Security Analysis of the Honeywell Wi-Fi 7-Day Programmable Thermostat

Alexis Dalforno, Julio Sandino, Yousef Dost, Ryan McCrory, and Anthony Tom

***Abstract*—As smart technology infiltrates the modern day household, so does it's many vulnerabilities. Though the idea of an attacker gaining access to a thermostat seems minimal on the surface level, the victims who have suffered through their house heating to ninety degrees would disagree. There are many models and manufacturers in the game that have different security precautions making it difficult to know which should be trusted. Honeywell has been making technology for more than a hundred years and have signed a significant number of defense contracts leaving it to be a trusted source of smart products for most. In this paper we discuss the flaws present in the devices infrastructure and how to protect against any possible attack utilizing these weaknesses.**

***Index Terms*—Honeywell thermostat, Internet of Things (IoT), security and privacy analysis, mobile application security.**

I. Introduction

ARRIVING at work only to remember that the thermostat was not turned off is a frustrating realization and a detriment to the wallet. With the ever-evolving smart technology riddling peoples homes, a smart thermostat can seem desirable to those who want to shave off numbers from their electricity bills. Not only do they give someone the ability to set the temperature of their house from the comfort of any location, but they also offer extra amenities such as the option to set a temperature for a certain time every day. With all the benefits, there are negatives in the form of the device being vulnerable to outsiders. The news is already teeming with stories of smart device hacking and malicious use. Thermostats being among those at risk.

Having the threat of obscene temperatures being forced upon a household by a stranger, it is necessary that potential customers find a device with the best security practices. That being said, Honeywell might be on the list of companies to trust when it comes to smart devices. Honeywell has been in the thermostat industry for more than a hundred years and has since then specialized in security and defense [1]. Given their track record of defense contracts, it would be interesting to find that their smart thermostats have security pitfalls. That is why in this paper we examine the safety of their RTH6500WF model Wi-Fi thermostat.

In order to determine the security of the device, we will take a look at all data visible in the network communications of the device as this can reveal vulnerabilities to ready attackers. We will also explore the mobile application and website used to handle an account registered to the device. For a better understanding of the companies priorities, we report first on the privacy policy relating to data of the device.

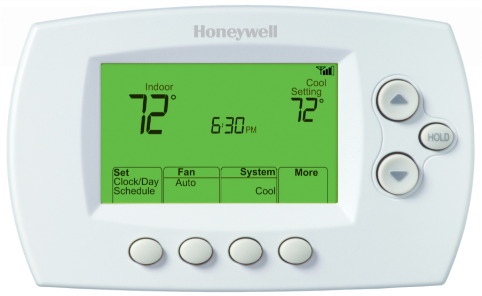


Fig. 1. The physical thermostat and the display screen on the device.

II. Device and Mobile Application Overview

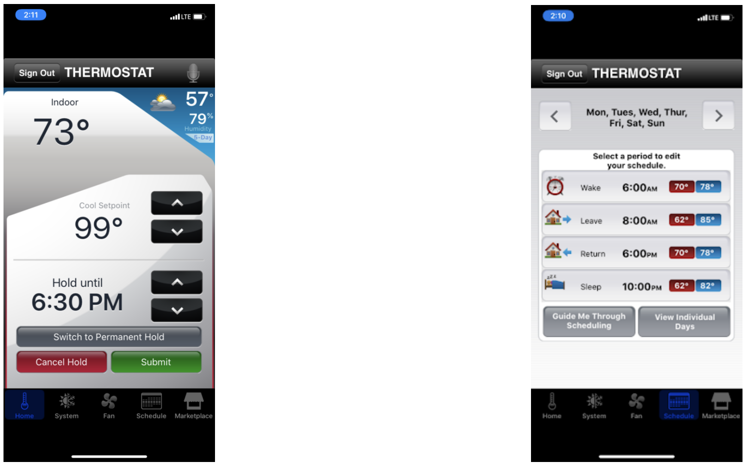
What makes the Honeywell Wi-Fi 7-day programmable thermostat unique from an ordinary one is the luxury of accessing the settings from anywhere in the home or world. Customers are also given the opportunity to program their thermostat all seven days of the week so that it can be exactly sixty-five degrees after a long day at work [2]. It mounts to the wall as any other thermostat with a C-wire for power (Figure 1).

A. Setting up the device for the first time

When the device first receives power, it will immediately display it's own network with the name ”NewThermostat_123456”, the numeric value being the least significant three bytes of the devices MAC address. The user must then connect to the network and sign into their home or office network through the web page popup. Lastly, the device needs to be registered through the *Total Connect Comfort* website and linked to an account. The thermostat can be adjusted after account creation.

