Security Risks of Home Automation

By Bradley Frizzell

The “Smart House.” For many, it is the ideal of what a home could be. Whether it is vacuuming, doing the dishes, or turning all the lights off automatically when you aren’t at home, a house that takes care of its own chores has been a dream for decades. From Rosie in *The Jetsons*, to Pat in the aptly named *Smart House*, a more intelligent home has always seemed just out of reach. While home automation technology has come in incremental steps, it had almost always been extremely expensive for any meaningful devices. However, over the last several years prices have dropped, and demand has exploded, leading to a market saturated with devices promising to automate anything and everything that has a power cord (and many things that don’t). Between 2013 and 2014, the overall Home Automation market jumped from $4.41B to $5.34B, and is predicted to grow to anywhere from $12.8B[6] to $21.7B[3] by 2020.

What is driving this growth? According to the *2015 State of the Smart Home Address*, the number one reason for purchasing home automation equipment is Security (with the number one home automation systems presumably still being security systems), with 90% of those polled citing it as a top reason. After security systems, the next most important reasons were potential savings to HVAC bills (70%), excitement over fully programmable and customizable features (48%) and finally potential environmental benefits (47%).[11]

The fact that many choose to buy home automation devices, like advanced security systems, to make their family more secure is admirable. However, this paper seeks to explore how buying certain home automation devices, such as various WiFi enabled hubs and controllers, can actually make one’s home and life less secure.

Internet (In)Security

Before computers, an individual’s personal information was stored on paper. If a criminal wanted to steal someone’s personal information, they had to go to that person’s house, and steal the files and papers that had the desired information. With the advent of the internet, modern society has shifted the storing of important information onto computers. Whether it is Social Security numbers or credit card information, millions of people now store their information either immediately online, or in a device that is connected to the Internet.

Digitizing our information has been undoubtedly the most significant step so far of the Internet, but with this step has come significant risks and dangers. To this end, recent studies show that every 2 seconds, an American has their identity stolen.[2]

For the average user of the Internet, the promise of convenience and the allure of new technology was more important and more talked about than any potential security risks. While the need for encryption in web and other internet traffic has been known for decades, widespread deployment of what is truly a basic security requirement did not occur until 2013 in light of the NSA spying revelations, and still remains incomplete.[10]

Home Automation - New Tech, Same Old Risks

And now we are entering into a new era, in which we are taking the devices of our lives and tethering them into the Internet as fast as manufacturers can ship products. Again, the allure of convenience outshines the question of whether or not these devices are secure. Just as users of the internet should have been informed of the inherent risks *before* they became users, home automation users now should ask just who they are trusting their home network with before they attach some company's "smart" device.

Before continuing, it is important to first clarify that the security *of* a device is different from a security device. A security device might be a home alarm system, that detects if a window is broken or a door opened However, that device's security refers to what safeguards exist to prevent a malicious user from hacking into the device itself. For instance, if that security system has an app for a user's phone, and the app communicates to the system over unencrypted channels, then a malicious user might be able to capture the communication, or even pretend to be the user and shut off the system remotely or do something else entirely. The possibilities are frighteningly endless.

The important takeaway here is that there is an implicit danger in connecting *anything* to the Internet. If a device can be reached by its intended user from anywhere in the world, that means that any other user can potentially access it as well. Take for instance Insecam.org. This website maintains a list of **thousands** of webcams that users have connected to the Internet without adding any sort of password protection.[8] The owners of these cameras typically have no idea that **anyone** can access their camera and view it in real time. Is it their fault for not understanding how this technology works? Is it the fault of the companies who make these cameras for not making it mandatory to set a new password to use the camera? These are questions that are being asked too late for all of those users.

An insecure webcam is certainly unsettling, but someone with an automated home might ask if any hacker would even want to access their WiFi enabled light bulbs, or check the temperature of their refrigerator. Frankly, the answer is yes. There is always someone out there who wants to break into someone else's system, whether it is to commit a crime, prove that a problem exists, or just show off their own talents. Unfortunately, this is not just speculation. Security vulnerabilities in many home automation products have already been discovered, and could be exploited to serious detriment.

