A firewall for Internet of Things

Conference Paper · January 2017

DOI: 10.1109/COMSNETS.2017.7945418

CITATION
1

READS
594

3 authors:

Naman Gupta
Indraprastha Institute of Information Technology
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Vinayak Naik
BITS Pilani, K K Birla Goa
61 PUBLICATIONS **1,452** CITATIONS
SEE PROFILE

Srishti Sengupta
Indraprastha Institute of Information Technology
1 PUBLICATION **1** CITATION
SEE PROFILE

A Firewall for Internet of Things

Naman Gupta
IIIT-Delhi
naman13064@iiitd.ac.in

Srishti Sengupta
IIIT-Delhi
srishti13108@iiitd.ac.in

Vinayak Naik
IIIT-Delhi
naik@iiitd.ac.in

***Abstract*—With the advent of the internet of things, privacy and security of sensitive data has become a major concern. Generally, Internet of Things devices are sensors which generate data and send it over the internet to a cloud database. The communication to the cloud database may be compromised, thereby raising security concerns. To solve this issue, we demonstrate a solution to safeguard all the Internet of Things devices in a home network scenario from potential attacks. A firewall is set up using a Raspberry Pi as a gateway which secures the communication with the cloud database. Furthermore, we plan to build a heuristics and a signature based traffic detection dashboard running on the Raspberry Pi.**

I. Introduction

A wide range of devices are connected to the internet in a home-network scenario. These IoT devices are mostly sensors which are low powered, low compute and have limited resources. Therefore, they may not support expensive encryption protocols. An adversary may sniff the packets going to the cloud service, and reconstruct the data leading to potential risks like leakage of sensitive information. Moreover, many companies may not provide enough security in order to reduce the cost. It may so happen that these devices come with default credentials which a naive user may not change. These factors lead to potential security risks which one would like to prevent otherwise.

November 20, 2016

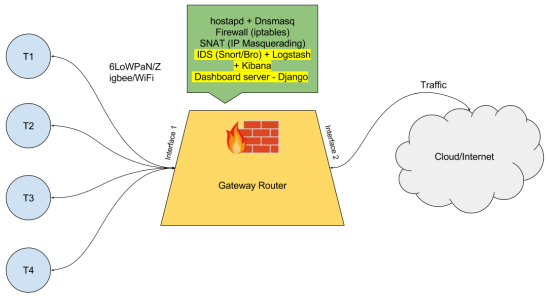
II. Solution Approach

To draw inspiration, we read about existing work which has already been done in the field of security in the internet of things [1], [2], [3], [4]. We learned that all the commercial solutions were expensive and the architecture and working was not openly accessible. Therefore, our aim is to design a cost-effective, openly accessibly system. We setup a firewall using a Raspberry Pi as a gateway, through which all IoT devices send their data. Public requests like HTTP pass through it, while it gives us freedom to create our own LAN.

A. Details about the firewall

A WiFi Hotspot local area network, called "Pi3-AP" (hereby referred to as the home network) was configured. The Raspberry Pi was connected to the IIIT Delhi network through the Ethernet interface and all the IoT devices were connected to the Pi3-AP LAN. The Raspberry Pi acts as the network gateway to forward all the packets from the WiFi interface to the Ethernet interface, over the IIIT Delhi network to a cloud service. We configured a firewall on the Raspberry Pi using iptables which supports the following rules:

Fig. 1. Architecture Diagram (Please note that the dashboard will be covered in the future.)



1) Enabled IPv4 Masquerading - The device acts as an Source-NAT gateway for outbound internet packets coming from LAN and Destination-NAT gateway for outbound LAN packets coming from LAN.
2) Enabled Spoof protection (reverse-path filter). Source Address Verification was turned on in all interfaces to prevent spoofing attacks. The firewall statefully tracks the requests from the IoT devices and verifies whether the source address in the response (coming from the internet) is present or not.
3) Does not accept ICMP redirects (prevent MITM attacks). Redirects are error messages for the sender of an IP packet. These are sent when a router infers that a packet is not being routed optimally. In that case it informs the sender to forward packets through a different gateway.
4) Enabled TCP/IP SYN cookies. These cookies are used for resisting SYN flood attacks. It is a form of DOS attack, where an attacker sends a series of SYN requests in order to consume the server's resources.
5) Enabled default connection tracking provided by iptables.

