IoT Security Gaps

The Internet of Things is a fairly new and fast-growing area of Information Technology. And as with any burgeoning tech, it is flawed, and more importantly, it is flawed in a very consequential way… security. We will explore some of these security gaps and some real-world examples of breaches as well as what can be done to prevent people and organizations from exploiting them. One hundred and twenty-seven IoT devices are connected to the internet every second. This year alone 31 Billion IoT devices will be activated and 35 Billion next year in 2021. By 2025 there will be more than 75 billion devices connected to the internet (Maayan, 2020). That creates billions of extra possible entry points for security breaches. With the proliferation of IoT devices, their often-inherent security deficiencies, and the human deficiencies in security practices, tremendous amounts of data and privacy are at stake as we enter this brave new world.

According to security researchers at F-Secure, cyberattacks on IoT devices increased 300% in 2019 to more than 2.9 billion events. The largest geographical origination of these attacks coming from China, Russia, The U.S., and Germany (Doffman, 2019). Some examples in the media include a Milwaukee-based family’s smart home setup. Samantha and Lamont Westmoreland reported that their home system was taken over through a compromised IoT device. The attacker played disturbing music at a high volume while talking to them through the kitchen camera and turning their thermostat up to 90 degrees Fahrenheit. They attempted to change their password but that did not help and ultimately had to change their network ID to solve the problem. The attacker had either hacked their Wi-Fi or their Nest system (Anonymous, 2020).

Another, more infamous incident, or series of incidents, occurred in 2016 and was known as the Mirai botnet. The botnet infected mostly older routers and IP cameras, but certainly enough of them, to flood the service provider, Dyn, with a DDoS attack, taking down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and other major websites in the process. The ultimate cause of the vulnerability was determined to be the lack of extra memory built into the devices to allow for firmware updates to keep up with ever evolving cyber-attack techniques (Wallen, 2017).

So then, what happens if IoT security does not get solved? Well, according to the article by Network World of the same name, there will be a backlash. Consumer confidence in the devices will drop and people will simply stop buying the devices. This will have a major economic effect as the growth of the industry is expected to be in the tens of billions soon (Paul, 2018).

We know the IoT will never be completely secure, but if we follow some simple security practices, we can minimize most intrusions into our devices and prevent invasions of privacy and frightening incidents. Once we feel more secure or at least hold the line on the feeling of security we have, be that as it is, our connectivity and the economy related to it can grow and improve our lives. Be safe, stay secure.

As of this point in time, it appears that the need for technology has surpassed the need for security. Mass Production of IoT devices is growing like wildfire, all the while security vulnerabilities voiced by professionals globally are being overlooked. So, the question of why we do not just install a security feature as a standard? Which is a simplistic idea that could easily be fixed if businesses had security as a primary concern.

As security professionals come to understand developing security issues with more and more clarity, they begin to question everything! Great and all, but those questions require answers. And the answer or solution begins back at the designing process. Some of the specific questions being asked are, how can we fit a security protocol in a resource depleted architecture that will detect and help mitigate an intrusion; and, will that provide the necessary authenticating properties to not only allow those with “like” protocols to communicate with it, but others as well?

           Currently with the minimalistic nature of devices, few companies, like IBM, have the capability of producing a microchip small enough to fit inside equipment that has enough processing power to handle the differentiating layers required for the device to be considered IoT. So then, which IoT architectural model would provide the resources and future properties needed for such a design? To begin with, you have different models required for different devices, such as the 3-layer, middle-ware, SOA based, and Five-layer models (Bilal, H. et al, 2019). The other factors to consider are resource constraints such as power consumption and device life cycles (Toomey, 2018).

Let us say we have found the company to make our chipset. We know which architectural model we are going to use for the application, network, and perception layers. Now the hardest and most overlooked portion… security! There are designs currently in trials in the form of lightweight protocols called cryptographic frameworks such as the "fully collusion-resistant framework. An identity-based symmetric-key establishment scheme is fully collusion-resistant if for any set of colluding 2 nodes no bit of a key shared by non-colluding nodes can be guessed with a probability higher than 1/2 in polynomial time". And, establish this within the network for "direct ID-based pairwise key establishment" (Garcia-Morchon. Et al, 2012).

While this framework is still under evaluation as more testing is needed. The information gathered is easily obtained and until this framework goes into effect this information has a vulnerability of being seen and thus the un-ethical have a head start on figuring out how to bypass it. With manufacturers currently prioritizing devices in a monetary sense, we are having to hit the ground running faster than ever. As soon as products hit the markets using technology, and protocols that have already been used or are currently in use they are more vulnerable than ever. Vendors are choosing the least costly hardware to throw into their devices. The time consuming and expensive security checks that should have been completed before shipment, or during the implementation of the operating system are often overlooked. After that, it is up to the individual vendors to ensure security protocols are installed. As individual vendors do not consider this one of their priorities, a consequence is that we are faced with an onslaught of constant differing innovations produced by the lowest bidders. They are then slapped together quickly, and just as quickly sent out into the world to be gobbled up by the next botnet; botnets that when created, could wreak havoc on businesses by issuing DDOS attacks on critical infrastructure. So, close those unused ports, change those usernames and passwords that are easy for kids to remember. And do your due diligence when buying IoT devices.

