UNIVERSITI TEKNOLOGI MARA

EFFECT OF FILE SIZES ON ENCRYPTION AND DECRYPTION IN CONSTRAINED DEVICES

NURNADIA BINTI SAPRI

Thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science

Faculty of Electrical Engineering

July 2015

ABSTRACT

TCP protocol can be used in the transmission of data from one host to another host. Simply, it is unsecure because the attacker can break security parameters to obtain access to the data that currently being sent. As a communication and transmission of files over Internet has increased exponentially since last few years, there is need of security in such file transfer. Therefore, the effect of file sizes on encryption and decryption in constrained devices have been analyzed using two types of cryptographic algorithm which is AES-128 (symmetric-key encryption) and RSA-2048 (asymmetric-key encryption) based on the different file size, execution time, and the throughput. AES-128 has faster encryption and decryption time, low power consumption, faster in hardware and software implementation, and high throughput compared to RSA-2048. Moreover, AES-128 algorithm provides higher security compared to RSA-2048. Therefore, AES-128 gives higher confidentiality compared to RSA-2048 and it will be most suitable encryption algorithm to be implemented in the TCP protocol.

Keywords—Transmission Control Protocol (TCP), Advanced Encryption Standard (AES), RSA algorithm, Asymmetric, Symmetric, Security, Confidentiality, File Transfer.

ACKNOWLEDGEMENT

This Master thesis project is the final step in obtaining my Master of Science in Telecommunication and Information Engineering (EE700) at Universiti Teknologi MARA(UiTM).

The thesis was conducted under the supervision of Professor Madya Dr. Habibah Hashim, lecturer in Computer Engineering Department of Faculty of Electrical Engineering at UiTM Shah Alam. I have been working on my Master thesis project from March 2015 to July 2015. While undertaking this project, I have had much encouragement from many people. I would like to express my sincere gratitude.

First of all I am particularly indebted to Professor Madya Dr. Habibah Hashim, my supervisor. She was been a great support since the beginning of the thesis and showed trust in me when I first approached her with the aim of finishing my thesis within one working semester. In some circumstances when I had unexpected problems during my project, she was there to find a solution and provide full guidance with patience and flexibility.

Secondly, I would also like to thank to Nur Nabila Mohamed and Mohd Anuar Mat Isa for guiding me during completing this project in the laboratory. Further, I would like to thank everybody who has helped me by proofing reading my thesis. Finally, I want to thank my family for their unwavering support.

TABLE OF CONTENTS

Page