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