
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 SSL protocol. It is designed for someone who would like to sacrifice some compatibility to pursuit a better security but still want 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 could be widely applied 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 Short title	3
2.1 The first section	3
2.2 The second, math section	3
2.3 third	3
A Some retarded material	5
A.1 It's over...	5
Glossary	7

Figures

Tables

Chapter 1

Introduction

Chapter 2

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

2.1 The first section

2.2 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, \dots, 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

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

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

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

2.3 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()  $\longrightarrow$  cart;
7 insert(cart, item)  $\longrightarrow$  cart;
8 observers
```

```
9 amount(cart)  $\longrightarrow$  int;
10 transformers
11 delete(cart, item)  $\longrightarrow$  cart;
12
13 axioms
14 forall c: cart, i, j: item
15
16 amount(create()) = 0;
17 amount(insert(c,i)) = amount(c) + price(i);
18 delete(create(),i) = create();
19 delete(insert(c,i),j) =
20 if (i == j) c
21 else insert(delete(c,j),i);
22 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