B. Functionalities of the mobile and web application

To change the temperature remotely, Honeywell provides a smartphone application called *Total Connect Comfort*. This application allows the user to turn the heat or cooling on and off, set the temperature, and exercise the schedule capabilities available. Thermostat settings can be held until a certain time or indefinitely. The main temperature adjustment page and scheduling screen can be found in Figure 2. Daily weather is shown in the top right corner of the homepage to allow users to plan their thermostat changes around what the natural temperature will be. It seems that the mobile application has not had a major update in some time given that there is a



2:10
Sign Out
THERMOSTAT
Mon, Tues, Wed, Thur, Fri, Sat, Sun
Select a period to edit your schedule.
Guide Me Through Scheduling
View Individual Days
Home
System
Fan
Schedule
Marketplace

Wake	6:00AM	70°	78°
Leave	8:00AM	62°	85°
Return	6:00PM	70°	78°
Sleep	10:00PM	62°	82°

(a) Home page

(b) Scheduler

Fig. 2. Screenshots of the Total Connect Comfort mobile application showcasing the ways in which the user can interact with the thermostat.

marketplace tab still present without any functionality. It is possible that this was an area to purchase other Honeywell products, but it has now since been disabled.

These thermostats can also be accessed from *Total Connect Comfort's* website with the same features. The website, however, allows additional thermostats to be managed with the same account. This allows a user to have multiple thermostats throughout the household, or access to an office device. There is more in depth device and account management available for a wide range of customization power.

C. Additional hardware information

The app, website, and device communicate with *Total Connect Comfort's* servers to give the user constant access to their devices anywhere. With the added middle man however, there is an increase of latency with thermostat instructions. If there were to be any technical issues with the servers or application services, there is still the option to manually adjust the thermostat.

To access advanced settings, the user must hold down the ”Fan” and up button for three seconds. The ISU values for adjusting the settings are explained further in the installation guide [3]. We had to utilize the Wi-Fi connection function, number 39, to reset the thermostat's network settings numerous times. This capability proves useful if the user needs to reset their device following a breach.

In the case of a power outage in the home or office, there is setting persistence. After unplugging the device for an hour or so, the network settings remained in place. However, after leaving the device unplugged overnight, the device reverted back to original settings upon powering up again. If a user experienced difficulty in accessing the advanced settings, there is always the option of disconnecting the device overnight to kick off any attackers for the time being.

III. Privacy Policy

A. The Hunt

The hunt for the privacy policy began in the user guide and manual provided in the box of the device. We found that it was not present in any of the pamphlets, rather it was present at the bottom of the *Total Connect Comfort* website. When the user creates an account to register their device, they are agreeing to the terms in the privacy policy and EULA. Additionally, the policy can be accessed at any time on the login screen in the mobile application discussed in Section II. Given that the user must create an account to begin utilizing their device, we agreed that the privacy policy is in an obvious enough place for someone to find.

B. Privacy Policy and EULA Summary

As a precursor to the following summary, let it be known that Resideo Technologies is a spin-off by Honeywell. We use Resideo going forward as legally the EULA and privacy policy are an agreement between the user and Resideo Technologies.

The policy begins with a thorough explanation of the terminology used within the document. They proclaim that they do not share contact permission without explicit consent and that any promotional emails can be stopped if the user so desires. A majority of the information they collect is used to notify user's of their electricity usage so they can better manage how they use the thermostat. They also mention that the data is provided to marketing third parties as long as the user continues to give consent.

Following general data, they delve into the specifics of their cookie usage. When ever the user uses the mobile or web application to adjust their device, they are consenting to Resideo's cookies. It is allowed to turn off these cookies, but it is warned that performance will decline. The data gathered is also sent through Google and Adobe analytics, which the user is again given the option to opt out of this sharing. There is a lot of talk of marketing in the agreement, much of which is contained in the explanation of the sites advertisement cookies.

C. Fair Information Practices

To see if Resideo's privacy policy follows Fair Information Practices (FIP) we will be looking for full disclosure and required user consent for data collection, minimized collection and identification of data, and minimized and secure data retention.

Resideo provides full disclosure of data collection as evidenced by their disclosure of the types of cookies used, the types of data collected such as system information, how the information is used, and if the data collected is anonymous or not. They also disclose the types of third party tools used for analytics as mentioned above.

Resideo does not require explicit user consent for collection of some type of data including contact service information, and usage information. In the case of these types of data, there is no mention of users having the ability to opt out of the collection of this type of data, but users consent to the collection by using the system and the *Total Connect Comfort* website. This could still fall under the consent requirement described in FIP.

The data collected is fairly minimum. There is excessive data given to marketing services, but overall there is no collection without reason. The only wording throughout the policy that seemed unclear was during the cookie usage information. ”The information these cookies collect may be anonymous” [5]. The keyword ”may” seems it could pose a loop hole to completely keeping cookie data anonymous. However, Resideo did make it apparent that all performance data did preserve anonymity.

