CAN IOT DEVICES BE TRUSTED? AN EXPLORATORY STUDY

Emergent Research Forum (ERF)

Donald Privitera
Kennesaw State University
dp1@nn1.us

Lei Li, Ph.D.
Kennesaw State University
lli13@kennesaw.edu

Abstract

The adoption of Internet of Things (IoT) devices has grown exponentially in recent years. There are increasing concerns on the security of those Internet connected devices. Research studies and news reports indicated IoT devices may contain backdoors either placed intentionally or discovered as vulnerabilities. US Government and international organizations are developing guidelines and certification standards for IoT devices to mitigate risks. In this paper, we studied IT professionals’ perception on the security risks of IoT devices by surveying the attendees of a large security profession conference. Moreover, we propose to investigate the effectiveness of IoT certification in identifying hidden backdoors in IoT devices. The research plan and implications of our study are discussed.

Keywords


Introduction

There has been exponential growth on the adoption of Internet of Things (IoT) devices in recent years. As illustrated in figure one, the number of Internet connected devices worldwide is forecasted to increase from 20 billion in 2017 to 75 billion by 2025 with the growth rate of 350%(I.H.S. (n.d.)).

Figure 1 - Forecasted Growth of IoT Devices
IoT devices are also known as “smart” devices. These devices contain tiny computers and are connected to a communication network with the Internet being most common type of network (N.I.S.T. 2018). IoT devices include things such as but not limited to routers, smart TV’s, security cameras, smart doorbells, smart refrigerators, smart thermostats, smart light bulbs, smart etcetera. Like all computers, these devices often contain vulnerabilities which make them a security risk. Of concern is that IoT devices generally do not get the rigor involved in the product development cycle to produce a secure product. Secondly, security updates are often rarely applied on a timely basis (let alone if at all). Therefore, any vulnerabilities are generally long lived. Given their massive numbers, this means that if cyber-attacks are coordinated on a large scale, billions of these kinds of devices could be compromised. It is conceivable that this could cause mass disruption affecting the US digital economy.

While IoT devices bring many benefits such as improved quality of life and cost savings, they also introduce security risks to our society. Research and news reports show that the IoT devices may contain both intentionally and unintentionally placed backdoors. No matter their origins, backdoors can be exploited by the 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 are embedded in the system by design. For example, researchers in 2012 created a novel method of scanning silicon and discovered an undisclosed intentional backdoor built into the actual silicon of a popular Field Programmable Gate Array (FPGA) chip made outside the US but used for US critical applications (Skorobogatov and Woods 2012). This implies that many more digital chips used in IoT devices could have undetected intentional backdoors hidden in their logic waiting to be exploited.

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 be used to disable or disrupt the fabric of US (or global) digital economy. For example, banks have reduced staff as their customers have adapted to using online banking functions. Should a massive disruption occur, banks would not be able to accommodate the needs of consumers at their branches. As another example, if household routers and smartphones were to have a hidden backdoor triggered that erased their firmware, the devices would forever stop working (also known as being “bricked”) which would be an example of loss of availability and the result of which could be catastrophic.

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, International Computer Security Association (ICSA) Labs also announced a cybersecurity certification standard for IoT devices (Higgins 2016). However, it is doubtful those standards can successfully mitigate the risks associated with hidden backdoors. As a point of note, Section 1 Scope of UL 2900 establishes limits of the standard as “This standard applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware” (Underwriters Laboratory 2017). The standard further goes on the establish limits for the standard, “... this standard contains no requirements to verify that the product functions as designed” (Underwriters Laboratory 2017). If a design includes a backdoor which is designed to be covert, then it stands to reason that UL 2900 by UL’s own definition would not be able to detect such a backdoor.

In this paper, we conduct an exploratory study to investigate people’s perception on the security risks of IoT devices and effectiveness of the certification programs on identifying intentional hidden backdoors.
Research Questions

User’s awareness of security threats and vulnerabilities is an important part of any security strategy. Despite the news stories concerning the security risks of IoT devices, what do people and community really think of backdoors, especially hidden backdoors in network-connectable devices? In addition, it is also interesting to compare the perceptions of common users and security professionals. This leads to following research questions.

