Smart Home Technology and Vulnerabilities

Kelly Gould

Dr. Philip Lunsford

ICTN 4040

17 April 2017

Smart Home Technology and Vulnerabilities

In today's homes, it is not unusual to see various devices connected to the internet intended to make our daily lives easier. These devices can oversee anything from keeping our homes at the proper temperature, to watering our garden, to giving us our daily news briefing, to locking our doors at night. While these devices are intended to make our lives easier, they can also cause a potential headache if the wrong people gain access. This paper will go over what smart home technology is and how it is used, various devices currently on the market, current vulnerabilities that have been found and used by hackers, and the current legal status pertaining to what is considered personal information and evidence regarding smart devices.

A smart home is defined as "a home equipped with lighting, heating, and electronic devices that can be controlled remotely by phone or computer" (Google). These devices are connected to your home network and are controlled by a central device. "The most popular home controllers are those that are connected to a Windows based PC during programming only, and are then left to perform the home control duties on a standalone basis" (Robles, Kim). Figure 1 shows how far you can take the idea of a "controlled" home. As shown in the figure, things as small as drapery control and leak detection can be controlled using your smart phone. To start with a smart home, there are devices integrated into a controller that turns the different devices on and off when the user manually sends a command or when a predetermined condition is met. For example, when the temperature in a home is above the set temperature, the programmed

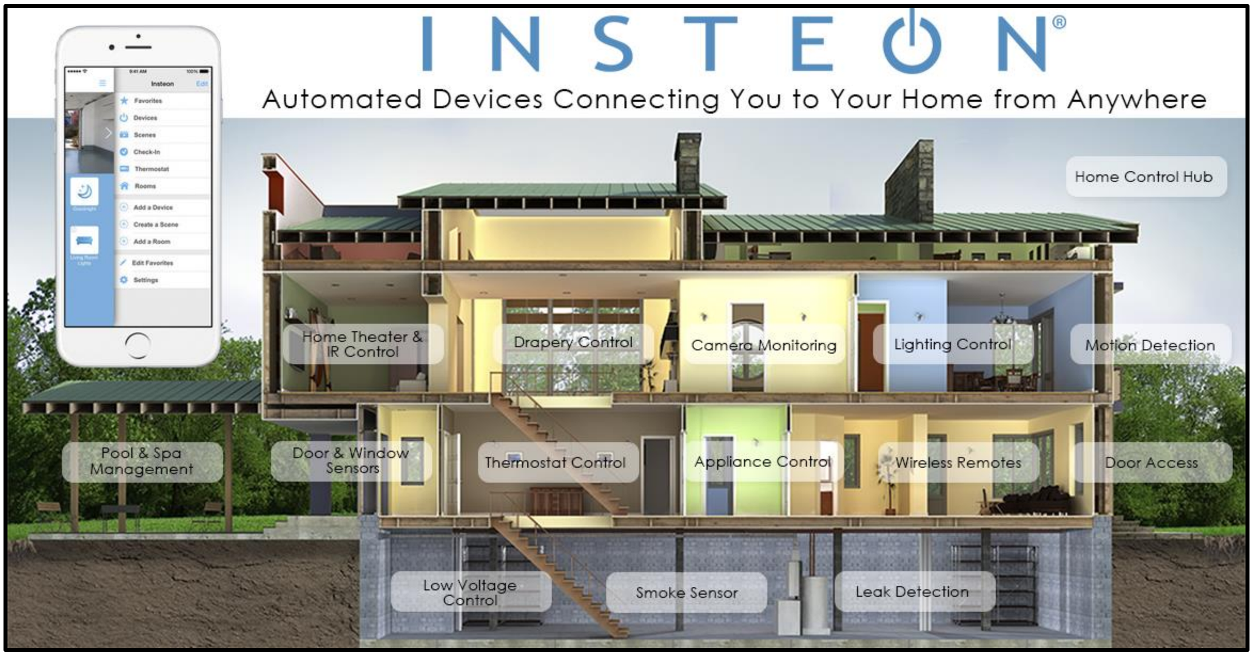

***Figure 1:** A variety of smart home devices that can be controlled using a smart phone through an app provided by Insteon*

thermostat device will automatically turn on to bring the temperature in the home back down to the programmed degree.

