

UNIVERSITI TEKNOLOGI MARA

**Simple Port Knocking Method against TCP Replay
Attack and Port Scanning**

MOHD AZUAN B MOHAMAD ALIAS

Dissertation submitted in partial fulfilment of the requirements
for the degree of

Master of Science in Computer Networking

Faculty of Computer Science and Mathematical Science

January 2012

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Merciful. With His permission, this study has been completed. I would like to express my grateful appreciation to all individuals who have contributed and help me in finishing this thesis. I am very thankful to my supervisor, Dr. Fakariah Mohd Ali for all his guidance and advices. Besides, I wish to express my sincere appreciation to Mr. Krishna Ramasamy my security guru and Mr Yusrul Nidzuan who has provided assistance at various occasions. Thanks to Micheal Rash, a guy who introduced Fwknop + SPA that share his experience.

Finally I would like to deliver sincere gratitude to my beloved wife,
. my son beloved parents and the whole family for their encouragement and motivations during the period of study in UiTM Shah Alam, Selangor. Last but not least to all colleagues, to who has given their support that will be remembered forever.

TABLE OF CONTENTS

CONTENT

CHAPTER 1

INTRODUCTION

- 1.0 Introduction
- 1.1 Problem Statement
- 1.2 Research Question
- 1.3 Objective
- 1.4 Scope
- 1.5 Project Significant
- 1.6 Thesis Structure

CHAPTER 2

LITERATURE REVIEW

- 2.0 Introduction
- 2.1 Basic of Port Knocking
 - 2.1.1 Advantages
 - 2.1.2 Disadvantages
- 2.2 How It Works
- 2.3 Issues on Port Knocking
 - 2.3.1 Packet Delivery Out of Order
 - 2.3.2 Network Address Translation
 - 2.3.3 Security through Obscurity
- 2.4 Attacks on Port Knocking

2.4.1	Direct Attack	16
2.4.2	Inception Attack	17
2.4.3	Eavesdropping	17
2.4.4	Man in the Middle	18
2.5	Improvement of Port Knocking Project	20
2.5.1	Port Knocking with Single Packet Authorization	21
2.5.2	One Time Knocking Framework using SPA and IP Sec	21
2.5.3	Advance Port Knocking Authentication Scheme with QRC using AES	23
2.5.4	Network Security Using Hybrid Port Knocking	25
2.5.5	Others Implementation	26
2.6	Comparison of related research	29

CHAPTER 3

METHODOLOGY

3.0	Introduction	32
3.1	Project Methodology	32
3.1.1	Gathering Information	33
3.1.2	Analysis	34
3.1.3	Design	34
3.1.4	Implementation	34
3.1.5	Testing	34
3.1.6	Result and Discussions	35
3.1.7	Documentation	35
3.2	New Port Knocking Method	36
3.2.1	Head to Head Comparison on Process Flow	40
3.2.2	Proposed Design Architecture	43
3.2.3	Design Features	44
3.3	Experimental Design	45
3.3.1	Test 1 (Sniffing)	47

ABSTRACT

Port knocking is a technique first introduced in the Black Hat to prevent attackers from discovering and exploiting potentially vulnerable services on a network host, while allowing authenticated users to access these services. Despite being a potentially useful tool, it suffers from various vulnerabilities such as TCP replay, port scanning, and etc. Most work in this area is proposed as a complex method to harden port knocking. This study presents an improved scheme over the existing Port Knocking by employing the Source Port sequences that will simplify a technique for the port knocking system. Source ports are usually automatically generated by the operating system. Source ports are pre-assign to generate a sequence. A technique to control when certain services start and stop was introduced to mitigate the problem with TCP replay attacks and port scanning. In addition, a proposed method does not need to integrate with a firewall like other port knocking methods. Experiments indicate that packet capture was able to grab port sequences but does not define what the service request is. In terms of performance, the proposed method works faster than other methods like Basic port knocking and Fwknop + SPA. The performance of the proposed method was evaluated by measuring the authentication time to knock the server. The proposed port knocking method is useful to system administrators who need to access the server remotely but has strict firewall rules.