Design and implementation of a firewall device with a new method to harden SSL introduced

Master's Thesis submitted to the
Faculty of Informatics of the *Università della Svizzera Italiana*
in partial fulfillment of the requirements for the degree of
Master of Financial Technology and Computing
main track

presented by
Bin Yong

under the supervision of
Prof. Student's Advisor
co-supervised by
Prof. Student's Co-Advisor

September 2023

I certify that except where due acknowledgement has been given, the work presented in this thesis is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; and the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program.

Bin Yong
Lugano, Yesterday September 2023

Abstract

Design and implementation of a firewall device based on Raspberry Pi. The firewall will use a new method to harden the SSL protocol. It is designed for someone who would like to sacrifice some compatibility to pursue better security but still wants some balance between security and convenience. A sensitive target, like an investigative journalist, could be a potential user of this device. The new method to enhance SSL security introduced in this article is widely applicable to firewall designs.

Acknowledgements

This document is a draft version of a working thesis of Bin Yong.

Contents

Contents vii

List of Figures ix

List of Tables xi

1 Introduction 1

2 Comparsion to existing works 3
2.1 Commercial hardware . . . 3
2.2 SSL proxy . . . 3

3 Short title 5
3.1 The first section . . . 5
3.2 The second, math section . . . 5
3.3 third . . . 5

A Some retarded material 7
A.1 It's over... . . . 7

Glossary 9

Figures

Tables

Chapter 1

Introduction

The goal of this work is to increase the chance of survival of the user from hacking, evasdropping, and digital fingerprinting. The device will work as a strict firewall which limits network activities and will also apply privacy enhancing technologies to reduce the attack surface of digital fingerprinting and it will also apply emerging technologies to increase the difficulty of eavesdropping. The device will run a SSL proxy to harden SSL protocol. It will use a screen to display selected real-time internet activities.

Using a hardware as a firewall has several advantages. Firstly, hardware firewall can provide complete isolation between highly unsafe code, like a browser, and firewall software (fun fact: I was hacked repeatedly through personally harddened latest version of firefox while writing this thesis). This could also work as a mitigation of CPU/BIOS level threats: Firmware malwares, bootkits, and doubtable proprietray technologies like Intel ME and the AMD PSP. Second, it will also provide convenience to the user: the configuration of this portable device will be applied to protect everything behind it, so people do not need to do the time consuming configuration work on different softwares and operating systems one by one. Even things that could not be configured will be under the limitation of the firewall. Not to mention that many things cannot be configured freely. In example, people cannot untrust a built-in trusted root certificate from iPhone via Settings app.

Chapter 2

Comparsion to existing works

2.1 Commercial hardware

Commercial firewalls are expensive. In switzerland, the price of a entry level firewall is more than twice of a raspberry pi. Raspberry Pi being used in this work could be replaced with some cheaper alternatives, making the cost will be even lower. Commercial firewalls also do not provide a screen to display network activities in real-time.

2.2 SSL proxy

Unlike traditional MITM SSL proxy, the proxy used in this device will work in non-intrusive way which means it will not decrypt SSL sessions.

Chapter 3

A chapter title which will run over two lines — it's for testing purpose

3.1 The first section

3.2 The second, math section

Theorem 1 (Residue Theorem). Let f be analytic in the region G except for the isolated singularities $a_1, a_2, \ldots, a_m$. If γ is a closed rectifiable curve in G which does not pass through any of the points a_k and if $\gamma \approx 0$ in G then

$$\frac{1}{2\pi i}\int_\gamma f = \sum_{k=1}^{m} n(\gamma; a_k)\mathrm{Res}(f; a_k).$$

Theorem 2 (Maximum Modulus). *Let G be a bounded open set in $\mathbb{C}$ and suppose that f is a continuous function on G^- which is analytic in G. Then*

$$\max\{|f(z)| : z \in G^-\} = \max\{|f(z)| : z \in \partial G\}.$$

3.3 A very very long section, titled "The third section", with a rather short text alternative (third)

Some Test

```
1 import IntSpec, ItemSpec;
2
3 sort cart;
4
5 constructors
6 create() ⟶ cart;
7 insert(cart, item) ⟶ cart;
8 observers
```

```
amount(cart) ⟶ int;
transformers
delete(cart, item) ⟶ cart;

axioms
forall c: cart, i, j: item

amount(create()) = 0;
amount(insert(c,i)) = amount(c) + price(i);
delete(create(),i) = create();
delete(insert(c,i),j) =
if (i == j) c
else insert(delete(c,j),i);
end
```

As you can easily see from the above listing **?** define something weird based on the BPEL specification [**?**].

Appendix A

Some retarded material

A.1 It's over...

Glossary

1