The Role Privacy Plays in the Greater Sociotechnical System of the Internet of Things

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jiafu Li

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

STS Research Paper

Introduction

Envision a scenario where a working adult opens the door to their house, and the lights flickers on like magic, followed by the heating or air conditioning, and finally the television, all without lifting a finger. Such an ideal system, where each device knows how and when to operate itself, can be achieved by something called the Internet of Things (IoT) (Su, 2022). IoT allows different machines to interact with one another via sensors. In the scenario mentioned above, when the owner of the house returns home at night, the door sends a signal to all the other machines. Upon receiving the signals, the lights, AC, and TV each performs certain actions. IoT encourages peer-to-peer connections between machines and puts less emphasis on human involvement. The system should be able to function properly without monitors; thus, the issue of security is a paramount concern for IoT. Without human monitoring, it is hard to tell if a data breach has occurred, and the machine's own security might not be enough to prevent data leakage. This research paper will tackle how privacy is important in the Sociotechnical system of the Internet of Things. Technological Determinism and Risk Analysis will be the two main STS frameworks that are used to analyze the issue of privacy. Technological Determinism is used to analyze how technologies affect the way society's function, and risk analysis is used to see to what extend are people comfortable with having their information be on risk before they decide it is too much (Mythen, 2004).

Research Question and Methods

What Role does Privacy Play in the Greater Sociotechnical System of the Internet of Things? This paper will serve as a guide to answer this question using two frameworks: Risk

Analysis and Technological Determinism. Risk Analysis is used to weight the positive and potential negatives of relying on IoT and have data be accessible on the internet. Technological Determinism is used to analyze the motivations behind using IoT in the current society and what is the driving force that pushes IoT to be widely accepted by the industry. The paper used the keywords “privacy, security, and IoT” as its main sources of research. This paper mainly focuses on IoT security and privacy, how to mitigate the risks of security breaches, and evaluate if IoT is worth using despite data safety concerns. This paper will discuss two different case studies followed by various IoT cyberattack methods. The first one is an IoT security breach and what can society do to prevent these breaches from ever happening again. The second one is a potential IoT security breach on medical devices and what the health industry can do to prevent possible breaches.

Supportive Background Information

IoT stands for Internet of Things, and a British scientist named Kevin Ashton first came up with this terminology (Ray, 2018). Ashton described IoT as a “sensors embedded system,” and it acts similar to a Smart City where data is transmitted electronically and calculations are made in real time (Ray, 2018). This form of data gathering and data processing is what will be the future of technologies. IoT encourages human-less interventions; the idea is that all devices within the IoT system should be able to communicate with one another using sensors. This concept is what is referred to as machine-to-machine interaction (Mehta et al, 2018). Data transmissions are automatic and can be done anytime and anywhere.

Before computers had the ability to gather information on their own, humans are the main source of data for computers. Humans captures data via various means that includes tapping buttons, taking photographs, and scanning onto computers. However, humans also have very limited time to spend on data capturing, and it would be difficult for humans to capture data in real time. Therefore, imagine the endless possibilities if machines could independently capture, store, and analyze data. Data capture via this means would be far more accurate, precise, and error-free (Shahrak, 2018).

To provide more context on how IoT can benefit society, medical applications is one of the top ideas that comes to mind. In fact, one of the best applications for the use of IoT is health monitoring (Sholla et al, 2017). Smart healthcare allows for healthcare agencies to keep an eye on their patients and gather various information on their health status as well has potential non-healthy habits.

Technological Determinism and Risk Analysis

Technological Determinism and Risk Analysis are the two main STS frameworks discussed in this paper. With growing technologies and more and more people having access to the Internet, there is simply too much data and information for one device to keep track of. Having a system like IoT can easily transmit and receive a large quantities of data without needing human interventions. IoT can be much more efficient and useful in data capturing and can easily change how data is recorded in the near future. In other words, IoT will most likely change the way humans look at data capturing and storing, thus shaping society in the near future. However, society must also consider how to best protect and store these data so they may not be used maliciously.

