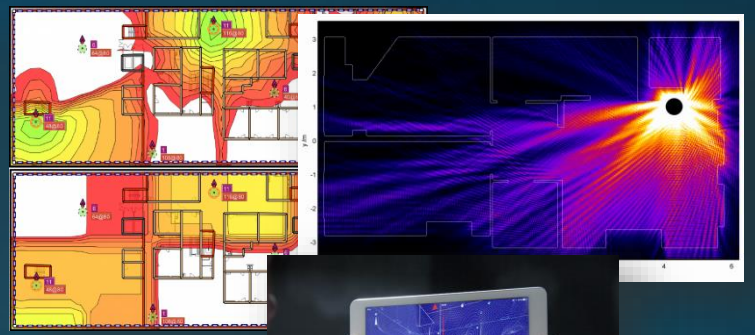
## Spectrum Analysis



## Packet Sniffing & Decoding



## Heat Mapping & Visualization



# Thank you!

Resources

- Chris Kocks chris.kocks@pureIntegration.com 678-467-7458 @Cgkocks
- SANS https://www.sans.org/
- OWASP https://www.owasp.org/index.php/Main_Page
- Texas Instruments http://www.ti.com/
- Silicon Labs http://www.silabs.com/Pages/default.aspx
- California Eastern Labs http://www.cel.com/
- Peryton's http://www.perytons.com/
- Wireshark https://www.wireshark.org/
- Linux Kali https://www.kali.org/
- Metasploit http://www.metasploit.com/
- KillerBee https://code.google.com/archive/p/killerbee/
- Airsnort http://www.shmoo.com/
- Netstumbler (maps networks with GPS) http://www.netstumbler.com/
- IOT Attack Scenarios http://www.pureintegration.com/services/internet-of-things/