AN ANALYSIS OF CYBERSECURITY IN THE AGE OF IOT

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

By

Yusuf Cetin

March 30, 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
Catherine D. Baritaud, Department of Engineering and Society

SECURING IOT IN THE INTERNET AGE

Security of online personal information in the Internet age is a facet of life that should not be compromised, yet attackers have been challenging this desired reality since the very genesis of the web. Cyber criminals have gained significant strength in recent years, especially with the advent of Internet of Things (IoT) devices, which are defined as “the network of physical objects consisting of sensors and actuators that exchange data to offer enhanced quality of services in everyday life” (Jithish et al., 2017). Some examples of IoT devices include smart thermostats, doorbells, and cameras. As this technology progresses, even devices requiring a high level of non-trivial physical security, such as lockboxes, will be implemented. That’s why our capstone group sought out to develop an Internet-connected lockbox with a creative and unexpected unlocking mechanism, through knocking or tapping on its sides as the entry procedure, deemed the “Tap Box”. Disguised as a tissue box, the Tap Box was designed to be an inconspicuous tool which stores small valuable items and can be considered from the STS research and framework perspectives described below.

The core of IoT’s impact on society and society’s impact on IoT specifically regarding cybersecurity must be adequately characterized before making any conclusions about the intertwining between technology and society. First, evidence of the central problem’s existence will be established, and the severity of its repercussions if left unattended will be examined. Then, summaries of relevant technical and non-technical solutions gleaned from literature review will be presented for the purpose of reaching a conclusion about what is the best course of action for the mitigation of cybersecurity measures in IoT devices, such as the Tap Box. Finally, the Social Construction of Technology (SCOT) STS framework will be used to emphasize the unavoidable connections between the technology and the various parties which directly affect and get affected by IoT. Presented in this fashion, it becomes painfully obvious that engineers cannot develop technology in a so called “bubble”. As it turns out, although often difficult, all considerations of a technology’s apparent and potential societal impacts must be accounted for.

As described, the technical product is tightly coupled with the STS topic, since, as an IoT device, the Tap Box’s development plays a major role in the future of IoT cybersecurity. Without built-in security measures, the device loses its integrity and, therefore, its sole purpose is greatly diminished. Stated generally, as more and more IoT products become widely integrated, the concerns that govern their use regarding cybersecurity must be resolved for the benefits to outweigh the potential risks.

THE RAPID EXPANSION OF IOT AND CYBER CRIME

In recent years, IoT usage has exploded. As noted by Hasan, the growth of the global IoT device market is predicted to increase 22% by the year 2025 (2021). This means consumers are purchasing more smart thermostats, security cameras, electronic door locks, and the like, forming an interconnected network within the home as well as in commercial buildings and beyond. While this local mesh provides many benefits like convenience and more extensive connectivity, attacks which exploit unprotected IoT devices to gain entry to the larger network unfortunately occur frequently and at scale. According to James, 90% of large organizations encountered cyber-attacks in 2019, while only 81% were encountered in 2018 (2019). The Internet Crime Complaint Center (IC3) also reported a total of 351,937 cybersecurity complaints from cybercrime victims in 2018, which equated to losses of about $7.45 billion worldwide (Abdullah, 2019).

To make matters worse, the unprecedented ravage of the pandemic in early 2020 forced people to be in their homes more, meaning a flourishing of IoT device usage. This influx brewed the perfect opportunity for cyber criminals. With more potential entry points into unsuspecting residential internet connections, hackers maximized their intrusion significantly. In fact, according to Forno, Mateczun, and Norris there was a 300% increase in cybercrimes between 2020 and 2021. While IoT's weaknesses is among the major reasons hackers can intrude, ease of monetary gain and low risk of punishment also contribute to malicious intents, catalyzed by the opportunities opened by the pandemic (2022).

