Rise of the Connected Home

Security Challenges & Opportunities

Michele D. Guel
Infosec Division
Cisco Systems
San Jose, California
mguel@cisco.com

Justin Vayda
Global Infrastructor Services
Cisco Systems
San Jose, California
jvayda@cisco.com

Will Vincent
Webex Security Operations
Cisco Sysetms
San Jose, California
wvincent@cisco.com

Abstract— In this paper we will examine the recent rapid growth in internet connected devices for the home. For many, they see these devices as an easy transition to home automation. This paper will cover some of the technology enablers and advancements which have fuel the rise of the connected home. We'll explore some of the common home automation technologies (e.g. lights, motion sensors, cameras) and the various protocols that are used. We'll dive into common attack patters and defense mechanisms, along with some suggestions for additional security controls. We'll specifically deep dive into three vendor products as a precursor to a project where we will attempt to capture traffic and compromise one or more devices. This paper aims to serve as a quick reference for homeowners and DIYers alike when considering and designing their connected homes.

Keywords — sensor networks, security, connected things, WeMo, CloubBits, Wink

I. Introduction

Ten to fifteen years ago the concept of a connected home was about the ability to put CAT5 wiring through the house, enabling a fully connected home, room-to-room. Within a few years, many homes had the option of wireless Ethernet offered by cable television providers such as ATT and Comcast. The term "connected home" then became one which full wireless network access in almost every room. No more cables needed and none of the limitations that came with them. By 2010 we began to see the first "smart" devices. PG&E supplied us with Smart Meters and we began to see commercial residential products, for example NEST, that offered new ways to connect your home.

Within the last 4 years there has been an exponential increase the variety and functionality of "smart devices" that give rise to the connect home. Almost any hardware store (e.g. Home Depot, Lowe's, Orchard Supply) carries a variety of devices by multiple vendors. The rapid increase and availability of these smart devices and the often creative ways that people are beginning to use them present both challenges and opportunities for home owners all around.

From a security practitioner's standpoint, anything that can be used for good can also be used for bad, and unfortunately, developers often do not consider "misuse" cases when designing technology. Thus careful consideration must be made when designing the connected home of tomorrow to ensure that security and privacy risks and concerns are addressed. What may be one DIYer fun weekend project may also be the open doors for a threat actor to breach the virtual perimeter of your home or property.

This paper will provide an overview of enablers and technologies for the connected home and then drill down on security concerns, attack patterns, privacy concerns and best practices for securing your connected home. It is the hope of the authors that this short paper can server as a handy reference/guide for the DIYer as well homeowner looking to enabler their environment as part of the Internet of Everything (IoE).

II. Background Information

A. *Enablers for the Connect Home*

The last decade has seen an explosive increase in the number of technological devices around the world. As the cost, size, and power consumption of hardware has come down, and with internet access becoming more pervasive, it has become easier and more economical to embed systems into common items, allowing for features previously not possible. Cars now have computers to allow for automatic performance tuning based on driving habits. Televisions connect to cloud services such as Netflix and YouTube natively. Cellphones are now more computer than phone. Today, millions of devices in our homes talk over the net; they just don't talk to each other.

As technology continues to grow more and more devices are capable of becoming connected. Devices such as RaspberryPi and Arduino allow normal household items to be remotely controlled and automated. Companies are also getting in on this front by building newer devices that are pre-built with automation in mind. Companies like Nest and GE are designing smart devices that natively allow for remote access through a growing number of systems like Wink, and WeMo. As the number of devices grows, users gain increasing control over their surroundings, allowing them to customize them however they want be it for maximum efficiency, security, or comfort.

B. *Types of Connected Home Devices*

Thanks to the ever shrinking size of technology, numerous devices all around the home are becoming aware. Normal, everyday appliances are learning to talk to each other and work together. People can now get smart window shades and lights, which can be set to automatically close or turn on depending on time of day to save power. Garage door openers can be controlled via the internet so if someone forgets to close it when leaving for work they don't need to go all the way back home. Thermostats can be set while on vacation or in traffic. An oven can be set to pre-heat, or turned down to keep food warm. By connecting all the appliances in a home the owner can tune the environment to run more efficiently, and more comfortably.

Beyond simple conveniences these new smart devices can help make a home more secure. An owner can set the doors to automatically lock at night or in the morning after they've left for work. The locks could also be set to send alarms if opened during set hours, which can then trigger a camera to turn on so they can see if it's an intruder or just the kids trying to sneak out. Smoke detectors can be set to monitor for multiple types of air quality, tell you which rooms are affected, and notify of severe weather. Lights can be set to turn on and off making it look like the house is occupied even if the owner is on vacation. Simple things like this can not only provide peace of mind but also save lives by providing fast, and clear alerts when a threat is detected.

