中國文化大學商學院資訊管理學系研究所

碩士論文

Graduate Institute of Information Management

College of Business Chinese Culture University

Proposal of Thesis

# Mifare Classic 模擬及安全性改良之研究

A Study on the Improvement of Mifare Classic Simulation and Security



李魁元

Lee, Kuei Yuan

指導教授：周立平 博士

孫振東 博士

Advisor: Chou, Li-Ping PhD

Sun, Jenn-Dong PhD

中華民國 101 年 1 月

January, 2012

論文名稱：Mifare Classic 模擬及安全性改良之研究 總頁數：102

校(院)所組別：中國文化大學資訊管理學系碩士在職專班
畢業時間及提要別：一百學年度第一學期碩士學位論文提要
研究生：李魁元
指導教授：周立平

論文提要內容：

本研究主要探討「非接觸式」的智慧卡，因為「非接觸式」智慧卡溝通是透過無線電的方式做傳送，因此很容易讓攻擊者以側錄的手段，獲取相關的資訊，造成安全上的問題，例如：複製卡片，竄改卡片的資料…等。

目前使用最廣泛的智慧卡是 Mifare Classic 卡，Mifare Classic 卡是一種可在同一張卡片處理多種不同應用的卡片，因此，本研究以 Mifare Classic 卡為對象。

2008 年開始有許多對 Mifare Classic 卡之安全性的研究被提出，這些研究發現有許多弱點並透過某些攻擊 可以取得卡片的金鑰，藉以更改卡片的資訊，本研究會對這些方式做相關實驗，驗證其可行性。本研究成功利用 proxmark3 設備去模擬 Mifare Classic 卡片，與相關讀卡機實驗，可通過門禁與餘額查詢機。

透過實驗了解到 Mifare Classic 卡鑑別上安全性之弱點，並從這些弱點中，提出改進的方式。對攻擊者可能產生的行為中，尋求因應的方法，能提高 Mifare Classic 卡安全性，減少被攻擊的機會，本研究提出相關的防禦方法能抵禦大部份現有攻擊方式。

關鍵字：非接觸式、智慧卡、Mifare Classic

A Study on the Improvement of Mifare Classic Simulation and Security

Student: Kuei-Yuan Li Advisor: Prof . Li-Ping Chou

Prof . Sun, Jenn-Dong

Chinese Culture University

## ABSTRACT

This study focused on the simulation and security problems of contactless smart card. Since contactless smart cards communicate through radio, it is easy for an attacker to eavesdrop and obtain the card related information. This causes security problems such as card duplicating and card data tampering.

Currently, the most widely used smart card is Mifare Classic card, which is used in a broad range of applications including transport ticketing, access management, e-payment, etc. Therefore, this study targets Mifare Classic card.

In the last few years, many articles have been devoted to the study of Mifare Classic card security. Their studies found that due to many weaknesses in Mifare Classic card the card key can be retrieved by certain attacks and accordingly the card data can be changed. According to their methods, this study conducts experiment to verify their feasibility. This study makes use of Proxmark3 device to read and emulate Mifare Classic card. In the card emulation experiments, the emulation card can be read by building access control reader and MRT balance inquiry machine, successfully.

According to the security weakness of Mifare Classic card authentication learned through experiments, an improved method is proposed to increase the security of Mifare Classic card. Since the proposed method aimed at possible attacker behaviors, it can defend against most existing attacks.

Keywords: contactless, smart card, Mifare Classic

# 誌　謝　辭

本論文幸蒙恩師周立平老師、孫振東老師之悉心指導，在恩師的諄諄教誨下，及在楊博宏、邱乙城、邱奕豪各位學弟的支持與幫助下，才能順利完成，師恩浩翰，無以回報，在此謹向恩師致上最高的敬意！

# 目錄

# 表目錄

# 圖目錄