CONSEQUENCES OF A VULNERABLE NETWORK

As discussed, the lack of an established cybersecurity system for IoT devices has resulted in a gaping hole for hackers to exploit to the fullest. The consequences associated with this fact encompasses all fields which require the aid of an electronic, connected system. Most commonly, the home outfitted with even a few smart devices comes into mind as a potential target.

Highlighted by James, "An attacker can easily attack an interconnection device such as gateway or smart home appliance device using its network or local communication interface and also an IoT device can be impersonated using its faulty authentication" (2019). This vulnerability in the home network has been historically problematic, with attacks strategically taking advantage of an IoT device to break in. One such example was the Mirai botnet which utilized Wi-Fi cameras, routers, and printers to carry out Denial of Service (DDoS) attacks in 2016, flooding servers in order to gain access to sensitive information. This attack was successful due to the unprotected nature of the devices, which had default usernames and passwords, allowing easy access for the hackers, all under the victims' noses (Aiken, 2020). As demonstrated, user awareness and familiarity of such attacks must also be mitigated in addition to secure software, something discussed in later sections.

The healthcare sector is another example of an especially vulnerable system. Wearable sensors, wireless monitors, and cardiac devices are amongst just some of the IoT gadgets used in patient care in and out of the hospital. An attacker gaining access to critical life-saving devices is obviously detrimental and can easily lead to loss of life without proper cyber protection (Gobinath, 2021). However, adding in cybersecurity features to a device that needs to be physically small means limited ability to make such additions. Furthermore, considerations such as updating software of continuous devices for security purposes can be problematic due to the need for a constant flow of information with no breaks, a hindrance when it comes to ensuring the most secure systems are being deployed (Gobinath, 2021).

LACK OF SECURITY IMPLEMENTATION

The average IoT device today has an underdeveloped or nonexistent cybersecurity protocol, leaving it vulnerable to hackers using its connection in the network as an access point to the host. Given that their nature is to be small in size and relatively large in quantity, these devices are designed to be low energy, generally meaning less hardware and memory available for use. Therefore, firewalls are generally minimally implemented in IoT devices due to their complexity and limited software capability of a smaller electronic device (Dagale & Maheshwari, 2018).

MANUFACTURER RESPONSIBILITY AND REGULATIONS

The most influential player in the question of IoT device security is obviously the makers of these devices. Manufacturers are responsible for the design and intended use of the device, which also includes any security protocols embedded into software. As previously mentioned, security is not monetarily beneficial as it requires more effort and cost to implement. However, device producers must oversee this and realize that the harm being done is on a much larger scale as this void of cybersecurity concern is left untouched. Government intervention is a good first step towards improving the state of this crisis.

Although subjectively shocking, none of the United States, except for California, currently has comprehensive laws governing consumer data privacy with IoT devices. Concerning cybersecurity, the IoT Cybersecurity Improvement Act of 2020 is the only bill that gives some level of management in the realm of IoT security, although minimal. In California, the California IoT cybersecurity law, SB-327, became effective January 1st, 2020, which requires manufacturers of devices to build in adequate security features, for example, a password setup prior to first use (IoT cybersecurity: Regulating the internet of things, n.d.). Another example of legal mandates exists in the realm of automotive cybersecurity and can be given as described by Burzio, Colajanni, Cordella, Marchetti, and Stabili, with the Society of Automotive Engineering's (SAE) Recommended Practice J3061. This protocol provides a design to end of life framework and guidance for development of cybersecurity measures in physical vehicle systems (2018). Given that the development of these legal measures is only recent, IoT as a security infrastructure still requires further advancement.

COMBATTING THROUGH RESEARCH

Regulations, as previously mentioned, stem from researching and testing counteractive measures. One example is the deployment of advancements like honeynets, which can provide great insight and progress towards making devices as safe as possible. In the technical work carried out by Bernabe, Calero, Skarmeta, and Zarca, honeynets are defined as simulated networks that attract hackers on purpose to study their methods. High-interaction honeypot (HIH) honeynets are even more cloaked to cybercriminals, meaning deeper information can be collected about a hacker with its implementation. However, being a large resource-consuming tool, and having little history with implementation in IoT devices, this technology needs what the researchers were able to devise, an automated framework to deploy a flexible honeynet (2020). Analysis and characterization of hacker behavior such as this is an important step in the direction of securing IoT devices in the broader network.

