پردیس بین الملل

پایان نامه کارشناسی ارشد

طراحي پروتكل امن براي كيف پول همراه

از

الهام قره شیخ لو

استاد راهنما:

دكتر رضا ابراهيمي آتاني

اسفند ماه ۱۳۹۱


بسم الله الرحمن الرحيم

دانشکده پردیس بین الملل

گروه مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی

طراحي پروتكل امن براي كيف پول همراه

از

الهام قره شیخ لو

استاد راهنما:

دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱

تقدیم به:

پدر و مادر عزیزم

تشکر و قدردانی:

در طول کار بر روی این پایان نامه دوستان بسیاری به طرق مختلف مرا مورد حمایت قـرار دادنـد. در اینجـا بایـد از استاد راهنما جناب آقای دکتر رضا ابراهیمی آتانی بخاطر تمامی کمک هایشان تقدیر و تشکر کنم. از جنـاب آقـای مهندس فرزاد توکلی به دلیل کمک های بی دریغشان تشکر می‌نمایم. اما تقدیر ویژه ام از خانواده عزیزم خواهد بود بخاطر حمایت مداوم و دلگرمی هایشان. در پایان از جناب آقای مهندس حجـت شـعبانپور بـه دلیـل حمایـت‌هـای پدرانهٔ ایشان کمال تشکر را دارم.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

چکیده

طراحی پروتکل امن برای کیف پول همراه

الهام قره شیخ لو

پرداخت همراه روش جدیدی جهت انجام عملیات و تراکنش‌های مالی به منظور انجام امور تجاری بر روی ابزارهای همراه بوده که از لحاظ ماهیتی با پرداخت‌های سنتی همانند چک و یا وجه نقد تفاوت اساسی دارد. پرداخت‌های همراه دارای مزایای غیر قابل انکاری چون راحتی، دسترسی و قابلیت تحرک و همچنین چالش‌های جدی نظیر امنیت و هزینه می‌باشند. تمامی روش‌های ارائه شده تاکنون سعی بر این دارند تا این چالش‌ها را تا حد قابل قبولی برطرف نمایند. پرداخت‌های همراه دارای کاربردهای فراوانی هستند. یکی از کاربردهای جدید پرداخت همراه استفاده از کیف پول همراه می‌باشد.

کیف پول همراه برنامه ای کاربردی است که بر روی ابزار همراه مثل تلفن همراه ذخیره شده و برای مشترکین امکان انجام تراکنش‌های مالی را فراهم می‌آورد. کیف پول همراه بر روی فناوری‌های ارتباطی مختلفی نظیر WAP، بلوتوث و یا پیامک قابل طراحی و پیاده سازی بوده که هر کدام مزایا و چالش‌های خاص خود را دارند. اکثر راه حل‌های ارائه شده در این زمینه نیازمند ارتباط همیشگی کیف پول همراه با شبکهٔ مخابراتی و اینترنتی بوده که این ارتباط بر مشتری هزینه تحمیل می‌نماید. در حالی که پرداخت هزینهٔ اتصال به شبکه برای هر تراکنش با ارزش مالی ناچیز، مقرون به صرفه نیست. حال اگر ارتباط با شبکه به هر دلیل مقدور نباشد و یا اینکه مشتری به دنبال دریافت خدمات اقتصادی تر برای این قبیل پرداخت‌ها باشد؛ باید از ساز و کارهای دیگری برای پرداخت استفاده نمود.

در این پایان نامه سعی بر آن است که پروتکل پرداخت خرد برون از خط جدیدی برای استفاده در کیف پول همراه ارائه و با استفاده از رمزنگاری متقارن و تابع چکیده ساز، امنیت آن تأمین گردد. روش تحقیق این پایان نامه مبتنی بر مدل سازی بوده و برای اثبات کارایی و امنیت پروتکل پیشنهادی از معیارهای موجود بهره گرفته و این پروتکل با نمونه‌های قبلی ارائه شده مقایسه می‌شود.

واژه‌های کلیدی: پرداخت همراه، کیف پول همراه، پرداخت خرد، امنیت، رمزنگاری متقارن، توابع چکیده ساز.

Abstract

Designing of a secure protocol for mobile wallet

Elham Gharehsheikhlou

Mobile Payments is a new method for operations and financial transactions in order to conduct commercial activities on mobile devices, which in terms of the nature has a major difference with traditional payment such as cheque or cash. Mobile payments have undeniable advantages like convenience, accessibility and mobility and also serious challenges such as security and cost. All methods have been proposed so far, is try to overcome these challenges to an acceptable level. Mobile payments have numerous applications. One of the new applications of mobile payment is the use of mobile wallet.