The connected home can also now include connected medical technology such as a glucose meter, blood-pressure meter and oximeter, among other things. For example, the refrigerator could be programmed that on the first opening of the morning, it would check to see if the glucose and/or blood pressure meter had been used and if not, reminder the owner to check their states. Perhaps at the end of the day, around dinner time, the smart refrigerator, over or crockpot would check the step count status on a Fitbit to remind the owner more steps needed or eat less food. Virtually almost any aspect of our lives can be sensed, monitored and reported on as we become increasing connected in every way.

Going just a bit further, emerging technology such as The Ubi voice activated, always-on computer, we can now give voice commands to our connected devices to make things happen. As our world becomes more connected, our personal threat landscapes expand providing amble targets for threat actors. [1]

C. *Sample Use Cases for the Connected Home*

The growing popularity of the Internet of Things, connected everything and "Maker" fairs have truly inspired innovation from the multitudes. The connected home can be almost anything we want it to be. From sensor controlled pet feeders, blind controllers, egg carton, thermostats, motion sensors and Ubi like devices, the combinations are just about endless. Automation and connectedness is really about maximizing resources and lower costs, enhancing user experience and making more time in our busy lives (the We Moments).

A typical connected home might have lighting sensors, a garage door sensor, alarm sensor, motion sensor and net cams. These devices provide the opportunity to provide lighting on demand when we walk in the room, shutdown or power off devices after we leave for work, send us an real-time update when an alarm (e.g. smoke alarm) goes off or video an attempted home-invasion.

More sophisticated uses of the connected home would be around energy consumption and water use. With a device like the WeMo Insight Switch, a homeowner can see exactly how much energy a specific devices use and the estimated monthly bill. Armed with additional information about which devices are drawing the most electricity, a homeowner could choose to switch products or reduce usage. Or during high energy consumption months where rolling brown-outs are common, the concerned homeowner can make appropriate choices.

In location where common resources are a premium (e.g. water in California), water sensors that can measure (through machine learning) water usage, detect leaks in the plumbing system or pressure changes may become common place. Homeowners could receive a deduction on the water bill for having sensors installed on all the sinks, toilets and outdoor water facets on the property. Valves could be shut off automatically if a leak or drop was detected or the homeowner could receive an alert about a potential pressure change or leak. It's also feasible to consider that water companies may collect stats from such sensors to make water rationing decisions about certain areas. For example, in some neighborhood with high water usage, home owner may be required to reduce or eliminate grass lawns.

One last use case we would like to propose for the Connect Home is monitoring of elderly people. Technology for rapid alert of medical response, such as Life Alert has been around for some time. These devices typically require the owner to wear a small pendant around their neck that has a push to call button. They have a special base station that would call the monitoring service. In the Connected Senior Home, you could install connect motion sensors in key areas such as bedroom, bathroom, kitchen or entrance hall, to provide status that occupant is moving around. You could also install a sensor alarm that responds to voice commands (or simple "Help") to send a real-time alert to a monitoring company or spouse or adult child. You could place a netcam in the kitchen which provides a visual of the senior to family or monitoring services. Sensors on key appliances such as space heaters, coffee makers or irons could ensure there were no fire dangers. Potentially, a connected home could allow an elderly person to life longer on their own rather than be placed in an assisted living environment.

III. Security Concerns and Attack Patterns

Most connected home setups follow a similar architecture pattern that usually consist of the following elements

- The sensor or device itself
- A mobile app and/or web interface that provides a UI
- Cloud Service that the sensor or device connects to make it cloud/internet enabled. Additionally, the cloud service many integrate with other cloud services, such as IFTTT (If This Then That), which may in turn integrate with other cloud services.
- Optionally, a hub that acts as an intermediary for a device that does not directly support a full TCP/IP stack, usually these communicate via some other local area protocol such as ZigBee

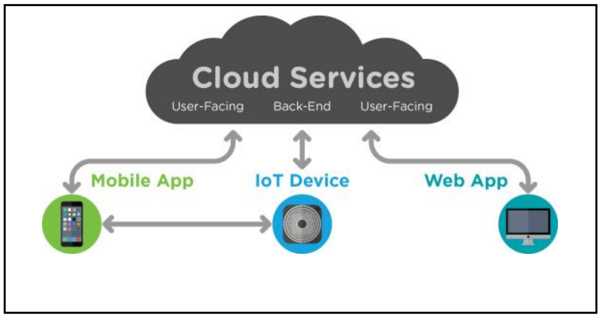


Figure 1: Typical Connected Home Architecture (http://www.techhive.com/article/2906664/many-connected-home-devices-lack-robust-security-features-security-firm-claims.html)

The majority attacks and areas of concern around vulnerabilities in the elements themselves or in the communication between those elements. The elements need each other to function. It only takes one weak link in the chain to compromise the security of the whole system.

