Modeling IoT Solutions: A Lack of IoT Device Security, and User Education

Benjamin Newlin
Christopher Newport University

Modeling IoT solutions
A lack of IoT device security, and user education

Benjamin Newlin
Prof. Christopher Kreider

Coastal Virginia
Cyber Collegiate Initiative

Abstract

The Internet of Things, more commonly known as IoT devices, is an ever growing topic, both in the marketplace and in cyber security. While new devices are released into the public every year, a lack of standardized security concepts is also growing ever so clear. By having a model or standard for IoT devices and manufacturers to follow, the customer-base of these devices will have an easier time identifying trustworthy devices as well as how to secure their own devices.

Introduction

IoT devices can be classified and organized into different categories, many of which have little overlap. Pulling from the papers cited, The definition that will be used in this paper is as follows. “Smart IoT is a collection of devices with network and/or communication abilities that is based off of a device which regularly does not need it.” While other forms of IoT devices that do inherently need network/communications technology also exist, the focus of this paper will not be discussion on these similar devices. From this definition, we can gather that relatively any computer with a network-facing component falls under the category of IoT. Other than with our definition, end user publications and articles often stray towards different terminology. In a product release from Bitdefender, end users seemed to dislike the term Internet of Things, due to their vague understanding of what the terminology means, associating it with Machine Learning or Artificial Intelligence. Rather than the preferred Smart Home terminology often used for Smart Thermostats or Smart Lights. (BERTE, 2018) It is due to this distinction, as well as the targeted audience of this paper being consumers, that we will be discussing primarily “smart” devices.This paper will address the following research questions:

RQ1: How can we quantity the levels of maturity manufacturers utilizes when communicating to customers regarding IoT device security

RQ2: Do the hardware or use cases for these IoT devices include unnecessary cyber related capabilities for an end user that could leave room for exploitation

RQ3: What form of continuous support or updates should be provided for consumers

RQ4: How does this model support and improve the device, as well as the manufacturer

The purpose of this paper is to develop an ordinal measurement instrument to assess the security guidelines and use cases for IoT devices, as well as to specify why it is important to have a baseline standard to follow. The rest of this paper will be structured as follows. We will first discuss literature related to IoT security standards, and what guidelines manufacturers have put in place to guarantee a secure service. Then we will discuss methods of ranking the products and manufacturers based on the level of service and support that is easily accessible. Finally, we will discuss our results and provide our discussion.

Lit Review

A Study on Device Security in IoT Convergence

Kim Et Al. (2016) explored consumer IoT devices and the categorization of them based on criteria. Such criteria follows service categories and domains of threats. The servicing categories included domains such as Energy Services, Smart Home Services, and E-Health. Then outlining threat cases in each domain. Finally specifying security requirements for IoT devices following lightweight cryptography, communication security, data protection, physical protection, device identification, and monitoring.

Consumer IoT: Security Vulnerability Case Studies and Solutions

Alladi Et Al. (2020) explores case study security threats involved with additional IoT devices introduced to networks. The attacks identified include device software failure, node tampering attacks, eavesdropping attacks, malicious code injections, unauthorized access, social engineering attacks, device hardware exploitation, and malicious node insertion. For each of these, countermeasures were proposed, much like rigorous quality testing, physical unclonable functions, lightweight encryption, integrity checks, regular monitoring/patching of upgrades, and security techniques.

Learning Internet-of-Things Security "Hands-On"

Constantinos Et Al. (2016) explores the network security implications of the IoT device market increasing in modern day. A major attack vector outlined is the increased likelihood for leakage of personal identifiable information, in cases such as personalized lighting information, remote watering systems, unauthorized execution of device functions, and architectural vulnerabilities such as unnecessary ports open on a home network.

Defining the IoT

BERTE Et Al. (2018) By utilizing other publications, BERTE sheds light on the confusing stature of the IoT terminology. Furthermore explaining the vague term and defining the different work flows and environments that IoT devices operate in. BERTE notes that there is a large difference between smart home devices and the IoT devices

common in industry. BERTE comments on a case study from Bitdefender about consumer support of “Smart” homes and devices increasing to an average of 14 IoT devices per household in 2017. BERTE also outlines a case from Bitdefender, this time noting that customers didn’t respond well to terms such as “IoT security hub”, rather opting for the more friendly “Smart Home security solution”.

