پردیس بین الملل

پایان نامه کارشناسی ارشد

طراحی مدل امن ارتباط مشتری و بانک و بالعکس
با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی

از

مونا پورقاسم

استاد راهنما:

دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱


بسم الله الرحمن الرحیم

دانشکده پردیس بین الملل

گروه مهندسی فناوری اطلاعات - تجارت الکترونیک

طراحی مدل امن ارتباط مشتری و بانک و بالعکس با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی

از

مونا پورقاسم

استاد راهنما:

دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱

تقدیم به:

پدر و مادر عزیزم برای همه خوبی‌هایشان

و به همسر مهربانم بخاطر همه همراهی هایش

تشکر و قدردانی:

شکر خداوند متعال را بجای آورده که توفیق نصیب من کرد تا این پایان نامه را به سرانجام برسانم و با سپاس از استاد ارجمندم جناب آقای دکتر رضا ابراهیمی آتانی که با صبر و توصیه های ارزشمند خود مسیر انجام این پایان نامه را آسان نموده و از حمایت های بیدریغ ایشان بهره مند شدم. از داوران محترم سرکار خانم دکتر راهبه نیارکی و جناب آقای دکتر هاشم صابری که زحمت داوری این پایان نامه را بر عهده داشتند، صمیمانه تشکر و قدر دانی دارم. همچنین از جناب آقای مهندس فرزاد توکلی به دلیل کمک های بی دریغشان تشکر می‌نمایم. اما تقدیر ویژه ام از همسر مهربانم خواهد بود بخاطر حمایت های مداوم و دلگرمی های ایشان.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

چکیده

طراحی مدل امن ارتباط مشتری و بانک و بالعکس با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی

مونا پورقاسم

در دنیای امروز استفاده از شبکه های کامپیوتری و مخابراتی، از ملزومات زندگی بشر محسوب می‌شود. در این میان ابزارها و ادوات همراه به دلیل در دسترس بودن، جایگاه ویژه‌ای یافته‌اند. این ویژگی علاوه بر بوجود آوردن تسهیلات فراوان همانند انجام تراکنش های مالی در هر مکان و زمان، حساسیت هایی را در زمینه تامین امنیت این دستگاه‌ها برانگیخته است.

زیرساخت کلید عمومی(PKI) یکی از الزامات اجتناب ناپذیر تراکنش های اطلاعاتی در کاربرد های تجاری و دولتی می باشد. چرا که، تمامیت پیام، احراز هویت کاربر و انکار ناپذیری تراکنش ها را با استفاده از امضای دیجیتال تضمین می‌نماید. چنانچه امنیت امضای دیجیتال تضمین گردد، از نظر قانونی می‌تواند معادل امضای دست نوشته شده در نظر گرفته شود. با توجه به گسترش سریع دستگاه‌های تلفن همراه، که مبتنی بر کارت های SIM/USIM، می باشند، این دستگاه ها را می توان به عنوان دستگاه‌های ایده‌آل برای ایجاد امضای دیجیتال در نظر گرفت. علاوه بر این، با بکارگیری امضای همراه، توسعه برنامه‌های کاربردی مبتنی بر این امضا برای ارائه دهندگان خدمات و برنامه‌های کاربردی همراه ساده می‌گردد. در تراکنش‌هایی همچون برخی از مراودات بانکی که احراز هویت مشتری از اهمیت بالایی برخوردار است، استفاده از این زیرساخت می تواند نقش بسزایی در ایجاد امنیت داشته باشد.

در این پایان نامه یک مدل امن به منظور ارتباط بین مشتری و بانک با استفاده از تلفن همراه و بر بستر اینترنت در شبکه های سلولی پیشنهاد شده است. که در آن از رمز نگاری متقارن برای ایجاد محرمانگی و از PKI به منظور احراز اصالت کاربران استفاده می شود. مدل پیشنهادی علاوه بر امنیت و کارایی با توجه به امکانات موجود شبکه تلفن همراه در کشور طراحی شده است. این مدل به گونه ای طراحی شده که با پیشرفت های شبکه تلفن همراه سازگاری لازم را داشته باشد.

