Home Automation

Joe Myshko

10/13/2018

A little bit about Joe

- Started my career at Commodore and built a world wide engineering network while the Internet was being started under the management of the National Science Foundation and the U.S. military.
- Joe graduated to the aerospace industry and has been involved in projects such as GPS, LandSat and Earth Observation satellites and has held high level security clearances.
- Over the past 3 decades, Joe's designed numerous Internet Gateways for Fortune 500 Companies such as GE, NBC, Vanguard, Mellon Bank, Martin Marietta and Lockheed.

A little bit about Joe

- Joe's skills include Internet security and especially securing Internet application layer protocols.
- Joe was one of a team of three that discovered the security breach and "break in" to General Electric's corporate network back in 1995 and helped to chase the notorious "Super Hacker" Kevin Mitnick who was eventually imprisoned for his activities.
- Citicorp has used Joe to design and rollout their corporate Email
- Now works for Comcast based in Philadelphia
- Co-Host of the Computer Corner Show every week on WCHE 1520 AM and 5dradio.com on Saturdays at 8am. http://wche1520.com and http://5dradio.com

A little bit about Joe

- Joe was one of a team of three that discovered the security breach and “break in” to General Electric’s corporate network back in 1995 and helped to chase the notorious “Super Hacker” Kevin Mitnick who was eventually imprisoned for his activities.
- According to the U.S. Department of Justice, Mitnick gained unauthorized access to dozens of computer networks while he was a fugitive. He used cloned cellular phones to hide his location and, among other things, copied valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted and stole computer passwords, altered computer networks, and broke into and read private e-mail. Mitnick was apprehended on February 15, 1995, in Raleigh, North Carolina. He was found with cloned cellular phones, more than 100 clone cellular phone codes, and multiple pieces of false identification.

Story of Mitnick's Takedown

"Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw", by John Markoff and Tsutomu Shimomura

What is Joe doing now?

- For the past 7.5 years, have been working for Comcast and helped to build the Xfinity X1 platform with virtualization and cloud technologies.
- Now has moved into Big Data for Comcast.

What is Home Automation?

- **Home automation** or **Domotics** is building automation for a home, called a **smart home** or **smart house**. A home automation system will control lighting, climate, entertainment systems, and appliances. It may also include home security such as access control and alarm systems. When connected with the Internet, home devices are an important constituent of the Internet of Things.

What is Home Automation?

- A home automation system typically connects controlled devices to a central hub or "gateway". The user interface for control of the system uses either wall-mounted terminals, tablet or desktop computers, a mobile phone application, or a Web interface, that may also be accessible off-site through the Internet.
- The word "*domotics*" (and "*domotica*" when used as a verb) is a contraction of the Latin word for a home (*domus*) and the word *robotics*.

History of Home Automation

- Early home automation began with labor-saving machines. Self-contained electric or gas powered home appliances became viable in the 1900s with the introduction of electric power distribution and led to the introduction of washing machines (1904), water heaters (1889), refrigerators, sewing machines, dishwashers, and clothes dryers.

History of Home Automation

- In 1975, the first general purpose home automation network technology, X10, was developed. It is a communication protocol for electronic devices. It primarily uses electric power transmission wiring for signaling and control, where the signals involve brief radio frequency bursts of digital data, and remains the most widely available. By 1978, X10 products included a 16 channel command console, a lamp module, and an appliance module. Soon after came the wall switch module and the first X10 timer.

History of Home Automation

- The three generations of home automation:
  - ***First generation: wireless technology with proxy server, e.g. Zigbee automation;***
  - ***Second generation: artificial intelligence controls electrical devices, e.g. Amazon Echo;***
  - ***Third generation: robot buddy who interacts with humans, e.g. Robot Rovio, Roomba,Neato, etc.***

Home AutomationTechnologies

- **X10** – a protocol for communication among electronic devices used for home automation (*domotics*). It primarily uses power line wiring for signaling and control, where the signals involve brief radio frequency bursts representing digital information. A wireless radio based protocol transport is also defined.
- **WeMo** is a series of products from Belkin that enable users to control home electronics remotely. The product suite includes electrical plugs, motion sensors, light switches, cameras, light bulbs, and a mobile app.