In 2014, security researchers at IOActive, Inc. uncovered multiple vulnerabilities in Belkin WeMo Home Automation devices, one of the most popular products in the home automation field.[7] WeMo offers various different products, including power outlets and light switches that users can remotely turn on and off with a smartphone app. The vulnerabilities discovered were initially projected to affect as many as 500,000 users,[9] and give attackers the ability to:

- Remotely control WeMo Home Automation attached devices over the Internet [7]

- Perform malicious firmware updates [7]
- Remotely monitor the devices (in some cases) [7]
- Access an internal home network [7]

The impact of these vulnerabilities was potentially massive. Belkin was quick to assure users that they had patched the flaws,[4] but the fact is that the flaws were at one point there. If they had been discovered sooner, these vulnerabilities allowed any WeMo device to be controlled from an attacker anywhere in the world. Not only did the issues with security allow an attacker to manipulate whatever was plugged into a WeMo device: attacking the WeMo device also gave an attacker a foothold in the WiFi network the device was running on, potentially allowing for propagation of additional viruses, worms, or other malware.

This was not an isolated incident. Security researchers at Trustwave found vulnerabilities in many other smart home devices, including the very popular Insteon HUB, which allows users to remotely control lights, garage doors, and other devices.[1] The system was left crawlable by search engines, and Insteon did not require usernames and passwords by default. The effect of this being that by simply searching the right pattern on Google and clicking a link, anyone in the world could remotely control these devices, no hacking knowledge required at all.[5]

Consumer Perception

To gain more insight into the consumer perspective of security in the Home Automation market, I conducted a survey on members of the HomeAutomation community on reddit.com/r/homeautomation (basically a forum for HA enthusiasts to share posts and communicate). Users were asked to list the top 3 most important factors they consider when purchasing home automation devices. They were given the choices of: Compatibility with other devices, Price, Security, Whether Open Source, Manufacturer, How easy it is to use/setup, and lastly a write-in for “other”. Then, they were asked to rank on a scale of 1-5 their perception of the state of security in the home automation field, with 1 being “Very bad” and 5 being “Very good.”

The results of this survey are as follows:

Factor	1st	2nd	3rd	Total
Whether Open Source	32	32	51	115
Price	65	160	144	369
Compatibility with other devices	305	101	51	457
Security	32	71	59	162

How easy it is to use/setup	34	64	89	187
Recommendations from peers	N/A **	45	63	108
Manufacturer	3	14	27	44
Other	24	9	13	46