واژه‌های کلیدی: زیرساخت کلید عمومی، امنیت، رمزنگاری، شبکه های سلولی

Abstract

Customer relationship and bank security model, using a public key infrastructure for cellular networks

Mona Pourghasem

In today's world the use of computer networks and telecommunications is essential for human life. Among these, mobile tools and devices due to availability, has been found a special place. This feature in addition to provide numerous facilities in every place and time, such as financial transactions, are raised the sensitivity in the field of security of these devices.

Public key infrastructure (PKI) is one of the unavoidable requirements information transactions in the commercial and governmental applications. Because, it is guaranteed message integrity, user authentication and transactions undeniable by using the digital signature. If security of digital signature is ensure, legally can be considered equivalent to a handwritten signature. Due to the rapid development of mobile devices, which are based on the SIM/USIM cards, these devices can be considered as an ideal device for creating digital signatures. Furthermore, with the use of mobile signatures, the development of applications based on this signature will be simple for service providers and mobile applications. In the transactions, such as some of bank exchanges, which client authentication is very important, the use of this infrastructure can have a significant role in security.

In this thesis a secure model has been proposed in order to establish a connection between customer and bank by using mobile phone and on the internet at the cellular networks. In which the symmetric encryption is used to provide confidentiality and PKI is used for authentication of user's authenticity. The proposed model in addition to security and efficiency is designed due to the existing mobile network facilities in the country. The model is designed in a way that would be have consistent with advances in mobile networks.

Keywords: Public key infrastructure, security, cryptography, cellular networks

فصل ۱:

مقدمه

۱-۱- مقدمه

در دهه‌ی اخیر نیازمندی های ارتباطی مردم به واسطه گسترش و نفوذ اینترنت و تلفن همراه تغییر نموده است؛ به طوری که مشترکان شبکه‌های مخابراتی خواهان ارائه‌ی خدماتی متنوع، همانند خدمات بانکی و یا دولتی با کیفیت مطلوب بر روی شبکه‌های عمومی می‌باشند. آمارها حاکی از آن است که سرعت رشد استفاده از تلفن همراه در شبکه‌های سلولی به مراتب بیشتر از سایر شبکه‌های سیمی می‌باشد و این به دلیل قابلیت ویژه‌ی تلفن همراه، که همان سادگی حمل و استفاده در هر مکان و زمان است؛ می‌باشد. به دلیل همین ویژگی ادوات مورد استفاده در شبکه‌های سلولی، حوزه جدیدی تحت عنوان "تجارت همراه" در "تجارت الکترونیکی" ایجاد شده است. از طرف دیگر بخش قابل توجهی از تجارت، عملیات و تراکنش‌هایی است که به واسطه‌ی بانک‌ها و موسسات مالی صورت می‌پذیرد.

سیستم‌های بانکداری همراه، این فرصت را فراهم می‌سازند تا مشتریانی که از این خدمات استفاده می نمایند بتوانند به راحتی به فعالیت‌های بانکی خود دسترسی داشته باشند. در بانکداری همراه از تکنولوژی‌های ارتباطی مختلفی استفاده می‌گردد که از آنجمله می‌توان به SMS[1]، IVR[2] و WAP[3] اشاره نمود. مشکلات تکنولوژی های ذکر شده همچون، قابلیت اعتماد ضعیف، سرعت نسبتا پایین و هزینه‌ی زیاد از یک طرف و همچنین سیر تکاملی سیستم های تلفن همراه که در جهت بهبود سرویس دهی می‌باشد از طرف دیگر، تغییرات زیادی را در ارائه‌ی سرویس‌های همراه بوجود آورده است. به همین دلیل امروزه با ارائه نسل ۲.۵ به بعد در شبکه‌های تلفن همراه که همان GPRS[4] و تکنولوژی های پس از آن در شبکه های نسل سوم و چهارم است، شاهد ارائه خدمات تحت وب بر روی شبکه‌های سلولی می‌باشیم. استفاده از وب، به دلیل سهولت استفاده و کاربر پسند بودن، همچنین امکان رهگیری فعالیت‌های انجام شده و هزینه بسیار کمتر در مقایسه با سایر روش‌ها، برتری ویژه ای دارد و به همین دلیل چنانچه بتوان فاکتورهای امنیتی را تامین نمود، می توان آن را به عنوان بستری مناسب، برای ارتباط بین مشتری و بانک مورد استفاده قرار داد.

