Smart Thermostat Security: Turning up the Heat

Matthew Burrough, Jonathan Gill
Department of Computer Science
University of Illinois at Urbana-Champaign
{burrogh2, jagill2}@illinois.edu

***Abstract*—The proliferation of smart phones, wireless networks, and micro-controllers has created growing demand for devices in the home that are "intelligent", connected, and easy to use. This trend, along with an ever-increasing concern over energy consumption, has brought home automation technologies into the mainstream. While a "smart home" has never been easier or less expensive to create, connecting formerly standalone devices to the Internet has a dark side. Security is often overlooked in the rush to get these in-demand products to market or is bolted on as an afterthought, after a web-controlled device is proven to be vulnerable to attacks. This paper surveys several popular home automation products and provides a detailed security assessment of select devices.**

I. Introduction

Increasingly, consumers are expecting devices around them to interact with each other, to provide rich, web-based experiences, and to offer user-friendly interfaces. As microprocessors have become smaller, cheaper, and more capable, manufacturers of appliances and small electronics have seen an opportunity to oblige these tech savvy customers. By taking advantage of the massive adoption of smart phones and nearly ubiquitous wireless network access, these companies can now give users a simple way to interact with devices throughout their home on a familiar screen that users carry with them everywhere they go.

According to industry research, an estimated one million home automation systems were installed in North America in 2012 [1]. This was triple the number installed in 2008, and half as many as are expected to be installed by 2014. Worldwide, it is estimated that 90 million homes will contain home automation systems [2]. For example, the United Kingdom saw an increase of 12% in home automation system installations in 2011, which accounted for £65 million in spending and was estimated to grow to £156 million by 2016 [3].

This growth has enticed numerous established companies to expand their product offerings in this area. Comcast, Time Warner Cable, Verizon, and AT&T have all begun offering products and services for customers to manage and monitor their homes. Existing alarm companies such as ADT are also branching out into home automation. Finally, venture capitalists have been looking favorably at home automation start-ups, committing hundreds of millions of dollars in total to companies like iControl, Alarm.com, Grid2Home, and OPower [4].

Home automation platforms open up the attack surface of a household, leaving them vulnerable to cyber-criminals with economic, privacy, and physical security motivations. The economic impacts can be identified through the ability to remotely control a vulnerable home thermostat. The U.S. Environmental Protection Agency (EPA) reports that the average household spends more than $2,200 a year on energy bills, with almost half of the cost going to heating and cooling costs [5]. Maliciously heating or cooling a home to extreme temperatures both increases utility costs and adds additional strain on HVAC systems. Vulnerabilities in home surveillance equipment can lead to serious privacy and security concerns. The ability for an unauthorized individual to remotely monitor audio and video within a household would concern any homeowner. Additionally, the monitoring enables intruders to target break-ins when homeowners are away. Along those same lines, security systems and smart locks aim to deter intruders while providing the homeowner the ability to remotely control access for intended guests. The convenience of providing remote access is the foundation of what an intruder would target when seeking vulnerabilities in physical security devices.

The arguments for ensuring endpoint security are compelling, but business decisions and release deadlines often supersede threat modeling and vulnerability testing. Thus, we seek to perform this testing to assess the impending economic, privacy, and security risks that home automation systems present. We have surveyed a number of different product offerings, evaluating market share, device capabilities, and cost. Our initial review has led us to acquire the Nest Learning Thermostat 2.0 and the Honeywell Wi-Fi Thermostat (RTH6580WF). Other platforms and solutions are intriguing, but due to the limited evaluation time and out-of-pocket cost, we focus our review on these platforms.

The rest of the paper is organized as follows: In Section II, we review a number of industry threat reports and predictions as well as recent publications by security researchers focused on hacking home automation platforms. In Section III, we survey a number of home automation solutions and discuss criteria for selecting platforms of interest. Section IV discusses our security evaluation plan and the devices we plan on testing. Lastly, Section V highlights our initial progress and findings.

II. Related Work

To further understand the state of home automation and smart device security, we examine global threat trends from industry leaders and vulnerability discovery reports by security researchers. We focus on both home automation protocols (X10, Z-Wave, ZigBee) and generic smart devices that operate over Wi-Fi. We find that the growth of the home automation

market and general lack of secure design has led to a prime target for finding security vulnerabilities.

Trend Micro released a recent white paper [6] revealing a forward-looking view of the increased risks that home automation solutions present. The focus is on IEEE 802.15.4, upon which the X10, Z-Wave and ZigBee protocols are based. The standard was developed to provide cheap, low-power, and low-speed communication across devices. It is common for home automation devices to leverage such protocols to form a mesh network so that various sensors and control panels can communicate. The growth of the home automation market has led to competition between Z-Wave and ZigBee for market share. Trend Micro predicts an increased overall security risk since each protocol and implementation present unique risks.

The reality is that Trend Micro's predictions are far from bold. In 2011, Simon and Kennedy [7] released the *X10 Sniffer* and *X10 Blackout* exploitation tools, capable of jamming X10 based signals in order to prevent security systems from triggering other devices. The lack of encryption in X10 and susceptibility to heavy interference highlights the underlying issues with using the protocol within safety critical systems. At that time, they reported that although Z-Wave provided encryption support with AES, that they didn't find any devices that supported it. Furthermore, they found that during the initial pairing of devices, the AES initialization key can be captured allowing for decrypting and tampering with communications. More recently, in 2013, Fouladi and Ghanoun [8] built a low cost Z-Wave packet capture and injection tool used to facilitate vulnerability discovery in Z-Wave devices. The tool was successful in exploiting an implementation flaw in the key exchange protocol that allowed them to remotely control wireless door locks. There has also been recent interest in ZigBee testing, as Joshua Wright presented a number of findings at the DEFCON conference in 2011. He developed the *Killer Bee* exploitation framework [9], providing tools for sniffing, decoding, manipulating, and injecting ZigBee packets. Similar to Z-Wave, he found that the over-the-air key provisioning mechanism that devices use to pair encryption keys was susceptible to eavesdropping. Other findings included lack of replay protection, allowing an attacker to replay valid packets in a malicious manner; consider replaying a packet that actuates water control valves or increases the temperature.