Table 1: Breakdown of results from survey

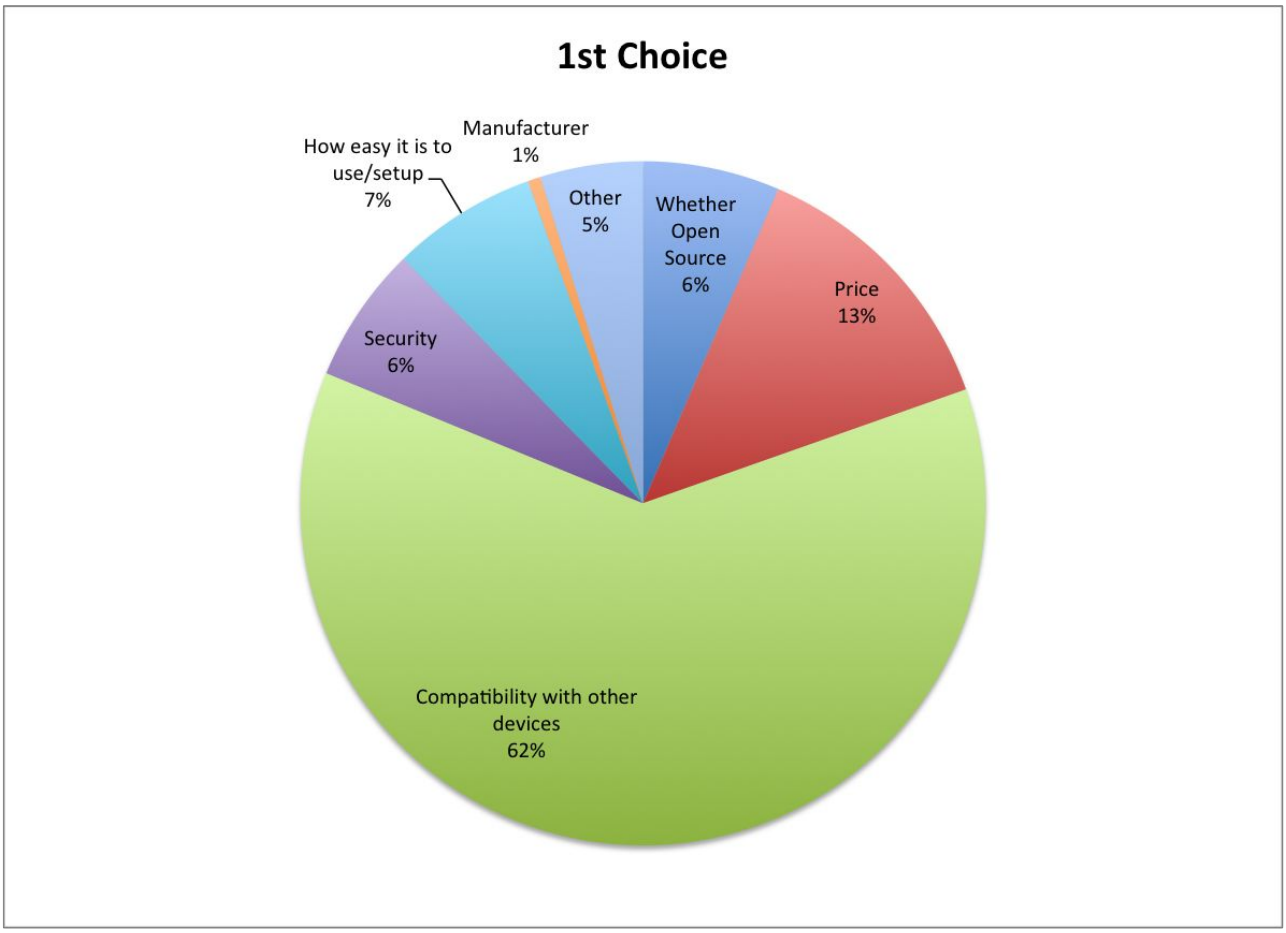


Figure 1: Breakdown of users' choices for 1st most important factor in choosing a home automation product.

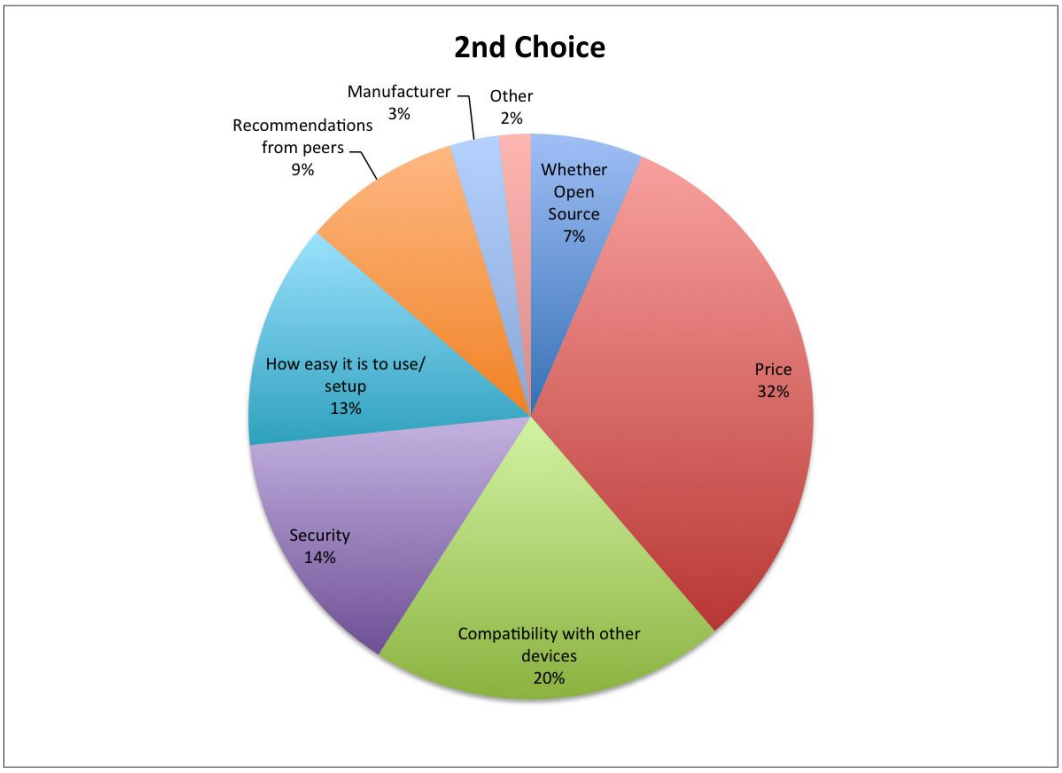


Figure 2: Breakdown of users' choices for 2nd most important factor in choosing a home automation product.

