Mitigating Security Difficulties in the Internet of Things -Work In Progress-

Keyonna Brown
Purdue University
Computer Information Technology
Coordinated Science Laboratory
brow1018@purdue.edu

Mohammad Noureddine
University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
nouredd2@illinois.edu

Masooda Bashir
University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
mnb@illinois.edu

ABSTRACT

In this paper, we review the importance of the Internet of Things and the rapid growth of today's digital age. We examine related work on standard security structure, past surveys on the Internet of Things, and discuss background information on this developing issue. This paper presents our methodology for creating and distributing surveys to willing participants. This paper will also present results that uncover different connections among participants of the survey. The results can then be used to implicate which layer, sublayer, and application are prone to certain cyber-attacks. The survey includes questions pertaining to demographics, Wi-Fi, privacy, and protection. The paper concludes with remarks referring to the survey findings and patterns, finally closing with a discussion of future work.

Keywords

Internet of Things; Security; Issues; Wireless Sensor Networks; RFID Sensor Networks; Privacy; Confidentiality; Challenges; Definitions

1. Introduction

The Internet of Things (IOT) is a concept that one day all daily objects and devices will be interconnected in a new digital era [1]. For example, smart phone users have increased their digital activity with approximately 70 million new handlers in the past five years within the United States alone [2]. There are many interconnected devices in the average user's home, and a security breach can become the difference between life and death in the future. There are cars, phones, laptops, tablets, homes, refrigerators, medical equipment and environmentally friendly tools that are linked to the IOT. Excluding PCs, tablets and smartphones, there will still be over 26 billion items connected to the Internet by the year 2020 [3]. The importance of the Internet of Things is that it connects all devices at one place. It is important to concentrate on the IOT as well as its applications to find a solution to the impending cyber security threats. The assumption is that the transport layer is the most important as well as the most accessible to cyber-security attacks [5], which will be discussed later in the paper. The IOT is a new, revolutionary, and efficient way to save data, but the interconnectivity also makes the devices more vulnerable to cyber-attacks, such as credit card fraud, identity theft, and denial of service (when network resources are made unavailable to the user). So far, there have been studies about the IOT in general, the security architecture, surveys and possible solutions with the need for further implementation. In this paper, we discuss literature reviews on the Internet of Things, which are ongoing. We also discuss the surveys given to willing participants that reveal perspectives of everyday users, which is the most important aspect of the Internet of Things and its success. Surveying users helps us to understand everyday user's activity in the IOT. This paper also benefits users because they will get to see the security architecture and may be prone to look for possible ways of vulnerability mitigation.

2. Related Work

The Acquity Group 2014 State of the Internet of Things Study surveyed more than 2,000 possible IOT consumers across the United States to gain an understanding of their likings for and obstacles against the use of the Internet of Things [7]. The survey analyzed the participants' behaviors across a variety of areas, including current IOT adoption, perception, barriers, and plans for future adoption. The outcomes were deconstructed based on demographics, including age, gender, and location [7]. The SANS Institute collected surveys from a broad range of institutes, such as the United States government and the Department of Agriculture [8]. The survey examined the participants' understanding, activity, impacts on their company, and opinions on the security of the IOT [8]. The survey also showed the greatest threats and risks that each company associated with the IOT [8]. Additional literature reviews will be added in the coming months.

3. Background Information

The standard structure of the Internet of Things is not yet firmly established due to the relative newness of this issue and its recent popularity. The Internet of Things is referenced closely with sensor networks, mobile communications, and the Internet to establish a structured foundation to build from when dealing with security. Taking these different structures into consideration, the Internet of Things is currently separated into three layers: the perception layer, the transportation layer, and the application layer [5]. Figure 1 shows a simplistic representation of the layers of the IOT and a brief description of its sublayers and applications.

The perception layer mostly contains data collection, object perception, and object control [4]. From here, the perception layer can be divided into two parts: the perception node (sensors or controllers) and perception network (communicates with the transportation network) [4]. The transport layer of the Internet of Things is the most important layer throughout the entire system, but this layer also has the most risks as stated earlier [4]. The transport layer, which is responsible for transmitting data, has 3 sublayers [4]. The first sublayer is the access layer, which includes wireless

Conference'10, Month 1–2, 2010, City, State, Country.

DOI: 10.475/1234

networks, such as Ad Hoc and Wi-Fi. The next layer is the core network, which is the central part of the telecommunications network. Last is the local area layer, which interconnects computers within a limited area. The vulnerabilities of these layers are Distributed Denial of Service, Trojan horse, and spam [4]. These vulnerabilities can result in information disclosure and even network paralysis [5]. The application layer is responsible for supporting many different business services and recognizing intelligent computation [4]. The application layer also deals with resource allocation in screening, selecting, producing, and processing data as well as becoming a vast and important network (it comes in second to the transport layer), which makes it easier to separate into additional parts. The application layer can be separated into four sublayers: middleware, machine-to-machine (M2M), cloud computing services, and the service support platform [4]. Due to the popularity of the cloud, the application layer can be a very dangerous place to store important data [4].

