View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2018 Proceedings | Southern (SAIS)

Spring 3-23-2018

ARE CERTIFIED IOT DEVICES TRUSTWORTHY? A PRELIMINARY INVESTIGATION

Donald A. Privitera
Kennesaw State University, dp1@nn1.us

Lei Li
Kennesaw State University, lli13@kennesaw.edu

Follow this and additional works at: https://aisel.aisnet.org/sais2018

Recommended Citation
Privitera, Donald A. and Li, Lei, "ARE CERTIFIED IOT DEVICES TRUSTWORTHY? A PRELIMINARY INVESTIGATION" (2018). *SAIS 2018 Proceedings*. 4.
https://aisel.aisnet.org/sais2018/4

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ARE CERTIFIED IOT DEVICES TRUSTWORTHY? A PRELIMINARY INVESTIGATION

Donald A. Privitera
Department of Information Technology
Kennesaw State University
dp1@nn1.us

Lei Li, Ph.D.
Department of Information Technology
Kennesaw State University
lli13@kennesaw.edu

ABSTRACT

Internet of Things (IoT) devices have been shown to be insecure in general. There are continuing research and news reports indicating Internet connected devices may contain backdoors either placed intentionally or discovered as vulnerabilities (Korolov, 2014). The backdoors in IoT devices, especially the deliberately hidden ones, present significant security risks to people, our society, and US economy as those devices are internet connected and deployed in massive numbers. US Government and organizations are developing guidelines and certification standards for IoT devices to mitigate risks. In this paper, we investigate the effectiveness of certification in identifying hidden backdoors in IoT devices. The research plan and implications of our study are discussed.

Keywords

Internet of Things, Backdoor, Certified IoT Devices, Security.

INTRODUCTION

There has been exponential growth on the adoption of Internet of Things (IoT) devices in recent years. Moreover, there are forecasted to be over 20 billion IoT devices in 2017 worldwide growing by over 350% to 75 billion by 2025 (I.H.S., (n.d.)). While those "smart" devices bring in many benefits such as improved quality of life and cost savings, they also introduce security risks to our society. Research and new reports show that the IoT devices may contain either purposely or inadvertently placed backdoors. No matter their origins, backdoors can be used by hackers or other malicious parties to gain unauthorized access and subsequently present significant risks to our society, economy, or even national security given the "connected" nature of those smart devices and their massive deployment numbers.

A backdoor is defined by the US National Institute of Science and Technology (NIST) as "An undocumented way of gaining access to a computer system. A backdoor is a potential security risk" (N.I.S.T., 2015). Backdoors in computer systems have the demonstrated ability to affect the real world. For example, an iron factory in Germany experienced a damaging explosion caused by a computer controlled blast furnace because hackers exploited vulnerabilities, gained unauthorized backdoor access to company computer systems, and programmed the blast furnace in errant manner (BBC News, 2014).

There are two types of backdoors: inadvertent and intentional. Inadvertent backdoors are often caused by bad software practices and are relatively easy to detect. On the other hand, intentional backdoors that are embedded in the system by design, are often the results of government mandates, debugging reasons, rogue programmers, or covert nation-state Information Warfare espionage and infiltration. It is conceivable that there could exist widespread undiscovered intentionally placed and hidden backdoors in IoT devices which, if coordinated on a large scale, could disable or disrupt the fabric of the digital economy.

Government and organizations recognize the cyber security concerns of IoT devices. The White House launched the Cybersecurity National Action Plan (CNAP) in February 2016 (FACT SHEET: Cybersecurity National Action Plan, 2016), and Underwriters Laboratory followed up with a certification standard UL 2900, for network-connectable products and systems in April 2016 (Canada Newswire, 2016). In May 2016, ICSA Labs also announced a cybersecurity certification standard for IoT devices (Higgins, 2016). However, it's not clear those standards can successfully mitigate the risks associated with hidden backdoors. In this paper, we examine whether these certification programs can be used to effectively detect hidden intentional backdoors in network connected devices.

RESEARCH QUESTIONS

The aforementioned cybersecurity IoT certification standards are mainly focused on black box functional testing of finished products. We argue that such testing isn't sufficient to detect intentionally hidden backdoors. This leads to our first research question.

Can IoT devices that are certified through the use of black box testing methods, be trusted to be free from intentionally placed and hidden backdoors?

User's awareness of the security vulnerability is very important part of the overall security strategy. We like to collect people's perceptions on the backdoors in IoT devices. We are also interested in finding out if security professionals and ordinary users will respond different to the survey questions.

What are the security professionals' opinions on the backdoors in IoT devices and associated risks? What are the ordinary users' opinions on the backdoors in IoT devices and associated risks?

RESEARCH METHOD

We designed a survey to collect people's perceptions on the backdoors in IoT devices. The survey instrument includes three types of questions: 1) background information and experience level in security; 2) assessment of general security threats; 3) assessment of risks specific to backdoor in IoT devices. In regards to respondents, we will use college students as being representative of ordinary users and use the participants in a national security conference as the pool for the security professionals.

To test the effectiveness of the certification program on IoT devices, we first establish a clear understanding of the testing methods listed in publicly accessible UL 2900 standard and ICSA Labs IoT Certification. We then examine literature in software testing as well as in detection of the backdoors in network-connectable devices. Finally, we will develop a logical proof on the effectiveness of IoT certification programs from UL and ICSA Labs.

DISCUSSION

Our research is in progress. We developed the survey and administrated it to the attendees of the Blackhat and DEFCON 2017 conventions in Las Vegas which is a national conference for security professionals. The results of the survey are compiled and we conducted additional data analysis at this point. We also plan to distribute the questionnaire to college students and compare the results of those two groups. We gained access to UL 2900 standard and are conducting analysis on its testing methods.

Our study, once completed, will not only raise people's awareness on the hidden backdoors issues in IoT devices, but will also benefit the IT Security community by highlighting the limitations of certifications based on black box testing and inspiring more research on more effective ways in detecting hidden backdoors in network-connectable devices.

REFERENCES

1. BBC News. (2014) Hack Attack Causes "massive damage" at Steel Works, Retrieved from: http://www.bbc.com/news/technology-30575104
2. Canada Newswire. (2016) UL Launches Cybersecurity Assurance Program, *Canada Newswire*.
3. FACT SHEET: Cybersecurity National Action Plan. (2016) *Office of the Press Secretary*, Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
4. Higgins, K. J. (2016) New Internet Of Things Security-Certification Program Launched. *DARKReading*, Retrieved from: https://www.darkreading.com/iot/new-internet-of-things-security-certification-program-launched/d/d-id/1325676
5. I.H.S. (n.d.) Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions). *In Statista - The Statistics Portal*, Retrieved from: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
6. Korolov, M. (2014) Major Chinese Smartphone Manufacturer Installed Backdoor on up to 10 Million Devices, Retrieved from: http://www.csoonline.com/article/2861116/malware-cybercrime/major-chinese-smartphone-manufacturer-installed-backdoor-on-up-to-10-million-devices.html
7. N.I.S.T. (2015) Guide to Industrial Control System (ICS) Security, (Special Publication (SP) 800-82 Revision 2.), *National Institute of Standards and Technology*, Retrieved from: http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf