Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices: A Scalable Approach

Ryan Williams, Emma McMahon, Sagar Samtani, Mark Patton, Hsinchun Chen
Management Information Systems
The University of Arizona
Tucson, AZ 85721, United States
{ryanwilliams12, mcmahone, sagars, mpatton}@email.arizona.edu, hchen@eller.arizona.edu

***Abstract*— The Internet of Things becomes more defined year after year. Companies are looking for novel ways to implement various smart capabilities into their products that increase interaction between users and other network devices. While many smart devices offer greater convenience and value, they also present new security vulnerabilities that can have a detrimental effect on consumer privacy. Given the societal impact of IoT device vulnerabilities, this study aims to perform a large-scale vulnerability assessment of consumer IoT devices exposed on the Internet. Specifically, Shodan is used to collect a large testbed of consumer IoT devices which are then passed through Nessus to determine whether potential vulnerabilities exist. Results of this study indicate that a significant number of consumer IoT devices are vulnerable to exploits that can compromise user information and privacy.**

Keywords—Internet of Things; IoT; vulnerability assessment; IoT security; Nessus

I. INTRODUCTION

Technological advancements have significantly reduced the barrier facing companies looking to design their products with smart capabilities. Internet-enabled devices provide significant value that was not previously available. Consumer devices such as webcams, thermostats, and TVs have all been given Internet capabilities for various functionality. These Internet-enabled devices make up a fraction of what is labeled as the "Internet of Things" (IoT).

The IoT has been dubbed as "the next generation of the Internet" [1]. While definitions vary, the IoT can be described as a combination of technologies, including sensors, actuators, and smart objects with the purpose of connecting "all" things for increased convenience and productivity [2]. The number of IoT devices is growing rapidly, with an estimated 20.8 billion devices being connected to the Internet by 2020 [3].

Unfortunately, many IoT enabled devices suffer from various security flaws that can allow malicious hackers to damage devices [4]. The Internet Census of 2012 scanned the entire IPv4 address range utilizing a botnet of 420,000 routers that had default login credentials, discovering 450 million accessible devices [5]. While the goal of the study was to map the internet, and not assess vulnerabilities, it did show just how insecure much of the Internet's infrastructure is.

Given the societal impact of IoT device vulnerabilities, this study aims to perform a large-scale vulnerability assessment of consumer IoT devices exposed on the Internet. Specifically, Shodan, a search engine for IoT devices, is leveraged to identify over a hundred thousand consumer IoT devices such as smart TV's webcams, and printers. All identified devices are then scanned by Nessus, a state-of-the-art vulnerability assessment tool.

The remainder of this paper is organized as follows. First, we review literature regarding the IoT security concerns and prevailing vulnerability assessment approaches and tools. We then detail our research design and testbed. Subsequently, we summarize our key findings and results. Finally, we offer several promising directions for future research and conclude this research.

II. LITERATURE REVIEW

To form the basis of this research, literature has been reviewed in two areas: 1) IoT, to understand what devices are being connected to the Internet, and 2) vulnerability assessment techniques, to understand approaches for assessing device security.

A. Internet of Things (IoT) Background

At its core, the IoT is a collection of connected devices [2]. While connected devices have been around for a while, what differentiates the IoT is how users interact with these devices. Some IoT devices require very limited interaction from users. Once the device has been set up, sensors allow it to generate data autonomously. Other devices, foster more interaction with the user by providing greater variety of access. An IoT device can be, but is not limited to, TV's with Internet capabilities for media applications, thermostats with sensors to monitor home activity, or webcams that can be viewed and controlled remotely [6].

IoT devices share a common architectural design [7]. Each layer within this design (perception, network, middle-ware, and application) brings its own set of security concerns that must be accounted for. On top of this, significant variations in software and hardware make IoT security a difficult problem to tackle [4]. For this reason, establishing a well-defined security architecture for IoT devices will help their adoption and future device iterations [7].

978-1-5090-6727-5/17/$31.00 ©2017 IEEE

As the IoT grows, these devices will find themselves in an overwhelming number of homes and business offices across the world. Poor security negatively impacts user privacy, making device security a top priority. Unfortunately, user privacy is often not considered when developing smart devices [8]. Performing vulnerability assessments of these devices is imperative in ensuring acceptable security and privacy [9].