Of the many smart devices on the market today the most popular ones found in homes are the Amazon Echo and the newer Google Home. Both devices are voice-activated speakers that allow the user to ask them questions such as what the weather is outside, or the daily news briefings by using a simple voice command and receive a voice response from the device, but can also be used to keep a list or to remember certain things. For instance, if you want your smart assistant to remember that you placed your keys in the top drawer of your bedroom nightstand, you simply ask it to remember the location for you so that when you do inevitably forget where you put your keys and you are in a rush to get to that important meeting, you can simply ask your hub where you put your keys and it will remind you. The Amazon Echo can also be paired with smaller Echo Dots so that you can now have an Echo in every room that can be synced together for things like playing music throughout your home. However, there are many more things on the market today that do more than these voice-activated speakers can do.

As smart home devices become more evolved, it can be helpful to have a central device that controls it all. These devices are called hubs and connect all the different smart devices in a cloud and gives the user access to the different devices through an app that acts like a universal remote. A user can use this hub to automate their gadgets and link them in a way that, for example, when the front door is unlocked the porch lights come on and the thermostat is turned onto a certain degree. Because smart home technology is still in an infancy, the different developers coming out with hubs are still working out the kinks (Prospero). Smart home hubs are going in the direction of being integrated with more and more devices as they are coming on the market. Soon, all devices will be able to be controlled using one central hub instead of users needing to worry if their devices are compatible with a specific hub.

Just like with all the other things on the internet today, smart home technology does pose a potential risk of being hacked and an unauthorized person gaining access to your different devices on your home network. A perfect example of this was when a group of students studying cyber security at the University of Michigan created an app to hack into a leading smart home hub, Samsung SmartThings, and gained access to a potential victim’s front door PIN code. They did this by writing and applying a script in four successful proof-of-concept attacks. In the first test they conducted, “they demonstrated a SmartApp that eavesdropped on someone setting a new PIN code for a door lock, and then sent that PIN in a text message to a potential hacker” (Moore). In other words, every time the home owner changed the PIN code to their door lock, their app would send a text message to the unauthorized person with the new lock code. The second attack “showed that an existing, highly rated SmartApp could be remotely exploited to virtually make a spare door key by programming an additional PIN into the electronic lock" (Moore). The SmartApp they were using was not originally intended to program PIN codes into locks. Using this strategy, a hacker would be able to set their own PIN code for someone's door lock and gain access whenever they wanted. The third attack involved turning off "vacation mode" in a SmartApp that the user is able to program the timing of various home devices such as lights and blinds while away. The last attack they performed "demonstrated that a fire alarm could be made to go off by any SmartApp injecting false messages" (Moore). These attacks are possible because of a common problem; that these SmartApps grant too much access to devices and to the messages those devices generate. The researchers at the University of Michigan refer to this as "over-privilege" (Moore). Further research into the different apps showed that "more than 40 percent of the nearly 500 apps they examined were granted capabilities the developers did not specify in their code" (Moore). Although the researchers told SmartThings about these vulnerabilities they found in their apps back in December 2015 and Samsung reported that they were working on fixes, the researchers went back after they reported the issues and were still able to reprogram a lock's PIN code.

There are a series of other attacks that can take place other than someone being able to set their own PIN code to your front door. Some of these attacks include malware spreading where "an attacker can develop malware and spread it to infect smart meters" (Aloul et al). A replay attack can occur where an attacker sends packets into a network with incorrect data such as wrong meter data that can cause a huge financial impact on the home owner. Some smart devices can also become the victim of a DoS attack. "DoS attacks might attempt to delay, block, or corrupt information transmission in order to make smart grid resources unavailable” (Aloul et al).