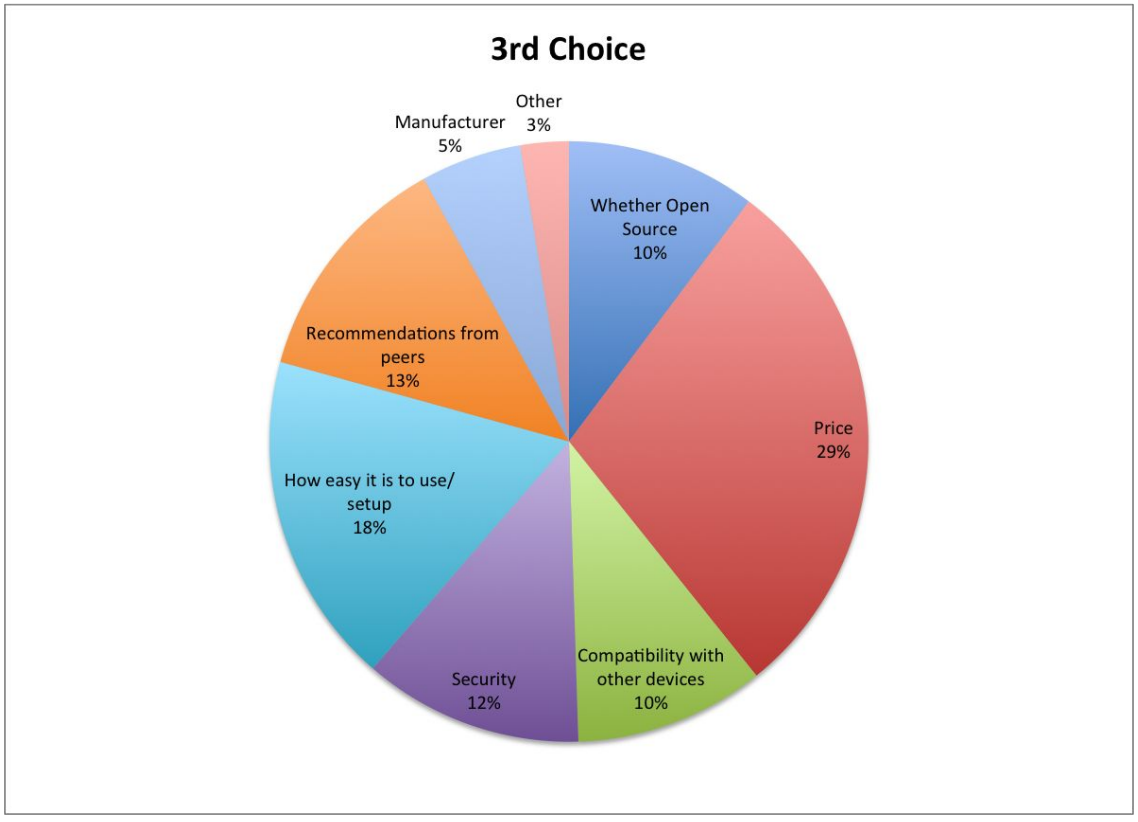
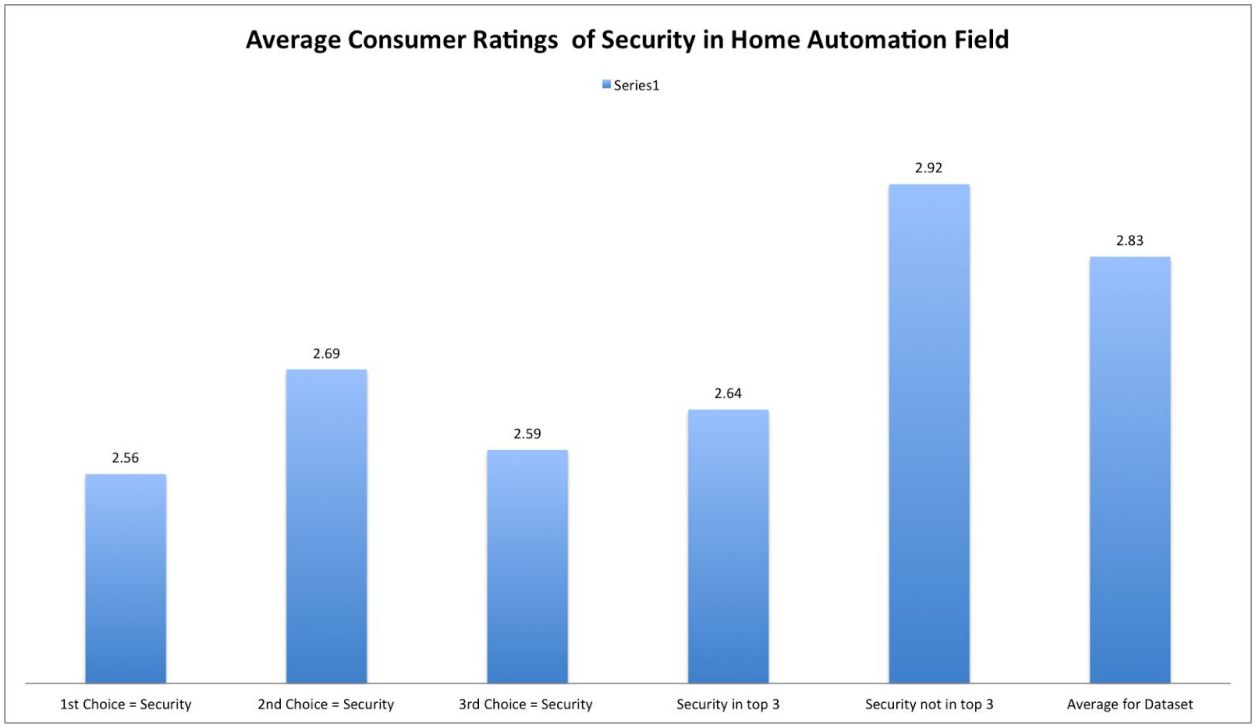


Figure 3: Breakdown of users' choices for 3rd most important factor in choosing a home automation product.

The average ranking of security in the home automation field by all participants in the survey was a 2.83, on a scale from 1 to 5, with 1 being Very Bad and 5 being Very Good. To get a better sense of the true meaning behind this data, the set of all responses was sliced into segments, those being the group of all those who ranked Security as their #1 concern, #2 concern, #3 concern, or not at all. The results, split this way, are seen below.



The average rating for security by those who stated that security was in their top 3 most important factors was a 2.64, compared to a 2.92 for those who did not include it in their top 3. The lowest rating group was those who ranked security as their top concern, with an average rating of 2.56. These results are unsurprising, as those who think that security in the field is bad would be predicted to be most concerned about buying products with good security.