Resideo does not mention the length of time they retain user data. According to Resideo, they are ”committed to protecting the security of your personal information and System”. They mention that they ”use a variety of security technologies and procedures to help protect your personal information”, though they do not specifically mention all the technologies and procedures they use for security of retained data. They do mention that they ”store the personal information you provide on computer systems with limited access that are located in facilities to which access is limited”. Resideo also ”cannot guarantee that the System or your personal information cannot be compromised or hacked” [5].

D. Final Thoughts

Despite some lines that we find suspicious, Resideo’s privacy statement is overall fair and follows FIP. Although advertising cookies track users’ web browsing outside of Resideo’s site, Resideo does allow for users to opt out by either not accepting cookies which will result in a decrease in performance or they can download the tools provided in the privacy statement to opt out of Google and Adobe analytics.

Resideo protects the security of personal information by storing it in supposedly secured systems. This obviously leaves the user to determine if they find that claim trustworthy or not. They also tout other security technologies and procedures, but fail to mention them in detail. There is no mention of data being stored in the cloud which could be reassuring to those who know the cloud can be insecure.

IV. Wireshark Packet Analysis

The pitfall of all network connected devices is the transparency of their communications in said network. If any valuable data is not encrypted within the packets easily viewed over free software, an attacker can be handed a direct vulnerability to any site or device. In the case of a smart thermostat, it is vital that any data revealing device connection information is encrypted so an attacker can not gain remote access.

A. Process

As mentioned previously, the device provides it’s own network when in the initial setup phase. This network is unprotected, allows multiple users and displays a web page over Hyper Text Transfer Protocol (HTTP). To examine the traffic over this network, two of us joined, one navigating the setup process and the other attempting to find any vital information in the communications. Given that the connection was not encrypted, it was very simple to view the contents of the packets.

We were able to see that the device was under the IP 192.168.1.1 while users who joined the network were distributed IP addresses starting at 192.168.1.100.

When connecting the device to a network in the setup phase, we gave it a mobile phone hotspot to ensure we were capturing mainly the devices traffic. Again, two of us joined the hotspot. One person visited the *Total Connect Comfort* website and adjusted the temperature settings while the other examined the traffic in Wireshark.

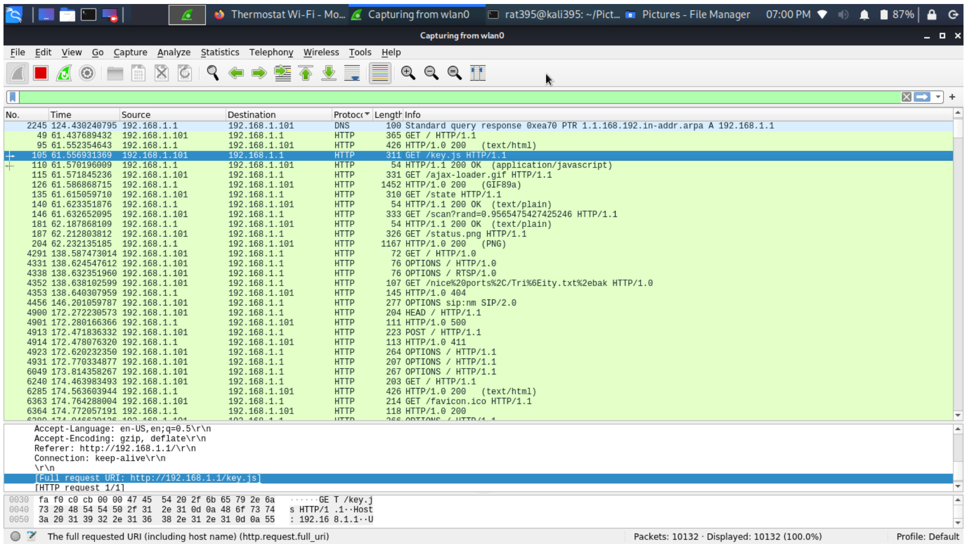
B. Findings

1) During initial setup: The data of interest present during this stage is the HTTP request and response between the client and the device. The information within the packets exchanged is all in plain text leaving possibly sensitive data available to an attacker [4]. The most concerning data we found was present in a server response containing a JavaScript file named ”key”.

This file contained Honeywell’s Total Connect registration link with the MAC address, OS index and CRC value of the unit passed as parameters (Figure 3). The file also includes the RSA public key (e and n values). Since the traffic is not encrypted between the thermostat and the device it is connected to, an attacker can perform a man in the middle attack using ARP spoofing. With the RSA public key it would be possible to decrypt the credentials of the victims Wi-Fi network. To remain unsuspected, the attacker can also re-encrypt the Wi-Fi credentials and forward the request similarly to how the device might.

Though an attacker may be able to retrieve a user’s network credentials in this form, it is worth noting that the data exchange of Wi-Fi credentials was not present in the HTTP communications we sniffed. When entering in the credentials a TCP communication can be spotted. This would imply that Honeywell possibly made each network form an iframe that connects over a secure encrypted connection instead.