In an essay titled "*Technological Determinism in American Culture*" written by Merritt Roe Smith, Smith discussed how technologies are designed to be able to perform tasks better than humans. Smith states, "in the competition for world markets, industrial societies pressed hard to develop technological capacities that would give them an edge and, in the process, made the machine rather than the human condition the norm against which all else was measured" (Smith, 1994). Smith argues how the standards for machines are different than for humans because machines can do a much better job than humans. IoT is one such example; IoT drastically improves the way data can be collected. IoT's ability to capture data in real-time improves efficiency and reliability of the data as well as achieving a much larger sample size. IoT has made data capturing so convenient to the point where almost all technology companies should consider using them and explore more options out on the web. In fact, it is unwise not to consider IoT if companies want to stay ahead and stay competitive. Furthermore, the web has attracted many internet users since the introduction of Wi-Fi. More and more users are actively learning how to use Wi-Fi all on their own without the needing commercial advertisement. It can be argued that growing user popularity has forced companies to adapt to the current trend and focus more on improving Wi-Fi, which, in term, continues to attract and grab ahold of user attention. However, what the author failed to articulate is how, although IoT will shape societal values, we as the humans can refuse to adapt to such changes. If the issue of security grows with increasing concern and no plausible solutions, we can deem this technology as unsuitable despite the many advantages.

Automated machines are more susceptible to security concerns because they are not moderated by humans. IoT requires little to no human intervention, and so when there is a data breach or loophole, it can take a long time before someone notices the concern. The question then becomes whether or not the data breach is an “acceptable” risk? Given how efficient the IoT is in collecting and managing the flow of data, does this one advantage outweigh the security disadvantage? Is the risk acceptable enough for people to still trust in IoT to handle personal data? In a paper titled *Defining Risk* written by Gabe Mythen, Mythen discusses the importance of risk identification and the recognition of existing risks. Mythen states that every risk also comes with some “level of public knowledge” that recognizes such risk (Mythen, 2004). It is essential for all participants who share information via the IoT system to be aware that IoT is more vulnerable to cyber-attacks because there are no cyber security specialists on watch to ensure the safety of the network. Furthermore, it is easy to overtake an IoT network because every machine that participates in the network is connected to one another. Hijacking a single one of them will give access to the rest of the network, which can be very alarming. The result of these attacks can lead to large scales of damage as there can be a large magnitude of personal information falling into the wrong hands. One guaranteed way to avoid data leakage is to simply not access the internet, but this is not very feasible as the majority of data exchanges happen online, and there are convincing reasons for this choice. Online data transmission is both cost effective and time-saving because it eliminates the need for large hardware transportation. The positive outcomes associated with using the web are simply too large and too effective for companies to ignore. However, Mythen fails to elaborate further on some aspects of Risk Analysis. For example, Mythen did not clarify what is considered “public knowledge.” Is it fair to explain technical concepts to people with no technical background and expect them to fully understand? Not all individuals possess the necessary educational background to fully assess the risks and benefits associated with specific technologies.

Results and Discussion

IoT has long revolutionized how society handles data transmission and communication. Smart cities can send messages with great operational efficiencies and reduce data handling costs. While data security and privacy has been a huge concern for IoT due to its nature of being an automated system, it is difficult to dismiss IoT due to its functionality and benefits it has brought to society. Every technology inevitably comes with some form of risks, but it is important to acknowledge and assess what those risks are. Only through understanding and anticipating potential failures can future engineers help secure IoT.