اهمیت موضوع تامین امنیت، در تراکنش‌هایی که توسط دستگاه تلفن همراه انجام می‌شوند به دلیل این است که این تراکنش‌ها به طور ذاتی در بسترهای ناامنی همچون شبکه های بی‌سیم انجام می‌پذیرد و کاربران تنها هنگامی حاضرند تراکنش‌هایی چون تراکنش‌های مالی را بر روی تلفن همراه خود انجام دهند، که از امنیت آن اطمینان کامل داشته باشند.

با توجه به اینکه انجام تراکنش‌های مالی بین بانک ها و موسسات مالی و مشتری، بخش مهمی از تجارت همراه به شمار می رود؛ حفظ امنیت و اطمینان، از نگرانی‌های بزرگ در تجارت همراه به شمار می‌رود. چرا که علاوه بر

[1] Short Message Service (SMS)
[2] Interactive Voice Response (IVR)
[3] Wireless Application Protocol (WAP)
[4] General Packet Radio Service (GPRS)

مسائل امنیتی در شبکه‌های سیمی، برخی از مسائل خاص امنیتی با توجه به محدودیت های موجود در شبکه‌های تلفن همراه باید لحاظ گردد. در واقع حفظ امنیت و اطمینان از هویت طرفین در زمان انجام تراکنش‌ها به صورت آنلاین، از ضروریات این موضوع به شمار می آید. در این خصوص از پروتکل‌ها و تکنولوژی‌های مختلفی استفاده می‌گردد. استفاده از زیرساخت کلید عمومی در شبکه های سلولی به این دلیل که احراز و تصدیق هویت در آن توسط مرکز تصدیق هویت کاربر که یک مرجع قانونی است، انجام می‌پذیرد از قابلیت اطمینان بیشتری نسبت به سایر روش ها برخوردار است.

زیر ساخت کلید عمومی کلیه فاکتورهای لازم به منظور استفاده از امضای دیجیتال را فراهم می‌آورد. امضای دیجیتال در زمینه هایی مانند تجارت الکترونیک و دولت الکترونیک از زمانی که برخی از ویژگی های جالب توجه از قبیل یکپارچگی، احراز هویت و انکار ناپذیری را فراهم می‌کند، بحثی اساسی می‌باشد. به همین دلیل، امروزه تعداد بسیار زیادی از برنامه‌های کاربردی مختلف نیاز به استفاده از امضای دیجیتال و سرویس‌های انکار ناپذیری دارند. هدف از امضای دیجیتال این است که صحت و تمامیت اسناد الکترونیکی را در راه معادل سازی آن با امضایی که در اسناد کاغذی نوشته شده است تضمین نماید.

چنانچه امضای دیجیتال با استفاده از ادوات همراه تولید شود، "امضای همراه" نامیده می شود. امضای همراه به عنوان یک روش جهانی برای استفاده از یک دستگاه همراه به منظور تایید شهروندان در ادامه انجام تراکنش پیشنهاد گردیده است. علاوه بر این، یکی از مزیت های این پدیده آن است که امضایی که در یک دستگاه همراه تولید شده، ممکن است در هر مکان و هر زمان مورد استفاده قرار گیرد. بنابراین می‌توان گفت امضای همراه طراحی شده تا ارائه دهندگان نرم افزارهای کاربردی مجبور به توسعه راه حل‌های متعدد برای طیف وسیعی از دستگاه‌های همراه، سیستم عامل‌های ادوات همراه و فناوری‌های امضای دیجیتال که برای دستگاه های تلفن همراه وجود دارد، نباشند.

در این پایان نامه، یک مدل امن ارتباط بین مشتری و بانک و بالعکس با استفاده از زیر ساخت کلید عمومی بر روی شبکه های سلولی پیشنهاد گردیده و تلاش شده است با بررسی جامع روش‌ها و استانداردهای موجود، بهترین گزینه ها برای ارائه این سرویس ارائه گردد. همچنین در طراحی این مدل پیشنهادی سعی بر آن شده که با پیشرفت های شبکه تلفن همراه سازگاری لازم لحاظ گردد.