Research by Crowley, Bryan, and Savage [10] further backs up our claims that network-controlled embedded devices are unlikely to take security into account in their designs. Of ten platforms reviewed, including home automation control units, smart thermostats, and media gateways, exploitable flaws were found in nearly all. In most cases, simply having local network access was sufficient to control the devices as many did not employ any authentication measures. Additionally, security measures were not in place when accessing the devices remotely from the Internet. The majority of testing focused on web services and APIs that provide remote management to the devices. The lack of security in these devices impose risks to both the devices they control and make home networks as a whole more vulnerable.

At DEFCON 21, Joe Grand unveiled the JTAGulator [11], an open source hardware tool aimed to assist in the identification of on-chip debug (OCD) interfaces on embedded systems. OCD interfaces are a well-known attack vector that can allow an attacker to extract program code and data, modify memory contents, impact device operation at runtime, access debug output, or gain access local console access to the device. It is generally inconvenient for vendors to remove OCD interfaces, as they are often used during development and can be critical in debugging returned equipment that is malfunctioning. It can often be difficult and time consuming to identify OCD interfaces, thus the JTAGulator provides an interface to probe and determine pin functionality. It is capable of identifying IEEE 1149.1 JTAG (Joint Test Action Group) and UART (Universal Asynchronous Receiver/Transmitter) interfaces. We aim to use the JTAGulator in hopes of identifying UART interfaces that can provide local console access to the target device. Local device access should allow for enumerating the file system and identifying software components that are critical to the services responsible for communicating with remote clients.

III. Survey of Devices

In order to select target devices for testing, we first survey a variety of devices including consumer-grade smart thermostats, home surveillance, and home security systems. The criteria for choosing devices include cost, device popularity and review, availability, feature set, and remote management services. Our selection does not intend to target any particular vendor or country of manufacturing for the purpose of negatively or positively impacting brand reputation. All vulnerabilities will be responsibly disclosed to the vendors to allow them the opportunity to address the issues in upcoming software releases.

A. Nest Learning Thermostat - 2nd Generation (T200577)

The Nest Learning Thermostat aims to profile end user heating and cooling preferences to provide a comfortable environment, while conserving energy when the user is not home. The device retails for $249, making it one of the most expensive consumer thermostats on the market. A September 2012 report [12] revealed that Nest sold "in the mid-hundreds of thousands" of the first-generation device. It is ranked first in number of sales in Amazon.com's programmable thermostat category.

Nest has a variety of sensory devices that are used to make informed decisions regarding heating and cooling. In addition to a standard temperature sensor, short range, long range, and ambient light sensors are used to learn about home activity. Additionally, to reduce power consumption, the LCD interface is only displayed when someone approaches the device.

In addition to the learning capabilities, Nest offers 802.11 b/g/n and 802.15.4 Wi-Fi support (both at 2.4 GHz) for remote management and data collection. A cloud portal, iOS, and Android applications offer an energy-use dashboard and the ability to remotely control the current temperature settings.

Although the security implications of a thermostat on the surface may seem less concerning than home security systems, home behavior patterns can be inferred from recorded energy data and future thermostat schedules. This data would thus be a valuable target for intruders.

We contacted Nest and gave them the option of providing one of their devices for inclusion in our evaluation, but they declined. However, due to the popularity of the Nest device, we opted to purchase one at retail for assessment.

B. Honeywell Seven-Day Programmable Wi-Fi Thermostat (RTH6580WF)

Honeywell is a natural choice when considering thermostats to assess. With 40% of thermostat market share and an install base of 150 million homes, Honeywell clearly has a dominant position [13].

Honeywell is obviously intent on maintaining this strong hold. In 2012, it engaged Nest in patent litigation, claiming infringement on 7 patents which Nest is contesting [14]. To invigorate consumer interest, Honeywell has also released several new products in recent years with "smart" features. They offer several models of Wi-Fi enabled thermostats, each controllable from Apple and Android apps, as well as via a web browser. Additionally, they offer a model with a Z-Wave interface that integrates with their home security systems. Finally, they just announced their latest Wi-Fi thermostat which also includes voice control. It is scheduled for release in November 2013 [15].

Honeywell thermostats are commonly installed by HVAC companies because Honeywell's products are frequently re-branded and sold under the name of the heating and cooling systems being installed. For example, Mitsubishi Electric's web-controlled P- and M-Lines are actually Honeywell devices [16]. (One of this paper's authors recently had a Trane-branded non-Wi-Fi Honeywell touchscreen thermostat installed in his home.)

We contacted Honeywell and gave them the option of providing one of their devices for inclusion in our evaluation, but they did not respond. However, because of the factors described above, we opted to purchase one of their devices at retail for assessment.

Based on our device selection criteria, we chose to assess the Honeywell 7-Day Wi-Fi programmable non-touchscreen thermostat (RTH6580WF) for several reasons. This model is readily available at stores such as Lowe's, The Home Depot, and Amazon.com. It is also sold under several other brands, like Mitsubishi Electric. In terms of smart features, all three of Honeywell's currently available Wi-Fi thermostats seem to use the same web interface and applications to control them. The main difference between them is buttons vs. touchscreen and monochrome touchscreen vs. full color touchscreen [17]. Given that the connected features appear to be the same in all three, and this is the area we will focus on, the lowest cost, non-touchscreen model seemed the most practical. Although it would be interesting to test the new Wi-Fi + voice controlled model, it will not be released in time to be included in this report. We opted not to test the Z-Wave based thermostat as it requires a larger investment in an overall Honeywell security ecosystem, and because Z-Wave attacks, while possible, are less common than web based or Wireless LAN originated attacks [8].