B. *Vulnerability Assessment*

A vulnerability is defined as "a flaw within a system, application or service which allows an attacker to circumvent security controls and manipulate systems in ways the developer never intended" [10]. Vulnerability assessments aim to test a computer system, network, or application to identify, measure, and rank vulnerabilities within the system for systematic mitigation [11]. Today, there are dozens of tools (e.g., Nessus, Qualys, Burp Suite) that automatically assess vulnerabilities in various systems. Among these, Nessus is recognized as the gold-standard among the information security community [12]. Nessus is a scalable enterprise-level software with over 80,000 user configurable plugins designed to test vulnerabilities for a variety of devices and applications. For example, Nessus can scan ports, identify web application issues, discover unpatched OS/software, and attempt default credentials. Nessus categorizes each vulnerability into different thresholds of risk ('Critical', 'High', 'Medium', 'Low', and 'None') based on the open industry standard Common Vulnerability Scoring System (CVSS) [13].

III. Research Gaps and Questions

Although IoT literature notes a myriad of possible vulnerabilities afflicting IoT devices, little work has leveraged the maturity of vulnerability assessment techniques to identify IoT vulnerabilities on a large scale. To help address this gap, we pose the following research questions for study:

- Which IoT device categories are most vulnerable?
- What vulnerabilities are consumer IoT devices susceptible to?

IV. Research Design and Testbed

Our research design has three major components: device identification, vulnerability assessment, and results evaluation. Fig. 1 illustrates our design.

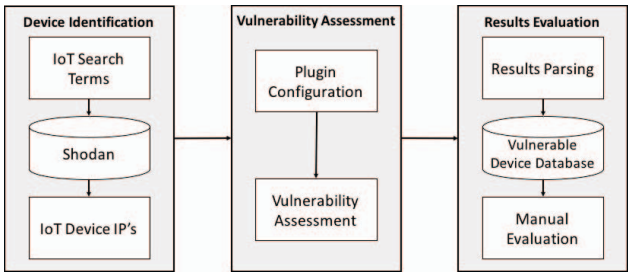

Fig. 1. Research Design Overview

Consistent with prior literature, we select a set of search terms to retrieve IoT devices with the Shodan API [13][14]. Overall, we used 11 keywords (e.g., product:"smart tv") to retrieve 28,085 Smart TV IP's, 21 keywords (e.g., product:"D-Link DCS") to retrieve 102,230 webcam IP's, and 4 keywords (e.g., product:"HP LaserJet") to retrieve 26,365 printer IP's. These devices were chosen because of their pervasive nature and significant potential to compromise consumer privacy if not secured.

We utilized Nessus for vulnerability assessment over other prevailing tools, such as Burp Suite or Qualys, because of its scalability (capable of scanning thousands of devices at a time) and robust set of assessment options. Since IoT devices often differ in hardware and software, we configured Nessus to utilize the majority of its plugins including testing for vulnerabilities in different operating system distributions, web exploits, and default credentials. Three machines with 200 GB storage, 60 GB RAM, and 36 CPUs each scanned selected devices . After scan completion, all results were parsed into a database for further evaluation.

V. Results and Discussion

The results from Nessus showed that 20,237/156,680 (12.92%) consumer IoT devices in our collection have 'Critical', 'High', 'Medium', or 'Low' risks. Out of these vulnerable devices, 2,141/20,237 (10.58%) devices had one or more 'Critical' vulnerabilities, 8,165/20,237 (40.35%) devices had one or more 'High' vulnerabilities, 13,753/20,237 (67.96%) devices had one or more 'Medium' vulnerabilities, and 8,508/20,237 (42.04%) devices had one or more 'Low' vulnerabilities. As the numbers show, some devices have multiple different vulnerabilities at different risk levels. Table 1 summarizes selected vulnerabilities for each device category.

Out of the 20,237 vulnerable devices, 8,127 (40.16%) were webcams. The majority of these devices, 5,852/8,127 (72.01%), were D-Link brand webcams, followed by Axis (9.65%), and AVTECH (7.48%) webcams. 1,437 (7.1%) of the vulnerable devices were smart TVs. The top manufacturer for this category was Samsung, with 382/1,437 (26.58%) vulnerable devices. Finally, 10,675 (52.75%) of the vulnerable devices were printers, with HP being the most common brand at 8,855/10,675 (82.95%).

The most common critical vulnerability for webcams deals with devices running outdated versions of MiniUPnP, a network discovery and communication protocol. This vulnerability can be exploited in several ways, ultimately allowing attackers to perform denial of service attacks using the vulnerable webcam. NAT-PMP detection, the most common high vulnerability among exposed webcams, can allow attackers from outside the network to gain more information about the webcam's network and break into it utilizing the NAT-PMP protocol. Finally, the most common medium vulnerability for webcams is an unencrypted telnet server. Telnet is a network protocol that allows a user to remotely access a computer through a command line interface (CLI). Telnet does not encrypt data transmitted between the user and the remote computer, meaning an

attacker could eavesdrop on the user's communication to the remote host and capture important information such as login credentials.