۱ – ۲ – هدف

هدف از این پایان نامه طراحی یک مدل امن برای ارتباط بین مشتری و بانـک با استفاده از زیرساخت کلید عمومی (PKI) برای شبکه های سلولی می باشد. که در آن سعی بر آن شده تا راهکاری عملیاتی برای اجرایی نمودن آن با توجه به وضعیت گذار از شبکه های نسل دوم به سوم در کشور ارائه گردد. در این طراحی خدمات امنیتی محرمانگی داده، تمامیت داده، احراز اصالت، انکارناپذیری و سایر ویژگی‌های افزون امنیتی در نظر گرفته شده است.

۱-۳- ساختار کلی پایان نامه

جهت بررسی موارد فوق، در ادامه فصول مختلفی از نظر خواهد گذشت که در اینجا به معرفی عناوین آنها پرداخته می شود:

- فصل دوم به بررسی ادبیات فنی می‌پردازد. در این فصل، پس از مروری بر تجارت همراه، روند تکامل شبکه های سلولی مطرح خواهد شد. همچنین فاکتورهای امنیتی بیان شده و معرفی زیرساخت کلید عمومی مورد مطالعه قرار می گیرد. در خاتمه نیز به تعریف و جزئیات SIM کارت به عنوان یک بستر مناسب برای احراز اصالت پرداخته می شود.
- در فصل سوم کارهای انجام شده در خصوص زیر ساخت کلید عمومی در کشور بیان شده و همچنین مدل‌های موجود که در خصوص استفاده از این زیر ساخت بر روی شبکه‌های سلولی پیشنهاد شده‌اند، مورد مطالعه قرار می‌گیرد. در بررسی این مدل ها به بیان مزایا و محدودیت های هر کدام نیز پرداخته می شود.
- فصل چهارم بر اساس آنچه در فصول قبل بیان شد، فاکتورهای لازم در خصوص نحوه عملکرد امضا با استفاده از کلید عمومی، که در طراحی مدل پیشنهادی مورد استفاده قرار می گیرد ارائه و معماری مدل تشریح و مورد ارزیابی قرار می گیرد. همچنین به جهت اطمینان از عملیاتی بودن آن، سرویس بخش‌های مربوط به کاربر شبیه‌سازی می‌گردد.
- در نهایت در فصل آخر (فصل پنجم)، به جمع‌بندی مسئله و فعالیت‌های صورت گرفته در خصوص موضوع مورد بحث پرداخته و نوآوری های حاصل شده از طراحی مدل پیشنهادی مطرح می گردد. همچنین، در ادامه نیز پیشنهاداتی در ارتباط با ادامه تحقیقات در آینده تبیین می گردد.

فصل ۲:

مروری بر ادبیات فنی

۲-۱- مقدمه

گسترش و نفوذ ادوات و ابزارهای همراه، تغییرات زیادی را در نیازمندی های جوامع بشری بوجود آورده است. تلفن‌های همراه، دستیاران دیجیتال شخصی (PDA[1]) و تلفن های هوشمند، امروزه به یک ابزار ضروری برای انجام بسیاری از کارها تبدیل شده اند. به دلیل کوچک و نسبتا ارزان بودن، این ابزارها می توانند نه تنها برای ایجاد تماس های صوتی و تصویری و یا ارسال و دریافت پیام های متنی و چندرسانه ای مورد استفاده قرار گیرند؛ بلکه می توانند در نقش یک کامپیوتر رومیزی نیز ظاهر شوند [1].