C. ecobee Smart Thermostat

Ecobee offers two consumer models of thermostats as a central part of their energy monitoring and management solution. The "Smart" is a full color touch-screen based model and the "Smart Si" is button based with a smaller color screen. Both are Wi-Fi enabled and can be controlled from either a web portal or the company's iOS, Android, and Blackberry apps. Ecobee also sells two commercial versions of these devices that appear to be very similar to the consumer grade offerings [18]. Finally, ecobee also makes "Smart Plug" devices that are similar to Kill-a-Watt single outlet power meters, however the Smart Plug sends its information back to the ecobee Smart thermostat via ZigBee. (A Zigbee module for the Smart thermostat is an optional upgrade. [19])

Ecobee is unique in that it also provides an API for developers to interact with their devices [20]. This provides an interesting opportunity to access the device programatically, and potentially opens up another attack vector against the Smart thermostat.

Unfortunately, the ecobee Smart Thermostat did not meet our selection criteria due to availability, adoption rate, and cost. Unlike the other devices in this section, the ecobee thermostats are not directly sold to consumers, but rather must be acquired from a HVAC installer. Because of this, it appears the ecobee likely has a much smaller install base than the Honeywell or Nest systems. Unlike these two brands, no documented market share figures could be located. Ecobee also does not appear to sell their products re-branded under different companies names, as Honeywell and Radio Thermostat do. Finally, even if it was available, the list price of the Smart Thermostat is $469, which is significantly more expensive than the other thermostats under consideration [21]. We contacted ecobee and gave them the option of providing one of their devices for inclusion in our evaluation, but they declined.

D. Motison CyberStat CY1201

Motison appears to be a small company with only two products - the CyberStat CY1201 and its predecessor the CyberStat CY1101. Both devices appear to be quite similar, with the second generation receiving support for Android, adjustable temperature tolerance, adjustable brightness, 802.11 G support, and the ability for the thermostat to start the HVAC system early to achieve a given temperature at a desired time [22].

The Motison devices are both priced at $79.99, with the CY1101 being sold on Amazon and the CY1201 available directly from the manufacturer as well as Amazon. At this price, these are the lowest cost Wi-Fi enabled thermostats we surveyed. The products are #87 and #49 respectively in Amazon's Programmable Thermostat sales ranks. Both also

have between 4 and 4.5 stars with 86 cumulative Amazon reviews.

In terms of features, the Motisons are the most basic of the thermostats surveyed here. The unit only contains three buttons (temperature up, down, and mode), as well as 6 LEDs (Wi-Fi status, a setting indicator, and four to indicate the selected mode: auto, heat, cool, and fan), and two 8-segment LEDs to display the temperature. Through a combination of pressing two of the three buttons at once, it is possible to perform some rudimentary programming of the device, however most any task aside from simply changing the current temperature or switching between heating and cooling would realistically need to be performed from one of the company's smart phone apps [23].

We contacted Motison and provided them the option of providing one of their devices for inclusion in our evaluation, but they did not respond. Given the relatively limited features and small install base, we opted not to assess the CyberStats.

E. Venstar ColorTouch T5800

Venstar makes a number of thermostats, although only their ColorTouch series offers Wi-Fi capabilities. The ColorTouches include the T5800 (residential thermostat), T5900 (residential with humidity control), T6800 (commercial) and T6900 (commercial with humidity control). The commercial units include easier programming for a retail schedule. Otherwise the units appear to be the same.

An interesting feature is the SD card slot on the device which can be used to display up to 100 photos on the ColorTouch's full color screen. The SD card also allows for the import and export of thermostat settings [24].

The ColorTouch also uses a different method to join the wireless network than the Honeywell and the Motison. While both of those companies' products create an add–hoc network which a PC or phone can connect to and configure the thermostat to join the location's actual Wi-Fi network, the ColorTouch provides a UI on its touchscreen to enter the SSID and network password [25].

Two variants of the Venstar ColorTouch are ranked #41 and #47 in Amazon's Programmable Thermostat sales rank and have a total of 64 reviews with an average of 4.5 stars. The T5800 is available on Amazon for $149.50.

We contacted Venstar and provided them the option of providing one of their devices for inclusion in our evaluation, but they declined. In spite of the unique features, with a limited testing budget we opted to omit the ColorTouch from testing in favor of the more popular models from other manufacturers.

F. Radio Thermostat Company of America CT30

Radio Thermostat Company of America (hereafter Radio Thermostat) manufactures two Wi-Fi enabled thermostats: the CT30 and CT80 models. While not a well known brand in its own right, the company also partners with a number of other companies and sells their products under different brands. For example, the 3M Filtrete 3M-50, Homewerks CT-30, and LockState Connect LS-60i all appear to be CT30 thermostats with different labels.

Like most other vendors, Radio Thermostat's two models appear to use the same application to control them and likely have the same underlying Wi-Fi stack. The main difference between their CT30 (priced at $139.95 direct from the manufacturer) and the CT80 ($249.95) is the screen and physical appearance of the units. Additionally, the CT80 can support additional stages of heat and maintain seven programmed temperature changes per day, over the CT30's four. The CT80, unlike the CT30, does not appear to be sold under different brand names. As such, we focused on the CT30 which is more readily available and thus likely has a larger install base.

From a feature standpoint, the CT30 has a surprising number given its cost. There are iPhone, Android, and web-based apps to control the thermostat remotely. The thermostat itself also has both buttons and a touchscreen for local input [26]. Additionally, ZigBee and Z-Wave radios are also available as separate modules [27].

Although variants of the CT30 are available from The Home Depot, Amazon, and direct from Radio Thermostat, the product doesn't seem to have nearly the adoption rate of the Honeywell or Nest. The variants sold at Home Depot have a total of 23 reviews on Home Depot's website compared to 46 Nest reviews and 233 reviews for Wi-Fi enabled Honeywell thermostats on the same site. The CT30 is ranked 26th on Amazon.com's best seller list for programmable thermostats. On Amazon, the Honeywell Wi-Fi thermostats have 169 reviews, the Nest has 1,253, and the Radio Thermostat variants have 226. (Note that the Honeywell products are not sold directly by Amazon and are only available through their marketplace sellers.) Given this, we opted not to purchase a CT30 for assessment. We contacted Radio Thermostat and provided them the option of providing one of their devices for inclusion in our evaluation, but they declined.