Following the Wi-Fi setup for the device, the user needs to enter their email and password as well as the MAC address and CRC value of the unit that is provided in the manual to complete registration. Both of these values can also be found in key.js file as mentioned before. Using these values, an attacker could register the thermostat to themselves with the user unable to do anything to prevent such.


Thermostat Wi-Fi - Mo...
Capturing from wlan0
rat395@kali395: ~/Pict...
Pictures - File Manager
07:00 PM
87%
Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.  Time           Source         Destination    Protocol Length Info
2245 124.430240795  192.168.1.1    192.168.1.101  DNS       100 Standard query response 0xea70 PTR 1.1.168.192.in-addr.arpa A 192.168.1.1
  49 61.437689432   192.168.1.101  192.168.1.1    HTTP      365 GET / HTTP/1.1
  95 61.552354643   192.168.1.1    192.168.1.101  HTTP      426 HTTP/1.0 200   (text/html)
 105 61.556931369   192.168.1.101  192.168.1.1    HTTP      311 GET /key.js HTTP/1.1
 110 61.570196009   192.168.1.1    192.168.1.101  HTTP       54 HTTP/1.1 200 OK  (application/javascript)
 115 61.571845236   192.168.1.101  192.168.1.1    HTTP      331 GET /ajax-loader.gif HTTP/1.1
 126 61.586868715   192.168.1.1    192.168.1.101  HTTP     1452 HTTP/1.0 200   (GIF89a)
 135 61.615059710   192.168.1.101  192.168.1.1    HTTP      310 GET /state HTTP/1.1
 140 61.623351876   192.168.1.1    192.168.1.101  HTTP       54 HTTP/1.1 200 OK  (text/plain)
 146 61.632652095   192.168.1.101  192.168.1.1    HTTP      333 GET /scan?rand=0.9565475427425246 HTTP/1.1
 181 62.187868109   192.168.1.1    192.168.1.101  HTTP       54 HTTP/1.1 200 OK  (text/plain)
 187 62.212803812   192.168.1.101  192.168.1.1    HTTP      326 GET /status.png HTTP/1.1
 204 62.232135185   192.168.1.1    192.168.1.101  HTTP     1167 HTTP/1.0 200   (PNG)
4291 138.587473014  192.168.1.101  192.168.1.1    HTTP       72 GET / HTTP/1.0
4331 138.624547612  192.168.1.101  192.168.1.1    HTTP       76 OPTIONS / HTTP/1.0
4338 138.632351960  192.168.1.101  192.168.1.1    HTTP       76 OPTIONS / RTSP/1.0
4352 138.638102599  192.168.1.101  192.168.1.1    HTTP      107 GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
4353 138.640307959  192.168.1.1    192.168.1.101  HTTP      145 HTTP/1.0 404
4456 146.201059787  192.168.1.101  192.168.1.1    HTTP      277 OPTIONS sip:nm SIP/2.0
4900 172.272230573  192.168.1.101  192.168.1.1    HTTP      204 HEAD / HTTP/1.1
4901 172.280166366  192.168.1.1    192.168.1.101  HTTP      111 HTTP/1.0 500
4913 172.471836332  192.168.1.101  192.168.1.1    HTTP      223 POST / HTTP/1.1
4914 172.478076320  192.168.1.1    192.168.1.101  HTTP      113 HTTP/1.0 411
4923 172.620232350  192.168.1.101  192.168.1.1    HTTP      264 OPTIONS / HTTP/1.1
4931 172.770334877  192.168.1.101  192.168.1.1    HTTP      207 OPTIONS / HTTP/1.1
6049 173.814358267  192.168.1.101  192.168.1.1    HTTP      267 OPTIONS / HTTP/1.1
6240 174.463983493  192.168.1.101  192.168.1.1    HTTP      203 GET / HTTP/1.1
6285 174.563603944  192.168.1.1    192.168.1.101  HTTP      426 HTTP/1.0 200   (text/html)
6363 174.764288004  192.168.1.101  192.168.1.1    HTTP      214 GET /favicon.ico HTTP/1.1
6364 174.772057191  192.168.1.1    192.168.1.101  HTTP      118 HTTP/1.0 200

    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://192.168.1.1/\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://192.168.1.1/key.js]
    [HTTP request 1/1]

0030  fa f0 c0 cb 00 00 47 45  54 20 2f 6b 65 79 2e 6a   ······GE T /key.j
0040  73 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   s HTTP/1 .1··Host
0050  3a 20 31 39 32 2e 31 36  38 2e 31 2e 31 0d 0a 55   : 192.16 8.1.1··U