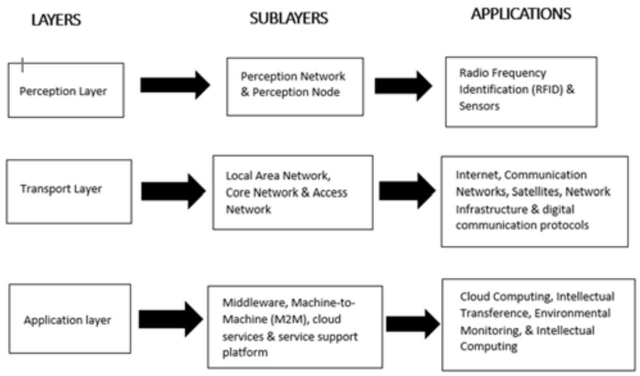
LAYERS
SUBLAYERS
APPLICATIONS
Perception Layer
Perception Network & Perception Node
Radio Frequency Identification (RFID) & Sensors
Transport Layer
Local Area Network, Core Network & Access Network
Internet, Communication Networks, Satellites, Network Infrastructure & digital communication protocols
Application layer
Middleware, Machine-to-Machine (M2M), cloud services & service support platform
Cloud Computing, Intellectual Transference, Environmental Monitoring, & Intellectual Computing

Figure 1.0 – Security Architecture

In this preliminary study, these layers are explained in order to give the reader a better understanding of the security architecture of the IOT. Users that are also victims of cyber-attacks helped us to further implicate which layers are the most accessible to cyber-attacks. Depending on the answers the user provides to the survey, we can pinpoint which layer, sublayer, and application has been breached. In the following section, we will discuss the methodology of the user-perspective survey.

4. Methodology

As part of the user-perspective process, surveys were distributed in order to see if there are any user patterns that may contribute to security issues in the long run. A total of 60 users online and in person were surveyed. Participants were asked questions pertaining to Wi-Fi, the degrees of importance between privacy and protection, and demographic questions as well. Before the survey began, participants were required to sign a consent form for an IRB approved survey. Most participants took less than 5 minutes to complete the survey on paper and online. After the data collection of all surveys, data analysis was performed on all the participants' answers. Preliminary results of the survey are discussed in the following section.

5. Results

Results showed that 98% of users have cell phones and use them to access personal information on password-protected networks. 96% of users reported that they had Wi-Fi in their homes, out of the 96%, 93% of users have password-protected Wi-Fi. Sixty-seven percent of women and sixty-one percent of men in our survey (excluding the participants who were unsure or preferred not to answer) stated that they were victims of some type of attack on their personal information. These attacks included identity theft, credit card fraud, password breaches, distributed denial of service, and the option to enter or describe a different type of security attack. Another very interesting pattern found from our survey is the following: that the privacy and protection of a user's information is very important; however, participants do not believe that their devices are safe from cyber-attacks. 93% of participants stated that the privacy of their information is vital. In addition, 95% of participants said that the protection of their information is also very important. However, 58% of survey participants stated that they are not convinced their devices are safe from cyber-attacks. As precautions, a majority of users have back-up protocols in case their information may be tampered with or stolen.

6. Concluding Remarks

In this paper, we discussed the importance of the concept of the IOT, and the related surveys and background information on the security architecture of the IOT. The security architecture is used to present different layers as we survey participants and further implicate which layers, sublayers, and applications are more susceptible to attacks. Preliminary results indicate that privacy and protection of the user's information are very important to users but that a majority of users do not believe that their devices are convincingly safe. While these findings are preliminary, we believe that's it's a solid start for understanding user-perceptions. The findings of this study are indeed limited and further research needs to be done to make concrete conclusions.

7. ACKNOWLEDGMENTS

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

8. REFERENCES

[1] Janssen, Cory. (N.D.). Internet of Things. DOI = http://www.techopedia.com/definition/28247/internet-of-things-iot.

[2] eMarketer. 2011. The Future of Smart Mobile Devices. DOI = http://www.emarketer.com/Article/Future-of-Smart-Mobile-Devices/1008228

[3] Rivera, J. Van der Meulen, R. 2013. Gartner Says the Internet of Things Base Will Grow to 26 Billion Units by 2020. DOI = http://www.gartner.com/newsroom/id/2636073

[4] Lu, J., Qi, J., Qiu, D., Vasilakos, A.V., Wan, J. 2014. Security in the Internet of Things: perspectives and challenges. DOI = http://link.springer.com/article/10.1007/s11276-014-0761-7

[5] Hui, Suoa. Jiafu, Wana. Caifeng, Zoua. Jianqi, Liua. 2012. Security in the Internet of Things: A Review. DOI = http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6188257&tag=1.

[6] Acquity Group 2014. 2014. The Internet of Things: The Future of Consumer Adoption. DOI = http://www.acquitygroup.com/news-and-ideas/thought-leadership/article/detail/acquity-group-2014-internet-of-things-study.

[7] SANS Institute. 2013. Securing the Internet of Things Survey. DOI = https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.