Personal Device IoT Security

The Mirai Bonet was a large-scale Distributed Denial-of-Service (DDoS) attack that shut down a large portion of the internet, including Twitter, Netflix, and CNN in 2016. An DDoS attack uses the collective computing powers of devices to send large volume of spam to disrupt traffic and allowing attackers to steal credentials and hack into other devices (Zhang et al, 2020). A Botnet is a collection of internet-connected devices that attackers have compromised and can use to carry out attacks (Almazarqi et al, 2021). Mirai performs a multitude of functions such as scanning for ports, protocols, and actively sending ipv4 addresses to find other devices, putting huge emphasis on devices that uses weak or default passwords for its credentials. Once Mirai infects one device, the attacker will send automated commands to those infected devices so they may continue to send, spread, and infect the rest of the devices within the server (Griffioen 2020). No devices are safe from Mirai if it is connected to the internet. The impressive and scary part about this attack was that Mirai started from just a single scanning IP, and all it took was 2 hours of scanning for Mirai to infect 25,000 devices, and 640,000 devices within 24 hours (Antonakakis et al, 2017). Mirai eventually grew big enough to the point where it was able to take down Krebs-On Security, and it peaked at 600,000 infections with around 200,000 to 300,000 devices compromised due to default credentials.

Most consumers often only look at the price and functionalities when purchasing devices, overlooking or disregarding completely the security of the device. In fact, most consumers do not know what it entails when they use a device that can be connected to the internet, they may not even know how to secure their device or lack the motivation to do so. While the risks involving a device that can be connected to and accessed by thousands of other devices cannot be rquantified in a single value or term, it is fair to draw the conclusion that any devices out on the web can be vulnerable to cyber-attacks. The risks can grow significantly higher if the devices are using default or easy passwords for authentication. The types of data that are potentially exposed will vary from person to person, and users should be aware that their data might be stolen when they decide to use web-connected devices. The concept of IoT has been around for roughly two decades, and the number of internet-connectable devices will only continue to grow, yet most of them lacks modern security protocols (Rejeb et al, 2022). All of these devices should implement stricter safety conventions such as closing unused ports, enabling multi-factor authentications, controlling access privileges, and performing automatic updates (He et al, 2023). It is impossible to completely eliminate the risk of having personal data be stolen when it is being shared online, but it is possible to take steps to minimize the risks involved.

Medical Related IoT Privacy Concerns

Over the years, consumer IoT has been on the rise and is gaining popularity in the medical fields. Hospitals and healthcare industries are introducing IoT devices and applications to its patients for remote health monitoring. Activities and health data of the patient can be transmitted via the internet so patients do not have to remain in the hospital and be tied to machines. IoT has impacted how some hospitals handle patient care, and there seems to be little reason to stop using IoT other than concerns for data privacy. If a patient's personal data were to be accessed or tampered with by outside sources, then it could lead to a life-endangering situation as the collected data would be flawed.

In August of 2016, the Muddy Waters Research firm published a paper that highlighted the potential risks of medical device hacking (Baranchuk et al, 2018). The two types of attacks discussed are a pacemaker attack and a battery drain attack. The level of risks intensifies as healthcare devices error could lead to patient deaths. The research highlights Cardiovascular implantable electronic devices (CIED) which includes pacemakers, implantable cardioverter defibrillator, and cardiac loop recorders. All of these devices are designed to control and monitor irregular heartbeats of patients with some forms of heart rhythm disorders or heart failures (Baranchuk et al, 2018). These devices can be connected to the internet and used remotely, which puts them at risk of potential cyberattacks.

Security on devices must be implemented early in the development lifecycle and monitored throughout. Cyber vulnerabilities may even interfere with the monitor process and turn off any potential firewalls. In the likelihood that a CIED is breached, patients using these devices remotely at home could be in immediate medical danger and may even result in miscommunication between the patient and the hospital. Looking at it in the long run, the patient may even have to schedule an in-person appointment to fix the device. According to the medical facility, the chances of performing CIED updates may result in a complete loss of function is 0.003%, loss of device settings is 0.023%, and failure of update is 0.161% (Baranchuk et al, 2018). These values are fairly small and most users are okay with performing updates as the risk of update malfunction is much better than the risk of being a victim of a cyberbreach. Another important question to consider is how should physicians communicate with patients regarding possible cybersecurity risks. Should the patient be explained thoroughly the risks of using CIED, and will providing numerical statics be enough to educate and warn them? What if the patient is an elderly person with no knowledge of the internet and how it works? How can the medical facilities ensure their patients fully understand the risks and reach an educated and shared decision. Technology determinism oversimplifies the interactions between IoT and patients. This particular case study is more deterministic because the benefits of using IoT to monitor patients are immense, and it will likely stay and continue to change how future hospitals run patient treatments. However, the drawbacks and risk involved should not be overlooked.