G. Iris Home Management System

Lowe's home improvement stores recently entered the home automation market with their own line products. The Iris Home Management System is comprised of a base station known as the "Iris Smart Hub" and a variety of first- and third-party accessories that communicate with the Smart Hub over Z-Wave or ZigBee. These include alarm panels, electronic locks, door and window sensors, power outlets, switches, smoke detectors, cameras, key fobs, and thermostats [28].

The Smart Hub connects to the user's wireless network and provides them with remote monitoring and control of the devices paired with the hub via smart phone apps and a web interface. The thermostat itself is actually manufactured by Radio Thermostat of America and appears to be a Z-Wave variant of the CT30. The actual model number of the Iris thermostat is CT101 [29].

Since the Iris is a Lowe's product, it is not available from other retailers. The cost of a starter kit with a Smart Hub, thermostat, and one "Smart Plug" outlet is $179. Lowe's does not reveal sales figures on its site, through the stand-alone

Smart Hub has 16 reviews with an average of 3 stars, the kit with thermostat has 13 reviews averaging 4 stars, and the stand alone thermostat has 9 reviews averaging 4 stars. Lowe's also sells a larger starter kit with both a thermostat and an alarm panel with several sensors and a Smart Plug for $299, which has 65 reviews averaging 3.5 stars. The apps on the Android and iOS stores each have 2.5 stars, and have 120 and 93 ratings respectively.

We contacted Lowe's and provided them the option of providing one of their devices for inclusion in our evaluation, but they declined. Given the seemingly limited number of installations based on product and app reviews, we opted not to test the Iris system.

IV. Evaluation Plan

Our initial survey has led us to acquire the Nest Learning Thermostat 2.0 and the Honeywell Wi-Fi Thermostat (RTH6580WF). Other platforms and solutions were considered, but due to the limited evaluation time and out-of-pocket cost, we will focus our review on these platforms.

Without access to source code, we will take a black box approach in our testing. Under the assumption that the devices are likely to be running Linux, we first focus our efforts on gaining administrative root access to the system. It is likely that the vendors have a need for this level of access to enable debugging the devices during development and troubleshooting defective devices. However, it is possible that this access may require credentials or may not be enabled by default. Thus, we will take one of the following approaches for analyzing the system software:

- Extraction of firmware off non-volatile storage by removing storage device and analyzing in corresponding memory card reader
- Extraction of firmware off non-volatile storage via JTAG commands
- Reverse engineering of firmware upgrade packages

The boot ROM of consumer embedded devices often consists of a boot loader, Linux kernel, and compressed file system. Access to the file system allows a static view into the system start-up scripts and binaries. By modifying and repackaging the firmware, we should be able to make sufficient changes to the system to allow remote access via SSH or Telnet. If console or SSH access if available by default, analyzing the file system may aid in identifying credentials that may be statically configured. At a minimum, access to the system binaries allows us to analyze and reverse engineer core system components to target vulnerability discovery.

Local system access or firmware reverse engineering is not required, but simply aids in finding vulnerabilities as there is more visibility in how the system operates. Regardless of the success of our initial testing, we focus the second stage of vulnerability discovery on the following tests:

- Evaluation of the communication methods between the target device and remote management clients/portals
- Web security audit of cloud management portal or web services running locally on the device
- Evaluation of any management APIs (may include fuzzing)
- Port scanning and evaluation of any available services running on the thermostat

Since all of the target devices can be controlled remotely, we know that there is a communication mechanism between a cloud portal managed by the vendor and the device itself. Since most Wi-Fi devices deployed in homes are using NAT, we expect the devices to continuously poll the cloud for updates. However, it is possible that the devices could be deployed with a public facing IP address, so we will also focus on the available network services that are running. We will assume various levels of access and deployment when considering different threat scenarios. The primary focus of all of our testing will be to find vulnerabilities that allow the ability to maliciously control the smart thermostats under test.

V. Findings

A. Nest Learning Thermostat - 2nd Generation (T200577)

1) Hardware Analysis: A previously completed device teardown [30] reveals a list of key components on the the main motherboard in Figure 1. The micro USB port provides an alternate source for charging the thermostat and provides a mass storage device to the host. Initial review of this file system includes a configuration file that includes serial number, MAC address, and software version information. It is anticipated that this interface could be used by support engineers, although this mechanism was not identified. Our review of the startup scripts do not indicate any services that take action based on the content of this file or the presence of any other files on the storage device.

Component	Specifications
CPU	Texas Instruments AM3703CUS Sitara ARM Cortex A8 microprocessor
Memory	Samsung K4X51163PK 512 Mb mobile DRAM
Storage	Micron MT29F2G16ABBEAH4 2 Gb NAND flash memory
Wi-Fi	Texas Instruments WL1270B 802.11 b/g/n Wi-Fi
USB	Texas Instruments TPS65921B power management and USB single chip
ZigBee	Ember EM357 integrated ZigBee / 802.15.4 system-on-chip
ZigBee	Skyworks 2436L high power 2.4 GHz 802.15.4 front-end module

Fig. 1. Nest Hardware Components

2) Firmware Analysis: Nest's open source compliance report [31] reveals a number of packages to indicate that it is likely running a Debian Linux OS. Analysis of the firmware upgrade packages from Nest's site includes a Linux JFFS2 filesystem. Using a publicly available tool [32] allows us to extract the Linux file system, providing access to the system configuration files and system utilities.

First, we take a brief look at the configuration files. Static analysis of the password shadow indicates a number of user accounts, but none of which contain any password hashes

for offline cracking. The system initialization scripts include the typical Linux startup utilities to bring up services such as networking, syslog and SSH, but also include the EM357 ZigBee radio and other proprietary services.