1) What are the security professionals’ opinions on the backdoors in IoT devices and associated risks?
2) What are the ordinary users’ opinions on the backdoors in IoT devices and associated risks?

There are two major certification standards being proposed to address the security concerns of IoT devices: UL 2900 and ICSA Labs IoT Security Testing Framework. We propose to examine the testing methods used in those two standards and determine the effectiveness of the certification in detecting backdoors in IoT devices. This leads to the third research question.

3) Can IoT devices that are certified through UL 2900 or ICSA Labs, be trusted to be free from intentionally placed and hidden backdoors?

Research Design

We employ empirical methods in this study given the nature of our research. A questionnaire is developed to collect participants’ perceptions on IoT devices security issues. The survey instrument includes three types of questions: 1) background information and experience level in security; 2) assessment of general security threats and vulnerabilities; 3) assessment of risks specific to backdoors in IoT devices. In terms of respondents to the survey, we recruit college students as representatives of common users and the attendees from two national security conferences as the pool for the security professionals.

To test the effectiveness of the certification programs 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.

Preliminary Results

A survey was developed and administered to the attendees of the BlackHat USA 2017 and DEF CON 25 conferences held in August 2017 in Las Vegas, Nevada. BlackHat and DEF CON are international conferences hosted for security professionals with more than 40,000 attendees combined. To increase the participation rate, 120 hardcopies of surveys were personally administered to BlackHat and DEF CON attendees who had badges displayed on their person and who were standing in various lines around the conferences. The survey administrators stood by while the participants completed their surveys. We received back 113 completed surveys. Seven surveys were returned over half incomplete and not counted. The completion rate is 94%.

Our survey respondents are from thirteen different countries and an overwhelming majority (82%) are from the US. 46% of respondents have a bachelor’s degree as their highest level of education and 38% of them have a graduate degree or higher. 75% of the respondents reported that they have a technical role in the cybersecurity industry with a broad range of expertise and respondents were categorized as technical respondents. The other 25% were categorized as non-technical respondents. Most of the respondents (66%) have more than 5 years working experience in the security industry and 48% of them have worked in security field more than 10 years.

Regarding levels of expertise within the cybersecurity industry across 20 cybersecurity categories, respondents rated themselves on an integer scale from 0 (no experience) to 5 (expert). The top 5 categories that technical respondents indicated their highest average scores were in “computer security” (3.43), “network security” (3.07), “security architecture” (3.01), "encryption" (2.69), and "data security" (2.66).
Non-technical respondents had a slightly different result: “security consulting” (2.72), “computer security” (2.68), “network security” (2.60), “intrusion prevention” (2.48), and data security (2.40).

Among respondents concerns about security risk as it applies to a scope of geography, the respondents indicated their concerns on an integer scale of 0 (no concern) to 5 (grave concern) ranging from the individual to local to regional to national to global. Technical respondents felt that “national security” and “individual security” both tied as a top concern at (3.87), followed by global security (3.71), regional security (3.11), and local security (2.93). Non-technical respondents had similar thoughts but did not quite feel as concerned as their technical counterparts about “individual security”. Their scores are as follows “national security” (3.85), “global security” (3.64), “individual security” (3.47), “regional security” (3.03), and “local security” (2.94).

On the same scale as above, in regard to a focus on US cybersecurity risk areas, technical respondents felt the following were most concerning: “infrastructure” (4.04), “digital economy” (3.55), “government” (3.41), “military” (3.18), “businesses” (3.15), “entire economy” (3.14), and lastly “civilians” (2.81). Non-technical respondents ranked the same categories as follows: “infrastructure” (4.00), “government” (3.91), “businesses” (3.85), “military” (3.67), “digital economy” (3.61), “entire economy” (3.36), “civilians” (2.97).

