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 (IoT), privacy and security of sensitive data has become a major concern. In general, sensors which are the enablers for IoT, send the sensed data to a cloud database over the internet. The communication to the cloud database may be compromised by an adversary, or the database maybe accessed by a curious database administrator, thereby raising security concerns. To solve this issue, we demonstrate a solution to safeguard IoT devices in a home network scenario from potential attacks. A firewall is set up using a Raspberry Pi as a gateway which secures their communication with the cloud database. Furthermore, we plan to build a location-aware (physical location in the home network scenario) heuristics and a signature based traffic detection dashboard running on the Raspberry Pi, in order to control the IoT devices and log their network behavior.**

***Index terms*—** Internet of Things, privacy, security, firewall

I. Introduction

A wide range of IoT devices (referred to as the things, hereafter) are connected to the internet in a home-network scenario. They are mostly sensors which are low powered and have limited computing 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 the leakage of sensitive information. Moreover, many companies do not provide enough security in order to reduce the cost. The things may 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.

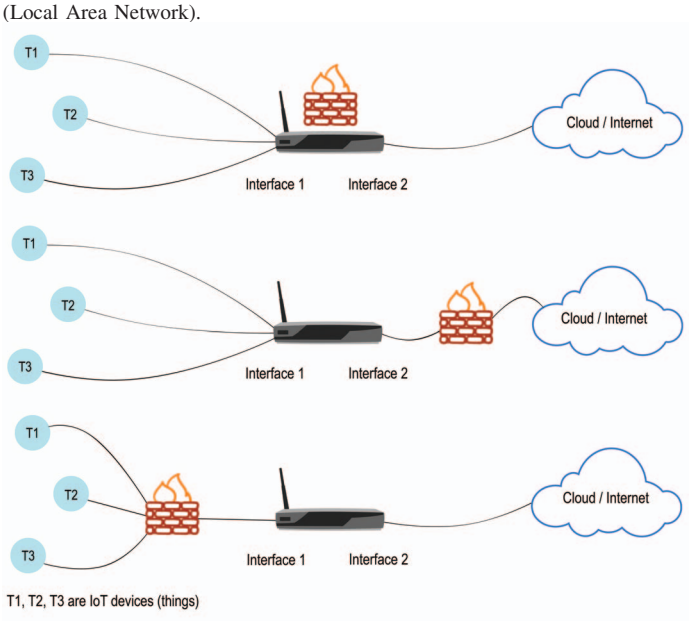
II. Solution approach

State-of-the-art [1], [2], [3], [4] suggest that the commercial solutions are expensive and the technical details are not open-source. Therefore, our aim is to design a cost-effective and open-source system. We setup a firewall using a Raspberry Pi as a gateway, through which all the things send their data. This will help us in activity/behavior detection of the things. Public requests like HTTP pass through it, giving us the freedom to create our own LAN.

A. Details about the firewall

We configured a LAN with all the things connected to it. The Raspberry Pi was connected to the internet through the ethernet interface and to the LAN through it's WiFi interface. Currently, we connected one thing (Motorola FOCUS 66) to the LAN. The Raspberry Pi forwards all the packets from the WiFi interface to the ethernet interface, which then goes over the internet to a cloud server. We configured a firewall on the

Fig. 1. Architecture Diagram - The firewall can be on the gateway router, on the access point outside the LAN or on the access point inside the LAN (Local Area Network).



Raspberry Pi using `iptables` which support the following rules:

1) Enabled IPv4 Masquerading - The device acts as a Source-NAT gateway for outbound packets coming from the LAN and Destination-NAT gateway for inbound packets coming from the Internet.
2) Enabled Spoof protection (reverse-path filter). A reverse path filter allows us to check whether the source address of a packet is routable. In case a packet is not routable, it is dropped.
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, which is a form of DOS attack. An attacker sends a series of SYN requests in order to consume the server's resources.
5) Enabled default connection tracking provided by `iptables`.