Conveniently, most of the proprietary software is clearly identifiable through the directory structure and filename conventions. The applications include a combination of 32-bit GNU/Linux 2.6.16 ARM executables and bash shell scripts. All of the compiled executables are stripped of their symbol tables, which can make reverse engineering a bit more difficult. However, the footprint is fairly small, as the largest of all applications is nlclient which is only 2.9 MB. The listing of some of the key applications are listed in Table 2.

Process	Description
nlscpm	Nest Labs System Control and Power Management (SCPM) daemon
nlheartbeat	Nest Labs Heartbeat Software / Watchdog process
nlclient	Nest Labs Learning Thermostat process
nlswupdate	Nest Labs Software Update process
nlzbupdater	Nest Labs ZigBee Update process
nlsuspend	Nest Labs Wi-Fi Suspending process

Fig. 2. Nest Applications

3) Setup Phase: The fully featured rotary and push-button display of the Nest makes configuration quite simple. After confirming that the thermostat is wired correctly, the second phase attempts to connect Nest to a Wi-Fi network. The user can either select from the list of available networks or specify their own.

Once the Nest is online, it can be registered to a user account on Nest's website. In order to provide a seamless setup process, the Nest website recognizes if the client is connecting from the same IP address as the unregistered Nest thermostat, and displays a dialog box on the Nest display asking if it should be registered to the associated Nest account. The other option is to request that Nest obtain a registration code, which is then displayed for the user to enter into the web portal to complete the registration process. The registration code is seven characters, consisting of three digits followed by a four character English word. Once registered, the Nest website allows for acquiring past thermostat history, as well as changing the current thermostat settings.

Once online, the Nest makes only a few outbound connections, most of which are to servers in Nest's domain, as displayed in Table 3. It is assumed that the initial connection to the Nest frontdoor server is made to obtain basic configuration settings for the device, which might include a particular transport server to communicate with. Because all communication between the thermostat and the cloud is encrypted, no sensitive data is leaked. Investigation of the Nest firmware includes Certificiate Authority (CA) certificates Nest, GoDaddy, and ValiCert. The presence of these CA certificates allow the Nest to confirm the identity of the remote web servers when establishing TLS connections. Further testing highlighted that the Nest was not susceptible to a man-in-the-middle attack when presented with a self-signed certificate.

Host	Port	Protocol
frontdoor.nest.com	443/tcp	HTTPS
time.nestlabs.com	123/udp	NTP
ipv4.connman.net	80/tcp	HTTP
transportXX.transport.nest.com	9543/tcp	Nest TLS
devices.nest.com	443/tcp	HTTPS
wunderground.com	80/tcp	HTTP

Fig. 3. Nest Network Connections

4) Post Setup: When not actively controlled by an end-user, the Nest appears to be offline. The device does not respond to ICMP Echo Requests, yet responds immediately to cloud-based temperature control changes. TCP keep-alives are sent to transportXX.transport.nest.com:9543 every two minutes. This will keep the PAT entries updated to prevent a home router from dropping the connection. Investigation of the file system shows utilities responsible for waking up the wireless LAN controller based on the presence of packets originating from Nest transport servers or when the motion sensors are triggered. A number of Texas Instruments utilities for managing wireless interface are present so that the device operates in a low-power setting. In order to perform a port scan against the thermostat, it is required that the thermostat is "awake." By interacting with the thermostat or triggering the motion sensors, persistent connections can be made to the thermostat. However, no TCP or UDP ports appear to be open, in contrast to some of the expectations based on Linux startup utilities.

By maintaining a long-lived TCP session, temperature changes configured through the cloud interface or mobile app allow update on the thermostat almost immediately. A flood of encrypted traffic is sent from the Nest transport server to the thermostat whenever changes are made. Through the technical info interface on the thermostat, the "Nest Server URL" setting is set to *devices.nest.com/upload*. Once again, this traffic was found to be encrypted and the web server certificate signed by the Nest CA.

B. Honeywell 7 Day Programmable Wi-Fi Thermostat (RTH6580WF)

1) Hardware Analysis: No previous tear-downs could be found for Honeywell Wi-Fi thermostats, so our first action after opening the Honeywell's box was to disassemble the unit. The components discovered are listed in figure 4. The thermostat consists of two PCBs, connected by a 4-pin header. The main board consists mainly of an Atmel XMEGA 128 micro-controller on the back side which appears to handle button input, driving the LCD, and interfacing with the HVAC equipment. The remainder of this board is pretty basic. The front side of the board contains the large monochrome LCD, as well as contacts for the seven membrane switches. In addition to the XMEGA, the back of the PCB hosts some capacitors, resistors, and relays. It also has 6 pads which are exposed through the back of the casing if one sticker is removed.

Presumably these pads are an interface to reprogram, test, or debug the unit, although they are unlabeled.

A daughter-board attaches to the back of the main board and contains an Atmel SAM4 micro-controller and an Atmel 32 Mb flash storage chip. There are additional components under a metal RF shield, but no attempt was made to de-solder the shield from the board. The remainder of the PCB contains an etched-on antenna. Clearly this board contains the component needed for Wi-Fi communication. Presumably this board was designed to be modular so a different radio could be substituted, or perhaps to even offer a non-connected "dumb" version of the unit in the same form factor.

Component	Specifications
Main CPU	Atmel XMEGA 128B1-U
Radio CPU	Atmel ATSAM4S16BA-MU
Storage	Atmel 1310 25DF321A-SH 32 Mb Flash

Fig. 4. Honeywell Hardware Components

Given the limited storage and computation power of the identified chips in the Honeywell, it seems probable that the unit runs a small, custom built operating system. Additionally, the absence of any open source license disclosures anywhere in the product documentation, packaging, or website further suggest that, unlike the Nest, no open source operating system was used in the thermostat.

