An Efficient Decentralized Mobile Payment Protocol With Improved Security and Privacy

A DISSERTATION PRESENTED

BY

MOHAMMAD VAHIDALIZADEHDIZAJ

TO

THE DEPARTMENT OF COMPUTER SCIENCE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE SUBJECT OF

COMPUTER SCIENCE

PACE UNIVERSITY

NEW YORK, NY

MAY 2017

We hereby certify that this dissertation, submitted by **Mohammad Vahidalizadehdizaj** satisfies the dissertation requirements for the degree Ph.D. in Computer Science and has been approved.

Lixin Tao — 5/10/17

Dr. Lixin Tao — Date
Chairperson of Dissertation Committee

5/10/17

Dr. Charles Tappert — Date
Dissertation Committee Member

M. Badiì — 5/10/17

Dr. Mehdi Badiì — Date
Dissertation Committee Member

Seidenberg School of Computer Science and Information Systems
Pace University

Thesis advisor: Dr. Lixin Tao Mohammad Vahidalizadehdizaj

An Efficient Decentralized Mobile Payment Protocol With Improved Security and Privacy

Abstract

The exponential growth of mobile devices makes them a suitable computing platform for electronic payment. However, there are serious challenges in e-commerce transactions, such as privacy protection, security, bandwidth limitations of mobile networks, and limited capabilities of mobile devices to handle excess or indirect computational time. The traditional e-commerce payment protocols that were originally designed to keep track of the traditional flows of data from desktop computers are vulnerable to attacks, and because they were not designed for mobile platforms, have excessive engineering overhead. In this thesis, a new private mobile payment protocol is introduced that is designed specifically for the mobile platform. It is based on a client-centric model that utilizes symmetric key operations. The protocol reduces the computational cost (the engineering overhead) of Diffie-Hellman key agreement protocol by using the algebra of logarithms instead of the algebra of exponents. The protocol achieves proper privacy protection for the payer by involving mobile network operators and generating temporary identities. It avoids replay attacks by using random time-stamp generated numbers.

Contents

Listing of figures

I dedicate this thesis to my mother and father.

Acknowledgments

I would like to express my grateful appreciation and thanks to God. You gave me strength to never give up even in the hardest situations. A special thanks to my family. Words cannot express how grateful I am to my mother and father for all of the sacrifices that they made on my behalf. Their prayers for me sustain me always. I would also like to thank all of my friends who supported me in writing and encouraged me to strive towards my goal of contributing to the body of knowledge of Computer Science.

Lovers find secret places inside this violent world where they make transactions with beauty.

Jalaluddin Rumi

1 Introduction

E-commerce is commerce via the internet. E-commerce is any financial transaction over Internet like ordering a book from an online bookstore. Most of the time payer uses his credit card in this process. An e-commerce transaction involves purchaser or cardholder, merchant, purchaser's credit card issuer (bank), merchant's acquirer (bank), and certification authority for supporting secure transaction execution. Most of these protocols are using Diffie-Hellman for establishing a secure connection between the engaging parties. Most important challenges in this field are security and privacy. Mobile commerce or m-commerce is electronic commerce conducted via the mobile platform. An m-commerce transaction involves all e-commerce parties plus mobile network operators. [37].