A. *Attacks and security concerns against IoT sensors/devices/hubs*

Most devices/sensors/hubs contain some sort of web interface to initially set them up, and/or to provide an administrative console. A large number of attacks use well-known web application flaws to achieve the goal of owning the device.

These web attacks and concerns include

1) Command injection attacks – attackers will try to manipulate web requests to see if the any of those parameters are directly used in shell commands or other code execution contexts to be able to run arbitrary commands to gain root level access[2].

2) Other attacks leverage SQL injection to call DB functions that allow running shell commands.[3]

3) Cross-Site Request Forging (CSRF) - an attacker can leverage CSRF to trick someone with administrative access to upload tampered firmware that contains backdoors or other privilege escalation vectors. This has been technique shown to be effective against user’s home routers, it would not be difficult to extend this technique to IoT devices[4].

Other attacks and concerns include

- Many devices/hubs do not prevent or check, if the software on the device has been tampered, such as validating signed packages/images, or verifying if the hashes on files to check if they have been changed. If an attacker can access the file system they may be able add backdoors or change passwords.
- Physical attacks on RAM such as RowHammer has shown the need for robust hardware components. Many IoT devices are designed with goal of reducing cost with cheapest components as possible, these often lack the robustness of enterprise quality components.[5]
- Tampering with the physical hardware to force the device to boot up in boot loader mode.[6]
- Running outdated vulnerable software

B. *Attacks and security concerns against communication channels*

Communication between the various components needs to be secure. Typically devices/hubs communicate to the cloud via a TLS connection. For TLS to be effective to protect against Man-in the-Middle (MITM) attacks, validation of certificates is critical. Many hubs/devices fail to do so[7].

Communication between the device and hub are generally done via wireless protocols and may not be TCP/IP based. Some wireless technologies in use today are ZigBee, Wi-Fi, and Bluetooth.

ZigBee is a newer protocol that is designed around low power, low cost, short-range wireless access. As it is a newer protocol, it has advantage of learning from the security mistakes from Wi-Fi and Bluetooth, and has security in mind. ZigBee is considered a fairly secure protocol, but flawed implementations of the protocol have allowed devices to be compromised [8].

Wi-Fi with WPA2 encryption protection is also known to be fairly secure, but older encryption modes for Wi-Fi has known to have flaws such as those in WEP, and WPA1 and should avoided.

Bluetooth has also known to have weak keys and PIN numbers that could be fairly brute-forced [9]. Luckily, the newer standards such as Bluetooth Low Energy[10] used in most connected home devices has better encryption and is less susceptible to brute force attacks.

Lastly, other concerns involve the proper authentication/authorization between the device/hub and the cloud, and between the hub and devices. Without proper authentication, it is trivial for attacker to manipulate other devices that do not belong to him, or send fraudulent data to the cloud. For example, at attacker could impersonate a device/hub and give the false impression a door lock is locked, after it’s hacked and been remotely unlocked.

Some implementation use Oauth2 bearer tokens for authentication to the cloud's REST APIs via TLS. This generally considered safe, but many best practices with Oauth2 usually aren't being followed, such as periodically rotating/renewing tokens [11].

C. *Attacks and security concerns against cloud infrastructure*

The cloud infrastructure itself must be secure. This includes running updated patched software to protect against vulnerabilities in 3rd party code. Like any other cloud provider, the provider should be following best practices such as those provided by the Cloud Security Alliance [12].

D. *Attacks and security concerns against user facing UI controls*

Users of the connected home often interact with their devices via a web GUI or mobile client. Attacks against mobile and web platforms are well documented, and will not be discussed here. But there are concerns with making sure that how the user access these are protected.

This includes proper controls around

- Authentication – users should use strong credentials when accessing their connected home devices remotely.
- Authorization - users should only be able to access and interact with their own devices
- Secure communication – use TLS or other secure protocols

IV. Best Practices for Securing the connected home

With an understanding of how the Connected Home can be attacked and hacked, we can now examine what would be the ideal security features to be offered by home sensor devices. In doing research for this paper, we found very few resources on security best practices, or even vendor documentations for securing the sensors. Almost all artifacts were about the various attacks and hacks on home sensors [13].

