Universiti Teknologi MARA

A Study on One Way Hashing Function and its Application for FTMSK Webmail

Noor Hasimah Ibrahim Teo

Thesis submitted in fulfillment of the requirements for
Bachelor of Science (Hons) Information Technology
Faculty of Information Technology And Quantitative Science

November 2005

DECLARATION

I certify that this thesis and the research to which it refers are the product of my own work and that any ideas or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline

NOVEMBER 21, 2005

NOOR HASIMAH IBRAHIM TEO

2003327385

ABSTRACT

Password is a normal way for securing data from intruders. The widespread use of password is in email account. The advances of technology have reduced the function of password in security, where there are many chances of password to be sniffed or hack by intruders. FTMSK webmail is using password as an authentication method. The problem was, their lecturer is not allowed to send examination question through email. This means that they do not trust the security of webmail. There are several techniques use to transform plaintext password to other form of password. One of it is call one-way hashing function. One-way hashing function consists of several algorithms. However MD5 is the most common hashing function currently in use. The research are aim to determine security of using one way hashing function at client side for FTMSK webmail login system and design framework for one way hashing function. A prototype is developed using MD5 algorithm and based on prototype approach, since it study on existing system. Tests are run for both FTMSK webmail and prototypes to determine whether the plain text password can be retrieved. Furthermore framework for one way hashing function is designed. Password need to be store in database on server in the form of hashing value. Secure password during transmission can be obtained by running protection on the client side of client server architecture.

TABLE CONTENTS