Moving Forward

If security in the Home Automation field is to improve, consumers need to become educated, and vote with their wallets. Only buy products that guarantee 100% end to end encryption. Look for products that are open source. Actually learn about the company, and the ethics and practices that they adhere to. Learn about the product update cycle. Can the product's firmware be upgraded if a vulnerability is found? If the answer is no, you should probably consider buying something else.

But perhaps the most important thing consumers need to do is to simply be cognizant of the fact that attaching your home to the internet opens up a world of new dangers. Even the best companies make mistakes, and there is no guarantee that even the most highly educated consumer can prevent buying a product that gets hacked. Be aware of the tradeoffs you are making between security and convenience for every new device you add on to your network. Every WiFi hub or Bluetooth enabled light bulb is a potential vulnerability to your network, and all of the devices on it.

**Problems with research methodology: Mistake 1: An oversight on my part meant that a choice for Quality/Reliability was not included, which is obviously a big reason. The choices that were chosen were based on my own perception of reasons why users choose devices.
Mistake 2: A clerical error meant that the options on the survey for selecting the first most important factor had “recommendations from peers” accidentally left out. It was present for #2 and #3 most important factors. For the purposes of analyzing the dataset as a whole, we will assume that if a user would have put “recommendations” as their 1st choice, it would surely then have gone as their 2nd or 3rd.

Works Cited

1. Constantin, Lucian. "Home Automation Systems Rife with Holes, Security Experts Say." *Computerworld*. Computerworld, 30 July 2013. Web. 10 Dec. 2015. <http://www.computerworld.com/article/2484542/application-security/home-automation-systems-rife-with-holes--security-experts-say.html>.
2. Ellis, Blake. "Identity Fraud Hits New Victim Every Two Seconds." *CNNMoney*. Cable News Network, 6 Feb. 2014. Web. 10 Dec. 2015. <http://money.cnn.com/2014/02/06/pf/identity-fraud/>.
3. "Global Home Automation Market to Reach US$21 Billion in 2020." *Global Sources*. N.p., 13 Mar. 2015. Web. 10 Dec. 2015. <http://www.globalsources.com/gsol/I/Access-control/a/9000000133399.htm>.
4. Goodin, Dan. "Password Leak in WeMo Devices Makes Home Appliances Susceptible to Hijacks (updated)." *Ars Technica*. N.p., 18 Feb. 2014. Web. 10 Dec. 2015. <http://arstechnica.com/security/2014/02/password-leak-in-wemo-devices-makes-home-appliances-susceptible-to-hijacks/>.
5. Hill, Kashmir. "When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet." *Forbes*. Forbes Magazine, 26 July 2013. Web. 10 Dec. 2015. <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/>.
6. "Home Automation and Control Market worth $12.81 Billion by 2020." *Markets and Markets*. N.p., n.d. Web. 10 Dec. 2015. <http://www.marketsandmarkets.com/PressReleases/home-automation-control-systems.asp>.

7. "IOActive Lights Up Vulnerabilities for Over Half a Million Belkin WeMo Users." *IOActive*. IOActive, 18 Feb. 2014. Web. 10 Dec. 2015. <www.ioactive.com%2Fnews-events%2FIOActive_advisory_belkinwemo_2014.html>.
8. "Network Live IP Video Cameras Directory Insecam.com." *Insecam*. N.p., n.d. Web. 10 Dec. 2015. <http://www.insecam.org/>.
9. Smith. "500,000 Belkin WeMo Users Could Be Hacked; CERT Issues Advisory." *Network World*. N.p., 18 Feb. 2014. Web. 10 Dec. 2015. <http://www.networkworld.com/article/2226371/microsoft-subnet/500-000-belkin-wemo-users-could-be-hacked--cert-issues-advisory.html>.
10. Timberg, Craig. "Net of Insecurity." *Washington Post*. The Washington Post, 30 May 2015. Web. 10 Dec. 2015. <http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/>.
11. "2015 State Of The Smart Home Report." *Icontrol Networks*. N.p., 24 June 2015. Web. 10 Dec. 2015. <http://www.icontrol.com/blog/2015-state-of-the-smart-home-report/>.