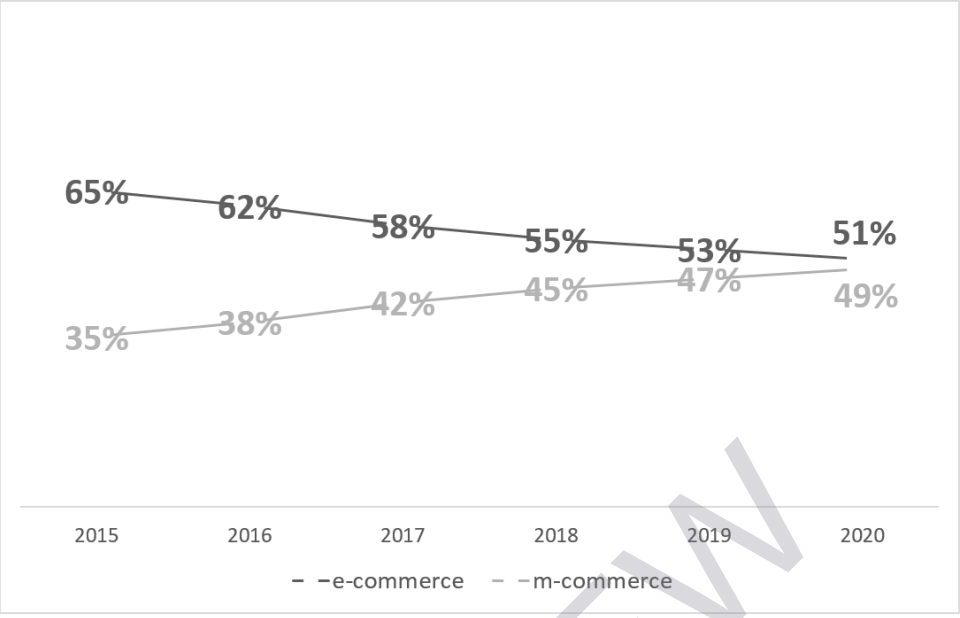

Figure 1: Mobile commerce share of e-commerce

In a typical payment scenario, the customer should open a credit card account in a bank that supports electronic payment. The payer may receive a digital certificate signed by the bank (based on the protocol that his card issuer is using). Then, the customer selects his items or services by browsing merchant's website and order them. The customer should send a message that includes two parts. The first part that includes order information is for the merchant. The second part is for merchant's bank that includes payment information. Merchant's bank should check this payment information with the issuer of the credit card for authorization. After a successful authorization, merchant's bank informs the merchant that the payment information is acceptable. Then, merchant completes the order, sends confirmation and invoice to the customer, and captures the transaction from his bank. Note that, for m-commerce, the mobile network operator may be involved in this process.

Mobile commerce (m-commerce) is e-commerce activities conducted via the mobile platform. Principals of m-commerce are the same as e-commerce plus

mobile network operator. M-commerce inherits the challenges of e-commerce. Moreover, most of the e-commerce protocols are based on public key cryptography that is not efficient in mobile and wireless networks. Some of these protocols are keeping credit cards information on mobile devices or using this information in transactions without proper protection. Therefore, they are vulnerable to attacks [35].

Mobile devices like smartphones and tablets are becoming very popular among people worldwide. People carry these devices and use them in different situations and locations. There are more mobile devices in the world than there are computers. Also, these mobile devices are the most accessible computer in daily lives. Most of these devices are light, easy to carry, and convenient to use. Mobile devices are compatible with networks like 4G LTE that is available in outdoor spaces. More than half of the internet access in the world is through the mobile devices (instead of personal computers). Also, people would rather order their needs (goods or services) online through their smartphone [3].

The growth of m-commerce sales continues to be rapid even with the challenges that m-commerce face like slow download times. Forrester predicted 11 percent (of whole e-commerce) growth in m-commerce between 2016 and 2020. Currently, m-commerce has 35 percent of e-commerce transactions. Forrester predicts that m-commerce will be 49 percent of e-commerce in 2020. This amount is 252 billion dollars in sales. You can see m-commerce growth forecast in figure 1 [5]. The amount of Chinese mobile payment (m-commerce), has exceeded Japan's GDP. This is because of reliable mobile payment services in China. China smartphone payments have been doubled to about USD5.44 trillion in 2016. It seems going out without cash and wallet is becoming reality for the Chinese people by the help of mobile payment [1].

1.1 Mobile Payment Challenges

M-commerce has its own challenges like security and privacy. Mobile devices have limited computational power, less stable network, limited memory, limited storage, and etc. Most of the e-commerce protocols are based on public key cryptography that is not efficient for mobile devices and wireless networks. The client may need to do heavy calculations in this type of cryptography. So, this type of cryptography is not suitable for mobile platforms.

Some of these protocols are using a mechanism to authenticate the certificate of the engaging parties. However, this step may become costly for a mobile device via a network that is not as stable as a wired network connection. Some of these protocols are keeping credit card's information on mobile devices or using this information in transactions without proper protection. These issues make the existing protocols vulnerable from the aspect of security. Most of these protocols were designed to keep track of the traditional flow of data. This flow should be carried between client and merchant as a transaction. These protocols are vulnerable to attacks like transaction or balance modification attack. There is no proper notification in these protocols after a successful transaction as part of the protocol.