Mobile wallet is an application which store on the mobile devices like cell phone and gives subscribers the ability to perform financial transactions. Mobile wallet can be designed and implemented on different communication technologies such as WAP, Bluetooth or SMS, which each one has its own advantages and challenges. Most of the proposed solutions in this field require wallet continuous communication with network and internet which would impose a cost to the customer. While the network connection fee for each micro payment is not cost effective, if the network connection is not possible for any reason or customer is looking to receive more economical service for these payments, other mechanisms should be used for payment.

This thesis has tried to propose a new Off-line micro payment protocol to use in mobile wallet, and by using the symmetric encryption and hash function its security will be provided. The methodology used in this thesis is based on modeling and the existing criteria are used to prove the efficiency of the proposed protocol and the protocol has been compared with the previous proposed samples.

Keywords: Mobile payment, Mobile wallet, Micro payment, Security, Symmetric encryption, Hash functions.

فصل ۱:

مقدمه

۱-۱- مقدمه

در گذشتهٔ نه چندان دور، پرداخت‌ها به شکل سنتی انجام می‌گرفت. فروشندگان، بازرگانان و در کل مردم برای پرداخت، پول را به صورت نقد جا به جا نموده و یا از روش‌هایی مانند چک و حواله استفاده می‌کردند. دیری نپایید که با نفوذ فناوری به همهٔ زوایای زندگی بشر و ایجاد تغییرات بنیادین در خواست‌ها و نیازمندی‌های او این بُعد از زندگی دستخوش تغییراتی شگرف گردید. در راستای همین دگرگونی‌ها بود که مکملی نوین برای پرداخت سنتی معرفی گردید و آن چیزی نبود جز پرداخت الکترونیکی[1]. پرداخت الکترونیکی عبارت است از تراکنش جا به جایی ارزش بین فروشنده، مشتری، بانک و یا به طور کلی بین تمام اعضاء مشمول در یک معامله بر روی بسترها و شبکه‌های الکترونیکی مانند اینترنت، از طریق ابزار و ادوات الکترونیکی همانند کامپیوتر. پرداخت الکترونیکی بدون محدودیت زمانی انجام می‌شود، اما عموماً از نظر مکانی محدود است.

تغییرات به همین جا ختم نگردید. با فراهم آمدن بسترهای جدید ارتباطی مانند شبکه‌های بی سیم و یا شبکه‌های تلفن همراه و همچنین ظهور و گسترش ابزار و ادوات همراه، پرداخت الکترونیکی حصار محدودیت مکانی را شکست و جای خود را به پرداخت همراه[2] داد. پرداخت همراه، سیستمی است که در آن تراکنش‌های ارزشمند پولی از طریق شبکه‌های بی سیم و با استفاده از ابزار همراه انجام می‌گیرد. پرداخت همراه دارای مزایایی چون عدم وابستگی به مکان کاربر و زمان، در دسترس بودن، و صرفه جوئی در منابع است. هر چند محدودیت‌هایی چون پهنای باند ارتباطی محدود، عمر کوتاه باتری و محدودیت‌های فنی موجود بر روی ابزار همراه جزء لاینفک این نوع پرداخت می‌باشد.

کیف پول همراه[3] یکی از کاربردهای جدید پرداخت همراه می‌باشد که قابلیت جایگزینی کیف پول معمولی و بسیاری از کاربردهای دیگر را دارد. کیف پول همراه کاربردی است پیشرفته شامل تراکنش‌های همراه، و سایر موارد موجود در کیف پول معمولی. در واقع کیف پول همراه برنامه ای است که بر روی تلفن همراه ذخیره شده و به کاربران امکان انجام انواع تراکنش‌های مالی را می‌دهد. کیف پول همراه بر روی فناوری‌ها و خدمات ارتباطی مختلفی نظیر ارتباط حوزهٔ نزدیک (NFC[4])، بلوتوث، پیامک (SMS[5]) و یا WAP[6] قابل طراحی و پیاده سازی است که هر کدام مزایا و چالش‌های خاص خود را دارند. معمولاً انجام این تراکنش‌ها نیازمند اتصال به شبکهٔ مخابراتی و اینترنتی حین عملیات پرداخت است که همواره مورد تأیید و پسند کاربر نیست. به علاوه، پرداخت هزینهٔ اتصال به شبکه برای هر تراکنش مقرون به صرفه نمی‌باشد. بسیار اتفاق می‌افتد که کاربران در هنگام

[1] electronic payment(e-payment)
[2] mobile payment(m-payment)
[3] mobile wallet
[4] Near Field Communication (NFC)
[5] Short Message Service (SMS)
[6] Wireless Application Protocol (WAP)

استفاده از کیف پول همراه خود به شبکه‌هایی نظیر اینترنت دسترسی نداشته و یا به دنبال دریافت خدمات اقتصادی تر برای این قبیل پرداخت‌ها باشند. بنابراین باید این امکان فراهم آید تا کاربران در لحظهٔ پرداخت نیازمند اتصال به شبکه نباشند.