IoT vulnerabilities

Improving IoT security is by no means an easy task, as IoT vulnerabilities can be divided into three different groups: hardware, software, and capturing data in transit. The hardware threats use physical aspect of the hardware to perform modifications or tampers with the circuits of the device. One example of such a threat is called the "Side Channel Attack." The attacker will target the leakage of physical information by monitoring things such as power, radiations, timing information, and sound. The beauty of IoT is that it can operate entirely by itself without needing a human monitor. That being said, these devices are also physically "defenseless." An attacker can realistically get physically access to the device and meddle with it however they wish. Often times, malicious hardware might be installed onto the device that can both hide its existence as well as modify the behavior of the device.

The software threats use code to tamper with the inner operating system of the devices and change its algorithms to perform other tasks. Examples of these threats include botnets, spoofing, and Denial of Service (DoS). Botnet are similar to zombies where if one device gets infected, the remaining devices can also potentially get infected (Dwyer et al, 2019). All it takes is one device where some form of malicious software gets installed, and the malicious software will run commands telling these devices to carry out all forms of other attacks such as phishing, spamming, or more installations to infect other devices. Spoofing occurs when the attacker pretends to be an authenticated user so he may gain access to all the available user privileges to commit evil deeds. DoS occurs when the attacker tries to flood or overload a device with large amounts of incoming data in hopes of creating a crash. The device simply receives too many requests to the point where it just stops operating because it does not know how to handle all these requests.

Data in transit is done when the attacker tries to capture and steal data while it is passing through the spectrum. The attacker will then attempt to filter out only the valuable information such as sensitive credentials or other personal data. The attacker can also perform what is known as the “Man in the Middle Attack” where the attack serves as the messenger between the sender and the receiver (Williams et al, 2022). It can halt any ongoing communications, alter them, and then send them to the desired destination.

The internet has influenced and shaped how members of the society communicates with one another due to its convenience and accessibility. With the rapid progression of the web, it is difficult to imagine a world without the internet. However, the Mirai Bonet has exposed many problems regarding IoT, and with many IoT devices rolling out onto the market each year, security has become a huge concern. Similar to how Apple releases a new phone almost every year, the older generation of phones are still usable. It is important to highlight that the aging population of devices will likely be neglected, but these devices can still be connected to the web, and it is very challenging to detect the insecure devices among them and lock them out of the web (Dietz et al, 2018). Therefore, the internet will be highly vulnerable as getting possession of one device can and will put all the other vulnerable devices at risk (Mohsin et al, 2017).

It is also important to analyze the issue of IoT security from the manufacturers' point of view. There are low incentives in investing time on improving security of low-costs devices. Currently, there is no global consensus on how to define and enforce IoT security standards. Most manufacturers might not even consider attempting to offer maintenance or regulate updates for some of these low-end devices. Furthermore, there are no global organizations that regulate cybercrime. It is difficult to track down and arrest botnet creators because anyone can write programs and deploy them to the web. It is also extremely hard to track and take down host domains for these botnets if they are hidden.

The limitation of this research lies in the fact that as engineers look for ways to protect IoT, there are also malicious actors who are constantly looking for creative ways to exploit vulnerabilities. One possible direction for future studies is to evaluate how easy or difficult it is to try to hack into an IoT network, which could provide insights on areas of weakness that need to be addressed. Additionally, given IoT's rapid growth, it would be wise to anticipate what new devices could enter the market and how they may impact the current set of IoT network. Future research could seek to forecast the development of new devices and evaluate their potential impact.

