Combat security and privacy challenges of the Internet of Things, as an intelligent system

1st Haydar Teymourlouei  
Department of Technology & Security  
Bowie State University  
Bowie, USA  
hteymourlouei@bowiestate.edu

2nd Daryl Stone  
Department of Technology & Security  
Bowie State University  
Bowie, USA  
dstone@bowiestate.edu

Abstract— The prominent recent trend of making everything smart entails simple gadgets newly acquiring digital personalities and communicating among themselves and the outside world alike. Numerous types of IoT devices that perform ubiquitous sensing and activation are already on the market. Inherent resource limitations coupled with the speed of development and deployment cause many IoT devices to suffer from design and implementation vulnerabilities that can harm both the security and privacy of users. How can we detect vulnerable devices? How can malware be detected on an IoT devices remotely but with the challenge of hackers not close to the device? How can we remove important information and data from an IoT device without compromising the security of that information? What is the most efficient way for the machine to detect data breaches automatically with the use of an event logger? To this end, the goal of this research project is to develop and evaluate new techniques for securing IoT devices, such as Amazon’s Alexa, and networks throughout their entire life process and expectancy.

Keywords— Internet of Things, Security, Network, Vulnerabilities, Intelligent System

I. BACKGROUND

The applications of Internet of Things to our family, including our home and healthy habits in our daily life, are said to be the most useful in that it contributes to human life. The concept of IoT also uses in smart cities, where applications have used for acute lighting, surveillance cameras, cartage control, centralized & chip arrangement ascendancy and more. It mainly implies internet connectivity of things such as smart appliances or devices, sensors, actuators, communication protocols, big data management and analytics. Current, IoT produces large volumes of data, with the consequent need for collection, aggregation, processing and storage more effectively. IoT is projected to balloon to “50 billion” connected devices by 2020 [10]. Although these smart devices continue to transform our homes, healthcare, transportation, information technology and energy infrastructure, each new device adds to the potential attack surface for hackers and criminals. The Federal Trade Commission (FTC) on January 2015 report expressed security concerns regarding consumers’ use of IoT devices such as enabling unauthorized access, misuse of personal identification, expediting attacks on other systems [5].

IoT field is very vast in nature where the applications have seen from three different aspects: Internet-oriented applications, things-oriented applications and semantic oriented applications. In the context of these aspects, IoT has faced various challenges. The infrastructure of IoT is based on heterogeneous devices where different types of embedded sensor nodes based on low power systems. Building end-to-end security into IoT design is a lofty goal but one manufacturer’s must aim for to ensure an acceptable level of trust in their products [3]. The problem of IoT, it is an aggregation of many technologies, which makes the threat map and attack surfaces far larger. Correspondingly, there is no privacy because equipped has been keeping tracking the stocks and inform the householders whenever food needs to be replenished. However, these features are relevant for the life quality improvement, but for other purposes like energy demand side management or device performance, they are not relevant or enough.

II. INTRODUCTION

The Internet-of-Things (IoT) is a network of interconnected devices, systems and services within the existing Internet infrastructure [4]. The core of the IoT is that it allows for “all things connected” in the communication between devices and objects, creating a more direct integration between the physical world and computer-based systems. In IoT networks, the devices are controlled by existing communication systems and provide more benefits to the user by making the integration between computer-based systems and physical world. These technologies are offering more promotional, effective, and precise advantages to the users [1]. Different types of devices are available to make the data communication in the network with extraordinary characteristics due to their embedded computational systems.

IoT has found its way into offices, factories, nuclear power plants, and electric grids as personal computers, servers, routers, switches and supervisory control and data acquisition process controls [2]. The integration of these smart devices with software applications that power their network connectivity, sensors, large-scale analytics, social information sharing platforms, and cloud storage has created a new wave of embedded systems. The speed of adoption of IoT and the technological and social shifts it has generated remains unprecedented.
III. IOT PROS

The Internet can provide any information that we need via its search engines from various developers like Google is the most popular engine. The IoT can be used in almost any circumstance in which human activity or machine function can be enhanced by data collection or automation [6]. Everyone including consumers can use IoT devices to collect personal information towards monitoring health and automating household functions, among other things. Industry can use IoT devices to optimize processes and generate cost savings. Communities and other public sector entities can use IoT devices to address concerns such as changes in the environment.

