FIREWALL FOR INTERNET OF THINGS

Student Name: Srishti Sengupta Roll Number: 2013108 Student Name: Naman Gupta Roll Number: 2013064

BTP report submitted in partial fulfillment of the requirements for the Degree of B.Tech. in Computer Science & Engineering

on April 18, 2017

BTP Track: Research

BTP Advisors Dr. Vinayak Naik (Thesis Advisor) Dr. Donghoon Chang (Internal Examiner) Dr. Subhadip Raychaudhuri (Internal Examiner)

Indrapras
tha Institute of Information Technology New Delhi

Student's Declaration

We hereby declare that the work presented in the report entitled "Firewall for Internet of Things" submitted by me for the partial fulfillment of the requirements for the degree of *Bachelor of Technology* in *Computer Science & Engineering* at Indraprastha Institute of Information Technology, Delhi, is an authentic record of my work carried out under guidance of **Dr. Vinayak Naik**. Due acknowledgments have been given in the report to all material used. This work has not been submitted anywhere else for the reward of any other degree.

•••••

Place & Date:

Naman Gupta

Srishti Sengupta

Certificate

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Dr. Vinayak Naik

Place & Date:

Abstract

With the advent of the Internet of things, privacy and security of sensitive data has become a major concern. IoT devices generate a lot of data, and we need this data to go over the Internet in a secure manner. To solve privacy and security concerns we demonstrate a solution to monitor all home IOT devices and their communication using a simple Dashboard.

Keywords: Security, Internet of Things, Privacy

Acknowledgements

We would like to thank Dr.Vinayak Naik for his guidance as an advisor and mentor. This project has been a great learning experience and has broadened our mind.

The work was presented as a poster at the COMSNETS 2017 conference, Bangalore. We are thankful to the precious reviews and feedback from the evaluators of the conference. Friends and family have my eternal gratitude for all their love and support.

Work Distribution

Both have put in equal efforts and contributed equally to the work. Srishti Sengupta worked on literature review and Snort configuration/ PCAP analysis. Naman Gupta worked on the Dashboard implementation.

Contents

1	Lite	erature Survey	1
	1.1	Literature Review	1
	1.2	Background	2
2	Intr	oduction	3
	2.1	Problem description	3
	2.2	Recent attacks	3
	2.3	Existing solutions	4
	2.4	Our work	4
	2.5	Organization of this report	4
3	Imp	lementation	5
	3.1	Details about the Firewall	5
	3.2	Details about the Dashboard	7
4	Disc	cussion	12
	4.1	Conclusion	12

Literature Survey

We read a few papers in the previous semester to understand the work which has already been done in the field of security in the Internet of things. The relevant information is summarized in this section.

1.1 Literature Review

Altolini et al. [1] focus on security functionality in the link layer. They implement encryption and authentication mechanisms in software, and exploit a few hardware ciphers as well. The paper also discusses the memory footprint, execution time and relevant trade offs of various implementation modes. The purpose of IoT is to provide wireless communication to various physical objects which we use daily, and therefore is pervasive by nature since sensitive data is collected. Hence, it is crucial to ensure integrity, confidentiality and authentication of this data. The paper implements a MAC strategy to make battery last longer in resource constrained WSN (Wireless Sensor Network) nodes. The primary idea is to let the nodes sleep for the maximum amount of time, and wake up periodically for a small fraction of time where it senses the channel for data transmission. If it detects transmissions, it continues to receive the packet, else sleeps again.

Babar et al. [2] defined taxonomy and the principles to implement a safe IOT system (Objectives networking requirements, security requirements, threat taxonomy etc). Related work includes various frameworks for providing access control, authentication and authorization. The paper is very broad and covers only the principles of secure system, without any example of a real life system.