1.2 Desired Mobile Payment Protocol Attributes

A mobile payment protocol should be defined that is suitable for the mobile platform. This protocol should decrease the computational cost of payment process in order to make it suitable for the mobile platform. The computational power, communication speed, and variable size are the most important mobile platform limitations. Also, customer's privacy protection should be another feature of this protocol. Note that, privacy protection is a significant challenge especially in a mobile platform. Non-repudiation can be provided by using digital

signature. However, non-repudiation should be an optional feature, since it may have an extra computational cost for the mobile devices.

Furthermore, to avoid replay attacks in the protocol, random time-stamp generated numbers should be generated in its steps. Cloud messaging should be utilized to provide an extra layer of security for the payment protocol to prevent card not present fraud. Cloud messaging is available in all mobile operating systems like GCM for Android, BBPS for Blackberry, APNS for Apple, and MPNS for Microsoft. So, the customer can easily see the origin of the message when it comes as a cloud message. This protocol should help people to make their payment via their mobile devices in a secure and efficient way.

The recommended protocol should be based on the client-centric model. Temporary payer's identity, involving mobile network operators, and utilizing random time-stamp generated numbers should be used to provide suitable privacy protection for the payer and avoid replay attacks. Without this temporary identity, the payer's privacy will be more vulnerable to attacks. One of the goals is to hide payer's identity from merchant to protect his privacy (optional feature). The digital signature could be utilized in the payment protocol to provide non-repudiation. An improved key agreement protocol should be used instead of Diffie-Hellman. The protocol should be suitable for mobile devices from aspect of computational and communication cost.

1.3 Limitations of Current Solutions

There are many payment protocols for e-commerce like SET, iKP, KSL, and etc. Existing payment protocols are not designed for mobile devices and mobile or wireless networks. These protocols have heavy computations for the engaging parties. These computations are not suitable for the mobile platform. The cost of communication may be large in these protocols, since certificate authentication may be required. These protocols are using PKI encryption that is not proper for

the mobile platform because of its heavy computational and communication cost.

The mobile platform has limitations in computational power and network stability and network bandwidth. So, the existing protocols are not suitable for this platform. These protocols don't protect customer's privacy. Also, many people abandon online payment because of the issues in 3D Secure implementations [35]. Currently, 3DS implementations like Verified by Visa are a pioneer in online payment. However, none of these protocols are widely accepted by people so far.

1.4 Problem Statement

There are different types of limitations in m-commerce and mobile platform in comparison with other common e-commerce platforms. Another significant challenge in m-commerce is identity protection. There are several situations that people can use m-commerce protocols instead of e-commerce protocols. However, m-commerce protocols are not suitable for mobile platform. So, a payment protocol suitable for mobile platform is needed for m-commerce.

There are some assumptions in this protocol. It is assumed that the payer has a credit card that can be used in online transactions. It is assumed that the payer is using a mobile device through a mobile network like 4G LTE. It is assumed that their mobile network operators are supporting the recommended protocol. It is assumed that there exists a payment gateway named pay-center. This payment gateway is the medium between the banks and the other parties. The payment gateway will commit the transaction between the payer and the merchant.

In this m-commerce protocol, the focus should be on decreasing the computational cost and communication cost in the transactions. Decreasing the computational cost of the secure channel establishment protocol (Diffie-Hellman) will be suggested. The goal is to design a payment protocol for

mobile platform.

This mobile payment protocol should have lower computation cost in mobile devices. This protocol should use symmetric encryption instead of PKI encryption. This protocol should provide privacy protection for the customer. Using temporary ID for the customer will be suggested. This ID should not be reusable. It should be only for that transaction. Replay attack should not be possible in this protocol. Using random and time-stamp generated numbers in the transaction will be recommended.

1.5 Contribution

Contributions in this research are:
1) Introducing a new private mobile payment protocol based on client-centric model that is suitable for mobile devices via mobile and wireless networks.
2) Suggesting an improved version of Diffie-Hellman key agreement protocol for establishing secure connections among engaging parties. Logarithm will be used instead of powering in the process of the recommended key agreement protocol. This change will make the computation cost less and make the process proper for mobile platform even from aspect of required variable size.
3) Providing proper privacy protection for the payer by involving mobile network operators in the payment process and generating temporary identities.
4) Decreasing the risk of replay attacks by using random time-stamp generated numbers in the payment process.

1.6 Dissertation Roadmap

Related materials will be reviewed in chapter 2. The recommended key agreement protocols will be described in chapter 3. Chapter 4 describes the improved mobile payment protocol. Chapter 5 describes the experiments. The research will be concluded in chapter 6.