The current research which relates to IoT cybersecurity extends further, into systematic solutions for direct defense. Almalki, Alqarni, and Munshi describe an attack detection system which also utilizes honeypots to “trap” suspicious traffic using machine learning algorithms. Once malicious requests are caught, their IP addresses are noted and stored in a database for reference later for comparisons. This system is formulated into a blockchain model, which effectively ensures that suspicious network traffic is contained and isolated (2020).

The blockchain framework to systematically tackle malicious network traffic is agreed upon by many authors in this realm of research. Noted by the references of Abie, Pirbhulal, and Shukla, “authors developed a secure blockchain-based DT approach for a smart healthy city composed of layered model to maintain privacy, security, and trust” (2022). DT is short for digital twin, which is essentially a virtual “twin”, or counterpart of a specific aspect of the physical world. DTs are used for cybersecurity enhancing purposes by testing and evaluating network security features without the concern for disrupting an already functioning system. More specifically, DT technology is useful in the IoT sphere in healthcare, having applicability in quick multi-device security patch management, anomaly detection, autonomy, and improved risk management (Abie et al., 2022). These benefits mean that more secure IoT networks can be constructed with the use of DT technology given the breadth of devices employed in healthcare applications, ultimately improving the chances of health for patients.

Parallels in methodology of counterattack can be found upon examining ongoing research efforts. The home intrusion prevention system outlined by James is organized by using confidentiality, authentication, and access control. Confidentiality includes encryption as a line of defense, where authentication ensures strict password requirements to combat brute force attempts by attackers, and access control prevents DDoS attempts by triggering upon a set of false requests to halt further harm (2019). This system was tested via conduction of three major attacks, where the intrusion mitigation model proved robust.

A final technical and promising solution in the war against IoT hackers is brought forth by Dagale and Maheshwari, which works in the following fashion. The architecture revolves around the idea of decentralizing authentication and using a local authority device, which acts to off-load the authentication processes from each embedded IoT device encapsulated in a local server. This reduces hardware requirements to implement security software for each device, while still allowing for secure authentication system (2018).

Creating virtual network environments that allow for testing of hacker behavior and containment of malicious activity is one aspect of advancement towards implementation of more secure IoT systems. Coupled with organized intrusion detection and elimination strategies, IoT cybersecurity seems to have a hopeful future.

SOCIETAL CONSIDERATIONS

The process of building a sound IoT device in the business realm can be put into a framework that describes the development approach. Applied to IoT technology, Cooper, Coulton, Hands, and Lee describe the concept of New Product Development (NPD) (2019). At its core, NPD defines a market opportunity and results in the delivery of a product addressing this opportunity. Through validating assumptions in a linear fashion, products can be developed based on executive insights, focusing on consultation advice rather than customer thoughts. This process guidance, however, does not accurately describe IoT product creation, rather, a value “constellation” is a better depiction of demonstrating the interaction between customers and producers, as shown in Figure 1 on page 7.