The full requested URI (including host name) (http.request.full_uri)    Packets: 10132 · Displayed: 10132 (100.0%)    Profile: Default
```

Fig. 3. Wireshark packet capture showing the HTTP communication containing the key.js file.

2) After setup phase: As mentioned in Section II, once the device is setup, all communication is funneled through servers hosted by *Total Connect Comfort*. Since the communications to and from the server are done over SSL, we were unable to find any vulnerable data post setup.

C. Prevention

As mentioned in the findings section, there were files sent over HTTP by the web server of the device. One measure to secure the connection between the device and the computer is the usage of secure HTTP (HTTPS). This would prevent a third-party from being able to see any potentially sensitive data, as in Figure 2.

Another way to prevent an attacker from listening is to only allow one device on it's Wi-Fi connection at one time. Since the device broadcasts and manages it's own Wi-Fi it should be relatively simple to implement. However, this could potentially open the device to a DoS attack. An attacker could connect to the network before the user is able to connect and prevent them from setting up the device. There are a couple of ways of addressing this. The manufacturer can implement a switch on the thermostat to restart the Wi-Fi connection. The device also has a menu for configurations and one of them is to reset the Wi-Fi connection, however this configuration menu was pretty hidden and we only found it through online documentation, not in the box. Making the configurations menu more approachable is something that the manufacturer should work on. This would ensure that the user has physical access to the device and prevent a DoS attack.

Alternatively, the addition of a password for the Wi-Fi connection that the device broadcasts in setup would prove beneficial. Currently, the Wi-Fi network that the thermostat broadcasts is not protected. This password could be in the box similarly to the MAC address and CRC value, or shown on the device screen. This would prevent anyone without access to the physical device to snoop on the network. A common error is to give a device default passwords. We think that the password for the Wi-Fi should be something linked to the device like the MAC address or the serial number. A piece of information that the device already has, and is not particularly like the device model.

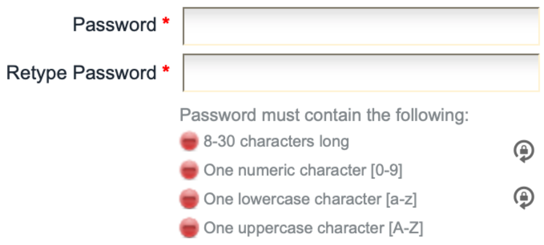
In the case that an attacker got passed the security measures mentioned before and is in the network and got past the SSL implemented with HTTPS, there is still potential for data leakage. To combat this, there could be a checksum for validating the static files that are being served by the device to the client. If one of them is tampered with, there could be a system in place to notify the user. Additionally, the server could restore the static files by reading them from a read-only memory location if they're tampered with. It is important to note that these solutions are strictly addressing issues with the security of the system in setup mode.

V. General Security Analysis

Outside of the visible communications of the thermostat, there can lie vulnerabilities in additional resources provided with the device. Every user is tasked with creating an account on Honeywell's Total Connect Comfort website in order to register the device, creating a larger playing field for malicious attacks.

A. Password Security

1) Requirements for initial password selection : For a user to access their portals and monitor their thermostat online, users must create a Honeywell account. Honeywell requires that users choose a password that is eight to thirty characters long and includes one numeric character, one lowercase letter and one uppercase letter (Figure 4). Although Honeywell has more restrictive requirements, users may make very simple changes to commonly used passwords by capitalizing the first word and adding a number to the end. Honeywell will accept the password ”Password1”. To note, ”password1” is one of the top ten most common passwords being used [6].



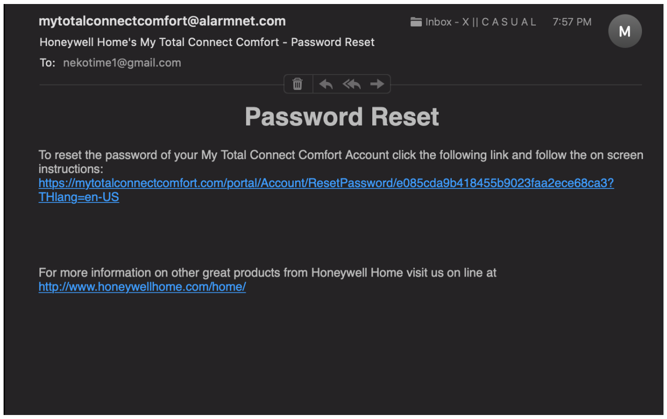
Password *

Retype Password *

Password must contain the following:

- 8-30 characters long
- One numeric character [0-9]
- One lowercase character [a-z]
- One uppercase character [A-Z]

Fig. 4. The list of password requirements in the initial user account creation.



mytotalconnectcomfort@alarmnet.com

Inbox - X || C A S U A L 7:57 PM

Honeywell Home's My Total Connect Comfort - Password Reset

To: nekotime1@gmail.com

Password Reset

To reset the password of your My Total Connect Comfort Account click the following link and follow the on screen instructions:
https://mytotalconnectcomfort.com/portal/Account/ResetPassword/e085cda9b418455b9023faa2ece68ca3?THlang=en-US

For more information on other great products from Honeywell Home visit us on line at
http://www.honeywellhome.com/home/

