A. Michele Parrish

Dr. Charles J. Lesko, Jr

ICTN 6875

17 July 2015

Are smart appliances safe?

ABSTRACT

More and more homes are getting smart appliances. They have refrigerators, toilets, garage doors, thermostats and other appliances that are connected to the Internet and can be controlled from anywhere. The problem is can they also be controlled by anyone or just the homeowners? With the proliferation of smart appliances are homeowners exposing their homes and therefore their private lives to outsiders without knowing it? In this paper I explain what are smart appliances and how and why the market is growing, why they are desired, how smart appliances can be compromised and how consumers and vendors can make smart appliances more secure.

INTRODUCTION

In today's world of instant, high-speed access we want to be able to gather information and control our environment at the touch of a button. This has expanded into controlling our homes. The development of smartphones has allowed us to use the phones to control our homes through smart technology (Adan, Ayu, Mantoro 429). A smart home is made up of multiple devices that include sensors, actuators, displays and computational elements that work with users to exchange

information to provide an automated, customized, secured and comfortable environment (Adan, Ayu, Mantoro 429). Smart appliances are appliances that are connected to a network, either wirelessly or wired, and can work together (Adan, Ayu, Mantoro 429). Smart appliances and homes are part of the Internet of Things (IoT) which is the term used to describe how people connect with products, and how products connect with each other (Bilton 5).

Interest in smart homes, also referred to as home automation, is growing. In the 2015 State of the Smart Home Report conducted by iControl 50% of those surveyed for the report said they plan to buy at least one smart appliance within the next year (iControl 13). The report showed that today there are "1.9 billion smart appliances/devices, and that will grow to 9 billion by 2018, roughly equal to the number of smartphones, smart TVs, tablets, wearable computers, and PCs combined" ("2014 State of the Smart Home"). In the past smart home technology was expensive and hard to install. Today a person can walk into the local hardware store and purchase a control hub, smart bulbs and motion detector for less than $200 (Mone 15). The increase in the availability of products, the ease of installation and configuration, and a lower cost has made the technology available and attractive to the average person.

GROWTH

Vendors are interested in smart appliances because the market is expected to grow from $40 million in 2012 to $26 billion in 2019 (Hargreaves, Hauxwell-Baldwin, Wilson 463). There is a lot of money to be made. The leading vendors in the market – Samsung, LG Electronics, Electrolux and Whirlpool – are increasing the money and effort for research and development for smart technology ("The Global Smart Appliances Market to Grow at a GAGR of 11.9 Percent

Over the Period 2012-2016"). Other vendors that have an interest in information technology but not appliances are also investing in the research and development of smart appliances. MIT, Siemens, Cisco, IBM, Xerox, and Microsoft have home labs set up (Hathaipontaluk, Li, Luo al 247). Google bought Nest, a smart thermostat, in early 2014 for $3.2 billion dollars and they announced at I/O 2015 Project Brillo and Google Weave (Parker). Brillo will be used to control smart appliances and Weave is the program language used to talk to Brillo enabled devices (Parker). Apple has also entered the smart home market with HomeKit, which will provide one platform to control all devices in your smart home (Mone 15).

If it's an appliance in your home, it can become a smart appliance. Your door lock, microwave, stove, dvr, hvac system, security camera or lightbulb can be smart. A Pew Research report about the IoT showed that in the future we may have toothbrushes that can email our dentist, toilet paper dispenser that will know we are out of toilet paper and order a new roll from a vendor and an alarm clock that could start the coffee maker minutes before it goes off (Bilton 5). As research and development continues and the interest increases it is sure that more and more devices will obtain the smart technology needed.

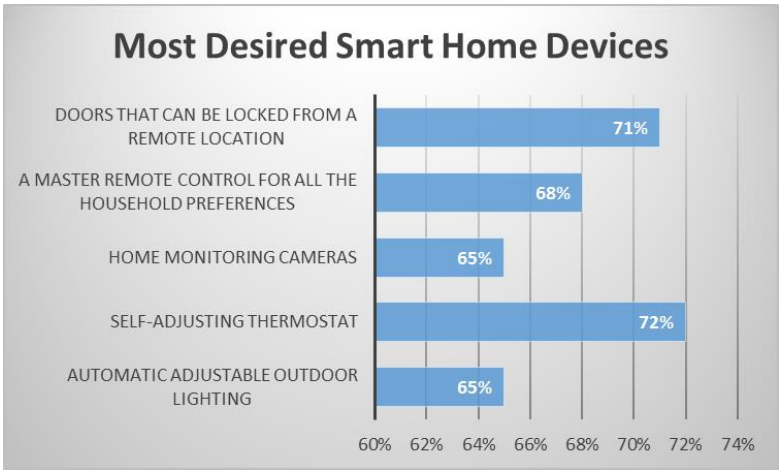

Chart 1: Most Desired Smart Home Devices (iControl 5)