TABLE I. SELECTED NESSUS VULNERABILITES FOR DEVICE TYPE

Device Type (Total #)	Risk Level	# of Devices	Top Vulnerability Per Risk Level (# of affected devices)
Webcams **(8,127)**	Critical	635	MiniUPnP < 1.4 Multiple Vulnerabilities **(213)**
	High	981	NAT-PMP Detection (remote network) **(310)**
	Medium	3,345	Unencrypted Telnet Server **(859)**
Smart TV's **(1,437)**	Critical	275	SNMP Agent Default Community Names **(58)**
	High	340	SNMP Agent Default Community Name (public) **(256)**
	Medium	1,159	SSH Weak Algorithms Supported **(313)**
Printers **(10,675)**	Critical	1,231	SNMP Agent Default Community Names **(668)**
	High	6,844	SNMP Agent Default Community Name (public) **(5,808)**
	Medium	9,249	Anonymous FTP Enabled **(5,291)**

The most common critical and high vulnerabilities for smart TVs were related to the Simple Network Management Protocol (SNMP). This protocol allows servers to share information about themselves in a structured manner. Often times, the SNMP agent is installed on a system by default without the owner knowing it, making the vulnerability difficult to mitigate. Default community names allow attackers to successfully guess the community string (often "public" to read and "private" to write) needed to authenticate certain actions. With these community names, attackers can gain more knowledge about a device, including its operating system. This information would allow an attacker to utilize known exploits for that OS to cause more harm to that device and network.

Like smart TVs, the most common critical and high vulnerabilities for printers were related to SNMP. As described above, these vulnerabilities can allow attackers to gain more knowledge about a device and subsequently the network it resides on. Since printers are prominent devices found in many homes and offices, this vulnerability is especially dangerous.

VI. CONCLUSION AND FUTURE DIRECTIONS

The IoT is quickly growing as a collection of connected devices with the purpose of creating smarter homes, cities, and infrastructures. While there are many benefits and added conveniences provided by these smarter devices, they also invade our privacy on an unprecedented scale. This study has shown that a significant number of IoT devices, specifically consumer devices, are vulnerable to exploits. Devices in our homes, workplaces, and cities have the potential to collect vast amounts of information about us [15], making these potential exploits all the more concerning.

There are many promising and interesting directions for expanding this research in the future. More device types can be assessed within the IoT space. This could include medical devices, scientific instruments, other consumer IoT devices, and more. Also, a geographical study could be applied to this research. For example, IoT device vulnerabilities can be assessed based on country to determine where the most vulnerable devices are located. These expansions would provide a greater understanding of IoT security flaws and help bring awareness to information security.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. NSF DUE-1303362 (SFS).

REFERENCES

[1] Li, S., & Da Xu, L. (2016). Securing the Internet of The Internet of Things.

[2] IEEE. (2015). IEEE-SA Internet of Things (IoT) Ecosystem Study, 1–35. Retrieved from http://standards.ieee.org/innovate/iot/study.html

[3] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. (2015). Retrieved from http://www.gartner.com/newsroom/id/3165317

[4] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. In Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014.

[5] Internet Census 2012. (2012). Retrieved from http://census2012.sourceforge.net/paper.html

[6] Vermesan, O., & Friess, P. (2014). Internet of Things Applications - From Research and Innovation to Market Deployment. River Publishers.

[7] Farooq, M. U., Waseem, M., & Khairi, A. (n.d.). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7).

[8] Rutledge, R. L., Antón, A. I., & Massey, A. K. (2016). Privacy Impacts of IoT Devices : A SmartTV Case Study, 5, 261–270.

[9] Markowsky, L., & Markowsky, G. (2015). Scanning for vulnerable devices in the Internet of Things. In Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015.

[10] Kennedy, D., Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit. (W. Pollock & T. Ortman, Eds.). William Pollock.

[11] Hu, Y., Sulek, D., Carella, A., Cox, J., Frame, A., Cipriano, K., & Wang, H. (2016). Employing Miniaturized Computers for Distributed Vulnerability Assessment, 57–61.

[12] Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. (W. Pollock, Ed.) (1st ed.). William Pollock.

[13] Samtani, S., Yu, S., Zhu, H., Patton, M., & Chen, H. (2016). Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques, 25–30.

[14] Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited connections: A study of vulnerable devices on the internet of things (IoT). Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014, 232–235.

[15] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4662(c), 1–1.