
بسم الله
الرحمن
الرحيم

دانشگاه قم

دانشکده فنی مهندسی

پایان‌نامه کارشناسی ارشد رشته فناوری اطلاعات گرایش تجارت الکترونیک

عنوان:

مقایسه روش‌های امنیتی برای افزایش اطمینان در پرداخت سیار با استفاده از تکنولوژی ارتباط میدان نزدیک NFC

استاد راهنما:

دکتر فرانک فتوحی قزوینی

استاد مشاور:

دکتر یعقوب فرجامی

نگارنده:

غدیر صفاء مجید

شهریور/ ۱۳۹۳

تقدیم به:

آستان حقیقت

و آنان که وصالش را می‌جویند،

آنان که در آغوشش کشیده‌اند و

آنان که خود، عین حقیقت‌اند

تشکر و قدردانی

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود.

در اینجا بر خود لازم می‌دانم از تمامی اساتید بزرگوار، به‌ویژه اساتید دوره کارشناسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت و فضائل اخلاقی یاری نموده‌اند تقدیر و تشکر نمایم.

از استاد گرامی و بزرگوار سرکار خانم دکتر فرانک فتوحی قزوینی که راهنمایی این‌جانب را در انجام تحقیق، پژوهش و نگارش این پایان‌نامه تقبل نموده‌اند نهایت تشکر و سپاسگزاری را دارم. همچنین از اساتید محترم جناب آقای دکتر یعقوب فرجامی، به‌عنوان استاد راهنمای دوم به خاطر راهنمایی‌های ارزنده، مساعدت‌ها و دلسوزی‌هایشان در طول انجام این پژوهش کمال تشکر را دارم.

از اعماق قلبم سپاسگزار خانواده‌ام هستم که همواره پشتیبان من بودند و از انجام هیچ کاری برای کمک به من فروگذار نبودند.

چکیده:

با افزایش نفوذ تلفن همراه و توسعه تجارت سیار، استفاده از تلفن همراه به‌عنوان ابزار پرداخت روزبه‌روز گسترش می‌یابد. به دلیل اهمیت امنیت در تجارت و پرداخت و نیز ویژگی‌های منحصربه‌فرد شبکه‌های بی‌سیم و محدودیت‌های موجود در ابزار پرداخت، پروتکل‌های پیشنهادی در حوزه پرداخت سیار علاوه بر تأمین کارایی می‌بایستی از امنیت مناسبی نیز برخوردار باشند. ارتباط میدان نزدیک(NFC)، ارتباط غیر تماسی را درب تعامل دستگاه‌های تلفن همراه نزدیک به هم از طریق یک کانال بی‌سیم را ایجاد می‌کند. تکنولوژی آن، با استانداردهای کارت هوشمند موجود، سازگار است.

مصونیت اطلاعات در پرداخت امری حیاتی است. استراق سمع یکی از بیشترین حملاتی است که فن‌آوری‌های مختلفی همچون کیف پول گوگل، NFC و دستگاه شناسایی فرکانس رادیویی(RFID) را مورد هدف قرار می‌دهد. محققان و کارشناسان امنیتی مکانیسم‌های مختلف دفاعی، برای حفاظت داده‌های خصوصی در مقابل دسترسی‌های غیرمجاز را طراحی کرده‌اند.

این پایان‌نامه یک لایه‌ی امنیتی را، با ادغام دو نوع مکانیسم دفاعی شناخته‌شده اضافه می‌کند، برای جلوگیری حمله بین دو دستگاه ارتباطی در حالت فعالیت مناسب است. این پروتکل‌ها برای انجام پرداخت ایمن به کار می‌روند. اولی با استفاده از الگوریتم رمزنگاری متقارن و پنهان نگاری کار می‌کند و پروتکل دیگر با استفاده از الگوریتم رمزنگاری کلید عمومی و امضای دیجیتال مکانیسم دفاعی را ایجاد می‌کند. پروتکل ادغامی توسط برنامه‌نویسی اندروید برای دستگاه تلفن همراه پیاده‌سازی شد. این پروتکل به‌صورت یک لایه امنیتی در دو برنامه مجزای مشتری و تاجر در یک سیستم پرداخت به کار گرفته شده است.

کلمات کلیدی: سیستم پرداخت سیار، ارتباط میدان نزدیک(NFC)، امنیت، حالت نظیر به نظیر، تلفن همراه، برنامه‌نویسی اندروید

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل اول:

کلیات پژوهش

۱-کلیات پژوهش

۱-۱مقدمه

فن‌آوری‌های اولیه تلفن همراه، از کاربردهای محدودی مانند ایجاد تماس و پیام تعریف شد و به سمت استفاده پیچیده‌تر رفت. رشد سریع دستگاه تلفن همراه، تحولی در ارتباطات بی‌سیم ایجاد کرد. کاربران به‌راحتی می‌تواند معاملات مختلف و انتقال اطلاعات از طریق دستگاه‌های تلفن همراه خود انجام دهند. تلفن‌های هوشمند، تلفن همراهی است که باقابلیت محاسبات پیچیده‌تر و یک سیستم‌عامل است. برای استفاده از ویژگی‌ها و امکانات تلفن‌های هوشمند، برنامه‌های کاربردی در محدوده سرگرمی(برنامه بازی) به تراکنش آنلاین (پرداخت غیرتماسی) طراحی شده است. تلفن‌های هوشمند را می‌توان برای انواع حالات تراکنش پرداخت، مانند هزینه پارکینگ، کرایه حمل‌ونقل استفاده کرد. مشتریان می‌توانند در طول راه، برای تسریع زمان خرید، از تلفن‌های هوشمند خود، به‌عنوان روش پرداخت به‌جای استفاده از روش سنتی (نقدی و سکه) استفاده کنند[۱]. یک فن‌آوری مهم برای پرداخت سیار ارتباط میدان نزدیک[۱] نامیده می‌شود[۲] و[۳].

ارتباط میدان نزدیک NFC ارتباطات برد کوتاه بین دستگاه‌ها و برچسب‌ها را قادر می‌سازد[۴] و [۵]. انتظار می‌رود که پرداخت از طریق NFC بازار انبوهی تا سال ۲۰۱۵ داشته باشد[۶]. این فن‌آوری، تا پایان سال ۲۰۱۶، حدود ۴۴۸ میلیون کاربر و ارزش کل تراکنش سالانه برای پرداخت‌های تلفن همراه به ۶۱۷ میلیارد دلار خواهد رسید. همچنین، در حال حاضر بسیاری از تولیدکنندگان بزرگ تلفن همراه، تراشه‌ی NFC را در گوشی‌ها جاسازی کردند.

---

۱ Near Field Communication (NFC)

بااین‌حال، آسیب‌پذیری در فن‌آوری‌های جدید در پرداخت و صنعت بانکداری هدفی برای هکرها و سازمان‌های جنایی خواهد بود. یک حمله موفق، ممکن است اعتبار ارائه‌دهنده پرداخت و یا بانک از دست برود و احتمال اعتماد به فن‌آوری جدید از بین برود. بنابراین ارائه‌دهنده پرداخت باید هدف از ساخت یک روش پرداخت NFC امن و مورد اعتماد دنبال کنند.

۱-۲ضرورت پژوهش

آخرین تحقیقات نشان می‌دهد که در آینده نزدیک، حدود بیست کشور از تکنولوژی NFC، برای پرداخت استفاده خواهند کرد.