978-1-5090-4250-0/17/$31.00 ©2017 IEEE

Fig. 2. A RTMP packet carrying encoded video data.

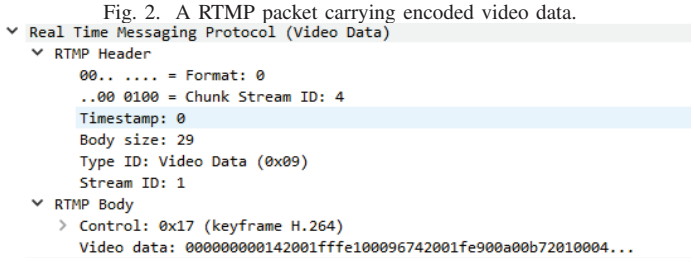
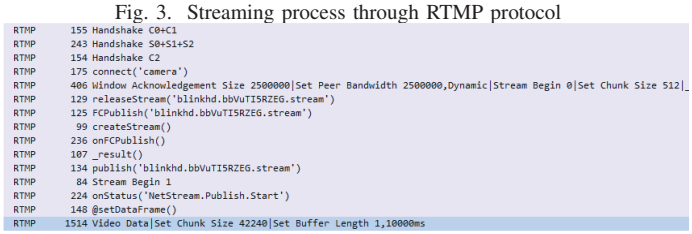


Fig. 3. Streaming process through RTMP protocol



A Raspberry Pi is configured as a WiFi access point using `hostapd` and `dnsmasq` to setup the `DHCP server` [5]. We aim to support profiling of traffic generated by the things connected in the home network. To initiate the efforts, we tried to profile the behavior of just one IoT device, Motorola FOCUS 66: a smart security camera which streams audio and video to a remote application.

B. Discussion

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

1) Connection Establishment stage: The camera was initially off, and then turned on.
2) Data Streaming stage: The camera was kept on, and streaming was turned on using the remote cloud based 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. It establishes a TCP with TLS connection with 'api.hubble.in'. It was seen thereafter, that the camera polled the cloud application after every few seconds to check for a signal to start recording.

In the second stage, streaming is initiated on the remote Hubble cloud application causing it to emit a signal for the camera to start recording. The camera and the application mutually authenticate each other using a basic challenge/response protocol by generating random nonces and exchanging signatures. The camera then starts sending realtime audio and video data to the cloud application using RTMP (Real Time Messaging Protocol).

C. Recent attacks

The recent attack on Dyn DNS service were studied, which is touted to be the largest IoT-based DDOS (Distributed Denial of Service) attack in history. The attack was carried out using the "Mirai malware" [6], which turns the things into remotely controlled "bots". These can be used as part of a botnet in a large-scale network attack. The things become vulnerable when users forget to change the default credentials and settings shipped by the company. They get infected when the malware tries to connect to them using a set of factory default credentials. The malware spreads by infecting the neighborhood things which creates a DDOS attack scenario. It has been observed that the infected things start performing at a higher bandwidth (which will be detected by our system) than their normal regular use.

One way to make our gateway prevent such DDOS attacks will be to allow connection establishments only from certain whitelisted IP addresses. The gateway will act as a middleware which caches DNS requests and corresponding IP addresses. It blacklists any other external IP address which may be those of the infected devices. Thus, preventing any foreign connection (possibly from devices infected by the malware) other than the trusted ones.

III. Future Work

We implemented a system to secure the home network against privacy breaches, confidentiality threats and related attacks. The future plan is to setup a generalized intelligent heuristics based traffic profiling dashboard running on the Raspberry Pi. This dashboard would contain information like the frequency of sending data, location of the things and other such classification for each thing in the home network.

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, just like in a DOS scenario. We plan to use multiple firewalls (refer Fig. 1) or the gateway with a load balancer 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.

[6] Anna-senpai, "Mirai (malware)," https://en.wikipedia.org/wiki/Mirai_(malware), 2016, accessed: 2016-11-28.