Further exploration was performed into the 6-pad header hidden under a sticker on the rear of the casing. Since we had identified that each Honeywell contains unique web server files that include the device serial number, we anticipated that this header could be used during manufacturing to program the flash chip with this content. Thus, we soldered wires on to the PCB and hooked up the JTAGulator to enumerate the possible interfaces. However, our testing yielded inconclusive, as the JTAGulator failed to identify a JTAG or UART pin-out.

2) Setup Phase: The Honeywell creates its own unencrypted wireless network when first powered on with the SSID "NewThermostat_X" (where X is a 6-digit number that corresponds to the last 6 digits of the unit's MAC address). On the thermostat's screen, the words "Wi-Fi Setup" blink above the clock to indicate that the thermostat has not been configured. Once connected to the network, the product documentation instruct the user to open a web browser and connect to http://192.168.1.1. From this page, the thermostat presents a list of available networks in the area, as well as their signal strength and encryption type, if any. No password is required to access the configuration page.

A port scan against the device during this initial setup revealed that TCP port 80, UDP port 53, and UDP port 67 were the only open ports on the device. Port 80 serves the configuration web page while 53 runs DNS to redirect web traffic to the configuration page. Port 67 runs the DHCP service to provide IPs to clients that connect to the network. The IP lease pool begins at 192.168.1.100. Attempting to connect multiple devices to the network succeeded. A second device connected to the Wi-Fi network was granted IP address 192.168.1.101, and that PC was also able to browse to the setup web page.

Viewing the source of the setup web page revealed that most of the configuration functions are JavaScript based and contained in the page itself. The page does reference a key.js file, which contains an RSA public key (e and n values), as well as the URL of Honeywell's Total Connect site with the unit's MAC address and OS version, and a CRC value as parameters. Finally, it has the name of the service ("Total Connect Comfort") and the text "REGISTER THERMOSTAT".

In a network trace between the thermostat and the device configuring it the traffic is sent unencrypted. This initially appeared to be a problem, considering the Wi-Fi password must be supplied using this form. However analysis of the packets reveals the password is never sent in plain-text across the network. Closer examination of the JavaScript reveals two things: first, that the code is obfuscated to make reading difficult, and second, that the network selection and connection credentials are protected using the RSA values found in key.js, along with some further encoding done in the JavaScript.

As soon as the Wi-Fi registration mechanism was discovered, we purchased an additional thermostat to compare key values. We had hoped that all thermostats used the same keys, and we had planned on trying to recover the private key from flash storage which would allow for passively decrypting user-submitted Wi-Fi passwords. This was found to not be the case, as each thermostat contained unique RSA values. However, with the thermostat network unsecured and the web transport unencrypted, there are no measures to prevent a man-in-the-middle attack. An attacker could simply perform an ARP-spoofing attack and supply attacker-chosen RSA values that would allow the attacker to decrypt the credentials once submitted. Additionally, with access to the device-specific keys, the attacker could seamlessly re-encrypt the credentials and forward the request such that the user would not recognize any interference.

As a test, arpspoof [33] was executed on one computer joined to the thermostat's network with the IP of the thermostat set to redirect to this computer. A second computer was able to join the network and a review of its ARP tables showed it believed the MAC address of the thermostat to be the MAC address of the computer running arpspoof. Using this setup, a motivated attacker could script the replacement of the values of key.js to their own chosen RSA values while passing through all other traffic, which should allow for the decryption of the information submitted to the web form. Granted, the attacker would need their computer to be close enough to the thermostat to be able to remain connected to its network and wait for the end user to connect to and configure the thermostat. As such, the risk of such an attack is presumably quite low.

Once the credentials for the network were entered on the thermostat, it displayed a page instructing the user to reconnect to their normal network and to click a button on the page to go to a registration page on the Honeywell Total Connect website. On this page, aside from typical website registration

details such as name, email, address, and password, the form requested two details about the thermostat so it could be associated with the new account. The first was the MAC address of the thermostat and the second was a 4-digit CRC value of the MAC address. Both of these values are included on an index card provided with the owner's manual.

One concern with this approach is that an attacker could discover a non-configured thermostat while war-driving and would immediately know the MAC address of the thermostat. Once connected to the thermostat, they could simply browse to the key.js file to discover the MAC CRC value in plain text. Alternatively, they could deduce the CRC value of the MAC address (perhaps using a tool such as CRC RevEng [34]). Once they had the MAC and CRC values, they would be able to register the thermostat themselves and then have subsequent control over the settings of the thermostat.

This scenario isn't as far-fetched as it might initially sound. One could easily envision a scenario where a HVAC contractor installed one of these Wi-Fi thermostats but left the Wi-Fi configuration up to the end user, as it is probable that in new construction, the thermostat would be installed before there was a wireless network at the site. Even if a contractor is replacing an existing HVAC system and installs a Wi-Fi thermostat, they likely do not know the connection information for the customer's network. While the flashing Wi-Fi Setup message might trouble some users enough to configure the thermostat, this could easily be a case of another piece of unconfigured technology for many (dubbed the blinking 12 problem by Neal Stephenson [35], referring to the ubiquitous unprogrammed clock on devices such as VCRs).

If an attacker were to take over the thermostat, this would be incredibly difficult for a normal user to detect and remedy. No where on the thermostat itself is the name of the network being used displayed. Additionally, none of the standard menus provide the user with the ability to view or modify the network settings. Once configured, the only way to clear the programming is to access a hidden installer menu by holding the second option button from the left and the temperature up button simultaneously for 3 seconds. From there, the thermostat displays a series of integer key/value pairs that the user must reference in the manual. For example, the option to clear the Wi-Fi configuration is item number 39, and the value must be set to 0 [36].

3) Post Setup: Once registration to the Total Connect service was complete, the Total Connect website showed a thermostat-like user interface, along with the current weather forecast for the unit's zip code. Watching network traces between the wireless access point the thermostat was connected to and the router providing access to the Internet, no traffic was observed being pushed to the thermostat from the Total Connect server. Additionally, watching the thermostat revealed that the temperature did not change based on input to the Total Connect website in real time.