Brachmann et al. [3] talk about providing a secure end-to-end tunnel at the transport layer of smart devices in a Low-power and Lossy Network (LLN). This would be done by means of protocols such as 6LoWPAN and CoAP. It describes several attacks at transport layer against a LLN, launched from the Internet. It also introduces approaches to ensure E2E security between two devices located in homogeneous networks using either HTTP/TLS or CoAP/DTLS by proposing a mapping between TLS and DTLS. The key takeaways are 6LoWPAN, CoAP, DTLS, 6LBR, WAP, WTLS, ITLS. It also speaks about 'resource exhaustion attack' and how DTLS prevents it.

1.2 Background

Snort is an open-source intrusion detection system (IDS) which we have used for getting alerts and logs about the connections an IoT devices makes.

Before going ahead with Snort IDS which a signature based IDS, we tried using Bro which is a behaviour based IDS. In Snort rules are written on the basis of existing knowledge about attacks. In case any event matches a Snort rule, an entry corresponding to it is made in the alert file. Bro, on the other hand captures a series of events, after which a Bro-script tries to detect anomalous behaviour, if any. [6]

After going over a lot of options, we narrowed down to Snort and Bro. Bro was complicated to set up, whereas Snort is more user friendly and has greater community support. Moreover, Snort provided us with a signature based IDS which was more beneficial to us as compared to Bro.

We have used Django to implement our web based application. Django is a free and open-source web framework, written in Python, which follows the model-view-template (MVC) architectural pattern.

Introduction

2.1 Problem description

A lot of devices are connected to the Internet in a home-network scenario. This is called the Internet of Things. These IoT devices are mostly sensors which are low powered, low compute and have limited resources. Therefore, they may not support encryption which is a very expensive task. The task of these IoT devices is to send sensor data to a cloud service. In this case, an adversary may sniff the packets and reconstruct the data leading to potential risks. The data from IoT devices is usually sensitive information like body parameters from fitness trackers, camera feed from homes and so on. Moreover, IoT devices are made cheap and not many companies provide an additional layer of security in order to reduce the price. It may be so that they come with default credentials which a naive user may not even change. These factors (any many more) lead to potential security risks which one would like to prevent otherwise.

To understand anomalous behaviour, and insecure communication we need to monitor all the IoT devices. Currently, there exists no such open source platform or dashboard where one can monitor the communication and data usage of their IoT devices in a home network.

2.2 Recent attacks

We studied the recent attacks on Dyn DNS service, which is touted to be the largest IoT-based DDOS attack in the history. We interacted with the hacker news community to consolidate information about the attack. The creator of the 'Mirai botnet' released the source code behind the attack and open-sourced it on Github. Mirai botnet brute forces the username and passwords which are set by default by the manufacturers, one by one for all the devices. These default passwords are rooted inside the firmware of the device, and maybe hard to change. It tries to establish a connection from a distributed set of devices and does a dictionary attack (using a huge database) until it overshoots the threshold of connections supported by the device.

2.3 Existing solutions

We studied how IoT networks in home and public environments talk over the Internet and also investigated potential risks. These have been summarized in Section 1.

In most cases, existing solutions solve this problem by either directly sending the data over the Internet or by using a trusted gateway which connects these devices to the Internet. Moreover, there exist commercial solutions like [4] Cujo, which is a smart firewall for a home network. This is very similar to what we are doing, but it is closed source and expensive. We focus on an affordable and open source solution which can provide security to the IoT devices within a home network, along with monitoring their activity and displaying relevant alerts and statistics through a dashboard.

2.4 Our work

We setup a firewall using a Raspberry Pi as a gateway. All the IoT devices or sensors send their data through this RPi. All public requests like HTTP pass through it, while it gives us freedom to create our own LAN. We have procured some IoT devices in order to test our Firewall.

We have created a dashboard where an administrator can add several information corresponding to an IoT device. The dashboard displays information such as URLs accessed, URLs blocked, the number of hits on a URL, IoT devices present in the home network, their location etc. The dashboard also allows the administrator to choose the location (in the home) and permissions or policies of an IoT device.