REASONS FOR GROWTH

There are many reasons that consumers want to have smart appliances. In a paper by Hargreaves, Hauxwell-Baldwin and Wilson, they presented three views of why interest in smart homes and research and development are growing: functional, instrumental and socio-technical. The functional view says that smart homes/appliances lead to a better life by providing support for the consumers' lifestyle, management of energy and security. The instrumental view argues that consumers want smart technology in order to make the best use of energy. Lastly the socio-technical view contends that smart homes are the "in" thing and the next evolution of technology and society. (465-467)

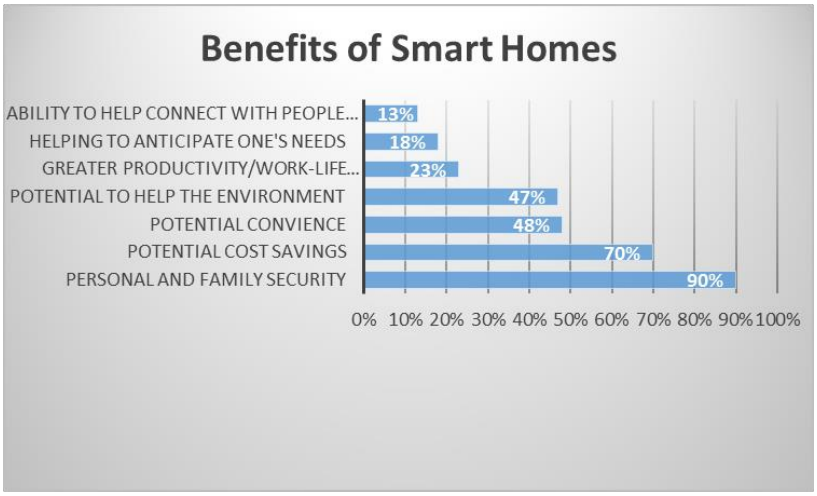

Chart 2: Benefits of Smart Homes (iControl 6)

CONCERNS

Along with the benefits of smart technology there are also concerns. When we connect our smart appliances and home to the Internet so we can control our devices we are also opening ourselves up to the potential to be hacked and for devices to be used in a manner that was not

intended. Hackers have hacked into baby monitors that were connected to the Internet and screamed obscenities at babies (Boreli et al 79). Proofpoint, a security firm, discovered spam coming into their network and when they traced the traffic back it didn't come from a computer but it originated from various devices including a smart refrigerator (Mone 16). Researchers have been able to hijack a Bluetooth enabled toilet and open and close the lid and squirt a stream of water at users ("Smart Appliances"). In 2013 hackers were able to hack into Philips Hue light-bulbs by taking advantage of vulnerabilities in the HTTP protocol (Boreli et al 82). A researcher was able to take advantage of badly written code with allowed buffer overflow and gain access to an embedded home router and control access to peripheral devices (Pishva, Takeda 235). Consumers should be concerned with how secure are these smart appliances, the privacy of their data and potential for misuse of the appliances. Vendors of smart appliances need to be concerned about the traditional areas of security, confidentiality, integrity and availability, but also the operational or physical safety of these devices (Chen, Luo 217). Encryption, authentication and key management should be implemented to provide security of smart appliances (Boreli et al 79).

SECURITY ISSUES/VULNERABILITIES

This section will explore various security issues/vulnerabilities that exist with smart appliances and possible solutions.

Transmission security: Many smart appliances rely on wireless transmission. Because of the nature of wireless signals it is important to make sure that a third-party cannot intercept this transmission (Arora et al 597). One task that can be done to help protect wireless transmissions

is to make sure to encrypt wireless communications. The most secure encryption method is Wi-Fi Protect Access, version 2 (WPA2). This should be deployed at the wireless router and on any device that needs to communicate with the router. A good password should also be chosen as the key for WPA2. Consumers may also want to turn off broadcasting of the Service Set Identifier (SSID) for the router so the name of the router is not able advertised and must be known to make an association with the router.