After several seconds, the thermostat showed the updated temperature. Further analysis of the network trace showed that every 15 seconds, the thermostat creates an SSL connection to one of two Total Comfort servers (204.141.*.*). Each of these exchanges consists of 9 packets, which total 600 bytes in size (104 bytes of actual payload). There was no observed DNS traffic, so these addresses are likely either hard-coded, or were cached during setup.

The Honeywell Android application was tested next. The app does not communicate directly with the thermostat, but instead signs into the Total Connect service and submits changes to the servers. The thermostat then picks up the change on its next polling attempt, the same as it would from changes made directly on the website. The app uses SSL to protect traffic between the phone and the servers.

A port scan was performed against the thermostat once it was in its completely configured state. The scan revealed that the previously open ports had all been closed, and that no open ports existed on the device.

To test the resiliency of the settings, the power was removed from the thermostat for about one minute. When re-applied, the unit remembered its configuration and reconnected to the wireless network almost immediately.

As a final test, the existing wireless network was powered off. After 30 seconds, the unit stopped showing the signal strength indicator in the upper right area of the screen. After several minutes, it began blinking "Connection Failure". Once the network was restored, the unit reconnected in about one minute.

VI. Recommendations for Vendors

A. Nest

Evaluation of the Nest did not yield any specific vulnerabilities that warrant attention of the vendor. In fact, the limited attack surface, the proprietary executables being stripped of symbols to hinder reverse engineering, and prevention of man-in-the-middle attacks indicate that Nest considers security to be a top priority.

B. Honeywell

Overall, the Honeywell device is reasonably secure. Once configured and joined to its permanent Wi-Fi network, it exposes no ports or services that could be attacked. Additionally, requests/responses between the thermostat and the Honeywell back-end servers use SSL.

The main concerns are during the initial configuration and registration of the device. During setup, it is possible an attacker could register (and subsequently remotely control) the thermostat with Honeywell by gathering information readily provided by the thermostat's web server before an end-user ever has a chance to register the device. It is also conceivable that an attacker could perform a man-in-the-middle attack between the end user's computer and the thermostat and thus gain access to the user's Wi-Fi network credentials.

To prevent these attacks, we suggest Honeywell implements the following changes:

- For the registration of the thermostat, require a secret value that is either included in the box on a card (as the MAC CRC value is today), or is displayed on the

thermostat screen. The value should not be discoverable by connecting to the thermostat's network or viewing files on its web server.
- Secure the Wi-Fi network by implementing a protocol like WPA2. A key for the network could again either be a unique value printed on a card in the box or displayed on the thermostat's screen. This would further protect the Wi-Fi selection traffic and help prevent man-in-the-middle attacks during initial configuration.

VII. Future Work

While this paper presents a good overview of areas in which a smart thermostat could be attacked, there are some areas where deeper investigation might yield interesting results.

For the Nest, further exploration into the supported OCD interfaces for the TI AM3703CUS microprocessor could be investigated, although there did not appear to be any easily available headers. More testing using the registration code setup method could be performed to determine if this is susceptible to brute force attacks or remote registrations. Finally, attempts to replace the on-board system files with attacker-modified versions could be attempted, avoiding the built-in auto-update feature and installing rogue binaries to allow remote access for further analysis.

The Honeywell would benefit from several additional tests as well. First, it would be helpful to review other models of Honeywell web-enabled thermostats to verify that all of their models do indeed use the same underlying system. It would also be interesting for someone with more electrical engineering experience to attempt to map exactly how the exposed debug pads on the back of the device can be used. Additionally, one could also attempt to extract the memory contents from the three Atmel chips on the board, in an attempt to learn more about the nature of the operating system, and to see if settings such as the Honeywell server addresses or the Wi-Fi password could be viewed or changed. Next, it would be interesting to observe a device receiving a firmware update from the Honeywell server, to determine if that process could be spoofed. Finally, a more thorough man-in-the-middle attack could be performed against the device in the setup phase to see if it would be possible to extract network name and credentials being exchanged between the user and the thermostat.

VIII. Conclusion

When considering "smart" home automation devices, particularly ones like thermostats that can have large impacts on utility bills, comfort, and even safety, it is crucial that the user carefully considers how secure the device is, and what the risk of a compromise could mean.

Overall, we were pleasantly surprised by the security found in the Honeywell and Nest devices. Neither exhibited open ports or services once configured, and at no time were credentials for the devices, their associated services, nor wireless network passwords seen being sent in plain-text across the network. Further, both devices use authenticated, encrypted channels and poll their respective web services for changes, both preventing users from having to open ports on their router for in-bound traffic and preventing man-in-the-middle attacks between the device and its service.

Still, the Honeywell thermostat does have a few small security shortcomings. Notably, it is vulnerable before it is fully setup, where an attacker could register the device using remotely available information and gain full control over the device, locking out or overriding the legitimate owner. Additionally, the lack of Wi-Fi and web server security during setup could allow an attacker to perform a man-in-the-middle attack and extract the consumer's Wi-Fi credentials. Due to the timing and proximity requirements for the attacker, the Honeywell issues are not critical enough that we would suggest avoiding the product, but they are concerns that end users should keep in mind.

IX. Vendor Response

We followed responsible disclosure best practices and submitted our findings to both Honeywell and Nest for review. Honeywell has updated their firmware and states that it has addressed the provisioning issue and man-in-the-middle attack. We have not performed testing on the updated firmware. Nest did not provide a comment.

