مطالعات علوم کاربردی در مهندسی
دوره ۳، شماره ۴، زمستان ۱۳۹۶
صفحات ۴۷- ۳۹

Online ISSN: ٢٤٧٦-٤٥٠٧
Print ISSN: ٢٥٣٨-٢٠٥٥
www.irijournals.com

تشریح امنیت در فناوری های ارتباط از فاصله نزدیک[1] و ارائه روش هایی به منظور بهبود امنیت در آن

امید موقّر

دانشجوی کارشناسی‌ارشد مهندسی کامپیوتر، دانشگاه تبریز، تبریز، ایران

چکیده

NFC یا همان Near-Field Communicationیک نوع از ارتباطات بی‌سیم کوتاه برد و مجموعه‌ای از استانداردها است که برای دستگاه‌های‌کوچک و قابل حمل به منظور ایجاد ارتباطات رادیویی با یکدیگر طراحی شده است. برای اولین بار ایده تکنولوژی NFC در سال ۲۰۰۴ شکل گرفت. در واقع این فناوری بیشتر برای تلفن‌های همراه هوشمند و ابزارهای مشابه، با هدف تعریف یک ارتباط ساده بوجود آمد. دستگاه‌های مجهز به تکنولوژی NFC می‌توانند به عنوان کارت‌های هوشمند بدون تماس عمل کنند و همچنین قادر به خواندن ونوشتن داده‌ها هستند. از آنجا که فناوری NFC یک استاندارد بی‌سیم است، مشخص است که در این زمینه بحث امنیتی از اهمیت بالایی برخوردار خواهد بود. دراین مقاله مسائل مربوط به امنیت NFC مورد بررسی قرار خواهد گرفت و راه حل‌هایی به منظور بهبود امنیت آن ارائه خواهد شد.

واژه‌های کلیدی: NFC، امنیت، حملات، پرداخت الکترونیکی

1 NFC

۱- مقدمه

NFC یک فناوری ارتباط بی‌سیم با فرکانس بالا و دامنه کوتاه مشابه فناوری بلوتوث است که انتقال داده بین دو دستگاه از فاصله ۰ تا حدود ۱۰ سانتی‌متر با فرکانس ۱۳/۵۶ مگا هرتز و بدون نیاز به تنظیمات کاربر را فراهم می‌نماید. فناوری NFC بر اساس شناسایی فرکانس رادیویی RFID[1] ساخته شده که به یک گجت امکان می‌دهد تا به گجتی دیگر امواج رادیویی ارسال نموده و پس از شناسایی یکدیگر، عملیات مشخصی بین آنها انجام گردد. برای اینکه دو دستگاه بتوانند با هم ارتباط برقرار کنند کافی است آنها را در کنار هم قرار دهیم. در ارتباطات NFC همیشه یک طرف آغازگر و طرف دیگر هدف در نظر گرفته می‌شود که آغازگر با ارتعاش امواج رادیویی برد کوتاه باعث ایجاد انرژی در هدف شده و به شکل‌گیری نوعی فرمان در هدف منجر می‌شود. در عین حال، برقراری ارتباط میان یک دستگاه NFC و یک چیپ NFC بدون منبع انرژی که به آن TAG گفته می‌شود نیز ممکن می‌باشد. برای اینکه گوشی هوشمند شما بتواند با دستگاه‌های دارای NFC ارتباط برقرار نماید، بایستی از چیپ NFC برخوردار باشد (تیمالسینا[2] و بوزال، ۲۰۱۲).

۲- NFC در پرداخت های الکترونیکی

امروزه با پیشرفت علم و تکنولوژی رفته رفته رو به سوی تحولات عظیمی در زمینه‌های مختلف هستیم یکی از این مواردی که باید در مورد آن صحبت کنیم مشاهده تغییرات بارز و آشکاری در باب پرداخت به صورت الکترونیکی است. با استفاده از فناوری نوین NFC که در بسیاری از کشور ها در حال پیشرفت فراوانی می‌باشد می‌توان در امر پرداخت بدون وجود اسکناس و همچنین پرداخت از راه دور اقدامات مهمی را انجام داد که البته این موارد باعث می‌شود تا در هزینه‌های مختلفی که مهمترین آن در مصرف کاغذ برای اسکناس و همچنین وقت است صرفه جویی‌های قابل ملاحظه‌ای رخ دهد. از آنجا که NFC یک رابط ارتباطی است برای وسایل مجهز به NFC حالت های ارتباطی مختلفی را فراهم می‌کند که می توان به ۳ دسته‌ی اصلی آن را طبقه بندی کرد (استرامر[3] و همکارانش، ۲۰۱۲).