ازآنجاکه NFC برای کاربردهای حساس امنیتی مانند پرداخت و کنترل دسترسی استفاده می‌شود، امنیت NFC مسئله‌ی مهمی به شمار می‌رود. بااین‌حال، پروتکل‌های در حال حاضر، به‌خودی‌خود حاوی چند اقدامات امنیتی است که این مسئولیت‌های امنیتی به توسعه‌دهنده‌ی برنامه‌یNFC، به نرم‌افزار سیار اضافه می‌کنند. دانستن آسیب‌پذیری‌ها و حملات احتمالی از NFC در گوشی‌های هوشمند یک گام مهم در ایجاد برنامه‌های کاربردی امن‌تر است. هنوز در NFC آسیب‌پذیری وجود دارد[۷] و[۸]. تمرکز تحقیقات روی دستیابی به معاملات پرداخت امن و احراز هویت کاربر در محیط پرداخت‌های تجاری متداول است. راه‌حل‌های پیشنهادی فن‌آوری‌های مختلف موجود مانند نسل دوم تکنولوژی تلفن‌های بی‌سیم (G۲)، فن‌آوری تلفن‌های بی‌سیم نسل سوم (G۳) و کارت‌های هویت شهروندی و کلید عمومی زیرساخت (PKI) همراه با NFC برای تأمین امنیت قوی و سهولت استفاده است. این پایان‌نامه آسیب‌پذیری‌های NFC را بررسی کرده و سپس به ارائه راه‌کار عملی برای حفظ امنیت در پرداخت از طریق این تکنولوژی، می‌پردازد.

طبق انجمن رسمیNFC [۹][۱]، این فن‌آوری جدید را، به علت تعامل برد کوتاه تضمین نمود. حتی باوجود سطح امن، نمی‌توان استراق سمع را رد کرد، چراکه ارتباط از طریق فرکانس رادیویی است. روش‌های حمله به‌طورکلی برای نرم‌افزار منحصربه‌فردند، تکنیک‌های متداول صورت می‌گیرد. استراق سمع عمل مخفیانه گوش دادن به مکالمه خصوصی دیگران بدون رضایت آن‌ها است[۳].

۱-۳اهداف و سؤالات پژوهش

هدف اصلی این پایان‌نامه، ارائه لایه امنیتی برای برنامه‌های NFC است. در راستای رسیدن به این هدف، اهداف فرعی زیر تعریف شده‌اند.

---

۱ NFC Forum

-شرح انواع پرداخت‌ها تماسی و غیر تماسی
-شرح مدل پیچیده NFC در ارتباط غیرتماسی از طریق تلفن همراه هوشمند.
-شرح آسیب‌پذیری‌های و تهدیدات NFC و راه‌های مقابله با آن
-شرح الگوریتم‌های مناسب برای NFC،
-ایجاد کانال امن از طریق الگوریتم‌های رمزنگاری متقارن و نامتقارن برای احراز هویت و پرداخت برخط و غیر برخط.
-شرح مختصر درباره سیستم‌عامل اندروید و بسته‌های مربوط به رمزنگاری
-پیاده‌سازی کانال امن از طریق رمزنگاری متقارن و پنهان‌نگاری.

اما سؤال‌هایی که این پایان‌نامه پاسخ می‌دهد:
آیا می‌توان سیستم پرداخت از طریق NFC را در تلفن‌های همراه پیاده‌سازی کرد؟
- بررسی حمله‌هایی که NFC را تهدید می‌کند؟
- بهترین روش امنیتی برای مقابله با حملات پرداخت NFC کدام است؟
- لایه امنیتی نرم‌افزاری مخصوص تلفن‌های همراه چگونه پیاده‌سازی می‌شود؟

۱-۴جنبه جدید بودن و نوآوری پژوهش

بامطالعه منابع پژوهشی مشخص شد که تاکنون پژوهشی جامع در زمینه حملات و تهدیدات صورت گرفته درNFC انجام نشده و همچنین لایه‌های امنیتی فقط به‌صورت تئوری بیان شده و راهکار عملی روی تلفن هوشمند دارای قابلیت NFC، صورت نگرفته است. این پژوهش، دو روش جدید رمزنگاری، برای مصونیت پرداخت از حمله، برای استفاده از تلفن همراه در پرداخت را ارائه کرده است.