Fig. 5. Email sent to the user requesting to begin the forgot password process.

We find the maximum character limit of thirty for the user's password to be sufficient as brute forcing thirty characters will take an attacker an exorbitant amount of time. Although thirty characters are sufficient, Honeywell may improve its security by not limiting the maximum number of characters that a password can have. Of course, the thirty character limitation may be due to some storage issue or some other internal issue that we are not aware of, in which case, thirty characters is sufficient.

2) Forgotten password process and precautions: In the case that a user forgets their account password, Honeywell allows for users to regain access to their accounts by clicking the ”Forgot Password?” link just underneath the login credentials. The link will lead the user to a password reset page where the user is prompted to enter the email address of the relevant account. The website requires a specific email format when the user enters in their email. If the email entered in does not follow the email format, Honeywell will respond with an error message telling the user, ”The email address is not in the correct format”. Users will also need to pass an image based CAPTCHA to prove that they are not a bot. The CAPTCHA will help ensure that an attacker cannot find emails associated with user accounts by using some script. If an email that is not registered with any account is entered into the form, Honeywell will try to associate that email with the relevant account but will ultimately not find any. Honeywell will then tell the user that their email address was not found. This is typically not good practice as it informs an attacker the contents of the database indirectly. Best practice is to claim a reset email was sent to the provided email even if it does not exist within the database.

If the email that a user entered does belong to an account, Honeywell will redirect the user to another page where it tells the user that their password was reset successfully. The email received contains a link to confirm that the user asked for a reset of the password. If the password reset request was sent by an attacker, there is no information from Honeywell to inform the user what to do in such a situation (Figure 5).

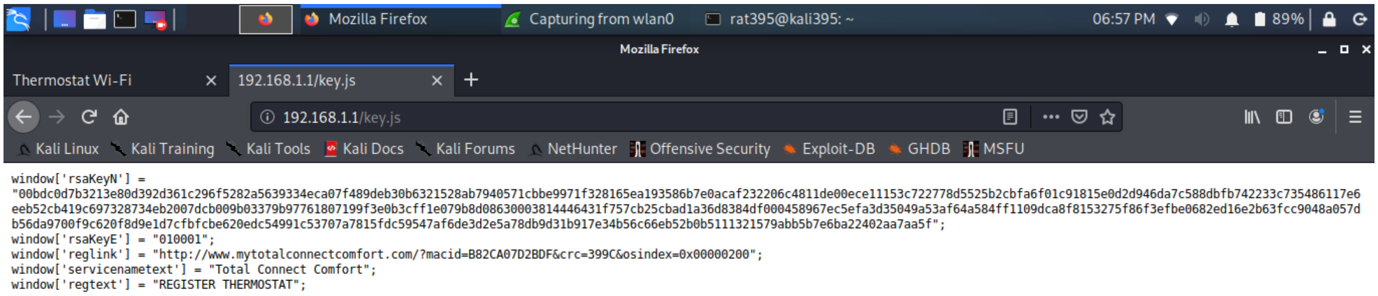
Once the user has clicked on the link provided, the user will be redirected to a page where they can create a new password. The new password has the same requirements as those found when creating an account. After the user has entered a password that fits the criterion, the user will be taken to a page that tells them that the change is successful. If the user were to go back to the previous site through the back button located on the user's browser, the user would be taken to a page that tells the user that the password reset is no longer valid. This page has two buttons, one for reset and the other for done. If the user clicks on the reset button, Honeywell will redirect the user back to the reset password screen where they had to enter their emails. If the user clicks ”done,” then Honeywell will redirect the user back to the login page.

3) Overall thoughts on the password security services: Honeywell follows fairly common practices when dealing with account passwords. The requirements are complex enough to make the cracking process more difficult, though there could be possible improvement with the requirement of a special character. The forgot password process is similar to most sites. Security questions may be overboard, but the dangers of a hacked thermostat could make it worth it. The password email should have some information or help desk contact in the case that the user did not request a password reset and is possibly being infiltrated.

B. Vulnerable Device Setup

As we did reconnaissance on the thermostat, we recognized that the device is very insecure in the setup stage, and relatively secure in post setup. For setup, the thermostat broadcasts a Wi-Fi connection that a user must connect to in order to setup the thermostat. The Wi-Fi connection is not password protected, this means that it is effortless for an attacker to enter the network with a victim. An attacker could connect to the network, and visit 192.168.1.1 in order to receive the files for the local website to setup. In the file contents there are static variables for the MAC address of the device, and the CRC code (Figure 6).

An attacker could register the thermostat with their account, and the user of the thermostat would not necessarily know that it has been activated by someone else. There is no message on the thermostat that alerts the user that someone else has registered the device. Without this knowledge, a victim could just put the thermostat on their Wi-Fi network, and use the thermostat normally, but would not know that someone else also has control of it, and access to its state. This vulnerability comes from exposure of sensitive data, but there are other



