Smart Router

Thibault Debatty [1] Pietro Michiardi [2] Olivier Thonnard [3] Wim Mees [1]

[1]Royal Military Academy, Brussels, Belgium

[2]EURECOM, Campus SophiaTech, France

[3]Symantec Research Labs, Sophia Antipolis, France

Introduction

The number of IoTs devices present in our houses is constantly growing up. Smart-TVs, smart-lights,IP-cameras and number others are all connected to the Internet to be managed from outside our homes. But how can we, in as SOHO context, monitor these devices to be sure they only do the work they should. So how to be sure they are not botnets ?

Goal

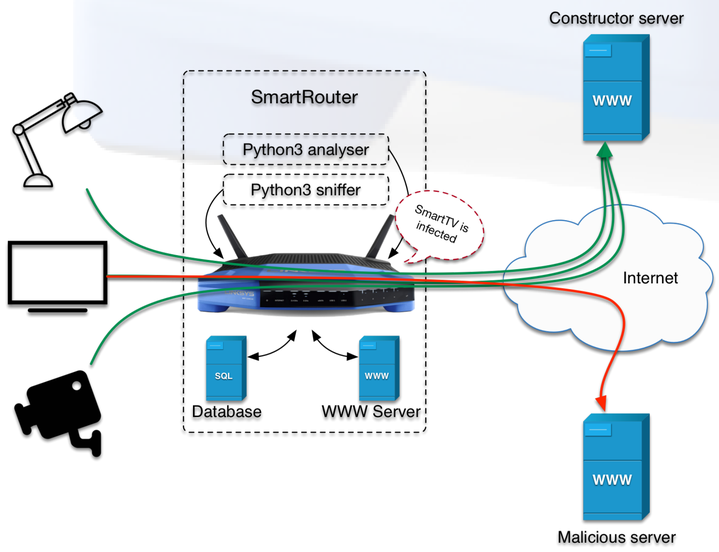
The goal of this project is to monitor IoT traffic of a SOHO (Small Office, Home Office) network. By sniffing and analyzing it, this project can send alerts when an IoT has an unusual network traffic. For example, if it suddenly begins to send random request to random IP addresses around the world.

Only IoT traffic is interesting for this type of project because Iot devices only go to the same servers. Devices like laptops are used for example to surf the web and then it is never the same destinations. So sniffing non-IoT traffic is not the goal of this project.

Architecture

The smart router is designed to be installed between the connected devices and the Internet, such that it can intercept and analyze the traffic generated by the devices. It is composed of 3 main modules:

- Traffic sniffer,
- Traffic analyzer,
- Web interface



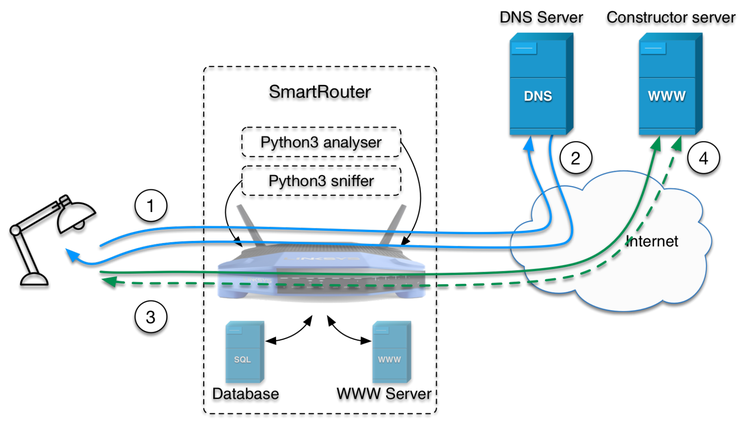
Traffic sniffer

The traffic sniffer is a process that captures all SYN packets with destination port TCP/80 && TCP/443. This allows to detect all connection tentatives from the devices on the local network. For each tentative, following fields are stored in the database:

- Source MAC address,
- Destination IP address,
- Timestamp of the request

To be able to know to which domain corresponds each destination IP, DNS packets are also sniffed and then data are correlated to make IP correspond to a domain. If no domain corresponds to an IP, IPs are reversed lookup to try to have a domain.

Schematically, the process is the following :



1. First, the IoT sent a QNS query to *constuctor.com* (assuming that this domain is the domain used for the IoT management, and which, in this case is legit).
2. Second, the DNS server will reply to the previous request with the corresponding IP address of the previously asked domain. This request is sniffed, the domain and corresponding IP address are stored in the database
3. Third, the IoT will contact the server behind the previously asked domain. Only the SYN packet will be sniffed and an entry will be created into the database,
4. Finally, the rest of the request (non only SYN packets) will not be store into the database.