- **حالت عملیاتی خواندن/نوشتن:** دراین حالت گوشی موبایل و یا هردستگاه مشابهی که به فناوری NFC مجهز است امکان خواندن یک برچسب از نوع RFID و یا نوشتن داده بر روی آن را دارد. در این حالت دو گوشی تلفن همراه ابتدا با ارسال سیگنال‌هایی به برچسب NFC ارتباط با آن را آغاز نموده و سپس با ارسال فرامین به برچسب NFC اطلاعات آن را می‌خوانند.
- **حالت عملیاتی نظیر به نظیر**: دراین حالت دو دستگاه NFC فعال با ایجاد لینک رادیویی بین خود به تبادل اطلاعات می‌پردازند. رابطهای ارتباطی نظیر به نظیر از پروتکل NFCIP-1 که "مدل درخواست پاسخ" بین دو دستگاه فعال را قادر است، استفاده می‌کند. در این حالت، تلفن‌های همراه مجهز به NFC می‌توانند هر نوعی از اطلاعات مانند کارت های ویزیت، تصاویر دیجیتال و غیره را با یکدیگر مبادله کنند.
- **حالت شبیه ساز کارت هوشمند:** یک دستگاه مجهز به NFC زمانی که به این مد تغییر وضعیت می‌دهد، می‌تواند به عنوان یک کارت هوشمند عمل کند. در این مد عملیاتی، دستگاه کارت‌خوان نمی‌تواند تفاوت بین کارت هوشمند (غیرتماسی) و دستگاه مجهز به NFC را تشخیص دهند همچنین در این حالت دستگاه های مجهز به NFC، کاملاً با استانداردهای مربوط به کارت های هوشمند (غیر تماسی) مبتنی بر ISO14443 نوع A، نوع B و Felica سازگارند. این مد عملیاتی برای کاربردهای مرتبط با پرداخت الکترونیک و پرداخت بلیت مناسب می‌باشد. در جدول شماره ۱ مزایای هر روش اورده شده است:

1 Radio Frequency Identification
2 Timalsina, S. K., Bhusal
3 Strommer

جدول ۱. مزایای هر یک ازحالت های ارتباطی در NFC

حالت عملیاتی شبیه سازی کارت	حالت عملیاتی نظیر به نظیر	حالت عملیاتی خواندن/نوشتن
کنترل دسترسی	سادگی در تبادل اطلاعات	افزایش تحرک
شبیه سازی المان فیزیکی	جفت شدن با اکثر دستگاه ها	پیاده سازی آسان

۳- امنیت و مسائل مربوط به آن

فناوری NFC ذاتاً با نگرانی‌هایی همراه است، زیرا می‌تواند داده‌های بسیار حساس را از طریق امواج انتقال دهد و این داده‌ها حین انتقال توسط امواج به طور غیرمجاز مورد دسترسی قرار بگیرند. نکته جالب توجه این که پروتکل NFC به خودی خود در مقابله با شنود داده‌ها از تمهیدات امنیتی کمی برخوردار است. تمهیداتی که مجمع NFC مورد توجه قرار داده به جنبه های فیزیکی این پروتکل محدود است. به عنوان مثال، حداکثر برد NFC در انتقال داده بین دو دستگاه، چهار اینچ است و از این رو شنود یا دسترسی غیرمجاز به داده ها در این محدوده کوچک بسیاردشوار خواهد بود (حیاتی، بحرینی و اصلانی دویچ، ۱۳۹۶).