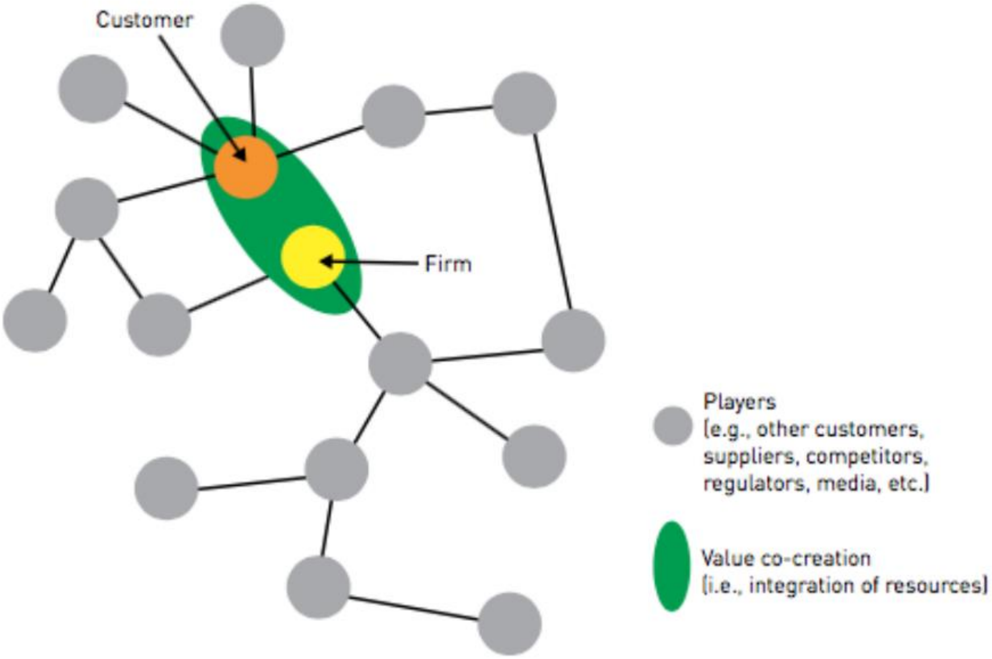
Customer
Firm
Players
(e.g., other customers, suppliers, competitors, regulators, media, etc.)
Value co-creation
(i.e., integration of resources)

Figure 1: The “value constellation” demonstrating the co-creation of IoT technology with a customer and the production firm. The interconnects are clearly shown as grey nodes, which could correspond to big data, business analytics, and other influences (Cooper et al. 2019).

Given the connections of the IoT and cybersecurity to society at large, an STS framework can be applied as a summary of this network. With the Social Construction of Technology (SCOT) model, arrows go in both directions because groups inform the IoT device’s activities and the characteristics of the technology, while the product is equally providing value to each group. Business development will facilitate the process of making the product to fulfilling customer needs, all while allowing monetary gain. Government regulations will mandate the technology with current laws, which the technology will also help develop, in a feedback type manner. Manufacturers, of course, play a role in the product as well, who are expected to provide standardized, reliable components. Cybersecurity concerns, as described in detail, allow for the IoT product to develop effectively and will change as the product demands more security measures. Finally, the end user, the most important group, will determine whether a certain IoT product is necessary or up to par with their needs, allowing for revisions and redesigns. These groups govern the development of the IoT device, and the IoT device changes each group's perceptions with its development, as illustrated in Figure 2 below.

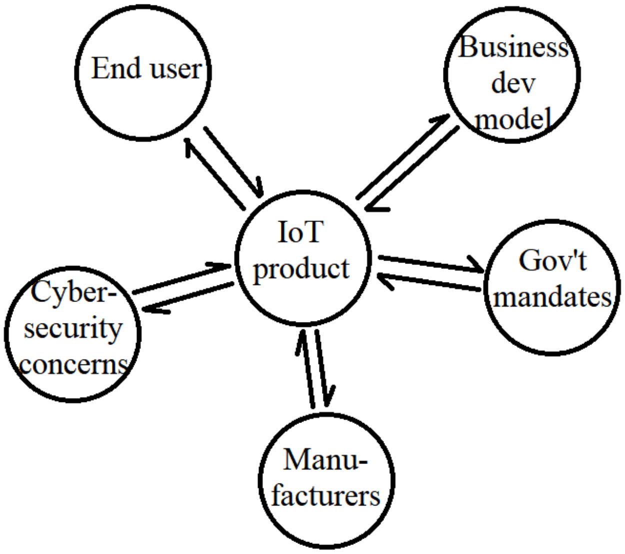

Figure 2: SCOT model for an IoT product. The product at the center transfers and receives value to and from each of the labelled groups (Adapted by Cetin (2022) from Carlson, 2009).

