UNIVERSITI TEKNOLOGI MARA

IMPLEMENTATION OF LOCAL PROPRIETARY SYMMETRIC AND ASYMMETRIC ALGORITHM AS SECURE PLUG-IN ON MICROSOFT OUTLOOK

MOHD IZHAR BIN JAAFAR

Dissertation submitted in partial fulfillment of the requirements
for the degree of
Master of Computer Networking

Faculty Of Computer & Mathematical Science

January 2012

ACKNOWLEDGEMENT

In the name of Allah, who is the Most Gracious, Most Merciful and Him alone is worthy of all praise. To Him all the praise go and to Him all the thankfulness of giving me the opportunity to live day in and day out.

A million thanks to my supervisor, Dr Fakariah Hani Hj. Mohd Ali who has given all the supports, guides in giving remarkable idea as well as reviewing my draft reports and have put such a constructive suggestion and comments for a better improvement.

Last but not least, my deepest gratitude and love to my parents and family members, for their unconditional love that make everything possible. My earnest thanks to all the helpful people that I have not mentioned here. Thank you for contributing directly and indirectly to the success of my project. With all the support. I gain more than just special topic report but also the inspiration of a lifetime. For all my friends in CS778, I would like to thank for their help, friendship and countless support to me. May Allah S.W.T. bless all of them for their kindness and supported.

Thank you

ABSTRACT

Email is the most important communications system in the world. However the internet traffic between the sender and recipient is routed through many countries, even they live on the same area and the content of email messages are generally not encrypted and unsecured. They need to communicate in secure environment to avoid eavesdropping or interception. The purpose of this study was to design and develop new secure plug-in on Microsoft Outlook using integration of symmetric and asymmetric cryptographic algorithm. The design was combined with two types of cryptographic algorithm to have an extra level of security value. It have increase complexity of process encryption and decryption. New integration also have an extra value security because of the symmetric algorithm was developed locally in Malaysia. Apart from symmetric algorithm, Public Key Infrastructure technologies that one of the asymmetric algorithm have been select as a part of new integration. It have been utilized the Public and Private Key to have an extra level for user authentication. Security analysis was performed to verify the new secure plug-in in encrypted format during transmission over the network. It was conducted to intercept transmission between the sender and recipient. The findings show that the new integration has capabilities to send encrypted messages during transmission process and give the secure communication channel especially for secure email system. For future research, the new integration can be proposed to integrate with digital signature to avoid interception.

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 1

INTRODUCTION

1.0. Background

Email is the most important business communications system in the world that help to enable organizations to efficiently interact with customers, clients, and business partners. However unprotected email poses a critical risk to a confidential sensitive data such as customer information, financial data, trade secrets, and other proprietary information. Exposure of this information to unauthorized parties can result in financial loss, legal ramifications, and brand damage. The institute that deals with classically sensitive data should seriously consider the benefits of secure email system which it is the best implementation for secure communication.

In this work, a secure communication architecture was discussed, in which the data is protected by local proprietary symmetric cryptographic algorithm as main engine. In this design, the permutation algorithm requires a hex as a key. The key is employed to permute the original message to an encrypted one. The session key will be encrypted using public key of recipient and then embedded into encrypted message. The final result is a encrypted message containing encrypted message with