۳-۱- حریم خصوصی

در رابطه با موضوع تکنولوژی و ارتباطات، حفظ حریم خصوصی همیشه یک موضوع بحث برانگیز بوده است. دستگاه‌های ان اف سی موجب نگرانی‌هایی در مورد حریم خصوصی می‌شوند. یک دستگاه ان اف سی غیر فعال به درخواست‌های خواننده بدون هشدار دادن به صاحبش پاسخ می‌دهد، چنین دستگاه‌هایی می‌توانند به طور خودکار زمانیکه وارد یک میدان مغناطیسی می-شوند فعال شوند. تمام دستگاه‌های NFC شناسه‌های یکتای خود را منتشر می‌کنند حتی دستگاه‌هایی که از داده ها با الگوریتم رمزگذاری محافظت می‌کنند. به عنوان مثال فردی که یک دستگاه NFC غیرفعال دارد به طور موثر شماره سریال ثابت را به خوانندگان مجاور پخش می‌کند. زمانیکه شناسه دستگاه فیزیکی به طور مستقیم یا غیر مستقیم با اطلاعات شخصی ترکیب شده باشد تهدیدها به حریم خصوصی افزایش می‌یابند، به عنوان مثال اگر شناسه دستگاه با اطلاعات مربوط به شخص ترکیب شود و کاربر یک معامله را با دستگاه انجام دهد یک کاربر مخرب قادر به ایجاد یک لینک بین شناسه دستگاه و اطلاعات شخصی کاربر است. این یک مشکل شناخته شده است و فقط منحصر به تکنولوژی NFC نمی‌باشد بلکه مربوط به سایر تکنولوژی های بی‌سیم مانند بلوتوث نیز می‌باشد.

۳-۲- عنصر امن در NFC

برای جایگزینی کارت هوشمند معمولی با تکنولوژی NFC، مهم ترین عاملی که باید در نظر گرفته شود امنیت سیستم است. برای حل این مشکل عناصر اضافی به عنوان "عنصر امن" به NFC اضافه شده است. عنصر امن امنیت و ذخیره سازی امن را برای دستگاهها و برنامه های کاربردی قادر به تکنولوژی NFC فراهم میکند و شامل موارد زیر است (مالدمیر[1] و همکارانش، ۲۰۰۸):

- **سخت افزار تعبیه شده:** یک جز که داخل تلفن همراه تعبیه شده و توسط کاربر قابل شخصی‌سازی است.

1 Madlmayr

- **کارت حافظه امن**: توسط مموری و عناصر کارت‌های هوشمند تولید می‌شوند.
- **سیم کارت های یکپارچه:** سیم‌کارت‌های هوشمند امن که از اطلاعات شخصی کاربران محافظت می‌کنند.

۳-۳- تهدیدهای امنیتی

بسترهای NFC همچنان مستعد حملات هستند. خطرات امنیتی مختلفی در این فناوری وجود دارد که مهم‌ترین آنها به همراه با راهکارهای مقابله با آنها در جدول ۲ آورده شده است (لنیون و همکارانش[1]، ۲۰۱۲).

- **استراق سمع:** از آنجا که ارتباطات سیستم NFC از طریق امواج می‌باشد استراق سمع یک حمله منطقی است که فرد مخرب با استفاده از آنتن‌های قدرتمند و تقویت سیگنال ها می‌تواند این کار را انجام دهد. این حمله محرمانه بودن سیستم NFC را مورد تأثیر قرار می‌دهد.
- **تغییر و تخریب از اطلاعات:** مهاجم با بهره‌گیری از مدولاسیون سیگنال اقدام به دستکاری پیام می‌کند امکان این حمله بستگی به شدت در مکانیزم برنامه‌نویسی برای مدولاسیون و داده ها دارد. این حمله صحت اطلاعات سیستم NFC را مورد تأثیر قرار می‌دهد.
- **افزودن اطلاعات:** اگرمدت زمان زیادی دستگاه منتظر پاسخ شود مهاجم می‌تواند اطلاعات خود را ارسال نماید. این حمله صحت اطلاعات سیستم NFC را مورد تأثیر قرار می‌دهد.
- **حمله مرد میانی:** در این حمله شخص سوم جایگزین و رابط بین دستگاه و سیستم NFC می شود. این حمله محرمانه بودن و صحت یک سیستم NFC را مورد تأثیر قرار می‌دهد.