A Raspberry Pi is configured as a WiFi access point with hostapd and dnsmasq to setup the DHCP server [5]. We aim to support profiling of traffic generated by IoT devices connected in a home network. To initiate the efforts, the authors tried to profile the behavior of just one IoT device, Motorola FOCUS 66: a smart security camera. The future plan is to setup an intelligent heuristics based traffic profiling framework running

Fig. 2. A STUN packet

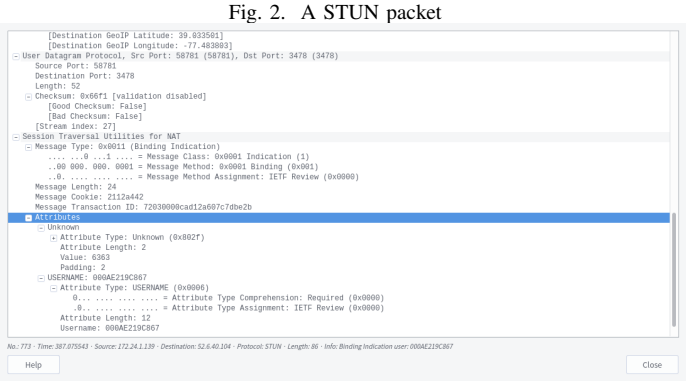
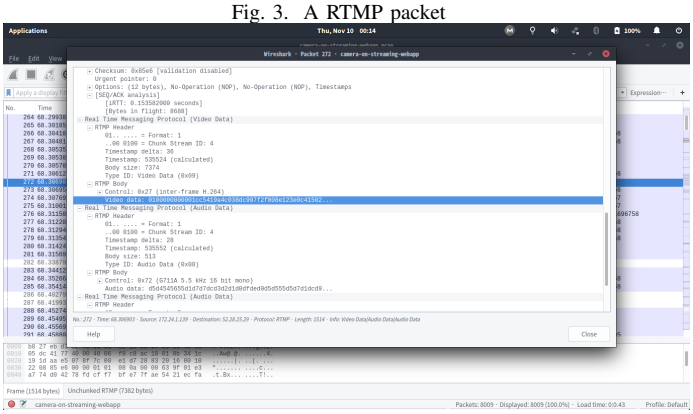


Fig. 3. A RTMP packet



on the Raspberry Pi.

B. Discussion

The analysis on the Motorola FOCUS 66 has been described here. The process was performed in 2 stages as follows -

1) The camera was initially off, and turned on after some-time.
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.

In the first stage, the camera acquires an IP address from the DHCP server running on the Raspberry Pi using mDNS. Then, the camera synchronizes the NTP time information from 'ntp.hubble.in'. The camera establishes a TCP with TLS connection with 'api.hubble.in'. The camera established a connection after every few seconds to receive signal (from the hubble application) to start recording.

The camera sends a STUN packet to 'stun.hubble.in', see figure 2. The STUN packet contained the username in plaintext in order to establish camera's identity with the hubble server.

In the second stage, streaming was initiated on the Hubble web application causing it to emit a signal for the camera to start recording. The camera starts sending the data to the AWS instance using RTMP (Real Time Messaging Protocol). It authenticates itself to the server with a basic challenge/ response protocol: C0 and C1 are random numbers generated by the camera. S0, S1 and S2 are the signatures for the server, camera and the destination server which will receive the stream output. The camera verifies the identity of the server and using these signatures further. Then, the camera and the hubble server negotiates the supported specifications of the RTMP protocol. The camera starts streaming the Video and Audio to the Hubble application.

C. Recent attacks

The recent attacks on Dyn DNS service were studied, which is touted to be the largest IoT-based DDOS attack in the history. The "Mirai botnet" bruteforces the default username and passwords which are set by the manufacturers. These default passwords are rooted inside the firmware of the device, and maybe hard to change. The malware 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. Our gateway device prevents various types of connection techniques to the IoT devices by the botnet i.e., Telnet, SSH, ICMP etc thereby stopping it from contacting any of the IoT devices at all. We plan to have an intelligent signature based blocking system for such attacks in the future.

III. Future Work

We implemented a gateway like system to secure the home network against privacy threats, confidentiality and related attacks. In the future, we will implement a traffic detection dashboard running on the Raspberry Pi. This dashboard would also contain information (for each IoT device in the home network) about the frequency of sending data, location of the devices, and classification based on this data.

Moreover, a lone Raspberry Pi working as a gateway acts like a single point of failure. Due to less computational power, it may not be able to handle a lot of connections, like that in a DOS scenario. We plan to use multiple firewalls or gateways with a load balancer so as to thwart the possibility of any DOS or DDOS attack.

References

[1] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the ip-based internet of things," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2012, pp. 1–5.

[2] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello, and M. Rossi, "Low power link layer security for iot: Implementation and performance analysis," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2013, pp. 919–925.

[3] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," in *International Conference on Network Security and Applications*. Springer, 2010, pp. 420–429.

[4] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "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*. IEEE, 2011, pp. 1–5.

[5] P. Martin, "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.