Traffic analyzer

A process is launched every X minutes (depending of the setup) to analyze all traffic and determine if the traffic is legit or malicious. This process is managed by a custom *init.d* script which is run at startup.
A "learning period" (which depend on the setup) is defined. Between the first request of an IoT and the end of the learning period, each packet and domains are considered as legit.
Beyond the period, if an IoT contact an unknown domain (which is a domain not contacted in the learning period), it will be considered like malicious. Is this case an alert will be generated and stored in the database.

Moreover, additional modules may be triggered when an alert occurs, like a Slack notification (see below), a notification on a dedicated app, a webhook etc.

Web interface Actually the web interface displays only a txt file containing alerts. An example of truncated alert file id the following :

```
3c:2e:ff:29:4d:93 -> ec2-35-157-172-34.eu-central-1.compute.amazonaws.com @ 2018-03-19 21:11:37.596877
b8:27:eb:18:6a:6f -> Philips-hue.lan @ 2018-03-26 11:09:45.644908
cc:44:63:ea:63:63 -> host-95-182-253-43.dynamic.voo.be @ 2018-03-27 18:13:48.133365
...
cc:44:63:ea:63:63 -> am2-005-edge.digitalhub.com @ 2018-03-27 20:21:25.473550
cc:44:63:ea:63:63 -> a23-40-246-12.deploy.static.akamaitechnologies.com @ 2018-03-27 21:34:14.803526
cc:44:63:ea:63:63 -> UNRESOLVED(17.248.148.104) @ 2018-03-28 07:55:03.703039
cc:44:63:ea:63:63 -> BenjaminMBP.lan @ 2018-03-30 11:12:25.202242
...
3c:2e:ff:29:4d:93 -> ec2-54-225-192-183.compute-1.amazonaws.com @ 2018-04-04 08:35:16.846425
3c:2e:ff:29:4d:93 -> UNRESOLVED(108.177.127.97) @ 2018-04-04 08:36:16.376180
3c:2e:ff:29:4d:93 -> ec2-54-76-216-221.eu-west-1.compute.amazonaws.com @ 2018-04-04 08:41:14.942256
3c:2e:ff:29:4d:93 -> UNRESOLVED(104.17.26.75) @ 2018-04-04 08:42:12.364664
3c:2e:ff:29:4d:93 -> server-54-192-32-45.stl2.r.cloudfront.net @ 2018-04-04 08:45:41.934358
...
cc:44:63:ea:63:63 -> moodle.uclouvain.be @ 2018-04-09 11:28:13.131310
```

In the next version of this project, a web interface could be used to configure the router and have a better view of the alerts.

Implementation

To test the detection system, we built a complete implementation, using OpenWRT, Python and Scapy.

The complete source code of the smart router is available at `https://github.com/RUCD/smart-router/`.

OpenWRT (*https://openwrt.org*)

The OpenWrt Project is a Linux operating system targeting embedded devices. So it was one of the possible choices for the Linux distribution. More specifically, OpenWRT was a compatible distribution for the router used for this project. The routers used are Linksys WRT1200ac.

Scapy

We used python and scapy to implement the traffic sniffer and the traffic analyzer. *Scapy is a packet manipulation tool for computer networks, written in Python by Philippe Biondi. It can forge or decode packets, send them on the wire, capture them, and match requests and replies.*

Web server

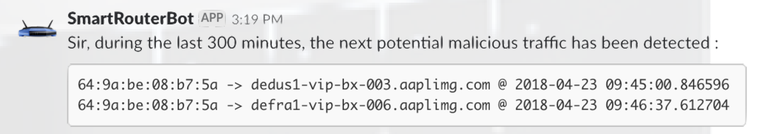
Due to portability issues and high resource consumption, we implemented a very simple web interface on the OpenWRT router: alerts are simply read on a text file and displayed vie a simple web server.

Testing

We tested the smart router in various real SoHo networks. To be able to easily collect the alerts produced by the different routers, we implemented a slack application. This is a simple slack integration working with tokens. All is implemented by slack.

Slack alert have the role of the initial application alert. A slack application has been integrated in a workspace. So with it, the Smart Router send alert to a specific channel, thanks to slack tokens.

This slack integration allow the receive notification like initially wanted, but without having to develop a specific application for it.



Future Work

Lots of modules can be developed in future work, for example we can imagine :

- More protocol sniffed : for now, only web and DNS traffic is sniffed, but it could be interesting to have a generic sniffer which allowed to sniff everything traffic,
- Web configurations : all configuration is done in command line, so a more user-friendly web interface configuration page could be a great idea,
- Target sniffing : a good idea will be to be able to detect IoTs and filter only this traffic. Actually, all traffic is sniffed, but some can be blacklisted not to be sniffed,
- Target analysis : actually, all traffic is reanalyzed every time an analysis is run. A better analysis will be to analyze only new traffic since the last analysis,
- Lots of other integration are possible to have better interfaces and configuration modules.

Conclusion

This project has a lot of other possibilities then experimented here. It also has a lot of optimization and machine learning possible.

Cyber Defence Lab
Royal Military Academy
www.cylab.be