Journal of Organizational and End User Computing
Volume 33 • Issue 2 • March-April 2021

A Key-Based Mutual Authentication Framework for Mobile Contactless Payment System Using Authentication Server

Brij B. Gupta, National Institute of Technology, Kurukshetra, India & Asia University, Taiwan & Macquarie University, Australia

Shaifali Narayan, National Institute of Technology, Kurukshetra, India

ABSTRACT

This paper presents a framework for mutual authentication between a user device and a point of sale (POS) machine using magnetic secure transmission (MST) to prevent the wormhole attack in Samsung pay. The primary attribute of this method is authenticating the POS terminals by an authentication server to bind the generated token to a single POS machine. To secure the system from eavesdropping attack, the data transmitted between the user device and the machine is encrypted by using the Elgamal encryption method. The keys used in the method are dynamic in nature. Furthermore, comparison and security analysis are presented with previously proposed systems.

KEYWORDS

Authentication, Contactless Payment, Magnetic Secure Transmission, Samsung Pay, Wormhole Attack

INTRODUCTION

The rapid growth in the technology has led to the development of many innovative services and applications in the field of payment systems. The transactions have turned from cashed to cashless. (Gupta & Quamara, 2018, 2019) discussed that to make the transactions cashless, smartcards were used as the credit/debit card, but they were prone to physical attacks, side channel attacks, and logical attacks. To make the cards more secure, different security algorithms that were combined with the smart cards and added biometric features for security and privacy (Nedjah et al., 2017, pp. 18-32). To reduce the time complexity and to provide ease to the user contactless smartcards were brought in use. Contactless smartcards were prone to sniffing attack and physical damage, and to overcome it mobile wallets and mobile contactless payment systems were used which are based on NFC (Near Field Communication) and MST (Magnetic Secure Transmission) (Andersson, 2016).

With the change in time, the methods to carry out the cashless transactions has also modified from smart cards to smart phones and internet banking. The current trends for e-cash payment includes the debit and credit cards, Samsung Pay, Google Pay, Apple Pay, Freecharge, Mobiwik, Jio money, SBI money, Paytm, Airtel money, pockets by ICICI, and many more mobile banking applications. These applications are provided by the bank, telecom industries and private industries. According to Wang et al. (2016), the key characteristics provided by the mobile wallets include the security, transferability, and anonymity. The mobile wallets are differentiated based on proximity payment technologies like NFC, MST, QR code, etc. There are certain threats to be considered against the basic mobile wallet components which are described in table 1.

DOI: 10.4018/JOEUC.20210301.oa1

This article, published as an Open Access article on December 18, 2020 in the gold Open Access journal, Journal of Organizational and End User Computing (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

NFC is a group of communication protocols which allows two electronic devices to establish communication by radio frequency, example- Apple Pay. NFC is a short-range half duplex communication protocol that creates communication between two devices at an operating frequency of 13.56 MHz. There are three modes of communication for NFC: reader/writer mode, peer to peer, and card emulation. MST is a technology for mobile payments which enables the smart phone to emit electromagnetic signals and mimic as the magnetic stripe on the credit/debit cards like Samsung Pay. MST sends the magnetic signals from user device to the card reader and emulates the swiping of a card. The transactions are made without upgrading the systems which is an advantage over the NFC. The NFC requires the card reader terminal to be upgraded in hardware and software aspect.

NXP semiconductors is a company that manufactures semiconductors and have splits the contactless possible application into four categories which depends upon the way the consumer will use the application:

1. **Touch and Go:** Application allows the consumer to tap the card on POS and no wait to confirm the transaction.
2. **Touch and Connect:** Link the two devices to exchange the data or money.
3. **Touch and Confirm:** User must confirm the transaction by entering password or fingerprint.
4. **Touch and Explore:** User is offered more than one features to make use.

Mobile contactless payment system stores the virtual debit and credit card information and allows the customer to use that information to securely pay for the purchases in store with those cards by tapping the smart phone in front of the radio frequency enabled readers (Andersson, 2016). The use of virtual card eliminates the threat to compromise of cardholder sensitive data. These systems working on the Near Field Technology (NFC) and Magnetic Secure Transmission (MST) technique provides notable advantages and is compliant to EMV standards. It provides multi-layer security and is convenient as it has eliminated the need to carry plastic cards. The popular applications which are in use nowadays are Apple Pay, Samsung Pay, Google Pay, and Pockets by ICICI bank (Bosamia, 2018). Other than the credit/debit cards loyalty cards can also be stored in these applications.

Depending on the amount of money transferred, the contactless payment can be divided into two groups - micro and macro. Micro payment is the one where the user makes a small contactless transaction. For this the user uses the contactless application 'touch and go', while the Macro payment is the one where the user transfers a big amount. For this the user will use the contactless application 'touch and confirm', where the transaction will be confirmed either by entering pin or by a physical signature.

To make the contactless transactions secure, the concept of tokenization is used. As these transactions are done without any physical connection with the terminal and the data is transmitted wirelessly, it is more prone to wormhole attack (Gupta & Narayan, 2020). Samsung Pay uses MST and (Korolov, 2016, para. 4) discussed that Salvador Mendoza detected eavesdrop on the MST transmission. (Vincent, 2016, para. 2, 3) discussed how this vulnerability enables the attacker to skim the cards and make fraud payments. (Kawamoto, 2017, para. 2,3) discussed how the leaked information can allow an attacker to learn much about the internal mechanism of Samsung pay, and the attacker can use the information for their own advantage.

In this paper we will propose a framework to secure Samsung Pay from wormhole attack with the help of an authentication server. The framework is different from the previously proposed schemes in multiple ways like complexity, data storage and key generation. The framework is designed to overcome the merchant threats, acquirer threat, payment application provider threat and threat to payment network provider. The rest of the paper is organized as follows- section 2 describes the background of the topic, section 3 describes the related schemes proposed to overcome the wormhole attack in contactless payment using MST, section 4 describes the proposed system, section 5 gives the details of implementation including the results and comparison and section 6 presents the conclusion.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-key-based-mutual-authentication-framework-for-mobile-contactless-payment-system-using-authentication-server/269371

Related Content

Perceptions of End Users on the Requirements in Personal Firewall Software: An Exploratory Study
Sunil Hazari (2007). *Contemporary Issues in End User Computing (pp. 174-196).*
www.irma-international.org/chapter/perceptions-end-users-requirements-personal/7036

Fundamentals of Multimedia
Palmer W. Agnewand Anne S. Kellerlan (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications (pp. 43-51).*
www.irma-international.org/chapter/fundamentals-multimedia/18169

Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users
Judy Drennan, Gillian Sullivan Sullivanand Josephine Previte (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications (pp. 1-18).*
www.irma-international.org/chapter/privacy-risk-perception-expert-online/18165

Are Information Systems' Success and Failure Factors Related? An Exploratory Study
Jeremy J. Fowlerand Pat Horan (2007). *Journal of Organizational and End User Computing (pp. 1-22).*
www.irma-international.org/article/information-systems-success-failure-factors/3824

Microcomputer Laboratory Maintenance
Norman A. Garrettand Terry D. Lundgren (1992). *Journal of Microcomputer Systems Management (pp. 13-20).*
www.irma-international.org/article/microcomputer-laboratory-maintenance/55684