More than just the vulnerabilities that smart home devices face, the legal system is also trying to find ground to use the data these devices collect as evidence in crimes. Recently a man in Bentonville, Arkansas was arrested and charged for the death of Victor Collins. The accused, James Andrew Bates, is an owner of an Amazon Echo and the “authorities in Bentonville issued a warrant for Amazon to hand over any audio or records” from his Echo device (Steele). While Amazon did not hand over any of Bates’ information logged on its servers, they did give authorities Bates’ account details and purchases. Authorities state that they were able to pull data off the speaker using that information, although it is unclear what kind of information they were able to access. Due to the “always on” feature of the Amazon Echo, the police are after any audio logs captured from that night. The issue however is not just with the Amazon Echo device in the home, it is with a smart water meter device that Bates also had installed in his home. “That piece of tech shows that 140 gallons of water were used between 1AM and 3AM the night Collins was found dead in Bates' hot tub” (Steele). Authorities believe the water used during this time was used to wash away evidence of the crime. This case raises the question of whether these smart home devices, that are becoming more common today, should be used against us in criminal cases. Many people argue that is should not, saying there is an expectation of privacy in your home and that “law enforcement should not use the technology that advances our quality of life against us” (Steele).

There is another ongoing case about a man, Ross Compton, being charged with the arson of his own house based partly on data collected from his pacemaker. Compton told authorities that when he saw the fire inside his home, “he packed some belongings in a suitcase and bags, broke a window with his cane and threw the items through the window before carrying them to his car" (U.S. News). Police were able to get a search warrant to retrieve electronic data stored on the heart device that included "Compton's heart rate, pacer demand and cardiac rhythms before, during and after the fire" (U.S. News). A cardiologist who examined the pacemaker data said it was "highly improbable" due to his medical conditions that Compton would be able to do all the packing and removal of items from his house in the short amount of time he had indicated to authorities (U.S. News). There have been more situations like this cropping up recently due to how common place smart home devices are becoming and it will be interesting to see how authorities and companies who make smart home devices work out the tension between serving customers, maintaining privacy, and pursing justice.

Smart home technology can range from a multitude of gadgets in charge of lighting control, appliance control, motion detection, door and window sensors, leak detection, smoke and CO sensors, camera monitoring, thermostat control, door access, drapery control, and pool or spa management. These devices are meant to be used to make the daily lives easier of their owners but they could cause a serious headache if not properly managed. While companies are trying to fix all the vulnerabilities that are found in these gadgets, it is more of an arm's race with hackers at the moment and owners of these devices need to do their best to keep their devices as secure as possible. The future of smart devices will only expand on what is out there already and it will be interesting what role the authorities will play in determining the line between what is personal data and what can be used as evidence against someone.

Works Cited

Aloul, Fadi, Rami Al-Dalky, Mamoun Al-Mardini, and Wassim El-Hajj. "Smart Grid Security: Threats, Vulnerabilities and Solutions." International Journal of Smart Grid and Clean Energy 1.1 (2012): 1-6. Print.

"Define: Smart Home." Google Search. Google, n.d. Web. 15 Mar. 2017. <https://www.google.com/search?q=define%3A%2Bsmart%2Bhome&rlz=1C1MSIM_enUS736US736&oq=defin&aqs=chrome.0.69i59l2j69i57j69i59j0l2.1139j1j7&sourceid=chrome&ie=UTF-8>.

"Man pleads not guilty in case based partly on pacemaker data." U.S. News & World Report. U.S. News & World Report, 07 Feb. 2017. Web. 18 Mar. 2017.

Moore, Nicole C. "Hacking into homes: 'Smart home' security flaws found in popular system." Hacking into homes: 'Smart home' security flaws found in popular system | University of Michigan News. University of Michigan, 2 May 2016. Web. 15 Mar. 2017.

Prospero, Mike. "Best Smart Home Hubs of 2017." Tom's Guide. Tom's Guide, 28 Mar. 2017. Web. 1 Apr. 2017. <http://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html>.

Robles, Rosslin J., and Tai-hoon Kim. "Applications, Systems and Methods in Smart Home Technology: A Review." International Journal of Advanced Science and Technology 15 (2010): 37-48. Print.

"Smarthome Solution Center." Smarthome Solution Center. Insteon, n.d. Web. 1 Apr. 2017. <http://www.smarthome.com/sc-solution-center>.