از آن گذشته، برای طراحی یک سیستم پرداخت موفق (در قالب کیف پول همراه و یا سایر اَشکال پرداخت) لازم است تا مواردی چون ترجیحات و علاقه مندی‌های کاربران، فرهنگ اجتماعی، توانایی‌های فنی و نیازمندی‌های قانونی در نظر گرفته شود که همهٔ این موارد و سایر چالش‌های موجود مانند سادگی، قابلیت استفاده، سرعت و هزینه، طراحی یک سیستم پرداخت همراه موفق را به موضوعی حساس و چالشی تبدیل نموده است. یکی از مهمترین چالش‌های موجود در طراحی یک سیستم پرداخت، تأمین امنیت پرداخت است. از آنجا که در عملیات پرداخت، ارزش و یا اعتبار منتقل می‌شود، کاربران تا زمانی که به سیستم اعتماد کامل نداشته باشند؛ حاضر به استفاده از آن در سطح وسیع نخواهند بود. برای ایجاد امنیت در سیستم‌های پرداخت همراه، روش‌ها و راهکارهای زیادی همچون استفاده از امضاء رقمی[۱]، ساز و کارهای رمزنگاری[۲] و یا توابع چکیده ساز[۳] ارائـه گردیده است که از آنها برای تضمین خدمات امنیتی چون محرمانگی داده[۴]، تمامیت داده[۵]، احراز اصالت[۶]، کنترل دسترسی[۷] و انکارناپذیری[۸] استفاده می‌شود. هر پرداختی که بتواند خدمات امنیتی فوق را پیاده‌سازی نماید در زمرهٔ پرداخت‌های امن قرار می‌گیرد. مقولهٔ دیگر حائز اهمیت، این است که ایجاد امنیت نباید لطمه ای به کارایی سیستم وارد نماید. سیستم زمانی کاربردی می‌شود که امنیت و کارایی در کنار هم پیاده سازی شوند.

اکثر طرح‌های پیشنهادی در زمینهٔ پرداخت همراه از رمزنگاری نامتقارن[۹] یا کلید عمومی[۱۰] برای تأمین امنیت استفاده می‌نمایند. گرچه کلید عمومی امنیت را در سطح قابل قبولی تضمین می‌نماید؛ اما برای پیاده سازی آن بر روی ابزار همراه با محدودیت‌های فنی ذاتی، کمی احتیاط لازم است. البته الگوریتم‌های سبکی در این زمینه ارائه شده که بر روی ابزار همراه قابل پیاده سازی و استفاده می‌باشند. با این حال انتخاب این نوع رمزنگاری برای تأمین امنیت بر روی ابزار و ادوات همراه موضوعی است که نیاز به بررسی بیشتر دارد.

در نقطهٔ مقابل، رمزنگاری متقارن[۱۱] است که از نظر هزینهٔ محاسباتی بسیار ساده تر از رمزنگاری نامتقارن بوده و می‌تواند گزینهٔ مناسبی برای تأمین امنیت در سیستم‌های پرداخت همراه باشد. نکتهٔ حائز اهمیت در استفاده از این نوع رمزنگاری وابستگی امنیت طرح به امنیت کلید است که باید بخوبی تأمین شود.

---

[1] digital signature
[2] cryptography mechanism
[3] hash functions
[4] data confidentiality
[5] data integrity
[6] authentication
[7] access control
[8] non repudiation
[9] asymmetric cryptology
[10] public key
[11] symmetric cryptography

۱-۲- تعریف مسئله

در این بخش به تعریف مسئله پرداخته تا ضرورت و کاربرد تحقیق، مشخص شده و خط مشیء طراحی پروتکل برای کیف پول همراه که هدف نهایی این تحقیق می‌باشد ترسیم گردد.

