Cryptographically Secured Micro Payment Scheme

Tanushka Sajith Balasooriya

158203K

Degree of Master Science

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

January 2019

Cryptographically Secured Micro Payment Scheme

Tanushka Sajith Balasooriya

158203K

Degree of Master Science

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

January 2019

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non - exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works.

_____ _____

Tanushka Sajith Balasooriiya: Date

Approved by:

_____ _____

LtCol Dr Chandana D. Gamage Date
Department of Computer Science and Engineering
University of Moratuwa

Copyright Statement

Abstract

As more and more commercial activity moves online and electronic commerce becomes the common way by which transactions are conducted, electronic payment systems will become a critical requirement for the success of many applications. The commonly used electronic payment scheme is to facilitate the online transmission of payment card data from credit cards or debit cards and to process such transactions through a payment gateway. Also, other schemes such as PayPal or ezCash provide a service where the payment is processed online using identification data specific to the service but using funds that are based on a pre-stored credit card, debit card or stored-value card system.

All these existing online payment schemes are similar in their design and operation to credit card based payments. While such schemes called macro payment systems are appropriate for transactions with a relatively high value compared to the service charges of the online payment providers, there are many e-commerce applications that are being developed for which such credit card style payment schemes are inappropriate.

As a solution to this problem, research has been conducted on an area called micro payment systems. The design of micro payment systems need to be radically different from the macro payment schemes as properties such as online real time availability of all participants, use of public cryptography schemes, availability of high computation power, etc that is common for macro payment systems are not desirable in micro payment systems. Taking into consideration the context in which micro payment schemes operate, where a transaction value is very low, micro payment systems need to be designed with a careful trade-off between reliability and cost of implementation.

This proposed research is intended to study the properties of existing micro payment systems, evaluate the strengths and weaknesses of those schemes, and prepare a model for a micro payment scheme with only the most essential properties. The research further envisages the selection of cryptographic mechanisms and development of protocols to implement this micro payment model.

Acknowledgements

First of all I would like to thank my supervisor Dr. Chandana Gamage whose encouragement, guidance, support, and criticism from start to the very end, allowed me to understand the objectives and challenges of a master degree thesis. I would also like to thank Dr. Indika Perera (Course Cordinator) for extensive advice, helpful feedback, and constant support.

Furthermore, my special thanks go to Dr. Shantha Fernando who provided an excellent, supporting, innovative, and inspiring environment in which it was a pleasure to create this thesis.

Finally, words alone cannot express the thanks I owe Mr. Premaratne my father, Mrs. Amara Weerasinghe my mother, Ms. Jeewantha Sandamalee my sister and Ms. Lakmi Bandara my loving girl friend for all the encouragement extended.

Abbreviations

CA - Certificate Authority
CAFE - Conditional Access for Europe
CSP - Communicating Sequential Processes
DoS - Denial-of-Service
FSTC - Financial Services Technology Consortium
ISP - Internet Service Provider
PAT - Protocol Analysis Toolkit
PKI - Public-key Infrastructure
POC - Proof of Concept
RSA - RivestShamirAdleman
SET - Secure Electronic Transaction
GSM - Global System for Mobile communication
NFC - Near Field Communication
SMS - Short Messaging Service
EMV - Europay MasterCard Visa

Table of Contents

List of Tables

List of Figures