2.5 Organization of this report

This report summarizes the work done in the across two semesters of the BTP. In the previous semester, the goal was to complete the literature survey, identify potential risks with IoT devices and build a secure gateway solution for further work. This semester, we have implemented a dashboard which the administrator can use to assign locations and policies to IoT devices in the home network. Here onwards we explain our firewall and our dashboard. Screenshots of our system are present towards the end of the next chapter, through which the dashboard can be understood better.

Implementation

3.1 Details about the Firewall

We configured a WiFi Hotspot local area network (hereby referred to as the home network), called "Pi3-AP" where the Raspberry Pi will be connected to the IIIT Delhi network through the Ethernet interface. All the IoT devices will be connected to the Pi3-AP LAN. The Raspberry Pi will act as the network gateway to forward all the packets from WiFi interface to Ethernet interface over the IIIT Delhi network to the cloud service.

As mentioned earlier, we used a Raspberry Pi as a WiFi access point with hostapd, and used dnsmasq to act as the DHCP server [5]

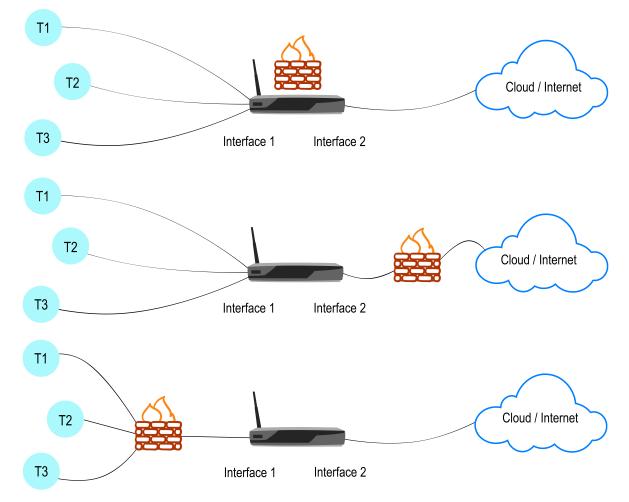
- hostapd This package allows us to use the built in WiFi as an access point.
- dnsmasq A combined DHCP and DNS server

We initially configured the Raspberry Pi's interfaces such that the wlan0 interface has a static IP. Then, we configured hostapd to create the new network "Pi3-AP". After this, we configured dnsmasq where we specified the interface, listen-address, bind-interfaces, DNS server and the DHCP range. We configured a firewall on the Raspberry Pi using Snort. We captured the packets using verbose tcpdump of the IoT device on the gateway and logged the hostapd service. Currently, we did the profiling for one of the IoT devices - Motorola FOCUS 66: a smart security camera.

Here is a brief description of the analysis on Motorola FOCUS 66. The process was performed in 3 stages as follows -

- 1. The camera was initially off, and turned on after sometime.
- 2. The camera was kept on, and streaming was turned on using the cloud based web application or mobile phone application. We noticed that the camera starts recording only when a streaming client is connected.

Figure 3.1: Architecture Diagram (The firewall and dashboard can be placed on the gateway, or any access point inside or outside the home network.)



T1, T2, T3 are IoT devices (things)

3. The streaming was turned off and accordingly the camera stopped recording.

3.2 Details about the Dashboard

This semester, our aim was to create a language for IoT devices, which a normal user can understand and use to control the devices easily.

After proper research (keeping in mind recent attacks and IoT device behaviour), we decided to keep the default policy for IoT devices as 'reject'. If a new device comes in the home network, it is assigned the least priorities, i.e. it can't receive any data from outside the network.

