UNIVERSITI TEKNOLOGI MARA

VULNERABILITY ASSESSMENT ON UITM STUDENT ID CARD

MUHAMAD HAZHA BIN HASHIM

Dissertation submitted in partial fulfillment of the requirements
for the degree of

Master of Science (Computer Networking)

Faculty of Computer and Mathematical Sciences

January 2014

ABSTRACT

The Mifare Classic is the most widely used contactless smart card in the world. Its communication protocol is based on the open ISO-14443-A standard, but the authentication and encryption protocols are proprietary. Several researchers have cracked its encryption and proposed attacks to recover the access keys. This paper will examine the MIFARE Classic 1K contactless card that being used as the student ID card in University Technology MARA (UiTM). In doing so, we have identified its major weakness and have recommended ways to mitigate it.

ACKNOWLEDGEMENT

In the name of Allah, the most Beneficent the most Merciful. First, praise to Allah, the Almighty, for I am thankful to Him that without His guidance and blessings, I would never be able to complete this project. Second, my sincere indebtedness goes to my supervisor, Dr. Kamarularifin bin Abdul Jalil, whose ideas, insights and constructive comments have assisted me tremendously throughout this project.

I would also like to convey my deep-hearted appreciation to my beloved mother and father, my dearest wife and kids for their continuous moral support, endless patience and encouragement in inspiring me, that as a learning individual, I will always be motivated to give my best no matter what the obstacles.

Finally, an honourable mention goes to my friends from the post-graduate studies (CS778), esteemed colleagues from HP Multimedia Sdn. Bhd. and fellow networkers who rendered their help and provided vital assistance during the period of completing this project.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Research Introduction

UiTM student ID card is a photo card that is issued to every enrolled student. Information such as the student's name, number, IC number, programme code, programme name, faculty, campus, and intake semester are printed on the card. This card has an embedded MIFARE Classic 1K chip that stores necessary information to authenticate itself with compatible readers. This card is currently used for parking access, door access, and library activities such as borrowing books from self-service machines, etc.

This research will address the MIFARE Classic 1K contactless smart card which is being used as a student ID card in University Teknologi Mara (UiTM). Other contactless cards and their technologies might be similar in operation, but are fundamentally different. The MIFARE Classic card has become increasingly popular in many countries and in education institutions that require the ability to issue and replace new cards at a low cost. MIFARE Classic cards consist of two parts; a microchip which holds data and a thin loop of wire which acts as an antenna and powers the chip through resonant inductive coupling (Layada.net, 2013). Operating on the 13.56 MHz frequency, when a MIFARE Classic card comes within a short distance of a compatible smart card reader, the electromagnetic field being emitted by the reader provides power to the embedded chip in the card. Next, a series of requests and responses are transmitted between the reader and the card to provide authentication. The MIFARE