You think of yourself as a citizen of the universe. You think you belong to this world of dust and matter. Out of this dust you have created a personal image, and have forgotten about the essence of your true origin.

Jalaluddin Rumi

2 Literature Review

A key agreement protocol is a protocol to generate a shared session key between two parties. In this chapter, the Diffie-Hellman protocol will be reviewed. Diffie-Hellman is the most dominant key agreement protocol for e-commerce transactions. Group Key agreement protocol is to generate a shared key between more than two parties. Then, DL08 and KON08 will be reviewed. These protocols are the most important group key agreement protocols. A payment protocol helps customers to do the payment via e-commerce. Then, current best payment protocols for e-commerce transactions will be reviewed. These protocols are SET, iKP, KSL, and 3DS [10, 14, 22].

2.1 Key Agreement Protocol

In this section, Diffie-Hellman key exchange protocol will be reviewed. This protocol is very successful in the market and it is the most common key agreement protocol among the existing key exchange protocols.

2.1.1 Diffie Hellman Key Agreement Protocol

Diffie and Hellman in their seminal work developed a key agreement scheme between two parties over an insecure channel. Before the actual key exchange begins, both parties agree on a prime number p and its primitive root g. You can see the steps to generate the shared session key in below.

1) Alice chooses her secret random number and computes her middle number. Then, she sends her middle number to Bob.

2) Bob picks his secret random number, computes his middle number and sends the result to Alice.

3) On receipt of the transmission, Alice calculates the shared key by her private number and Bobś middle number. Bob calculates his shared key by using his private number and Aliceś middle number [29].

The security of the Diffie-Hellman protocol is based on how difficult it is for an eavesdropper, Eve, to construct the key using the public information exchanged between Alice and Bob. Eve has to find Alice's secret number and/or Bob's secret number using the prime number that she can obtain by intercepting their communications. This is also known as the discrete logarithm problem. Discrete logarithm is a hard problem to solve.

Step	Action	Description
1	Alice and Bob agree on two numbers p and g	p is a large prime number and g is called base or generator
2	Alice picks a secret number a	Alicеś secret number = a
3	Bob picks a secret number b	Bobś secret number = b
4	Alice computes her public number $X = g^a \bmod p$	Alicеś public number = X
5	Bob computes his public number $Y = g^b \bmod p$	Bobś public number = Y
6	Alice and Bob exchange their public numbers	Alice knows p, g, a, X, Y Bob knows p, g, b, X, Y
7	Alice computes $k_a = Y^a \bmod p$	$k_a = (g^b \bmod p)^a \bmod p$ $k_a = (g^b)^a \bmod p$ $k_a = (g^{ba}) \bmod p$
8	Bob computes $k_b = X^b \bmod p$	$k_b = (g^a \bmod p)^b \bmod p$ $k_b = (g^a)^b \bmod p$ $k_b = (g^{ab}) \bmod p$
9	By the law of algebra, Alicеś k_a is the same as Bobś k_b, or $k_a = k_b = k$	Alice and Bob both know the secret value k

Table 2.1.1: Diffie-Hellman Key Agreement Protocol

It is considered infeasible to solve using current computing technology, for example, where the prime has more than 300 decimal digits, and a and b have more than 100 decimal digits [20, 21]. Heavy computation is needed to generate a shared session key in Diffie-Hellman key agreement protocol. It is not good for a mobile device with limited resources to do such a heavy computation for generating a shared session key [11, 24].

The fundamental math of Diffie-Hellman includes the algebra of exponents and modulus arithmetic. For this discussion, Alice and Bob will be used as a conventional example. The goal of this process is to agree on a shared secret session key for Alice and Bob. Alice and Bob will generate a shared key based on their selected private numbers. These are symmetric encryption algorithms that will be used to encrypt the data stream between them.

There are requirements on the numbers that the parties can pick. These requirements can be found in the references. This algorithm has been reviewed and discussed many times in a variety of papers. This algorithm has some problems that make it unsuitable for mobile devices [25, 26].

Note that, some of the numbers that each side may pick, may be very large for example if p is a 512-bit binary number, the minimum allowed in the standard, would be a number with up to 150 plus digits expressed in decimal notation. Implementation details are very important as typical mobile variables that cannot hold numbers as big as this, for example, a 512 bit (=64 byte) the number will not fit into a 4-byte integer field. In addition, these computations are too heavy for a mobile device with limited resources. You can see Diffie-Hellman steps in table 2.1.1.