MULTIMEDIA UNIVERSITY®

TPT1201
RESEARCH METHODS IN CS

Trimester 1, Session 2015 / 2016

Lecturer: Dr. Poo Kuan Hoong

Topic: Near Field Communication Based Payment System Using Information Hiding

BY

No.	Student ID	Student Name
1	1121115798	TAN JACK HAU
2	1122701188	LOW JIA MING

GROUP SECTION: <<CM01 >>

Contents

1 Executive Summary of Research Proposal **3**

2 Introduction **3**

3 Justification of Research **4**

4 Research Objective **4**

5 Literature Review **4**

6 Research Methodology **5**

Near Field Communication Based Payment System Using Information Hiding

Low Jia Ming, Tan Jack Hau

1 Executive Summary of Research Proposal

In this paper, we proposed a Near Field Communication (NFC) based payment system to enhance the current touch and go concept payment methods. The current payments method are having security problem, especially Visa payWave credit card. Users can do payment without any confirmation. It means that users is not required to show the ownership of the card. Steganography is implemented to overcome the problem. The system will request a photo from users and generate a passcode to embed into the photo. The system used the Least Significant Bit (LSB) Insertion technique to embed the passcode into the photo. Users is required to download and store it into smartphone. During the transaction, users are required to send the stego-photo to the NFC reader by simply touch on the smartphone screen in front of the Near Field Communication (NFC) reader or a tag. If the passcode is correct, the transaction will be proceeded and show the message. If the passcode not correct, an error message will be shown on the screen of the device. We can avoid the unauthorized people to access our account or use our credit card with NFC based payment system as they dont know the stego-photo.

2 Introduction

The technology become more advance and simplified human life. People enjoy the convenience brought by the high-tech services especially touch and go services. The traditional credit card had been improved by adding Visa payWave services. Users can make the payment without signature and password. However, the amount of information theft cases is growing instantaneously. The existing security problems of the Visa payWave credit card are the card information easy to be stole. [2] Unauthorized people that has the card or the information inside the card, and then he/she can do the transaction using the victims bank account. The information theft use Radio Frequency Identification (RFID) reader to steal

the payWave credit cards information by a simple tag. Cardholder will only feel touched by other people, but the information of the credit card was stolen by the theft. If the card is lost or stolen, cardholder will realize that the card was missing. However, no one will know the information of the card was stolen.

We proposed an Electronic Payment System using Near Field Communication (NFC) to enhance the touch and go concept payment method. There are two level of the protection we implemented. The first level is using the NFC technology for enhance the security level to protect users information. The second level of the protection is using information hiding technique to make the transaction secure. We chose the stego-photo as a key for users to verify themselves during the transaction.

3 Justification of Research

The purpose of this research is to enhance the security of the touch and go concept payment method. We proposed an Electronic Payment System using NFC to identify the correct cardholder without signature and password. User can complete the transaction by sending a stego-object to payment device using a single touch on the screen. Information thieves cant get the cards information from smartphone using RFID reader. If the smartphone lost, unauthorized people cant use the cards as they dont know the location of the stego-photo in the smartphone.

4 Research Objective

. To enhance the touch and go concept payment method by using NFC based payment system.

. To secure the user credit card information and account when the smartphone is missing

5 Literature Review

I *Steganography*
The stego-object will implement as a verification of authentication in the system. The system will generate a passcode and use information hiding technique to embed the code in to the object, such as, video, audio, image or text. Human cannot differentiate the stego-object and the original object. In this

paper, photo is used as the key to complete the transaction. The system will embed the generated passcode into the photo to produce the stego-photo. [3]

II *NFC smartphone based access control system*
A digital access control system by using near field communication (NFC) smartphone to unlock the door and replace the access card. They mentioned that if the system uses the access card or physical key as key to access the premise, then everyone who has the key can gain the access which is an insecure system. So, they provided a technique to overcome the problem by using stego-photo. [1] System will generate the passcode and embedded it into the users photo which will become the stego-photo. The NFC reader will receive the stego-photo sent by smartphone, if the passcode inside the stego-photo is not match with the passcode inside the database, a light emitting diode (LED) will be turned on to alert the unauthorized users. [7]

III *Secure payment with NFC Mobile Phone*
The paper concerned the security problem of the NFC-based payment system. In the paper, they said that smartphone services and payment services need a strong authentication to make it secure. [6] The management of the application should be standardize. The application should follow the standard of the intellectual property of the services provider. [4]

6 Research Methodology

We proposed NFC-based payment system using information hiding. Users should register an account through the website we provided. [4] It acts as an online banking system website for register an account to allow users to use the service. During the registration process, a Transaction Authorization Code (TAC) will be send to users smartphone by using message. Users need to use that to identify themselves. Users need to enter a passcode that is provided by the bank, and take a photo by using the system. Once the passcode is matched, the system will start to embed the passcode into the users photo. The stego-photo is generated. The users can download it through the smartphone by scanning Quick Response (QR) code. In the future, users want to go through the TAC verification first, then the system will only allow users to change the stego-photo. However, users can abort the credit cards information stored in the account without TAC verification.

When the users want to do the payment, users tap the NFC smartphone in front of the NFC reader or tag. An application will prompt out and require users to select the correct stego-photo in the smartphone. The stego-photo will send to a device to perform passcode decoding and send the passcode to the bank server.

After the passcode matching, result will be sent back to the device. If the passcode is correct, the transaction will be proceeded and show the message. If the passcode not correct, an error message will be shown on the screen of the device.

A *Least Significant Bit (LSB) Insertion*

LSB Insertion is information hiding method. LSB insertion use the binary representation of the hidden message and overwrite the LSB of each bytes of the cover photo by the messages binary code one by one. [5] The coverphoto is 24-bits color and approximate 1.7 million of colors inside a photo. The color is represented as pixel. A pixel is denote to three bytes in terms of Red, Green, and Blue (RGB). The messages characters will be translate American Standard Code for Information Interchange (ASCII) number. The number will be translated to binary representation. For example, the character A has an ASCII number, 65 and binary representation of 65 is 01000001. Three continuous pixels is required to embed a character A. Three pixels have nine bytes, so one bytes is left over. [7]

References

[1] Information hiding techniques for steganography and digital watermarking. 2000.

[2] E. Husni and A. Ariono. Development of integrated mobile money system using near field communication (nfc). pages 1–6, Oct 2014.

[3] H.B. Karaman and S. Sagiroglu. An application based on steganography. pages 839–843, Aug 2012.

[4] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger. Nfc devices: Security and privacy. pages 642–647, March 2008.

[5] Gaurav Narayana, Sujay; Prasad. Two new approaches for secured image steganography using cryptographic techniques and type conversions. pages 60–73, Dec 2010.

[6] T.M. Techoro, S. Butakov, S. Aghili, and R. Ruhl. Leveraging cobit5 in nfc-based payment technology: challenges and opportunities for security risk mitigation and audit. pages 1–6, Feb 2015.

[7] Peng-Loon Teh, Huo-Chong Ling, and Soon-Nyean Cheong. Nfc smartphone based access control system using information hiding. pages 13–17, Dec 2013.

Project Assessment

Title of your research project	
Member of you project	
Executive Summary (5 marks)	
Introduction (3 marks)	
Justification of Research (3 marks)	
Research Objectives (3 marks)	
Literature Review (6 marks)	
Research Methodology (8 marks)	
References (2 marks)	