```
window['rsaKeyN'] =
"00bdc0d7b3213e80d392d361c296f5282a5639334eca07f489deb30b6321528ab7940571cbbe9971f328165ea193586b7e0acaf232206c4811de00ece11153c722778d5525b2cbfa6f01c91815e0d2d946da7c588dbfb742233c735486117e6
eeb52cb419c697328734eb2007dcb009b03379b97761807199f3e0b3cff1e079b8d08630003814446431f757cb25cbad1a36d8384df000458967ec5efa3d35049a53af64a584ff1109dca8f8153275f86f3efbe0682ed16e2b63fcc9048a057d
b56da9700f9c620f8d9e1d7cfbfcbe620edc54991c53707a7815fdc59547af6de3d2e5a78db9d31b917e34b56c66eb52b0b5111321579abb5b7e6ba22402aa7aa5f";
window['rsaKeyE'] = "010001";
window['reglink'] = "http://www.mytotalconnectcomfort.com/?macid=B82CA07D2BDF&crc=399C&osindex=0x00000200";
window['servicenametext'] = "Total Connect Comfort";
window['regtext'] = "REGISTER THERMOSTAT";
```

Fig. 6. The JavaScript file containing the vital values need for device registration, displayed in plain text.

vulnerabilities from allowing multiple users on the Wi-Fi network concurrently.

An attacker could employ ARP spoofing in order to get in between the connection of the victim and the thermostat, and perform a man in the middle attack. It could capture the packet that contains the password for the Wi-Fi network that the thermostat is supposed to connect to. By ARP spoofing the attacker could redirect the user to a fake website running on the attackers machine. Asking the victim in the fake setup page to enter their personal information. Someone who has never setup the device before would not know that the page is fake. The manual does not include a visual representation of what to expect for the devices web page.

With this unknown, an attacker could ask for any type of information with the user being fooled to believe it is necessary in accessing the thermostat. Also, because the thermostat's WiFi network is always available before the thermostat is setup, an attacker could leave a device, like a raspberry pi, nearby constantly checking if new devices enter the network and then perform an automated attack once a victim enters. That being said, the thermostat requires a restart after ten minutes of not being setup, and won't serve the setup web page after the ten minutes. However, when the Wi-Fi network restarts there is still no password and the attacker can just join again.

After the device has been setup the vulnerabilities disappear. We were not able to capture any packets from the device after setup. We believe that it has the server IP hard-coded so it does not need to do a DNS request from the router.

C. Port Scanning the Device

While the device is in the setup phase, we were able to port scan the given IP to find port 80 to be open in order to display the web page for the user to visit (Figure 7). There was an additional service found but it was not deducible by nmap.

As for the suspected OS of the system, there were a few guesses of various types of embedded systems. The most suspected was Palmicro VoIP module at 86%. It also suspected the device was a VoIP phone altogether (Figure 8). Given the incorrect results, we speculate that the OS running on the thermostat is custom built for the device and not available to the general public.

When scanning the device after setup, all ports had closed and the device no longer displayed a Wi-Fi network. This situation proved strange for the device was still able to communicate to *Total Connect Comfort* servers over the Internet. To communicate through the Internet, the device would have needed to have open ports. Our speculation for how there are no ports open even when the device needs to communicate with the *Total Connect Comfort* servers is that the device opens ephemeral ports, a short-lived transport protocol port, to receive the data. The ports would open and close too quickly for us to be able to observe them in action.

D. Website and Mobile Application

Once the device is registered, the user predominantly interacts with the application and website designed by Honeywell for remote setting changes. If the users login information for either is leaked, the integrity of the device is compromised. Thus it is necessary to practice good mobile and web security.

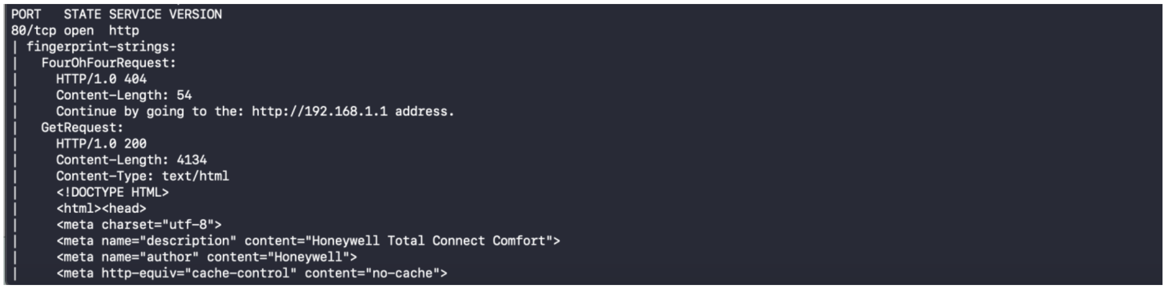
Since testing the security of the Total Connect Comfort website in depth is not a legal option, the only flaws observable are surface level. Looking at the mobile application, it is clear that the functionality is simply for device management, leaving the website the source for account adjustments. It was found, however, that the website did not give an option to remove any accounts from a device. Multiple accounts can register to the device, but they can not be restricted access if they are no longer in the home or office of the thermostat. This allows for thermostat tempering with the current user unable to kick off an attacker.

As for the mobile application, no flaws were apparent. A quick reverse engineering of the Android APK of the application showed perfectly obfuscated code using ProGuard. All important tokens were properly hidden mitigating any decryption capabilities. Debugging and application backup was also restricted protecting all users application data.

We were able to observe the databases and analytic software used by the company, though it has no impact on the security of the application. The services of note were Firebase, Localytics, and MySQL.

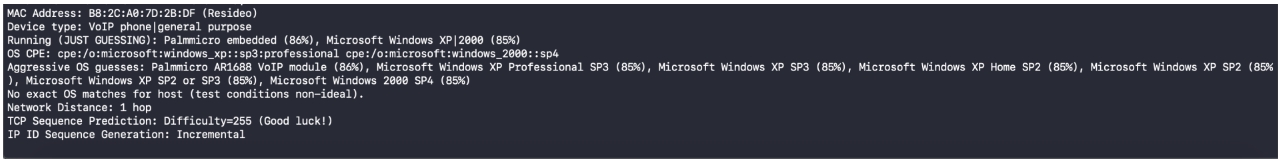
VI. Conclusion

When choosing a new smart thermostat it is important to ensure that an attacker will not be able to ramp up the electricity bill with uncomfortable temperatures. Honeywell has done a fair job of protecting their users for general usage,



