

**UNIVERSITI TEKNOLOGI MARA**

**SYMMETRIC ENCRYPTION  
USING PRESHARED PUBLIC  
PARAMETERS FOR A SECURE  
TFTP PROTOCOL**

**NUR NABILA BINTI MOHAMED**

Thesis submitted in fulfilment  
of the requirements for the degree of  
**Master of Science**

**Faculty of Electrical Engineering**

**February 2015**

## AUTHOR'S DECLARATION

I declare that the work in the thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree of qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

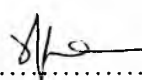
Name of Student : Nur Nabila binti Mohamed

Student I.D. No. : 2012629994

Programme : Master in Electrical Engineering (EE780)

Faculty : Electrical Engineering

Thesis Title : Symmetric Encryption Using Preshared Public  
Parameters For A Secure TFTP Protocol

Signature of Student :   
.....

Date : February 2015

## ABSTRACT

Due to rapid development of communication technology of constrained embedded systems, it is important to deal with security including integrity and confidentiality to maintain the accuracy while distributing data safely and efficiently. Trivial File Transfer Protocol (TFTP) is used for transferring files quickly and simply. The main advantage of using TFTP in embedded system is because of its speed and simplicity but it provides no security mechanism which makes it vulnerable to various attacks. This work proposes the security implementation of Diffie Hellman Key Exchange (DHKE) by presharing public parameters for mutual authentication that enables two communicating parties to achieve the same secret key. The concept is integrated with compression and encryption technique to significantly reduce the computational requirements in TFTP communication. The experiment is done on two embedded devices to perform the functionality of key exchange and data encryption in TFTP. The results were analyzed in terms of confidentiality and integrity of data, execution time, file scheme throughput, compression ratio, average file reduction percentage and transmission time using variable file size. The results show that the proposed work based on DHKE using preshared public parameters includes compression and encryption technique is an efficient solution to mitigate Man In The Middle (MITM) attack as well as manage security issues and large file sizes. The purpose of TFTP which acts as a simple file transfer protocol would bring huge advantages to be employed in ubiquitous computing environment if the basic security strategies were integrated with this protocol.

# TABLE OF CONTENTS

<b>AUTHOR'S DECLARATION</b>	<b>ii</b>
<b>ABSTRACT</b>	<b>iii</b>
<b>ACKNOWLEDGMENTS</b>	<b>iv</b>
<b>TABLE OF CONTENTS</b>	<b>v</b>
<b>LIST OF TABLES</b>	<b>viii</b>
<b>LIST OF FIGURES</b>	<b>ix</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xi</b>
<b>CHAPTER ONE: INTRODUCTION</b>	<b>1</b>
1.1 RESEARCH BACKGROUND	1
1.2 MOTIVATIONS	3
1.3 RESEARCH OBJECTIVE	3
1.4 RESEARCH PROBLEM	4
1.5 SCOPE OF STUDY	4
1.6 RESEARCH CONTRIBUTION	5
1.7 THESIS OUTLINE	6
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>7</b>
2.1 INTRODUCTION	7
2.2 FILE TRANSFER PROTOCOLS	9
2.2.1 Trivial File Transfer Protocol	11
2.2.2 Constraints in TFTP	15
2.3 OVERVIEW OF CRYPTOGRAPHY	17
2.3.1 Security Properties	18
2.3.2 Cryptographic Hash Functions	19
2.3.2.1 <i>Secure Hash Algorithm</i>	20

2.3.3	Asymmetric Key Encryption	20
	2.3.3.1 <i>Key Exchange Protocol</i>	21
2.3.4	Symmetric Key Encryption	27
	2.3.4.1 <i>Advanced Encryption Standard</i>	28
2.3.5	Constraints in Symmetric Asymmetric Encryption	31
2.4	DATA COMPRESSION IN COMMUNICATION	32
	2.4.1 Huffman Lossless Compression Algorithm	32
	2.4.2 Compression and Encryption Approach	33
2.5	RELATED WORKS IN SECURE TFTP	37
2.6	SUMMARY	38
 <b>CHAPTER THREE: METHODOLOGY</b>		<b>39</b>
3.1	INTRODUCTION	39
3.2	PROJECT WORK FLOW	40
3.3	DEVELOPMENT ON DESKTOP PLATFORM	45
3.4	TESTING ON EMBEDDED PLATFORM	46
3.5	COMPRESSION AND SECURITY PERFORMANCE	49
	3.5.1 Checking Both Sides Get Same Secret Key	50
	3.5.2 Execution Time of Compression/Encryption	50
	3.5.3 File Scheme Throughput	50
	3.5.4 File Compression Ratio	50
	3.5.5 Average File Size Reduction Space	51
	3.5.6 Execution Time of File Transmission	51
3.6	SUMMARY	52