۱-۵روش پژوهش

دو سناریو در این پژوهش مطرح شده است:

-فروشگاه‌های زنجیره‌ای وجود دارد که فروشندگان آن‌ها دارای تلفن هوشمند با قابلیت پرداخت از طریق NFC، می‌باشند. مشتری برای خرید خود نیاز است که بلیتی خریداری کند تا بتواند از این فروشگاه خرید کند. فروشگاه برای او بلیتی صادر می‌کند که دارای شماره بلیت و رمز مشترک بین فروشگاه و مشتری است. وقتی مشتری خریدی را انجام می‌دهد وارد برنامه‌ی مربوط به خود شده و با زدن شماره بلیت و رمز آن دستگاه خود را به دستگاه فروشنده نزدیک می‌کند و پیامی بین آن دو ردوبدل می‌شود. برنامه فروشنده

باز شده و رمز را وارد می‌کند. در صورت صحت رمز، شماره بلیت در برنامه فروشنده ظاهر می‌شود که صحت هویت مشتری را بیان می‌کند. در برنامه مشتری ابتدا شماره بلیت با استفاده از الگوریتم رمزنگاری متقارن رمز شده و همچنین برای مخفی کردن پیام، از پنهان‌نگاری استفاده می‌کند. در برنامه فروشنده پیام رمزگشایی می‌شود.

این سناریو را با استفاده از تلفن هوشمند Sumsung galaxy s۳ دارای تکنولوژی NFC پیاده‌سازی شد.

- پرداخت می‌تواند به‌صورت برخط و غیر برخط صورت گیرد. فروشنده و مشتری برای انجام عملیات پرداخت از طریق NFC، باید حسابی در بانک داشته باشد. بانک به او امضای دیجیتالی می‌دهد که در صورت انجام تراکنش، برای صحت احراز هویت خود برای طرف مقابل بفرستد.

برای خرید، ابتدا فروشنده پیامی که شامل مبلغ و امضای دیجیتالی صادر شده از بانک، را برای مشتری از طریق NFC، می‌فرستد.

درصورتی‌که پرداخت برخط باشد، مشتری چکی را برای بانک می‌فرستد تا در صورت داشتن مبلغ در حساب، بانک برای فروشنده پیام می‌دهد که این مبلغ به حساب او واریز شده است.

درصورتی‌که پرداخت غیر برخط باشد، مشتری در داخل برنامه خود این مبلغ را چک می‌کند که در صورت داشتن آن، چکی را برای فروشنده می‌فرستد تا بعد آن را به بانک بدهد و از او پول را واریز کند.

۱-۶ساختار پژوهش

در این پژوهش به‌منظور ارائه روش‌های جدید در پرداخت امن، از طریق NFC، پنج فصل زیر تدوین شده است:

فصل اول، کلیات پژوهش: در این فصل به ضرورت و اهداف و سؤالات این پژوهش را معرفی می‌کند.

فصل دوم، مرور ادبیات پژوهش و کارهای مرتبط: ابتدا به انواع روش‌های پرداخت و سپس به پرداخت سیار و معرفی فن‌آوری NFC و کاربردهای آن و سپس آسیب‌پذیری‌های آن در پرداخت و در آخر به مروری از تحقیقات مربوط به حمله‌ها پرداخته خواهد شد.

فصل سوم، معرفی الگوریتم‌های استفاده شده در پژوهش: ازجمله الگوریتم‌های رمزنگاری به‌کاررفته

در این، رمزنگاری متقارن AES و رمزنگاری با کلید عمومی و امضای دیجیتال است و سپس اشاره‌ای به پنهان‌نگاری خواهد پرداخت.

فصل چهارم، معرفی پروتکل‌های پیشنهادی و پیاده‌سازی یکی از آن‌ها با استفاده از زبان برنامه‌نویسی اندروید می‌پردازد.

فصل پنجم، نتیجه‌گیری و کارهای آتی: نتیجه‌ای از پژوهش و ارائه پیشنهادها برای کارهای آینده ارائه می‌دهد.

۱-۷چکیده فصل

در این فصل به‌منظور معرفی پژوهش، کلیاتی از آن شامل: ضرورت انجام پژوهش, اهداف پژوهش، جنبه جدید بودن و روش پژوهش و ساختار آن بیان شد. در پایان فصل نیز ساختار کلی پایان‌نامه به‌طور مختصر توصیف شد.