The first area to think about is the protocols supported by the sensor itself. Some sensors only support Wi-Fi, while others support a variety of protocols such as ZigBee, Z-Wave or Bluetooth. But, given the small size of most sensors, there is not a lot of computing power and memory to add security features. Encryption capabilities should be at the top of the list for consideration. All communication with the cloud provider, firmware update server or user facing web applications should be encrypted.

The devices should also support authentication with a password of reasonable strength and length and the password should not be stored in the clear. Firmware updates should provide the option to require a password, SSL certificate check or digest check for the firmware image so the user can have a level of trust for the authenticity of the update. Most connected home sensors run some flavor of embedded Linux O/S. There are O/S level controls and hardening, even in a tiny os implementation that should be done. Some examples are removing unnecessary programs, default users and not running software a privileged user [14].

Another idea for protecting the sensors themselves would to be create a sensor firewall or gateway devices such that all incoming connections for the sensors had to pass through the gateway. This option would require a non-vendor supported application such as the WeMoServer mentioned later in this paper.

The second area of opportunity to secure is the mobile app itself. The user should only download mobile apps from known, good sources. Updates and patches should be applied regularly as well. Ideally, the vendor of the mobile app used a binary or static scan process on the code to ensure basic vulnerabilities (such as XML injection) do not exist. The mobile app should require a login and password for each use, as well as the set-up process. For example, for added security the use could choose a "key" or "PIN" on set-up that would be required each time to change the rules or control the devices. Communication between the senor and the mobile app should take place over an encrypted channel to TLS.

The final area to consider is the use of a user facing web application such as the "If This Then That" or ifttt.com. The home user should consider how the devices are initially configured into that particular could service. How the username/password is set up and how the information is regarding your devices stored and how easy is it to remove your devices. For some connected home users, the best decision may be to not use such web applications or allow remote access to the sensor devices through the mobile application.

V. Evaluation of Sample Vendor Products

A. *WeMo Devices*

In this section we'll deep dive in to the WeMo line of products from Belkin. The name "WeMo" is short for "We Moment". One of the tag lines from Belkin for this product is "Can we WeMo that?" with the idea being that the more items you can WeMo in your house, the more time you have to have "we moments" with the ones you love. WeMo makes life simpler! Most of the WeMo devices are in the $29 - $79 price range. The HD Cameras and small appliances are $99 – $199 range.

The WeMo product line includes a growing family of products that are wifi enabled and can be accesses and controlled from a smart phone or table using the WeMo app which works on IOS, Android and in some cases Kendal. A number of the WeMo devices require the use of the WeMo Link which is not sold separately but does come with the two-pak lighting starter kit. WeMo products can also interact with "recipes" that are on the IFTTT cloud provider. The WeMo product connects using 2.4GhZ Wi-Fi to the Internet and the Local LAN. Within the LAN WeMo devices are visible at UPnP devices and use SOAP/XML to talk to each other. [15]

1) Available Products

The WeMo product line has been growing at a steady rate. The current collection of products includes the following categories of products:

a. Wall switches – There are three variety of call switches. The first is the standard "WeMo Swtich: wall switches come with a single plug and will turn off/on the device plugged into it. The second is a There is also a WeMO motion switch option that will allow you to turn devices off or on based on motion detected up to 10 feet away. For example, turn the light of if someone walks into the room. The third is a "Insight Switch" which allows you to turn devices off/on and also monitor energy use.

b. Light Switch – The light switch replaces the standard light switch and allows you to turn lights off/on from the WeMo app. The WeMo Switch requires the neutral wire and only works on a single station switch and metal face plates not recommend.

c. Lighting (Bulbs and Strips) – WeMo offers a variety of light products. The standard LED light bulbs are equivalent to a 60 bulb, but only consume 10 watts and last up to 22 years. They can be switched on/off or dimmed with the WeMo App. There is a WeMo Link device for bulbs that allows you to connect up to 50 bulbs and control them individually or as groups. They have a tunable bulb call the OSRAM Lightify that allows you to adjust the warm and hue of the light. They have several new types of light products that will be out in the near future. An outdoor RGB garden strip, a flexible adhesive strip that can be used as decorative lighting, and indoor/outdoor flood light and a recessed light.

d. High Definition Cameras - WeMo offers several cameras that have high definition, wide-angel lenses as well as nighttime (or low light) vision and a built-in microphone. The cameras also have a push-to-talk feature where you can speak directly into your iPad or smartphone and communicate with parties at the camera sight.

e. Sensors – The initial offering of fours sensors will be out sometime later this year. All of the sensor products require the use of the WeMo Link device. The first product is the room motion sensor. This device can detect motion 30 feet away and has a 90 degree field of view. The second product is an alarm sensor that detects when any alarm in the house goes off (e.g. smoke alarm). . The third device is a key chain sensor which is intended to be used to monitor where elders, kids or pets are located (in the house or not). You can also program your WeMo enabled devices to turn on with the key chain sensor enters or leaves area. The final product is the window/door magnetic sensor to indicate if the door or window has opened. You can pair this 4th product with an Insight switch and then toggle A/C or heater on depending on if window/doors are opened.