استفاده از ابزارهای همراه به عنوان یک کامپیوتر رومیزی، برگرفته از مفهوم محاسبات فراگیر[2] است که اولین بار توسط مارک وایسر[3] در سال ۱۹۹۹ مطرح گردید. محاسبات فراگیر مدل تعاملی بین انسان و کامپیوتر می باشد به گونه ای که داخل هر شی در محیط اطراف ما یک کامپیوتر تعبیه شده و عملیات محاسبات و پردازش اطلاعات را انجام می دهد [2]. به دنبال گسترش این مفهوم، استفاده از سایر ابزارها به عنوان کامپیوتر بیش از پیش مورد استقبال و توجه قرار گرفت. این موضوع تا جایی پیش رفت که در حال حاضر ۹۸.۸ درصد ریزپردازنده‌های تولید شده در کارخانه‌ها، به صورت ریز پردازنده تعبیه شده و در سایر دستگاه ها و ابزارها مورد استفاده قرار می‌گیرد و تنها ۱.۲ درصد ریز پردازنده‌ها برای استفاده در کامپیوترهای سنتی تولید می‌شوند [3]. همچنین، پیشرفت سریع تکنولوژی‌های ارتباطی و به دنبال آن تکنولوژی های بی سیم و شبکه های تلفن همراه باعث افزایش محبوبیت ادوات و ابزارهای همراه در بین مردم گردیده است. از ویژگی های برجسته و منحصر به فرد تلفن همراه دسترسی همیشگی و متحرک بودن آن می باشد. تلفن همراه همواره و همه جا با کاربر، همراه است. تلفن‌های همراه از شبکه‌های سلولی برای برقراری ارتباط استفاده می‌نمایند. از مهمترین تراکنش ها بر روی این نوع شبکه ها، ارتباط با بانک ها و سایر موسسات مالی می‌باشد.

در این فصل، برای دستیابی به یک مدل امن با کارایی و پذیرش کافی، پس از مروری بر تجارت همراه، روند تکامل شبکه‌های سلولی مطرح خواهد شد. در ادامه، فاکتورهای امنیتی بیان شده و معرفی زیرساخت کلید عمومی مورد مطالعه قرار می گیرد. در انتها نیز به تعریف و جزئیات SIM کارت به عنوان یک بستر مناسب برای احراز اصالت پرداخته خواهد شد.

---

[1] Personal Digital Assistant (PDA)

[2] Ubiquitous Computing

[3] Mark Weiser

۲-۲- تجارت همراه

امروزه با گسترش فناوری های الکترونیکی، و بالاخص فناوری های ارتباطی، انجام بسیاری از امور زندگی دستخوش تغییرات زیادی شده است. انجام امور تجاری نیز از این امر مستثنی نبوده و با پیشرفت تکنولوژی، روش‌های نوین جایگزین روش های سنتی انجام معاملات و بانکداری شده اند. در ادامه برای روشن شدن این تغییرات مروری مختصر، بر سیر تکاملی تجارت خواهیم داشت.

۲-۲-۱- روند پیشرفت تجارت

- تجارت سنتی (T-commerce[1]): به طور معمول، انجام هر گونه امور تجاری با استفاده از تلفن، نمابر و امکانات معمولی بانک ها، تحت عنوان "تجارت سنتی" شناخته می شود.
- تجارت الکترونیکی (E-commerce[2]): به انجام امور تجاری که با استفاده از فناوری های جدید (به خصوص امکاناتی که به واسطه‌ی گسترش اینترنت فراهم آمده اطلاق می شود. از جمله chat، e-mail و... که بدون محدودیت زمانی، تحت استاندارد های خاص انجام می‌پذیرد که از معتبرترین این استانداردها می توان به استاندارد بین المللی EDIFACT[3] اشاره نمود. یکی از مهمترین الزامات در این گونه تجارت، الزام به استفاده از امضای دیجیتال در انجام معاملات می باشد.
- تجارت همراه (M-commerce[4]): انجام امور تجاری، با استفاده از فناوری موبایل، تحت ضوابط تجارت الکترونیکی، بدون محدودیت زمانی و همچنین مکانی از ویژگی های این تجارت محسوب می‌شود.

با این تعاریف و با توجه به ویژگی های برتر تجارت همراه نسبت به انواع دیگر، همچون در دسترس بودن، سهولت استفاده، کم حجم بودن و قابلیت حمل ادوات همراه و امکان استفاده در هر مکان و هر زمان، اینگونه به نظر می‌رسد که استفاده از تجارت همراه در آینده جایگاه خاصی در جهان داشته باشد. در ادامه به بررسی بیشتر این تجارت خواهیم پرداخت.

[1] Traditional commerce
[2] Electronic commerce
[3] Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT)
[4] Mobile commerce