References

[1] "New research: Installed home automation systems are forecast to triple." *SDM: Security Distributing & Marketing*, vol. 40, no. 1, p. 86, 2010. [Online]. Available: http://search.ebscohost.com.proxy2.library.illinois.edu/login.aspx?direct=true&db=bth&AN=50743918&site=ehost-live

[2] D. Mass, "90 million homes worldwide will employ home automation systems by 2017." *Microwave Journal*, vol. 55, no. 7, p. 49, 2012. [Online]. Available: http://search.ebscohost.com.proxy2.library.illinois.edu/login.aspx?direct=true&db=aph&AN=77905863&site=ehost-live

[3] (2012) HOME AUTOMATION MARKET REPORT - UK 2012-2016 ANALYSIS. AMA Research. [Online]. Available: http://www.amaresearch.co.uk/home_automation_12s.html

[4] A. McHale. (2013) The US Home Automation Market is up for Grabs in 2013. [Online]. Available: http://www.automatedbuildings.com/news/jan13/articles/memoori/130109102505memoori.html

[5] "A Guide to Energy-Efficient Heating and Cooling," Environmental Protection Agency, aug 2009. [Online]. Available: http://www.energystar.gov/ia/partners/publications/pubdocs/HeatingCoolingGuide%20FINAL_9-4-09.pdf

[6] R. Romera, "Home Automation and Cybercrime." [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-home-automation-and-cybercrime.pdf

[7] R. Simon and J. Kelly, "Pentesting over power lines," in *19th DefCon Conference, Las Vegas*, 2011.

[8] B. Fouladi and S. Ghanoun, "Honey, I'm Home!! - Hacking Z-Wave Home Automation Systems," in *Blackhat USA 2013*, 2013. [Online]. Available: http://www.blackhat.com/us-13/briefings.html#Fouladi

[9] J. Wright, "Killerbee: practical zigbee exploitation framework," in *11th ToorCon conference, San Diego*, 2009.

[10] S. Crowley, Bryan, "Home invasion 2.0 - attacking network-connected embedded devices," in *Black Hat USA 2013, Las Vegas*, 2013.

[11] J. Grand, "Jtagulator: Assisted discovery of on-chip debug interfaces," in *21st DefCon Conference, Las Vegas*, 2013.

[12] A. M. Fadell, "From Apple to Nest Labs, Always a Designer," The New York Times. [Online]. Available: http://www.nytimes.com/2013/07/21/jobs/from-apple-to-nest-labs-always-a-designer.html?_r=0

[13] K. Tweed, "Honeywell launches new thermostat for auto demand response," Greentech Media. [Online]. Available: http://www.greentechmedia.com/articles/read/honeywell-launches-new-thermostat-for-auto-demand-response

[14] C. Schubarth, "Honeywell thermostat patent claims rejected in Nest lawsuit." [Online]. Available: http://www.bizjournals.com/sanjose/print-edition/2012/10/05/honeywell-thermostat-patent-claims.html?page=all

[15] Honeywell. Honeywell Achieves An Industry First: Voice-Activated, Cloud-Connected Thermostat For D.I.Y. Homeowners. PR Newswire. [Online]. Available: http://finance.yahoo.com/news/honeywell-achieves-industry-first-voice-120000743.html

[16] "The latest in hvac home automation." *Air Conditioning Heating & Refrigeration News*, vol. 249, no. 17, pp. 10 – 12, 2013. [Online]. Available: http://search.ebscohost.com.proxy2.library.illinois.edu/login.aspx?direct=true&db=bth&AN=90066266&site=ehost-live

[17] Wi-Fi Programmable Thermostats. Honeywell. [Online]. Available: http://www.wifithermostat.com/

[18] The ecobee Smart Thermostat. ecobee. [Online]. Available: http://www.ecobee.com/solutions/home/smart/

[19] The ecobee Thermostat & Accessories. ecobee. [Online]. Available: https://www.ecobee.com/buy/where/

[20] Getting Started with the ecobee API. ecobee. [Online]. Available: https://www.ecobee.com/home/developer/api/documentation/v1/index.shtml

[21] ecobee Lets You Control Your Thermostat From Your iPhoneecobee Lets You Control Your Thermostat From Your iPhone. ecobee. [Online]. Available: http://www.ecobee.com/uncategorized/ecobee-lets-you-control-your-thermostat-from-your-iphone/

[22] (2013) Motison CyberStat CY1201, The 2nd Generation. Motison. [Online]. Available: http://motison.com/index.html

[23] *CyberStat CY1201 User's Manual*, Motison. [Online]. Available: http://motison.com/eManualCY1201.pdf

[24] Import & Export Settings. Venstar. [Online]. Available: http://www.venstar.com/Thermostats/ColorTouch/Features/?t=sd

[25] *Venstar Installation Instructions SkyPort Wi-Fi Key ACC0454*, Venstar. [Online]. Available: http://www.venstar.com/Support/Manuals/ACC0454ManualRev2.pdf

[26] Control. RADIO THERMOSTAT COMPANY OF AMERICA. [Online]. Available: http://www.radiothermostat.com/control.html

[27] RADIO MODULES. RADIO THERMOSTAT COMPANY OF AMERICA. [Online]. Available: http://www.radiothermostat.com/radios.html

[28] (2013) What Is Iris? [Online]. Available: http://www.lowes.com/cd_What+Is+Iris_695688710_

[29] *Operation Guide CT101*, Radio Thermostat Company of America. [Online]. Available: http://www.lowes.com/campaign/iris/pdf/LOWE%20241_SmartThermostat_IM_Oper.pdf

[30] Nest learning thermostat 2nd generation teardown.

[31] Nest. (2013) Nest open source compliance. [Online]. Available: http://nest.com/legal/compliance/

[32] I. Skochinsky, "jffs2-dump - JFFS2 userspace dumper tool," 2009. [Online]. Available: http://git.openinkpot.org/contrib/jffs2dump.git/tree/jffs2-dump.py

[33] D. Song. (2013) dsniff. [Online]. Available: http://www.monkey.org/~dugsong/dsniff/

[34] G. Cook. (2013) CRC RevEng, an arbitrary-precision CRC calculator and algorithm finder. [Online]. Available: http://reveng.sourceforge.net/

[35] N. Stephenson. (1999) In the Beginning was the Command Line.

[36] (2012) FocusPRO Wi-Fi TH6000 Series Programmable Thermostat. Honeywell. [Online]. Available: https://customer.honeywell.com/resources/Techlit/TechLitDocuments/69-0000s/69-2738EFS.pdf