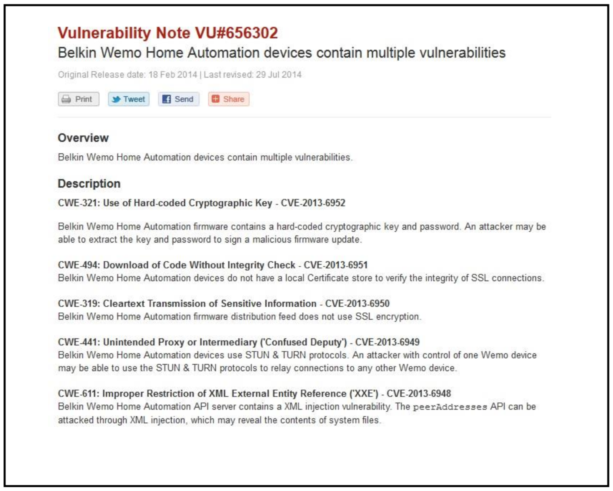
f. Small Home Appliances - WeMo offers a growing list of small appliances that are wifi enabled and work with the WeMo apps. With the app and WeMo enabled appliances you can control various features of the appliances (e.g. turn crockpot to low) or get alerts when there is an issue (e.g. humidifier low on water). The current list of appliances includes: Crockpot, 10-cup Coffee Maker, Humidifier, Air Purifier, and Room Heater.

g. WeMo Maker - The Maker device, just released this year, is designed for the DIYer, inventor or those who like to tinker with electronics. The Maker allows you to control low voltage (e.g. 5V) electronic devices. For example you can connect your garage door opening button.

h. Water Sensor – The WeMo Water if a future product in the development stages. This is bound to be a popular item in drought-stricken areas such as California. The Water device connects under your kitchen sink and can sense pressure changes, water leaks and uses machine learned to detect amount of flow. This sensor can be connected to bathroom sync, toilets, washing machine and home irrigation systems.

2) Security Concerns & Known Hacks

There have been a number of publicized security concerns with the WeMo devices dating back almost two years. Most of them have been corrected at this point in time. See a snippet of the CERT Advisory that was published in February 2014. Belkin claimed a few weeks later that they had released patches/fixes for those 5 vulnerabilities, some of which were released prior to the CERT Advisory. Most of the security articles that were found on WeMo issues are from February 2014 [16].



Vulnerability Note VU#656302

Belkin Wemo Home Automation devices contain multiple vulnerabilities

Original Release date: 18 Feb 2014 | Last revised: 29 Jul 2014

Overview

Belkin Wemo Home Automation devices contain multiple vulnerabilities.

Description

CWE-321: Use of Hard-coded Cryptographic Key - CVE-2013-6952

Belkin Wemo Home Automation firmware contains a hard-coded cryptographic key and password. An attacker may be able to extract the key and password to sign a malicious firmware update.

CWE-494: Download of Code Without Integrity Check - CVE-2013-6951
Belkin Wemo Home Automation devices do not have a local Certificate store to verify the integrity of SSL connections.

CWE-319: Cleartext Transmission of Sensitive Information - CVE-2013-6950
Belkin Wemo Home Automation firmware distribution feed does not use SSL encryption.

CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') - CVE-2013-6949
Belkin Wemo Home Automation devices use STUN & TURN protocols. An attacker with control of one Wemo device may be able to use the STUN & TURN protocols to relay connections to any other Wemo device.

CWE-611: Improper Restriction of XML External Entity Reference ('XXE') - CVE-2013-6948
Belkin Wemo Home Automation API server contains a XML injection vulnerability. The `peerAddresses` API can be attacked through XML injection, which may reveal the contents of system files.

Figure 2- Early WeMo Vulnerabilities

Several well-known security research centers, such as IOActive have provided details on the vulnerabilities. For starters, the firmware is digitally signed, but the signing key and password are stored in the clear on the devices. This means that a threat actor could replace/upgrade the firmware on the device with a bogus version creating a fully open door for future attacks. Belkin was using an unsecured RSS feed to notify Belkin users about the update.