Home AutomationTechnologies

- **Z-Wave** is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance, allowing for wireless control of residential appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers.
- **Zigbee** is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.

X10

- Household electrical wiring which powers lights and appliances is used to send digital data between X10 devices. This data is encoded onto a 120 kHz carrier which is transmitted as bursts during the relatively quiet zero crossings of the 50 or 60 Hz AC alternating current waveform. One bit is transmitted at each zero crossing.
- Whether using power line or radio communications, packets transmitted using the X10 control protocol consist of a four bit *house code* followed by one or more four bit *unit codes*, finally followed by a four bit command.

X10

- When the system is installed, each controlled device is configured to respond to one of the 256 possible addresses (16 house codes × 16 unit codes); each device reacts to commands specifically addressed to it, or possibly to several broadcast commands.
- Inexpensive X10 devices only receive commands and do not acknowledge their status to the rest of the network. Two-way controller devices allow for a more robust network but cost two to four times more and require two-way X10 devices.

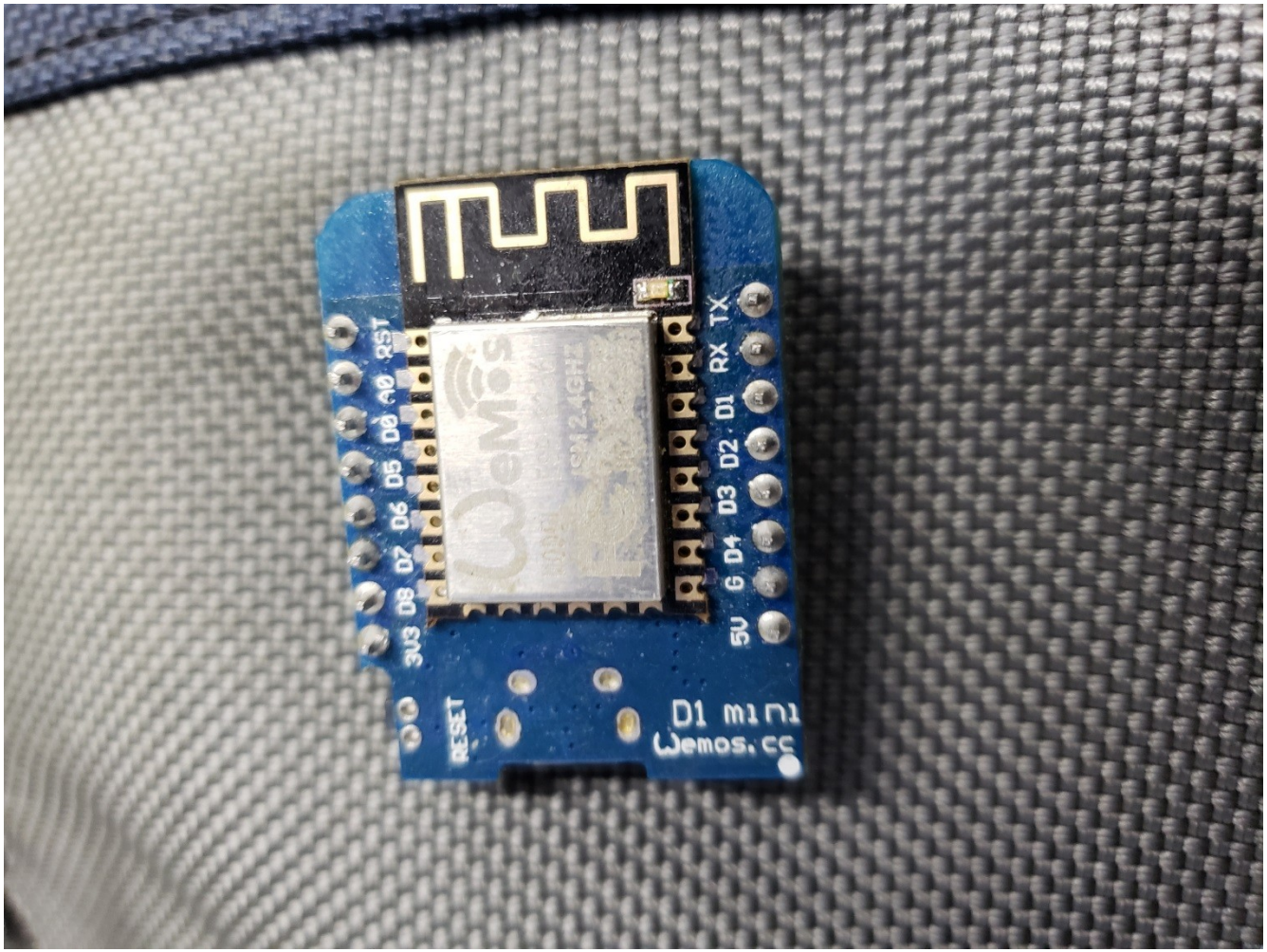
Wemo

- The WeMo Switch can be plugged into any home outlet, which can then be controlled from an iOS or Android smartphone running the WeMo App, via home Wi-Fi or mobile phone network.
- The WeMo Motion Sensor can be placed anywhere, as long as it can access the same Wi-Fi network as the WeMo devices it is intended to control. It can then turn on and off any of the WeMo devices connected to the WiFi network as people pass by.
- The WeMo Insight Switch provides information on power usage and cost estimation for devices plugged into the switch.

Wemo

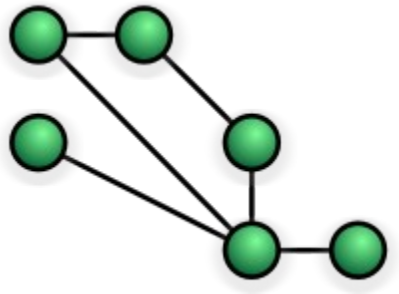
- The WeMo Light Switch is for use where a light is controlled by a single light switch. Multi-way switching is not supported at this time but can be approximated by installing a WeMo Light Switch at each location.
- The WeMo App controls the WeMo devices from anywhere in the world as long as the WeMo devices' wireless network is connected to the Internet. WeMo devices can also be controlled using IFTTT technology. WeMo devices can also be controlled by voice through the Amazon Echo, Google Assistant, and Apple's Siri (through the use of the WeMo Bridge).