Denial of Service (DoS) attacks: Smart appliances are basically a computer and can be used in an attack like a computer and attacked likewise (Pishva, Takeda 237). These appliances can be used to commence a DoS or Distributed DoS (DDos) attack. DoS attacks target a system and cause it to be so busy doing other tasks that it cannot do the tasks that it is assigned to do. For example, multiple home appliances could be directed to send pings to a designated target and the target would be so busy responding to the pings that it cannot respond to a valid request, for example a request for a file. This is a particular type of DoS called Ping of Death. This attack could also be reversed and multiple devices could ping your coffee maker and it would be so busy responding to the pings that it couldn't actually start the coffee brewing. A solution would be to not allow your smart appliance to respond to pings. Other protection mechanisms would be to provide appropriate authentication methods into the smart device, validation of user input and provide redundancy of components (Pishva, Takeda 237).

Alteration of Data: A change in the configuration of a smart appliance or change in the data being input into an appliance can cause the appliance to function in way that is not intended to function or not desired (Pishva, Takeda 237). For example a hacker could turn on the heat and

change the temperature setting of your thermostat to 99 degrees in the middle of the summer. They could intercept your command to close the garage door and actually cause the door to remain open which now makes your home vulnerable to theft. Authentication mechanisms with certificates and encryption could help protect about data alteration (Pishva, Takeda 237).

Malware: As defined by Wikipedia malware "is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs". Malware can infect smart appliances and they need to be protected against it. Anti-malware and anti-virus protection software should be installed on appliances to help protect against such software. The protection software must be updated regularly to protect against any new malware. Additionally firewalls could be configured to not allow specific types of traffic to the smart appliance (Pishva, Takeda 237).

Operating System (OS)/Software Vulnerabilities: The OS or software may have weaknesses and they can be taken advantage of by hackers (Pishva, Takeda 238). Programmers may not have written the program to validate the input which would allow buffer overflows. They may have installed backdoors and forget to remove them or they may be discovered by hackers (Pishva, Takeda 238). Vulnerabilities or security issues may have been discovered by the vendor and patches released but the consumer have not downloaded and applied the patches. It is important for this to be done. Programmers should thoroughly test the software before releasing it to consumers (Pishva, Takeda 238).

Privacy: Smart appliances and smart devices will help make lives easier because they will "know" things about you and will be able to adapt to your needs. This collection of data could be vulnerable to others and used in a way in which you do not want it used. Some appliances take advantage of Radio-frequency identification (RFID) technology (Fabian, Feldhaus 1148). Products have RFIDs in them and smart appliances are able to sense the products through the RFIDs. For examples refrigerators can "sense" whether you have the items you need to make a particular recipe by reading the RFIDs of the products in the refrigerator. There is concern that the RFIDs would be used outside of their normal intent. For example RFIDs could be used in a store to track the path you took in the store (Fabian, Feldhaus 1148). There is also some question about how far an RFID signal travels and could it be detected outside of your home to see what type of products you have bought. Global Positioning System (GPS) is also another privacy concern. Most people set their homes as their originating address. This information can be accessed and used to found where someone lives or to know that the person is away from home therefore making the house more vulnerable to theft (Elmaghraby, Losavio 494).

Privacy may also be a concern between users in a home (Hargreaves, Hauxwell-Baldwin, Wilson 473). If everything we do in our home is monitored and logged then others will be able to see what we are doing. No longer will a teenager be able to say they came home at 11 pm when they came home at 1 am. Because they used their smart phone to open the smart lock there will be a log of what time the door was opened.

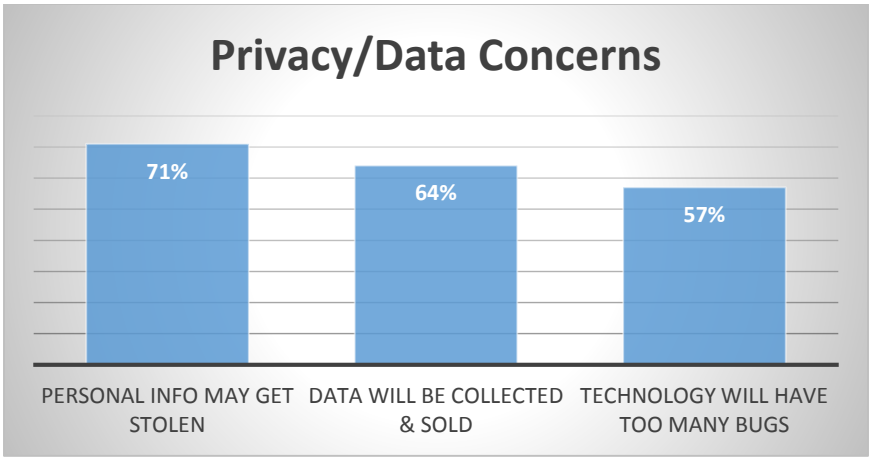

Chart 2: Benefits of Smart Homes (iControl 15)