IoT is rapidly changing the digital landscape and becoming the basic element of business technology; its IoT integration and adoption has occurred in several key areas of the society such as smart life, smart mobility, smart city and smart manufacturing. IoT applications are presently altering our lifestyles by saving time and resources and creating new chances for growth, innovation and knowledge transfer. In 2016 there were about “5.5 million new things being connected to the internet every day and by 2020 it is expected reach “20 billion” new devices daily [19]. The below is a chart depicting the evolution of how the IoT is growing.

<table>
<thead>
<tr>
<th>Category</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive</td>
<td>96.0</td>
<td>105.6</td>
<td>97.3</td>
<td>7,311.1</td>
</tr>
<tr>
<td>Consumer</td>
<td>1,941.1</td>
<td>2,244.5</td>
<td>2,074.9</td>
<td>13,172.5</td>
</tr>
<tr>
<td>Generic Business</td>
<td>352.2</td>
<td>475.4</td>
<td>625.9</td>
<td>3,156.0</td>
</tr>
<tr>
<td>Vertical Business</td>
<td>695.7</td>
<td>836.5</td>
<td>1,094.4</td>
<td>3,184.4</td>
</tr>
<tr>
<td>Grand Total</td>
<td>3,022.0</td>
<td>3,750.0</td>
<td>4,080.6</td>
<td>25,066.6</td>
</tr>
</tbody>
</table>

Source: Gartner (November 2014)

Fig.1. IOT by category [16]

IV. IOT CHALLENGES

After all the benefits and usefulness that Internet brings to people, there are challenges that individuals are having with Internet of Things. The smarter Internet of Things become, the more privacy and security concerns are raising, and people are now facing more cyber or Internet attack than before [19].

A. Privacy

Privacy means to respect customer’s information and their rights to determine how such data is used. Accountability, a key privacy principle is difficult to keep with IoT generated data because of the involvement of multiple stakeholders such as device manufacturers, third party applications and social platforms who collect, use or exposed data. IoT can jeopardize a person’s expectations of privacy in many ways as shown in Riley v. California.

B. Security

Data collected from IoT devices may not be restricted from being sent across jurisdictional boundaries as these devices communicate by using the Internet, and the Internet spans different jurisdictional boundaries. IoT devices can gather people’s data in one jurisdiction, transmit and store that information in another jurisdiction for processing and storage. This can become a legal problem if the data collected is private and sensitive and subject to data protection laws in multiple jurisdiction [14]. Encryption may be a requirement in one jurisdiction but not required in another jurisdiction.

C. Detect Vulnerable Devices

IoT devices are used across multiple sectors and by various groups and individuals to inform future actions and decision-making. Most of the IoT devices have vulnerabilities which provides easy path for hackers to attack. Design vulnerabilities are weaknesses resulting from a failure to include proper security measures when developing the IoT device [18]. It is obvious that consumer devices for instance, home and appliance monitors, automobile black boxes, personal health monitors, smartphones can have security and privacy challenges. Employee monitors generate huge amount of valuable data about their users’ activities, habits, personalities, preferences and attributes. This goes to expose the serious dangers of these IoT devices despite their flurry of benefits to mankind.

It is important to use artificial intelligence to monitor traffic in and out of each connected device and alert the network security professional when an attack is attempted, proactively blocking it in real time before any access can be gained and damage done. Also, intrusion-detection systems monitor an organization’s entire network with a mixture of human behavior and device behavior. By modifying IDS with AI (Artificial Intelligence), protection now can focus on the behavior of individual devices. The attack surface will be increased exponentially with each device that is added to a network. Because not only will devices increase, vulnerabilities, cyber-attacks, and thieves who will take benefit will increase proportionately.