While manufacturers play the largest role in this model, end users also possess the capability for attack prevention. Aiken, Rizvi, and Ryoo conducted a comprehensive survey which summarized how much IoT end users know and do in regard to security, targeting questions that deal with making choices to help security efforts (2020). Such simple efforts like resetting passwords of IoT devices goes a long way in preventing simple attacks. An approach proposed by Silverajan and Zhao coined as user-centered design (UCD) aims at placing the end user at the forefront of the design process, demonstrated by their visual dashboard system that allows residents to manage all IoT devices on the network. The design exhibited a bird's eye view, rather than technical details of network traffic of the IoT system, which was preferred by the end user (2022). Visually placing pertinent information for the end user amplifies their involvement and awareness and can improve identification of risks more effectively.

THE NEXT STEP FOR IOT

To succinctly battle potential societal and technical effects, cybersecurity as a whole must first be realized and understood. The IoT world is expanding and so are cybersecurity risks. Being able to manage and reduce these risks effectively will allow for less intrusion as well as higher levels of the public's trust in these devices. Especially in the case of personal sensitive information, security and confidence in the user must be prioritized. By researching and implementing technical solutions through overcoming software and hardware challenges, as well as making end user quality of use a priority, IoT can continue to enhance the quality of life, while remaining a safe way of doing so.

REFERENCES

Abdullah, A., Hamad, R., Abdulrahman, M., Elkhediri, S., & Moala, H. (2019). CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),* 1–6. doi:10.1109/CAIS.2019.8769560

Abdullah Almalki, N., Alqarni, N. A., & Munshi, A. (2020). DDOS Attack on IOT Devices. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS),* 1–5. doi:10.1109/ICCAIS48893.2020.9096818

Abie, H., Pirbhulal, S., & Shukla, A. (2022). Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications. *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring),* 1–5. doi:10.1109/VTC2022-Spring54318.2022.9860581

Aiken, W., Ryoo, J., & Syed, R. (n.d.). An Internet of Things (IoT) Security Assessment for Households. *IEEE*. doi:10.1109/ICSSA51305.2020.00017

Bernabe, J., & Calero, J., & Skarmeta, A., & Zarca, A. (2020). Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks. *IEEE Journal on Selected Areas in Communications, 38, 1262-1277.* doi:10.1109/JSAC.2020.2986621

Burzio, G., & Colajanni, M., & Cordella, G., & Marchetti, M., & Stabili, D. (2018). Cybersecurity of connected autonomous vehicles: A ranking based approach. *2018 International Conference of Electrical and Electronic Technologies for Automotive.* doi:10.23919/EETA.2018.8493180

Cetin, Y. (2022). SCOT model for an IoT product. [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Cooper, R., & Coulton, P., & Hands, D., & Lee, B. (2019). Value creation for IoT: Challenges and opportunities within the design and development process. *IEEE Xplore*. doi:10.1049/cp.2019.0127

Dagale, H., & Maheshwari, N. (2018). Secure communication and firewall architecture for IoT applications. *2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India*. doi: 10.1109/COMSNETS.2018.8328215.

Forno, R., & Mateczun, L., & Norris, D. (2022). The future of local government cybersecurity. *Cybersecurity and Local Government, 201-226*. doi:10.1002/9781119788317.ch12

Gobinath, K., Marshal R., & Rao, V. (2021). Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–4. doi:10.1109/IEMTRONICS52119.2021.9422615

Hasan, M. (2021, September 22). State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

James, F. (2019). IoT Cybersecurity based Smart Home Intrusion Prevention System. *2019 3rd Cyber Security in Networking Conference (CSNet)*, 107–113. doi:10.1109/CSNet47905.2019.9108938

Jithish, J., Rajan, A., & Sankaran, S. (2017). Sybil attack in IOT: Modelling and defenses. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2323–2327. doi:10.1109/ICACCI.2017.8126193