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)

“IT is our single biggest threat AND opportunity over the next 10 years.”
- Brand Name Fortune 500 Board of Directors

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: 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)
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

*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

**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

Contribution Source: R.J. Brownlow, Security Researcher
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

Contribution Source: R.J. Brownlow, Security Researcher
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

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/