The respondents also rated their concerns on various different types of security vulnerabilities on a 0 (no concern) to 5 (grave concern) integer scale. Their responses sorted based on rated security concerns of technical respondents, were shown in table one. Not surprisingly, technical respondents seem to have better understanding of the security vulnerabilities than the non-technical respondents as the range of technical respondents’ rated concern level score is wider than the ones of non-technical group. The top three security vulnerability are the same for both groups: OS unpatched exploits, spear-phishing attacks, and phishing attacks. Internet of Things exploits, and Backdoors hidden in digital connected devices are in the middle of the pack among the list of the vulnerabilities. Both technical and non-technical respondents indicated that significant risks introduced by those two vulnerabilities. Moreover, 56% of all technical respondents and 65% of DEF CON respondents thought that foreign made IoT devices could present a high to grave risk to US national security. 56% of BlackHat technical respondents felt that it could take longer than 90 days to recover from an attack involving millions of devices (three orders of magnitude less than the billions of IoT devices already in use).

<table>
<thead>
<tr>
<th>Security Vulnerability</th>
<th>Technical Respondents</th>
<th>Non-tech Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS unpatched exploits</td>
<td>4.24</td>
<td>4.03</td>
</tr>
<tr>
<td>Spear-phishing attacks</td>
<td>4.06</td>
<td>3.78</td>
</tr>
<tr>
<td>Phishing attacks</td>
<td>4.05</td>
<td>3.8</td>
</tr>
<tr>
<td>Malware software</td>
<td>3.84</td>
<td>3.62</td>
</tr>
<tr>
<td>Browser unpatched exploits</td>
<td>3.8</td>
<td>3.43</td>
</tr>
<tr>
<td>Web apps unpatched exploits</td>
<td>3.77</td>
<td>3.48</td>
</tr>
<tr>
<td>Internet of Things exploits</td>
<td>3.74</td>
<td>3.47</td>
</tr>
<tr>
<td>Backdoors hidden in digital connected devices</td>
<td>3.72</td>
<td>3.57</td>
</tr>
<tr>
<td>Cloud unpatched exploits</td>
<td>3.59</td>
<td>3.68</td>
</tr>
<tr>
<td>OS zero-day exploits</td>
<td>3.59</td>
<td>3.79</td>
</tr>
<tr>
<td>Browser zero-day exploits</td>
<td>3.48</td>
<td>3.21</td>
</tr>
<tr>
<td>Web apps zero-day exploits</td>
<td>3.36</td>
<td>3.28</td>
</tr>
<tr>
<td>DNS unpatched exploits</td>
<td>3.33</td>
<td>3.59</td>
</tr>
<tr>
<td>Cloud zero-day exploits</td>
<td>3.3</td>
<td>3.39</td>
</tr>
<tr>
<td>DNS zero-day exploits</td>
<td>3.22</td>
<td>3.38</td>
</tr>
</tbody>
</table>
Table 1 - Respondents’ Concern Level on Common Security Vulnerabilities

We also asked our respondents on methods to detect hidden backdoors in IoT devices. The generally accepted method for assuring software source code trust is via source code analysis and formal verification (Hartnett 2016). A substantial number of respondents, 84% of technical and 88% of non-technical, thought that source code analysis was important, more-than-important, or absolutely vital for cybersecurity purposes. In addition, 59% of technical respondents and 71% of non-technical respondents felt that testing such devices would be somewhat to not effective without source code analysis.

Discussion and Future Work

In this paper, we investigate the people’s perceptions on the security risks of hidden backdoors in IoT devices and ways to detect those backdoors. Our preliminary survey results showed IT security professionals indicated significant concerns on the vulnerabilities brought by the hidden backdoor and in efficiencies of current testing methods in detecting the hidden backdoors in IoT devices. Our research is in progress. We plan to distribute the questionnaire to college students in a large public university in southeast of US and compare the survey results of college students and IT security professionals. We gained access to UL 2900-1 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


Canada Newswire. 2016. UL Launches Cybersecurity Assurance Program, Canada Newswire.