Vulnerability with the WeMo devices involved the use of the Belkin Cloud Services without full validation of the SSL certificate. This means that a threat actor could impersonate the Belkin cloud services and control your devices. It also means that a threat actor could load Trojan firmware on the Belkin cloud site and infect thousands of users. We also found a website that demonstrates how to hack the API for the WeMo app [17].

Belkin at one point offered the WeMo Baby Monitor but have discontinued the product. There were a number of articles regarding security issues with the baby monitor. There are units available on Amazon and other web based shopping locations. Consumers should beware of these devices as they are no longer support so update firmware to correct security issues is not available. This product had its own mobile that that would allow you to monitor child/baby from a remote location. Major problem was that other people could monitor your child as well. The major security issue with this device, as many of the WeMo devices is that anyone with one time access to the device can authenticate and then no password required when using the app to connect to your device. There have been multiple articles and presentations on how people have successfully turned the WeMo baby monitor into a remote eavesdropping/spying device.

3) *Security Features*

The conscientious consumer will quickly find a server lack of documentation or guidelines on how to run WeMo devices securely. Once can only assume this is due to very limited, if any security features. After initial set-up all Belkin owners should update the firmware of their device. Although the more sever patches have bene out for some time, it's difficult to know how long a particular WeMo device has been on the shelf at the store. Aside from update the firmware to the latest version, there is the important decision of whether to enable you WeMo devices to be controlled remotely.

A number of the articles read, recommended against enabling remote access for WeMo through the Belkin WeMo provider and WeMo app. However, most people buy home automation devices so they can be controlled from anywhere at any time.

Another decision point is whether to enable remote access via the IFTTT site (IF This Then That), which is a third part cloud provider site where anyone can add new "recipes" for various technologies and then allow your rules located on a third party site to control your devices. Just like the Belkin cloud service for the WeMo app, you are dependent on security if the IFTTT site.

More recently, there are a few private third party offerings such as the WeMoServer that runs on windows or Linux box and allows you to connect your devices. There is also the NetHomeServer open source product for managing home automation. It appears that one of the security tenants is to not allow remote access to the WeMo devices and to limit other services (like posting/storing your cam videos on the third party cloud.

B. *CloudBits*

littleBits is a company that provides easy to assemble electrical modules to allow a non-technical person to easily assemble electronic circuits and projects. The module easily connects to other modules using magnets; no soldering or breadboarding skills are required. Additionally, littleBits have also gained a large following with the technically savvy crowd as a rapid-prototyping tool.

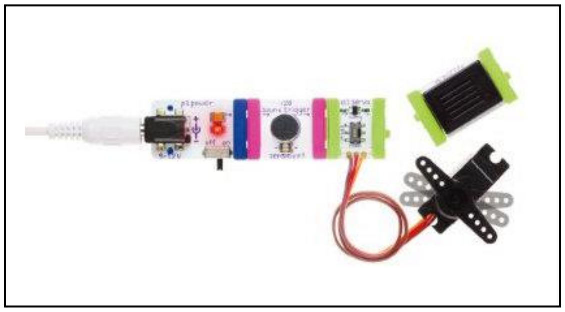


Figure 3 - Example littleBits project (from http://littlebits.cc)

Recently, littleBits has entered the Internet of Things (IoT) space, by introducing a component known as the cloudBit. The cloudBit allows any project to now be cloud-enabled.

The cloudBit is essentially a small Linux computer with Wi-Fi capabilities that allow it to connect to the littleBits cloud. This essentially allows the cloudBit two major capabilities. First, the cloudBit can receive electronic input from littleBit modules attached to the cloudBit, (such as motion sensors, buttons, microphones) and send that signal to the littleBits cloud. Secondly, data can be sent from the littleBits cloud to the cloudBit, which allows it to output an electronic signal to any attached output modules (such as motors, servos, relays, lights).

For example, one could build a simple a simple sprinkler system with the cloudBit that allows it to leverage the power of the cloud to find out weather reports from the week to determine how much water is needed

1) *Protocols supported*

The cloudBit currently supports Wi-Fi 11b/g/n. It acts as wireless client in normal use, but during initial setup of the device it acts as a wireless access point with a web server to configure what wireless network it should join. Encryption modes for the cloudBit Wi-Fi include Open (no encryption), WEP, WPA and WPA2 Personal (pre-shared keys). It does not support WPA2 Enterprise (802.1x authentication). Communication between the cloudBit and littleBits cloud is thru a raw HTTP over TLS socket initiated by the cloudBit using a REST based API with JSON messages. Authentication appears use Oauth2 bearer tokens.

2) Other Technical Information

- Processor: Freescale i.MX23 ARM926EJ-S
- RAM: 64MB
- Storage: 4GB on micro SD card (ext4 filesystem)
- OS: ArchLinux

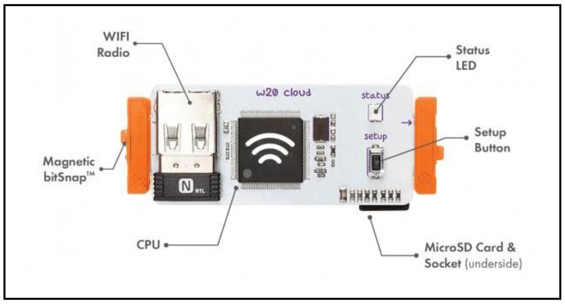


Figure 4 - cloudBit (from http:/littlebits.cc)

3) Types of Products

While littleBits does not sell home automation appliances, it primary business model is to allow you to build own with its collection of various models. There are a variety of input sensors and output modules. Here is a small sampling of various pre-built modules available. littleBits also provides a kit to make your own modules.

Input Modules

- Sound Trigger
- Light Sensor
- Button
- Motion Sensor
- Pressure Sensors
- Temperature Sensor
- Bending Sensor

Output Modules

- Servo
- DC Motor
- Vibration Motor
- LED
- Buzzer
- Speaker
- Number display

4) Security Concerns and Known issues

There are currently no known security issues with the cloudBit or the littleBits cloud. There are a few references from littleBits and other tinkers that have exposed some areas of concern.

The SD card on the cloudBit can easily be removed and mounted to any computer that understands the Linux ext4 filesystem. Since there does not appear to be any signing of packages, files, etc… It is trivial to change any part of the system. Users have been able to change the root password and enable SSH access on the file system [19]. Protecting physical access to the cloudBit would be important if it was left in a public area.

During the setup process, it cloudBit acts as an access point. No authentication is needed to connect to the access point; anyone in local proximity could configure the cloudBit to join its wireless network by sending requests to the cloudBit web interface [20].

The littleBits cloud seems to support weaker encryption protocol such as SSLv3, which is known to be vulnerable to various attacks such as POODLE. The upside is supports stronger cipher suites Diffie-Hellman for key exchanges, and AES encryption.

The littleBits cloud allows weak passwords to be set for its UI for controlling the cloudBit. The team was able to register with a short password with only lower case characters.
The littleBits website mentions their infrastructure used Node.js and Redis. Both of these packages have been known to contain security issues in the past. Checks should be done to make sure littleBits keeps up to date with patches [21].

C. Wink Device

The Wink Hub is a simple appliance that acts as an interpreter for various smart devices to connect to the Wink system. It uses an open architecture to allow devices built by multiple manufacturers to interface with the Wink App, which lets a user control all paired devices from their mobile device.

1) Protocols Supported

- Bluetooth
- WiFi (2.4 GHz only)
- Z-Wave
- Zigbee
- Lutron ClearConnect
- Kidde

2) Types of Products

- Light bulbs
- Switches and outlets
- Motion, Smoke, and other sensors
- Garage door systems
- Door locks
- Thermostats
- Air conditioners
- Water heaters
- Window shades

3) Security Concerns & Known Hacks

Command injection [22] – The device runs a web server that has a debug script (set_dev_value.php) deployed. This script allows for arbitrary code execution as root through the use of unfiltered POST variables. Attackers can gain root access to the hub or gain access to peripheral devices and execute commands against them, such as disabling locks or sensors. This issue has since been patched, but is still exploitable if done before the device can download the fix from Wink during initial configuration.

SQL Injection – The hub has a php script (dev_detail.php) located on it that takes user input unsanitized user input as a parameter into a SQLite query. When combined with a known SQLite vulnerability (creating a local database that can execute a php shell) the attacker can execute arbitrary code against the system through web requests. Once the malicious code is injected into the database the attacker can then execute arbitrary code against the hub or peripheral devices. This issue has been patched, but may still be possible if done before the device has a chance to download updated firmware upon first boot.

NAND Flash Glitch – The hub uses U-BOOT for the bootloader. By grounding the I/O output from the NAND memory once the kernel starts loading, U-BOOT will fail and load a privileged shell. From here an attacker can then modify kernel arguments and cause the system to load a root shell. This issue requires physical access to the device.

Weak passwords – Strong passwords are not enforced when creating an account for the app. Weak passwords can allow an attacker to gain access to a system with little effort and gain full control of a system [22].

4) *Security Features*

Certificate Pinning – Certificate pinning is "the process of associating a host with their *expected* X509 certificate". By pinning the certificate to the host this can harden the connection between devices and remove numerous attack vectors, such as Man-In-the_Middle [23].