           With the constant release of new products and the number of breaches only rising, companies are being pressured to increase their security measures. To increase the security of IoT devices, first user awareness must also be increased. “One of the biggest IoT security risks and challenges is the user’s ignorance and lack of awareness of the IoT functionality” (Anonymous, 2019).

Users rely on companies to release devices that will protect them from any chance of cyberattack, but they often bring malicious content upon themselves. One of the simplest ways for a hacker to gain information from another’s device is through email. More “technologically savvy” people tend to be able to pinpoint emails that are certainly spam or a potential threat, but others may see a malicious email as eye-catching or interesting.

In some cases, lack of action by employees leads to cybersecurity incidents. Human error has and will always be an issue but having preventative measures in places such as peer reviews or better training methods can reduce the number of cybersecurity attacks. “Employee carelessness and phishing/social engineering were major contributing factors for malware and targeted attacks” (Anonymous, 2018). Teaching users and business employees the importance of keeping information secure, how to avoid malicious content, and how to properly set up devices to keep information protected, would greatly increase user awareness and slow the number of breaches that occur for both homes and businesses.

           Another issue presented by IoT devices is the lack of a security standard. The European Union’s General Data Protection Regulation, which includes about 27 countries, has around 88 pages (after removing white space) of standards and guidelines for companies to follow that breaks down information on breaches, securing data, and consumer privacy. In the United States, the NIST Cybersecurity Framework is used as a security standard, which is slightly smaller, at around 40 pages. While crucial to make certain that information stays secure, these regulation guides make it difficult for companies to ensure that they hit every required standard; even the companies that attempt to comply with these standards have a difficult time keeping their devices fully secure. One of the main reasons for this issue is because the current security standards that are set are not up to date. “…following all the rules, while it will help, doesn’t mean you’re bulletproof since regulations generally don’t keep up with the evolution of threats” (Armerding, 2019). While compliance is necessary, to close security gaps in IoT devices, every company has to remain aware of current and future cybersecurity threats. From there they must continue updating and patching software rather than simply checking achieved standards off from a list.

           Although IoT devices come with security gaps, the general public tends to be more focused on the features of the devices rather than how safe they are. Typically, when breaches occur, concern is raised, and people begin to question whether companies truly have their best interest at heart. However, once a couple of months pass after the breach, the majority of those that had been affected continue using the device or software. The lives of people all around the world revolve around using IoT devices, and therefore even when trust is broken after using a device, we still rely on the software and devices to get us through each day. To close the security gaps in IoT devices, the focus must move from profit and functionality towards privacy and protection.

References and Citations:

Maayan, G. (2020). The IoT Rundown For 2020: Stats, Risks, and Solutions, *Security Today*. Retrieved from <https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2>,

Doffman, Z. (2019). Cyberattacks on IOT Devices Surge 300% In 2019,’Measured in Billions’, Report Claims. *Forbes*. Retrieved from <https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#9f38eda58926>

Anonymous, (2020). 10 IoT Security Incidents That Make You Feel Less Secure, Cisomag. Retrieved from <https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/>

Wallen, J. (2017). Five Nightmarish Attacks That Show the Risks of IoT Security, ZDNet. Retrieved from <https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/>

Paul, F. (2018). What Happens if IoT Security Doesn’t Get Solved? *Network World*. Retrieved from <https://www.networkworld.com/article/3278023/what-happens-if-iot-security-doesnt-get-solved.html>

Bilal, H., Faraz, I. K., Sufian, H. (2019). Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Hindawi*. Retrieved from <https://www.hindawi.com/journals/jcnc/2019/9629381/>

Toomey, M. (2018). IoT Device Security is being seriously neglected. *Aberdeen*. Retrieved from <https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/>

Garcia-Morchon, O., Gomez, D., Gutierrez, J., Tolhuizen, L. (n.d). (2012) Towards fully collusion-resistant ID-based establishment of pairwise keys. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.2669&rep=rep1&type=pdf>

Anonymous, (2019). Top 10 Biggest IoT Security Issues. *Intellect Soft*. Retrieved from

<https://www.intellectsoft.net/blog/biggest-iot-security-issues/#:~:text=One%20of%20the%20biggest%20IoT,gain%20access%20to%20a%20network.&text=Instead%20of%20targeting%20devices%2C%20a,a%20human%2C%20using%20the%20IoT.>

Anonymous, (2018). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. *Kaspersky Daily*. Retrieved from <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>

Armerding, T. (2019). Awash in Regulations, Companies Struggle with Compliance. *Forbes*. Retrieved from <https://www.forbes.com/sites/taylorarmerding/2019/08/30/awash-in-regulations-companies-struggle-with-compliance/#1ef8315e150e>