Figure 3.2 shows the database hierarchy containing the following tables:

- Permission These are policies which can be based on permissions of the room, the device type or owner. For example, a device residing in the living room should be accessible by all, but not a device which resides in a bedroom. Similarly, a child's device should not be allowed to access the internet post (say) 8:00 PM.
- State This is the state of the IoT device, i.e. whether it is switched on or off.
- Room This denotes the room an IoT device resides in. Every device type has associated permissions.
- Device Type There may be several types of IoT devices smartphones, bulbs, cameras etc. This table stores the types of IoT devices present inside the home. Every device type has associated permissions.
- URL This stores any URLs accessed by an any IoT device within the home network. A new entry is added to this table whenever a new URL is accessed by an IoT device.
- Connection This stores information about a connection like the type of request (TCP/UDP/DNS), source IP and destination IP. A new entry is added for every new connection opened by an IoT device.
- Owner Every device has an owner associated with it. An owner has their own respective permissions associated with it. An owner can be a parent or a child, and permissions of the devices belonging to the owner change accordingly.

The Dashboard can be controlled by an administrator. The administrator can set policies for IoT devices as they desire, through the Dashboard. Apart from setting policies, they can also add rooms, permissions, owners and devices to their home network through the Dashboard.

We ran a Snort daemon and a hostapd service. Snort is used to track TCP/UDP connections, DNS requests and for blocking or allowing requests according to the policies decided by the administrator.

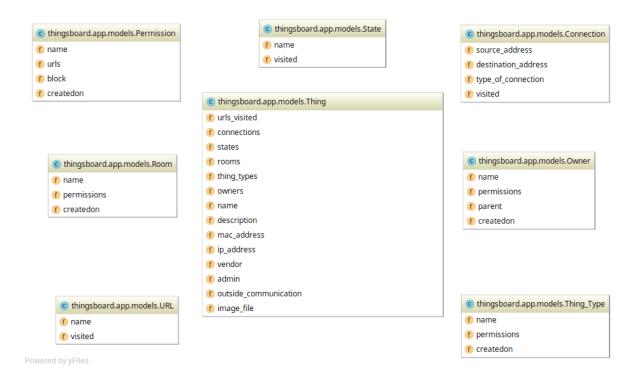


Figure 3.2: Database Diagram

We derive the manufacturer of the device using macvendors.co API. A GET request containing the MAC address is sent to the API, which returns the details of the manufacturer.

Since the Dashboard runs on a Raspberry Pi, which is the server/gateway or creator of the home network, it contains MAC (hardware address) : IP mapping of all the devices present in the home network. We use the ARP table to fetch an IP corresponding to the MAC address and vice versa.

We also track the type of connection and URLs visited through Snort IDS. Any connections or requests which matched a particular Snort rule, it is logged into the alert file.

The permission policy of an IoT device is inherited from an intersection of permission policy of it's owner, the permission policy of the type of the device and the permission policy of the room it is currently located in. We implement our default blocking strategy by adding a new rule to the local.rules file of Snort of the format:

drop tcp any any <> hexip any (content: weburl, msg: AccessDenied, react: block)

We also show statistics to give the administrator information about the running status of the IoT devices. We show the following:

- 1. Frequency of URLs visited for each IoT device.
- 2. Time-series plot of bandwidth used by each IoT device.

 ThingsBoard			Home	Create 🗸	Statistics	
	FOCL	JS 66				
Rooms	Kitchen Living Room Bed Room Washroom					
	Hold down "Control", or "Command" on a Mac, to select more than one.					
Thing types	Camera Smartphone Computer					
	Hold down "Control", or "Command" on a Mac, to select more than one.	-				
Owners	Naman Srishti Dr. Naik					
	Hold down "Control", or "Command" on a Mac, to select more than one.	-				
Name	FOCUS 66					
Description	A smart security camera	-				
MAC Address	80:6c:1b:ef:61:e9					
IP address	172.168.1.1	-				
Vendor	Motorola Mobility LLC, a Lenovo Company					
	Z Admin					
	Cutside communication					
Picture	Currently: image_file/u_10075166.jpg Clear Change: Browse No file selected.					
	ОК					

Figure 3.3: Editing details about an IoT device.

Figure 3.4: Creating an owner.