Traffic Encryption – All traffic between the devices and Wink servers are encrypted, preventing any sensitive data from being sniffed on the network.

Two-Factor Authentication – Two factor authentication is a more secure way to authenticate a user as it requires confirmation from two different sources. This means that should an attacker compromise your account they still will not be able to access your devices as they will not be able to access the system without the second source.

Constant app and firmware updates – The developers are constantly working on improving the security of the device by finding and fixing any vulnerabilities and sending updates to the systems and applying them automatically so that users are not responsible for maintaining the devices themselves [24].

VI. Conclusion

We have examined a wide variety of home automation devices and the security challenges present. Based on a large volumne of research done by many in the past 2-3 years, there is still much to be done to secure small sensor devices used in home automation. The idea of a fully connected, automated home seems like a great idea to add to help home owners save on energy costs, increase physical security and provide peace of mind about home occupants such as elderly parents or young children.

The average consumer of connect home products will undoubtedly have a security background or think about the misuse cases, lack of security features and widely publicized security hacks with available code. While there are a few suggestions and recommended actions to secure the connect home, there is much work still to be done. As such, we highly recommend that consumers do some homework before rushing out to the nearest Lowe's or Homedepot to join their neighbors in home automation. We hope this paper serves as a handy quick reference for the buyer to be.

References

[1] Ubi Voice of the Internet http://www.theubi.com/

[2] Wink Hub Command Line Injection Vulnerability https://www.exploitee.rs/index.php/Wink_Hub%E2%80%8B%E2%80%8B#set_dev_value.php_Command_Execution

[3] Wink Hub SQL Injection Vulnerability https://www.exploitee.rs/index.php/Wink_Hub%E2%80%8B%E2%80%8B#Wink_Hub_.22.2Fvar.2Fwww.2Fdev_detail.php.22_SQLi_for_root_command_execution

[4] Cross-Site Request Forgery Attacks Against Linksys Wireless Routers http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1020&context=techmasters

[5] RowHammer Side Effect - https://en.wikipedia.org/wiki/Row_hammer

[6] Wink Hub NAND glitch method https://www.exploitee.rs/index.php/Wink_Hub%E2%80%8B%E2%80%8B#NAND_Glitch_Method_.28Works_on_any_Wink_Hub_FW.29

[7] Many connected-home devices lack robust security features http://www.techhive.com/article/2906664/many-connected-home-devices-lack-robust-security-features-security-firm-claims.html

[8] ZigBee Wireless Security: A New Age Penetration Tester's Toolkit http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4

[9] https://en.wikipedia.org/wiki/Bluetooth#Security_concerns

[10] http://eecatalog.com/IoT/2014/08/13/increasing-wireless-security-with-bluetooth-low-energy/

[11] Oauth2.0 Threat Model and Security Considerations - https://tools.ietf.org/html/rfc6819

[12] Cloud Security Alliance homepage - https://cloudsecurityalliance.org/

[13] Widman J., Many Connect-home Devices Lack Robust Features Security Firm Claims (2014 April), Retrieved from http://www.techhive.com/article/2906664/many-connected-home-devices-lack-robust-security-features-security-firm-claims.html

[14] Baek K., Bratus S., Sinclair S., and Smith S, Attacking and Defending Network Embedded Devices. Retreived from www.cs.dartmouth.edu/~sws/pubs/bbss07.pdf

[15] WeMo Products - http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/

[16] Cert Vulnerability Note VU#656302 - http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/

[17] IOActive Advisory on WeMo - http://www.ioactive.com/pdfs/IOActive_Belkin-advisory-lite.pdf

[18] Network World Article on WeMo Baby Eavesdropping http://www.networkworld.com/article/2225628/microsoft-subnet/eavesdropping-made-easy--remote-spying-with-wemo-baby-and-an-iphone.htm

[19] https://github.com/yepher/littlebits/blob/master/CloubitFileSystem.md

[20] https://github.com/yepher/littlebits/blob/master/CloudBit_ProtocolNotes.md

[21] http://littlebits.cc/introducing-the-cloudbit

[22] The Wink Hub https://www.exploitee.rs/index.php/Wink_Hub

[23] "The Internet of Things: Security Research Study" *Veracode*. 2015. 14 May 2015. Retrieved from: https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf?mkt_tok=3RkMMJWWfF9wsRogv63BZKXonjHpfsX87u0tW66wlMI%2F0ER3fOvrPUfGjI4IScdlI%2BSLDwEYGJlv6SgFTbnFMbprzbgPUhA%3D/