Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 523 – Dr. Yahia Fadlalla

Not So Smart Devices

The Internet of Things is a newer development in the realm of technology; however, it has swept the world and dominates networks everywhere. IoT devices, or smart devices, as they are often called, are everyday tools, called "things", that have been modified to include computing elements to allow for sending, receiving, and processing of Internet data. The Internet connectivity of these things allow for the devices to sense inputs and communicate with one another. They are often able to control certain aspects of an environment, like air conditioning or lights. Several of these devices used together can produce what is often known as a "smart home." The problem, however, is that owning these smart devices might not be too smart after all. It turns out that many IoT things are simply unprotected and vulnerable to cyberattacks.

As a result of all of these "smart" devices taking over our world, we are creating what has been called by some, an "institute of things." These things send messages, receive messages, and act seemingly on their own free will (this is not true, but it often appears this way). With all of these devices communicating over the Internet, there are numerous new avenues of attacks against these communications. Devices can only do what they are programmed to do (this is debatable when the addition of artificial intelligence is considered), so they do not have the capability of making ethical decisions regarding safety and security. Much of the data that is sent across the network is full of dangerous information that could lead to an infiltration in the wrong person's hands. Unfortunately, this is not a problem that is going away any time soon. As of last year, there was somewhere between 12 and 15 billion IoT devices connected to the Internet. That number is expected to reach around 27 billion (approximately double) by 2025 [1]. While the number of these devices is increasing exponentially, the defenses for them unfortunately are not.

One of the driving forces behind the security issues in IoT devices is that they are not being designed with security in mind. If anything, security services are an afterthought for designers. Security needs to be in the everyone's mind who is working with producing devices, in particular the testing team. There are many testing platforms and methodologies available for IoT devices, but unfortunately, many manufacturers just seem to skip over the concept, and as such their software is poorly written and unsecure. Actions as simple as adding encryption to data communications would at least offer a little aid in the effort to protect smart devices, but unfortunately even this does not often happen.

This lack of testing often comes from the fact that many IoT devices are built overseas where there are little to no standards and devices are mass-produced in order to make the most amount of money. These overseas manufactures rarely have security teams to test out their products. The question may be, why wouldn't manufactures invest the money to make their products safe. It all comes back to money. They can produce more products without going through the extra steps of verifying security and the average customer couldn't care less. That is, of course, until they are victims of an attack.

Another driving issue behind the security issues of IoT devices is that they are too diverse. There is no single purpose behind all of these smart devices, except to make people lazier. Convenience is key and customers pay a high price to get a product that will make their life easier. But with all of the products being designed by different entities, yet communicating with each other, inconsistencies in design can lead to major failures and vulnerabilities.

The result of all of these vulnerable devices sitting on vulnerable networks in everyday, unprotected homes is that many cybersecurity experts are increasingly getting concerned about safety issues. The security world is worried about malicious actors who get way too much access to devices they have no business even knowing exist on a network. It is all too simple to run an attack against an unprotected smart device and begin to wreak havoc to one's personal devices, computer network, and ultimately, way of life.

Not only do cyberattacks affect computer systems and their networks, they have the chance of cause physical harm and danger. For example, over 90% of attacks against IoT devices are against routers and connected camera. Ring doorbells have become a standard in many neighborhoods. They serve their purpose of being an Internet connected doorbell, where users can view who is at their door from their phones, well, but unfortunately, while they are often used to protect houses from physical intruders, they actually let intruders into their home networks. When an attack gains network access, they can soon gain physical access by learning schedules, unlocking smart locks, and turning off alarm systems.

Another example would be that of cyberterrorism, were a malicious actor can wreak havoc in ways such as changing chemical amounts in water systems, shutting off electricity, or modifying pacemaker beatings. Losing your computer to a virus is no fun, but losing a loved one to a cyberattack would be heartbreaking. Cybersecurity is more than just a computer nerd's hobby; it needs to be a priority for individuals from all walks of life.

The problem is that, as devices get more complex, so will cyberattacks. Given the current trends in technology, this would mean the smarter the devices the more at risk everyone is. But it doesn't have to be that way. There are recommendations that have been presented to address cybersecurity issues. Several of these ideas will be considered and discussed.

One recommendation is to create a new federal agency that would be tasked with the IoT world. The reasoning behind this idea is that the Internet is too freewheeling and the potential for dangers are just too significant to not have a regulatory administration. Indeed, the technological world is very dangerous, but a regulatory organization may not be the best solution to this problem. Additional government controls could lend itself to some overreach. One such issue is that it is now an established fact that U.S. government, and likely many other countries', actively engage in information gathering.