ThingsBoard		Home	Create -	Statistics
	Add an Owner			
Name	Name			
Permissions	Social Network Search Fake News			
	Hold down "Control", or "Command" on a Mac, to select more than one.			
	Parent			
	ок			

ThingsBoard		Home	Create 🗸	Statistics	
	Add a Room				
Name Permissions	Name Social Network Search				
	Fake News Hold down "Control", or "Command" on a Mac, to select more than one.				
	ок				

Figure 3.5: Creating a room.

Figure 3.6: Creating a thing type.

ThingsBoard		Home	Create -	Statistics	
	Add a Device Type				
Name Permissions	Name Social Network Search Fake News				
	Hold down "Control", or "Command" on a Mac, to select more than one.				

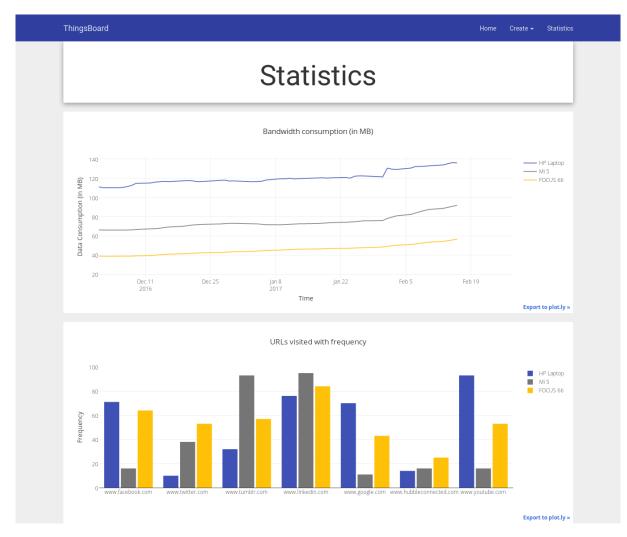
Figure 3.7: Home page displaying information about all the things connected to the Home network.



ThingsBoard		Home	Create -	Statistics
	Add a Permission			
Nan Ur	www.facebook.com			
	www.twitter.com www.tumbir.com www.linkedin.com			
	Hold down "Control", or "Command" on a Mac, to select more than one.			
	Slock			
	ок			

Figure 3.8: Creating a permission control.

Figure 3.9: Statistics



Discussion

4.1 Conclusion

In the first part of the BTP, we understood and appreciated the current efforts going on to secure the Internet of Things. We implemented a gateway like system to secure the home network against privacy threats, confidentiality and related attacks.

In this semester, we developed a Dashboard for monitoring IoT devices in a home network. Through this Dashboard, an administrator can add information about an IoT device and decide upon fine grained policies for these devices depending on their location, type or owner.

Bibliography

- ALTOLINI, D., LAKKUNDI, V., BUI, N., TAPPARELLO, C., AND ROSSI, M. Low power link layer security for iot: Implementation and performance analysis. In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC) (2013), IEEE, pp. 919–925.
- [2] BABAR, S., STANGO, A., PRASAD, N., SEN, J., AND PRASAD, R. Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (2011), IEEE, pp. 1–5.
- [3] BRACHMANN, M., KEOH, S. L., MORCHON, O. G., AND KUMAR, S. S. End-to-end transport security in the ip-based internet of things. In 2012 21st International Conference on Computer Communications and Networks (ICCCN) (2012), IEEE, pp. 1–5.
- [4] CUJO. Cujo-a smart firewall for your home. https://www.getcujo.com/, 2016. Accessed: 2017-04-17.
- [5] MARTIN, P. Using your new raspberry pi 3 as a wifi access point with hostapd. https:// frillip.com/using-your-raspberry-pi-3-as-a-wifi-access-point-with-hostapd/, 2016. Accessed: 2016-11-17.
- [6] SCHREIBER, J. Open source intrusion detection tools: A quick overview. https://www.alienvault.com/blogs/security-essentials/ open-source-intrusion-detection-tools-a-quick-overview, 2014. Accessed: 2017-04-17.