در کشور ایران، پرداخت همراه همگام با بانکداری همراه رشد ننموده و اکثر بانک‌ها و مؤسسات مالی کشور بانکداری همراه را به عنوان خط مشیء خود قرار داده و به ارائهٔ طرح‌هایی پرداخته اند که صرفاً ارتباط کاربر با بانک را تحت پوشش قرار می‌دهد؛ در حالی که پرداخت همراه تراکنش‌های بین فروشنده با مشتری و یا بین مشتری با مشتری را نیز شامل می‌گردد.

اکثر طرح‌های موجود نیز نیازمند ارتباط بر خط با سرور بانک یا عضو سوم مورد اعتماد در حین پرداخت هستند. این بدان معنی است که در لحظهٔ پرداخت باید هم دو عضو مشمول به شبکه متصل باشند؛ حال آنکه همه جا و در همه زمان این امکان فراهم نیست. مسافری را در نظر بگیرید که بعد از رسیدن به مقصد می‌خواهد با استفاده از کیف پول همراه خود کرایه تاکسی را پرداخت نماید. در مکانی که مسافر پیاده شده است (مثلاً پارکینگ یک هتل)؛ هیچ کدام از تجهیزات همراه او سیگنالی را از شبکه دریافت نمی‌نمایند. از طرفی این ارتباط بر کاربر هزینه تحمیل می‌نماید. به همین دلیل، انجام تراکنش‌های خرد برای کاربر به صرفه نبوده و عملاً برای پرداخت‌های کلان از این طرح‌ها استفاده می‌شود. مسئلهٔ امنیتی این طرح‌ها نیز جای بحث دارد.

۱-۳- هدف

هدف از ارائهٔ این پایان نامه، طراحی پروتکلی امن برای کیف پول همراه با بهره‌گیری از فناوری پیامک و اینترنت در قسمت بر خط[1] و استفاده از فناوری بلوتوث در بخش برون از خط[2] می‌باشد. کاربر می‌تواند با استفاده از این کیف پول و از طریق گوشی تلفن همراه پرداخت را انجام دهد. به همین دلیل این کیف پول به صورت نظیر به نظیر (P2P[3]) طراحی شده است؛ به طوری که کاربر برای پرداخت، نیازمند اتصال به عضو سوم مورد اعتماد نیست. نوع پرداخت همراه مورد استفاده، پرداخت خرد[4] و مبتنی بر انتقال نشانه (توکن[5]) است. در این طراحی خدمات امنیتی محرمانگی داده، تمامیت داده، احراز اصالت، کنترل دسترسی، انکارناپذیری و سایر ویژگی‌های افزون امنیتی در نظر گرفته شده است.

[1] on line
[2] off line
[3] Pree to Pree (P2P)
[4] micro payment
[5] token

۱-۴- ساختار کلی پایان نامه

پایان نامه پیش رو حاوی ۵ فصل است. فصل اول شامل مقدمه، تعریف مسئله و هدف پایان نامه می‌باشد. در فصل دوم، تعاریف پایه ای نظیر تجارت همراه[1]، پرداخت همراه، مزایا، محدودیت‌ها، روند رشد آن، معرفی کیف پول و امنیت پرداخت بیان می‌گردد. در این فصل سعی شده که کلیهٔ مفاهیم بکارگرفته شده در تشریح پایان نامه، مورد بررسی قرار گیرد.

از آنجا که تمرکز پایان نامه بر روی پرداخت‌های خرد است؛ فصل سوم به معرفی، تشریح پرداخت‌های خرد و مطالعهٔ موردی بر روی تعدادی از این پرداخت‌ها اختصاص می‌یابد. به منظور مقایسهٔ بهتر، معیارهایی جهت ارزیابی بیان گردیده و پرداخت‌ها در قالب این مجموعه از معیارها بررسی و تحلیل می‌شوند.

فصل چهارم حاوی تشریح پروتکل پیشنهادی اعم از ساختار کلی، جزئیات سیستم، بررسی، پیاده سازی و انتخاب الگوریتم‌های واجد شرایط برای استفاده در پروتکل، انتخاب بسترها و فناوری‌های ارتباطی مناسب می‌باشد. در این فصل پروتکل پیشنهادی با استفاده از معیارهای عنوان شده در فصل سوم مورد ارزیابی قرار گرفته و با سایر پرداخت‌های فصل پیشین مقایسه می‌گردد.

فصل پنجم یا فصل پایانی شامل خلاصه ای از اهداف پایان نامه و یافته‌های آن می‌باشد. جمع بندی، نوآوری و پیشنهادات آتی در حیطهٔ موضوع این پایان نامه در این فصل گنجانده شده است.

[1] mobile commerce(m-commerce)

فصل ۲:

مفاهیم پیش زمینه