Wemo Chip for Our Espresso Maker



Z-Wave

- Z-Wave uses a source-routed mesh network architecture. Mesh networks are also known as **wireless ad hoc networks**. In such networks, devices use the wireless channel to send control messages which are then relayed by neighboring devices in a wave-like fashion. The source device wanting to transmit is therefore known as the initiator. Hence, the name source-initiated mesh ad hoc routing.
- Devices can communicate to one another by using intermediate nodes to actively route around and circumvent household obstacles or radio dead spots that might occur in the multipath environment of a house. A message from node A to node C can be successfully delivered even if the two nodes are not within range, providing that a third node B can communicate with nodes A and C. If the preferred route is unavailable, the message originator will attempt other routes until a path is found to the C node. Therefore, a Z-Wave network can span much farther than the radio range of a single unit; however, with several of these hops a slight delay may be introduced between the control command and the desired result.



Z-Wave

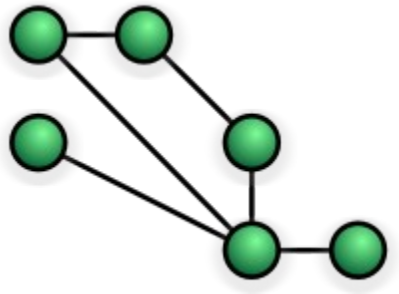
- The simplest network is a single controllable device and a primary controller. Additional devices can be added at any time, as can secondary controllers, including traditional hand-held controllers, key-fob controllers, wall-switch controllers and PC applications designed for management and control of a Z-Wave network. A Z-Wave network can consist of up to 232 devices, with the option of bridging networks if more devices are required.
- A device must be "included" to the Z-Wave network before it can be controlled via Z-Wave. This process (also known as "pairing" and "adding") is usually achieved by pressing a sequence of buttons on the controller and on the device being added to the network. This sequence only needs to be performed once, after which the device is always recognized by the controller. Devices can be removed from the Z-Wave network by a similar process. The controller learns the signal strength between the devices during the inclusion process, thus the architecture expects the devices to be in their intended final location before they are added to the system. Typically, the controller has a small internal battery backup, allowing it to be unplugged temporarily and taken to the location of a new device for pairing. The controller is then returned to its normal location and reconnected.