Conclusion

Despite the security concerns, IoT is here to stay. IoT has help improved data recording and transmission immensely, leading to recognizable benefits. The positives of IoT far outweighs the negative, and so IoT will continue to play a dominant role in society. Additionally, many computer users are already at risk of data leakage when they browse the web each day, and most people have become accustomed to such risk. It is difficult to predict what future security breaches might happen in the future, but having these security breaches will only help to identify vulnerabilities and improve IoT security, making it more resilient and more robust against future attacks.

References

A. Shahraki and Ø. Haugen, "Social ethics in Internet of Things: An outline and review," *2018 IEEE Industrial Cyber-Physical Systems (ICPS),* 2018, pp. 509-516, doi: 10.1109/ICPHYS.2018.8390757.

Almazarqi, H.A., Marnerides, A.K., Mursch, T., Woodyard, M., & Pezaros, D.P. (2021). Profiling IoT Botnet Activity in the Wild. 2021 IEEE Global Communications Conference (GLOBECOM), 1-6.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai Botnet. USENIX Security Symposium.

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D., Lakkireddy, D. R., & American College of Cardiology's Electrophysiology Section Leadership (2018). Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?. Journal of the American College of Cardiology, 71(11), 1284–1288. https://doi.org/10.1016/j.jacc.2018.01.023

Dietz, C., Castro, R.L., Steinberger, J., Wilczak, C.W., Antzek, M., Sperotto, A., & Pras, A. (2018). IoT-Botnet Detection and Isolation by Access Routers. 2018 9th International Conference on the Network of the Future (NOF), 88-95.

Dwyer, O., Marnerides, A.K., Giotsas, V., & Mursch, T. (2019). Profiling IoT-Based Botnet Traffic Using DNS. 2019 IEEE Global Communications Conference (GLOBECOM).

Griffioen, H.J., & Doerr, C. (2020). Examining Mirai's Battle over the Internet of Things. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.

He, Y., He, J., & Wen, N. (2023). The challenges of IOT-based applications in high-risk environments, health and safety industries in the industry 4.0 era using decision-making approach. *Journal of Innovation & Knowledge, 8*(2), 100347. https://doi.org/10.1016/j.jik.2023.100347

Mohsin, M., Sardar, M.U., Hasan, O., & Anwar, Z. (2017). IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. IEEE Access, 5, 5494-5505.

Mythen, G. (2004). Defining Risk. Ulrich Beck: A Critical Introduction to the Risk Society. (pp. 53-73). London, England. Sterling, Virginia. Pluto Press.

N. Su, "Internet of Things privacy security protection access control Research," *2022 IEEE 6th*

Information Technology and Mechatronics Engineering Conference (ITOEC), 2022, pp. 919-923, doi: 10.1109/ITOEC53115.2022.9734497.

Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H., & Zailani, S. (2022). The big picture on the internet of things and the smart city: A review of what we know and what we need to know. *Internet of Things, 19,* 100565. https://doi.org/10.1016/j.iot.2022.100565

Smith, M.R. (1994). Technological Determinism in American Culture. *Does Technology Drive History?: The Dilemma of Technological Determinism*. (pp. 1-17). Cambridge, Massachusetts. London, England. The MIT Press.

S. Ray et al., "A Survey Paper on Architecture of Internet of Things," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 908-913, doi: 10.1109/IEMCON.2018.8614931.

S. Sholla, R. Naaz and M. A. Chishti, "Incorporating Ethics in Internet of Things (IoT) Enabled Connected Smart Healthcare," 2017 *IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE),* 2017, pp. 262 263, doi: 10.1109/CHASE.2017.93.

V. Mehta, P. Bansal, K. Mohit and P. Banerjee, "Empowering the Security for Iot-Based Communications in Smart City," 2018 International Conference on Automation and Computational Engineering (ICACE), 2018, pp. 57-60, doi: 10.1109/ICACE.2018.8686995.

Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things*, *19*, 100564. https://doi.org/10.1016/j.iot.2022.100564

Zhang, X., Upton, O., Beebe, N. L., & Choo, K.-K. R. (2020). IOT botnet forensics: A Comprehensive Digital Forensic Case Study on Mirai botnet servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926