The Department of Homeland Security was created after the 9/11 attacks on the World Trade Center. There is a lot of controversy regarding DHS and its role in harvesting user data (consider the USA PATRIOT Act and Edward Snowden's whistleblowing), and a new governing authority would add to this debate. Besides that, Dr. Fadlalla points out that despite the formation of DHS and other commissions and organizations, cyberattacks are still occurring and don't appear to be slowing down.

Another recommendation is for lawmakers to get involved in the issue and to collaborate with technologists. Once again, in of itself, this isn't a bad idea. However, governments do have trouble with getting their hands too dirty and when bills and laws start being created, there is an increased likelihood of something underhanded taking place. That's not to say that no good could come from this, but lawmakers like money and there is no guarantee that they wouldn't give more priority to their wallets then to their ethics. Guarded lawmaker influence would be useful, though, even if in just spreading the word about the importance of security in IoT and the dangerous that are sitting in homes all over the world.

Another proposition is to build and finance IoT research centers. This would be a great idea and would likely be a good way of demonstrating the importance of this concept to manufacturers. Standardizations play a major role in most areas of technology and research centers that work on establishing standards and testing for vulnerabilities would be a worthy investment that would make the technological world a safer place (assuming the standards actually get implemented).

Keep in mind that the Internet is a powerful communications tool, but just like any great tool, there are potential side effects. It often seems to be the case that the most effective tools are those that are most dangerous. Does that mean the tools shouldn't be used? No, it means that they need to be used responsibly, and users need to follow the "instruction manual". That is, developers need to follow standardizations that are set in place and users need to take the prescribed precautions to keep their information safe.

Hackers are looking for vulnerabilities constantly. As such, everyone who uses the Internet, which at this point is nearly everyone, needs to be aware of the threats that can occur. We should all take action to protect ourselves against hackers and harden our online systems. Some vulnerabilities are unexpected, but are due to the ingenuity of hackers finding new ways to accomplish their goals. Two interesting and unique attack ideas that are being researched include the use of man-in-the-middle "Skills" for smart speakers and the use of lasers to inject commands into voice-controlled systems [2, 3].

As the number of devices connected to their Internet grows, and the more society is dependent on the technology, the number of attacks will also grow. There is a strong potential these increases will not be equivalent. Rather, as more devices are added and technology becomes more advanced, more capable malicious tools will also get produced. In fact, there is research being done regarding the use of machine learning to perform attacks against IoT devices [4]. Of course, there is also a chance that the number and abilities of devices that defend against attacks will also increase significantly, especially given the breakthroughs in artificial intelligence, but only time will tell ultimately who is most successful in winning the cyber battle.

Cybersecurity is no joke and it needs to be taken seriously. Unfortunately, this is not the case in many of today’s “smart” devices. At the same time, these are the most popular computing devise that are being purchased, as they make life easier. They do make life easier, but also make it a lot more dangerous. As Dr. Yahia Fadlalla puts it, IoT may actually stand for Internet of Threats, rather than Internet of Things. If you lived in a neighborhood full of criminals, would you leave your door wide open, just so you could get dinner delivered to your dining room table? It just simply isn’t smart, and yet that is what smart devices do in the middle of a cyberwar.

References

Unless otherwise states, the information for this report comes from Dr. Yahia Fadlalla's PowerPoint presentations on IoT and Cybersecurity and The Use of Cryptography in IoTs as a Defense Mechanism. Some of the information also comes from my own unpublished paper entitled, "IoT Devices: "Smart" Security Testing."

[1] M. Hasan, "State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," IoT Analytics, May 18, 2022. [Online]. Available; https://iot-analytics.com/number-connected-iot-devices/. [Accessed: August 26, 2022].

[2] R. Mitev, M. Miettinen, and A. Sadeghi, "Alexa Lied to Me: Skill-based Man-in-the Middle Attacks on Virtual Assistants," Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19), pp. 465-478, July 2019. [Online serial]. Available: Association for Computing Machinery, https://doi-org.athens.idm.oclc.org/10.1145/3321705.3329842. [Accessed: Oct. 10, 2022].

[3] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light Commands: Laser-Based Audio Injection Attacks on Voice-Controlled Systems," 29th USENIX Security Symposium, 2020.

[4] Z. Luo, S. Zhao, Z. Lu, Y. E. Sagduyu, and J. Xu, "Adversarial Machine Learning Based Partial-model Attack in IoT," Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (WiseML '20), pp 13-18, July 2020. [Online serial]. Available: Association for Computing Machinery, https://doi-org.athens.idm.oclc.org/10.1145/3395352.3402619. [Accessed: Oct. 10, 2022].