Z-Wave

- The Z-Wave chip is optimized for battery-powered devices, and most of the time remains in a power saving mode to consume less energy, waking up only to perform its function. With Z-Wave mesh networks, each device in the house bounces wireless signals around the house, which results in low power consumption, allowing devices work for years without needing to replace batteries. For Z-Wave units to be able to route unsolicited messages, they cannot be in sleep mode. Therefore, battery-operated devices are not designed as repeater units. Mobile devices, such as remote controls, are also excluded since Z-Wave assumes that all repeater capable devices in the network remain in their original detected position.
- Z-Wave operates at 908 MHz in the US, which has reduced noise and a greater coverage area.

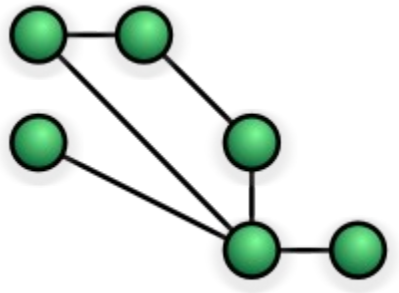
Zigbee

- Zigbee is a low-cost, low-power, wireless mesh network standard targeted at battery-powered devices in wireless control and monitoring applications. Zigbee delivers low-latency communication. Zigbee chips are typically integrated with radios and with microcontrollers. Zigbee operates in the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; though some devices also use 915 MHz in the USA and Australia, however even those regions and countries still use 2.4 GHz for most commercial Zigbee devices for home use. Data rates are 250 kbit/s (2.4 GHz band).
- Zigbee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate wireless personal area networks (WPANs). The specification includes four additional key components: network layer, application layer, *Zigbee Device Objects* (ZDOs) and manufacturer-defined application objects. ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, as well as device discovery and security.



Zigbee

- The Zigbee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of Zigbee routers to extend communication at the network level.
- A feature of Zigbee is facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames, and controlling device. It builds on the basic security framework defined in IEEE 802.15.4.



IFTTT

- **If This Then That**, also known as **IFTTT** , is a free* web-based service to create chains of simple conditional statements, called *applets*.
- An applet is triggered by changes that occur within other web services such as Gmail, Facebook, Telegram, Instagram, or many Apps
- For example, an applet may send an e-mail message if the user tweets using a hashtag, or copy a photo on Facebook to a user's archive if someone tags a user in a photo.
- * – there is free tier…

IFTTT

- In addition to the web-based application, the service runs on iOS and Android. In February 2015, IFTTT renamed its original application to IF, and released a new suite of apps called Do, which lets users create shortcut applications and actions. As of 2015, IFTTT users created about 20 million recipes each day. All of the functionalities of the Do suite of apps have since been integrated into a redesigned IFTTT app.
- There are a huge library of recipes that include many IOT automations.

IOT Security

- Internet of Things (IoT) security breaches have been dominating the headlines lately. WikiLeaks's trove of CIA documents revealed that internet-connected televisions can be used to secretly record conversations. Trump's advisor Kellyanne Conway believes that microwave ovens can spy on you—maybe she was referring to microwave cameras which indeed can be used for surveillance.

  And don't delude yourself that you are immune to IoT attacks, with 96% of security professionals responding to a new survey expecting an increase in IoT breaches this year.

IOT Security

- **IoT network security**: Protecting and securing the network connecting IoT devices to back-end systems on the internet. IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity. Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems.

IOT Security

- **IoT authentication**: Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics. Unlike most enterprise networks where the authentication processes involve a human being entering a credential, many IoT authentication scenarios (such as embedded sensors) are machine-to-machine based without any human intervention.

IOT Security

- **IoT encryption**: Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers. The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes, since poor key management will reduce overall security.

IOT Security

- **IoT PKI**: Providing complete X.509 digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation. The hardware specs for some IoT devices may limit or prevent their ability to utilize PKI. Digital certificates can be securely loaded onto IoT devices at the time of manufacture and then activated/enabled by third-party PKI software suites; the certificates could also be installed post-manufacture.

IOT Security

- **IoT security analytics**: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies. These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging. IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls.

IOT Security

- **IoT API security**: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs.

Q&A and Demos

- Thank you for coming!