V. DETECT MALWARE ON AN IOT DEVICES REMOTELY

Security should be one of the top priorities of any organization, if not the top priority. There many attacks take place like Target retailers’ company-wide cyber-attack that resulted in millions of dollars-worth of damages. These setbacks are devastating, and smaller companies have far less room for error than major businesses such as Target [9]. But the implementation of proper security should not just be limited to businesses and companies. Proper hardening should happen on personal networks and devices. Due to the estimated “30 billion dollars” increase in connected devices just over the horizon action is going to need to be taken now to secure that future [7]. Using AI (Artificial Intelligence) to differentiate between normal and abnormal communications, professionals can watch the device’s network behavior in real time and determine if the device is listening to or talking to networks, servers or people that it should not be. Therefore, when a hacker attempts to send malicious commands to a vulnerable device, the communication can be blocked or quarantined before the device is retrieved or controlled. The device remains unchanged, functionality is uninterrupted, and a dashboard alert is sent to the network’s security manager immediately.
A. Remove important information and data from an IoT device

iPhone is an IoT device that could be very vulnerable. A lot of people do not realize that iPhone logs and tracks cellphone location constantly. Apple also uses a similar voice recognition Amazon for its “Hey Siri” feature, which waits for triggers (in this instance, “Hey Siri”) to activate, record and listen to features. This means you can use various ways to remove important information and data from an IoT device [13].

VI. Secure IoT

Although there are many pros to having the latest technology there are cons as well. These cons include having your personal information stolen and someone easily finding out where you live. It is significant to protect our devices from security and privacy challenges. These are some methods to secure the IoT includes:

• Not connecting devices unless you need to: consider the functionality of the device, just because it can connect does not mean person have to connect it [10].
• Create a separate network: many routers support guest networking so that other users can connect to the network without gaining access to shared files or other network devices. This separate network can be used for devices with questionable security.
• Picking strong passwords and using a different password for all devices: when picking a password, it is important to make sure that is strong and not easily guessed like your age. Last, it is necessary to avoid using the same password for all devices [11].
• Chose reputable vendors when buy smart devices: when buying a new device purchase it from a vendor with a good reputation.

VII. Methodology

Attackers are always examining the Internet of Things everywhere and look for vulnerabilities. Many people are starting to become concerned about the sensitive information and their personal activities being collected by websites and devices. The implications for personal security are likely to be complicated. Criminals who are able to hack into such systems, could find out when a person is not home and that person can be “burglarized or possibly disable systems or spoof them into thinking everything is all right” [15]. Potential susceptibilities of the new connected devices could be exploited by terrorists or others to cause actual physical harm, including overloading devices to cause fires, or taking control of vehicles and crashing or disabling them. The following are methodologies which they will use to combat security and privacy challenges of the Internet of Things, as an intelligent system.

A. TOR Software

Tor (the Onion Router) is a software tool that users can use to defend against traffic analysis. “Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security” [8]. You can use Tor to keep websites from tracking you or your family members. Tor’s onion services allow users to publish web sites and other services without giving the information about your location. People also use “Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses”.

Tor protects you from traffic analysis that others can see from the internet. “Tor’s users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy” [8]. Tor can also allow companies to have an employee to connect to their home websites in another country without allowing anyone to know their location or company. Tor is used for a building hinder for software designers to make new specialized instruments with worked in privacy highlights.
B. Amazon’s personal assistant “Alexa”

In this paper we are going to look at a very popular IoT device that we personally believe are the most vulnerable to privacy. Amazon’s personal assistant, Alexa, is an IoT that uses voice recognition to complete demands. A device like that uses the microphone to complete these tasks. If someone were able to get into your network at home, they could map all the devices that are connected to the network and connect to your Alexa. From there, they can reprogram your Alexa, causing it to record any and everything you say based off key words or phrases.