Foundational Cybersecurity Activities for IoT Device Manufacturers

Fagan Et Al. (2020) Fagan Et Al. outline the lack of device capabilities, oversights, and support, proposing actions and strategies for IoT Manufacturers to combat such issues. Fagan lists six areas of impact to focus on before device development. These areas are Identification of expected customers and use cases, Researching cybersecurity goals of expected users, determining how to respond and address customer needs, planning the support options for customers, defining the approach for how to communicate with the end user, and finally deciding what to communicate to the customer. Fagan also notes about certain IoT devices relying on systems such as an IoT hub to gain security functions.

Methodology

This project will utilize a design science approach, a research methodology that designs new artifacts to solve a problem or make an advance (Vaishnavi and Kuechlar, 2015). Within this approach, we will utilize a qualitative case study approach interviewing stakeholders at a small state university (Lee, 1989). The feedback from these interviews will then be used to develop a categorization system for IoT security and support, a model of maturity around the information and methods used by other organizations is outlined.

Results

In an interview conducted with the Christopher Newport University information technology staff, the core components of security and authorizing IoT devices on a network are front and back-end network security, and a trust with the manufacturer to provide adequate security concepts and features to the device. Front-end security is the software or applications that implement security that the consumer will interact with regularly; however, backend-security is the application or moderation controls running in the background of networks or systems. Trust with the manufacturer, on the other hand, is proven on quality support and development of the device.

Below, we discuss our answers to our research questions

RQ1: How can we quantity the levels of maturity manufacturers utilizes when communicating to customers regarding IoT device security:

To quantify the maturity level scaled with a manufacturer, it is necessary to outline the guidelines that each company will be held accountable to. We do this by creating a scale that will display the level of depth related to security and education that a manufacturer is expected of.

RQ2: Do the hardware or use cases for these IoT devices include unnecessary cyber related capabilities for an end user that could leave room for exploitation

When in the development cycle, is it necessary to ask if the device is more capable than necessary. While it is beneficial to get the most out of your product to sell for a higher price, the more cyber-related hardware or features, the more likely backdoors are going to be present. This could allow for misuse of the device.

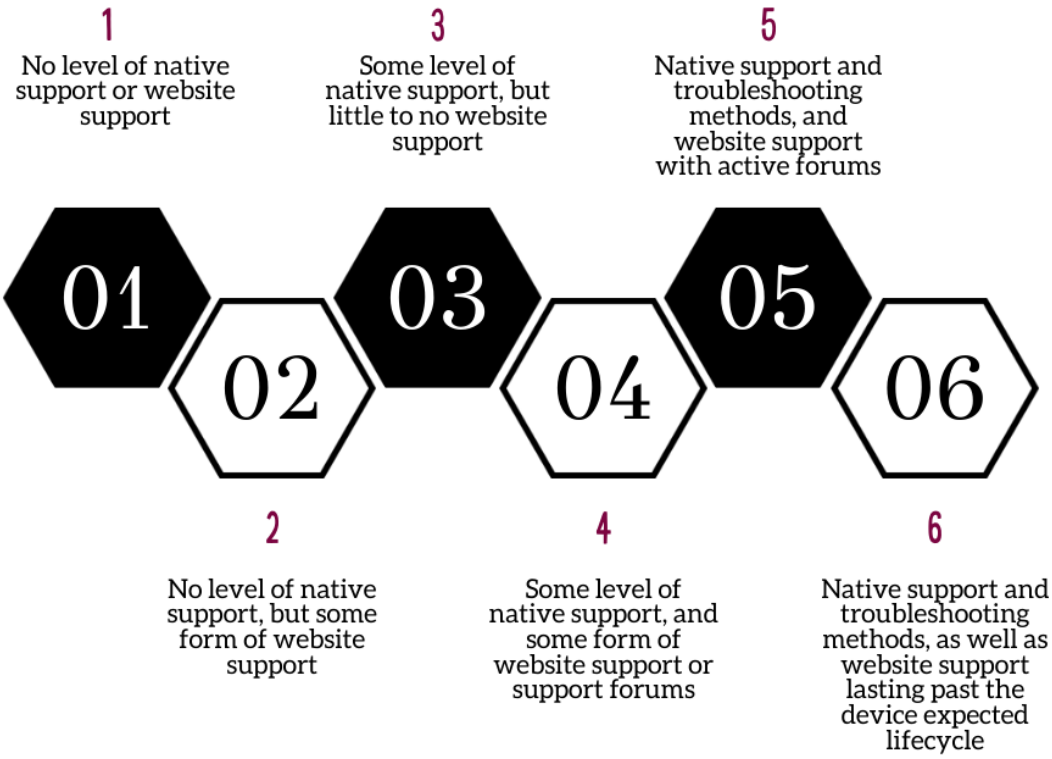
RQ3: What form of continuous support or updates should be provided for consumers:

At the end of the development life cycle, what methods of support are provided to the customer? Is it important for the device itself to have support methods built in, to allow end user help with troubleshooting past the device life cycle.

RQ4: How does this model support and improve the device, as well as the manufacturer:

By developing a maturity model of security features, we could place manufacturers, IoT devices, and companies against the model and determine what areas need to be developed more. The model will follow six specific levels of security and support competence, as well as how easy it is to find such features on a simple web search.

Having a model that manufacturers can follow and guarantee that every category is met not only allows for easier support for the end user, but also a greater perception of the company as a whole. Security features built into the device allows for active protection outside of backend support from the network, meaning that less work needs to be done on the customer's side.



Discussion

With the results of the model, we can apply companies such as Amazon, Apple, and Google to the model. Starting with Amazon's venture into IoT with Amazon's Alexa smart home assistant, Amazon's Security Best Practices outline the typical best practices that manufacturers and software developers should follow; however, through a quick web search, a solid troubleshooting guide or security features is not easily accessible. On the other hand, with Apple's AirTag, documentation of the AirTag and support is extremely accessible and clear. On the security side, the AirTag is extremely documented and transparent. AirTags are also synchronized with an Apple ID, allowing access to features like FindMy. This benefits from the security of using other devices designed by Apple to piggyback off of prior security mechanisms.

It is also worth note that while guidelines like the ones plotted in this paper are beneficial for general IoT devices such as a smart home assistant, router, or smart accessory, the model cannot be beneficial for each and every device.

References

- Kim, H.-J., Chang, H.-S., Suh, J.-J., & Shon, T.-shik. (2016, July 7). *A study on device security in IOT convergence*. IEEE Xplore. Retrieved November 3, 2022, from https://ieeexplore.ieee.org/abstract/document/7503989
- Alladi, T., Chamola, V., Sikdar, B., & Choo, K.-K. R. (2020, February 3). *Consumer IOT: Security vulnerability case studies and solutions*. IEEE Xplore. Retrieved November 4, 2022, from https://ieeexplore.ieee.org/abstract/document/8977812
- Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016, February 3). *Learning internet-of-things security "hands-on"*. IEEE Xplore. Retrieved November 4, 2022, from https://ieeexplore.ieee.org/abstract/document/7397713
- Berte, D.-R. (2018). Defining the IOT. *Proceedings of the International Conference on Business Excellence*, *12*(1), 118–128. https://doi.org/10.2478/picbe-2018-0013
- Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020, May 29). *Foundational cybersecurity activities for IOT device manufacturers*. CSRC. Retrieved November 4, 2022, from https://csrc.nist.gov/publications/detail/nistir/8259/final
- Alvarez, R.-A. S. (1987). *Nombres en -eús y nombres en -us, -u en micénico: Contribución al Estudio del Origen del Sufijo -eús*. Amazon. Retrieved December 3, 2022, from https://developer.amazon.com/en-US/docs/alexa/smarthome/wwa-security.html
- Vaishnavi, V. K. and W. Kuechler (2015). Design science research methods and patterns: innovating information and communication technology, Crc Press.
- Lee, A. S. (1989). "A Scientific Methodology for MIS Case Studies." MIS Quarterly 13(1): 33-50.