CONCLUSION

As more smart appliances are manufactured and technology becomes more sophisticated it will open up a broader spectrum of threats ("Smart Appliances"). As soon as criminal hackers figure out a way to make a profit off of hacking smart appliances the increase in attacks will rise ("Smart Appliances"). We must make sure users are educated in security and know the basic methods of how to protect themselves. Default configurations are deployed in most embedded systems (Adan, Ayu, Mantoro 429). Minimally users need to change default usernames and passwords and upgrade software ("Not so Smart?"). Smart appliances are smart but vendors and consumers need to work together to make them secure.

Works Cited

"2014 State of the Smart Home - Icontrol Networks." *Icontrol Networks*. N.p., 14 May 2014. Web. 12 July 2015.

Adnan, M.A.M, M.A. Ayu, M. A, T. Mantoro. "Secured Communication between Mobile Devices and Smart Home Appliances," *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on* (2013): 429 - 434. Web. 11 July 2015.

Arora, Jatin, Aditya Goyal, Bhanu Tyagi, and Upasana Bhardwaj. "Smart-digital Home." *International Journal of Advances in Engineering & Technology* 7.2 (2014): 596-604. Web. 9 July 2015.

Bilton, Nick. "Smart Homes are the Future but what if they Get Hacked?" *Irish Times*: 5. Jun 09 2014. *ProQuest.* Web. 17 July 2015.

Boreli, R., H.H. Gharakheili, S. Notra, M. Siddiqi, V. Sivaraman. "An experimental study of security and privacy risks with emerging household appliances," *Communications and Network Security (CNS), 2014 IEEE Conference on* (2014): 79-84, Web. 11 July 2015.

Chen, Yuxin and Bo Luo. 2012. S2A: secure smart household appliances. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (CODASPY '12). ACM, New York, NY, USA, 217-228. Web. 11 July 2015.

Elmaghraby, Adel S., and Michael M. Losavio. “Cyber Security Challenges in Smart Cities: Safety, Security and Privacy.” *Journal of Advanced Research* 5.4 (2014): 491–497. *PMC*. Web. 11 July 2015.

Fabian, Benjamin and Tobias Feldhaus. “Privacy-preserving data infrastructure for smart home appliances based on the Octopus DHT.” *Computers in Industry,* 65.8(2014):1147-1160. Web. 10 July 2015.

Hargreaves, Tom, Richard Hauxwell-Baldwin and Charlie Wilson. "Smart Homes and Their Users: A Systematic Analysis and Key Challenges." *Personal and Ubiquitous Computing* 19.2 (2014): 463-476. Web. 10 July 2015.

Hathaipontaluk, P., Li Bojun, Suhuai Luo, "Intelligent Oven in Smart Home Environment." *Research Challenges in Computer Science, 2009. ICRCCS '09. International Conference on* (2009):247 - 250. Web. 10 July 2015.

iControl. "2015 State of the StateOfTheSmartHome.com Smart Home Report." (2015): n. pag. Web. 12 July 2015.

"Malware - Wikipedia, the Free Encyclopedia." *Wikipedia*. Wikimedia Foundation, n.d. Web. 14 July 2015.

Mone, Gregory. "Intelligent Living." *Communications Of The ACM* 57.12 (2014): 15-16. *Applied Science & Technology Full Text (H.W. Wilson)*. Web. 12 July 2015.

Parker, Max. "Smart Home: How Apple, Google and Samsung Will Take over Your Home." *Smart Home: How Apple, Google and Samsung Will Take over Your Home*. Trusted Reviews, 6 June 2015. Web. 12 July 2015.

Pishva, D., K. Takeda. "A Product Based Security Model for Smart Home Appliances," *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International* (2006):234 – 242. Web. 10 July 2015.

"The Global Smart Appliances Market to Grow at a CAGR of 11.9 Percent Over the Period 2012-2016." *M2 Presswire.* Jul 05 2013. *ProQuest.* Web. 13 July 2015.

Thomson, Amy. "Not so Smart?; Appliances Risk 'Permanent Entry' by Hackers." *Leader Post.* Jun 21 2014. *ProQuest.* Web. 12 July 2015.

Thomson, Amy. "Smart Appliances Risk Giving Hackers Access to Homes." *The Windsor Star*. Jun 13 2014. *ProQuest.* Web. 11 July 2015.