Regarding Amazon’s Alexa personal assistant, the first one would be to change the wake word, the word that activates Alexa’s microphone to record and save data. Amazon also logs every time Alexa is activated. This info is saved to your Amazon account, and you can delete this information and review. A recommendation would be to review and delete what you are saving.

C. CyberGhost VPN

One of the issues with the Internet of things regarding security and protection is the way that everything is associated. Typically for such huge numbers of gadgets to speak with one another, the gadgets need to know where every gadget is located. This is when the GPS’s availability comes in. This steady requirement for an area to be required could represent an extraordinary risk. With a consistent area necessity, if a talented programmer could get your geolocation constantly, that data could be sold to individuals, for example, cheats or individuals meaning to hurt you. To battle this, one could utilize a VPN administration, for example, CyberGhost VPN. With CyberGhost VPN, for instance, the IP address of the gadget that is associated with the web would be changed to one that is not at your genuine area.

It does this by giving an immediate association from your PC to the web with the utilization of a passage convention. CyberGhost VPN goes about as a passage for the data bundles to go through and instantly ends an association when an interruption is identified and reconnects utilizing an alternate course, or totally new courses.

D. Turbo VPN

In addition to Ghost VPN, using Turbo VPN assist with preventing access to your Alexa devices. It is necessary to use a VPN or a secured WPA2 that you use to connect your Alexa device. This makes it difficult for any hacker to access your network and gain access to your device to actively record what you are saying. For your iOS device, we recommend turning off the “Hey Siri” function entirely, especially because you carry your phone with you almost everywhere. As far as tracking your location, we recommend either disabling the significant features or periodically clearing the logged locations so that people are unable to track your whereabouts [17].

To test one of these methods, we chose to use the free VPN, Turbo VPN, on a smartphone. Turbo VPN had a lot of great...
reviews and millions of downloads, thus we selected it for our research. As you can see in the first image, figure 7 shows the check for the address on Google Chrome, while figure 8 shows the activation on Turbo VPN. Without Turbo VPN, the correct IP address was revealed. However, figure 9 confirms the IP address was changed, the correct IP address not revealed, thus meaning the Turbo VPN worked. Installing and activating Turbo VPN draws from the user’s knowledge to install software. Thus, novice users are able to install VPNs, once they are aware of its importance.

**E. UPnP**

To implement added protection to devices on the IoT, we highly recommend turning off or disable universal plug and play because it is an easy opening for hackers. “UPnP is a convenient way of allowing gadgets to find other devices on your network and if necessary modify your router to allow for device access from outside of your network. Via the Internet Gateway Device Protocol, an UPnP client can obtain the external IP address of for your network and add new port forwarding mappings as part of its setup process”.

A user should disable UPnP because it does not require any kind of validation from the client meaning any application can ask the router to forward a port over UPnP. If individuals do not use their devices for port forwarding or gaming, they should disable UPnP completely. If users have UPnP enabled, their device will be exposed, which allows a hacker to find and gain access to their personal devices. To disable this feature, it varies depending on the device being used. We recommend checking the device manual or researching the web. To disable UPnP on a Windows 10 system, go to the Control Panel then click Network and Sharing Center, then on the left pane click change advanced sharing settings. Finally, select the option to turn it off and click save changes at the bottom of the page. See the picture below.

**VIII. CONCLUSION**

IoT devices are some of the most convenient and technologically advances devices available to users. However, users should be made aware that IoT devices are prone to hacking attacks. They are riddled with vulnerabilities: from their weak user interface to their unencrypted packets. You must go out of your way to protect your IoT devices. There are a few methods that everyone can employ to protect their IoT devices. They can hide their network or get encryption software for their Wi-Fi network. If you have a phone, you can use a VPN to protect yourself from attacks. We suggest Cyber Ghost and Turbo VPN. In conclusion, IoT devices have a lot of security
challenges but, coupled with some out of the box security methods, they can bring extreme convenience to the users.

REFERENCES