```
PORT   STATE SERVICE VERSION
80/tcp open  http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404
|     Content-Length: 54
|     Continue by going to the: http://192.168.1.1 address.
|   GetRequest:
|     HTTP/1.0 200
|     Content-Length: 4134
|     Content-Type: text/html
|     <!DOCTYPE HTML>
|     <html><head>
|     <meta charset="utf-8">
|     <meta name="description" content="Honeywell Total Connect Comfort">
|     <meta name="author" content="Honeywell">
|     <meta http-equiv="cache-control" content="no-cache">
```

Fig. 7. Results from running nmap during the initial setup of the device. The display of the HTML of the site is cut off in the rest of the scanning.



```
MAC Address: B8:2C:A0:7D:2B:DF (Resideo)
Device type: VoIP phone|general purpose
Running (JUST GUESSING): Palmmicro embedded (86%), Microsoft Windows XP|2000 (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3:professional cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Palmmicro AR1688 VoIP module (86%), Microsoft Windows XP Professional SP3 (85%), Microsoft Windows XP SP3 (85%), Microsoft Windows XP Home SP2 (85%), Microsoft Windows XP SP2 (85%
), Microsoft Windows XP SP2 or SP3 (85%), Microsoft Windows 2000 SP4 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
```

Fig. 8. The OS part of the nmap scan showing nmap's various guesses.

but fell short in the initial setup of the device. Leaving an opening for someone to register the user's device without any indication of a possible breach can not be excused. With very small changes such an attack can be prevented and the device's security would be near perfect.

Though we found this security flaw to be unacceptable, the device was at risk for much worse faults had the company been more careless. Overall the device is safe as long as the user takes care and makes haste during the thermostat's setup.

References

[1] "About Us," Honeywell. [Online]. Available: https://www.honeywell.com/en-us/company/about-us.

[2] "Wi-Fi-7-Day-Programmable-Thermostat-RTH6580WF," Honeywell Home Home. [Online]. Available: https://www.honeywellhome.com/en/products/thermostat/wi-fi-7-day-programmable-thermostat-rth6580wf.

[3] (2012) FocusPRO Wi-Fi TH6000 Series Programmable Thermostat. Honeywell. [Online]. Available: https://customer.honeywell.com/resources/Techlit/TechLitDocuments/69-0000s/69-2738EFS.pdf

[4] "Hyper_Text_Transfer_Protocol," Hyper_Text_Transfer_Protocol - The Wireshark Wiki. [Online]. Available: https://wiki.wireshark.org/Hyper_Text_Transfer_Protocol.

[5] Privacy Statement and End User License Agreement. [Online]. Available: https://mytotalconnectcomfort.com/portal/Home/TermsAndConditions.

[6] M. Burnett, "Today I Am Releasing Ten Million Passwords," Medium, 19-Mar-2018. [Online]. Available: https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495.