موارد امنیتی در خصوص تگ های NFC می‌بایستی در برد محدود و معمولا چند سانتی‌متر بررسی گردد، البته احتمال دریافت سیگنال ها در محدوده یک متر یا بیشتر توسط مهاجمین، بسته به نوع سیگنال نیز وجود دارد.

جدول ۲: انواع تهدیدات وراههای مقابله با آن

انواع تهدیدات	راه حل های مواجهه با تهدیدات
استراق سمع	کانال امن
تخریب اطلاعات	ایجاد قابلیت تشخیص توان مصرفی
تغییر اطلاعات	کنترل دائم میدان رادیویی، کانال امن
افزودن اطلاعات	ارسال پاسخ گیرنده بدون وقفه زمانی، کانال امن
حمله مرد میانی	عدم امکان وقوع این حمله با توجه به ویژگی های آن

۳-۴- انواع حملات بر روی لینک های رادیویی NFC

اتصال رادیویی بین دو دستگاه NFC نشان‌دهنده ی یک نقطه قابل توجه جهت حمله افراد مخرب به سیستم است. این نوع حملات به سه دسته تقسیم می‌شوند که مسائل امنیتی مانند محرمانه بودن، یکپارچگی و در دسترس بودن را نقض می‌کنند.

1 Leinonen

- **دسترسی غیرمجاز به داده‌ها:** این نوع حملات با مساله محرمانه بودن اطلاعات حساس مانند شناسه دستگاه و شماره پین مقابله می‌کنند، برای انجام این نوع حمله کاربر مخرب نیاز به تجهیزات مناسب مانند یک آنتن بزرگ برای ضبط سیگنال در فواصل زیاد به دلیل محدودیت در محدوده ارتباطات NFC دارد. به عنوان مثال فرد مخرب می‌تواند داده‌هایی که روی لینک رادیویی بین دو دستگاه قرار می‌گیرد را تحت کنترل بگیرد (کورتوت[1] و همکارانش، ۲۰۱۲).
- **حملات مربوط به یکپارچگی:** در این نوع حملات فرد مخرب قادر خواهد بود داده‌های کاربر را در لینک‌های رادیویی بین دستگاه‌های NFC تغییر، پخش و یا حذف کند (ازدنیزچی[2] و همکارانش، ۲۰۱۳).
- **حملات منع سرویس:** این نوع حملات اغلب مربوط به سیستم‌های بی‌سیم است و با هدف منع سرویس و قطع ارتباط می‌باشد. مزاحمان در این نوع حملات می‌توانند از ارسال داده‌های کاربر جلوگیری کنند (پورقمی[3] و همکارانش، ۲۰۱۲).

۴- راه حل های پیشنهادی:

زمینه هایی که موجب ایجاد نقص در امنیت NFC می شود را به طور خلاصه در بخش های قبل بررسی کردیم. در این بخش به منظور بهبود امنیت در ارتباطات NFC راه حل هایی را پیشنهاد داده و مورد بررسی قرار خواهیم داد.

۴-۱- استفاده از شناسه دینامیک

هنگامی که یک اتصال بین دستگاه‌های NFC آغاز می‌شود، شناسه منحصر به فرد هر دستگاه در سراسر کانال رادیویی ارسال می‌شود. این مورد می‌تواند باعث ایجاد یک مشکل جدی امنیتی و به خطر افتادن حریم خصوصی شود؛ بنابراین پیشنهاد ما استفاده از شناسه های دینامیک است. یک شناسه دینامیک، یک مولد شناسه‌های شبه تصادفی[4] است که خود یک دنباله‌ی تصادفی تولید شده است که از شناسه اصلی دستگاه مستقل است. دنباله شبه تصادفی یک توالی است که به طور کامل تصادفی نیست، اما بسیار سخت است که از یک توالی تصادفی درست بتوان آن را جدا کرد. پیش بینی توالی شبه تصادفی نیز سخت است، چرا که تعیین چند عنصر اول دنباله بسیار دشوار است. در این روش به جای استفاده از شناسه، از یک شناسه تصادفی طولانی استفاده می کنیم. این روش باعث جلوگیری از ردیابی دستگاه‌ها می‌شود. پیاده سازی روش پیشنهادی شناسه‌های منحصر به فرد ارتباطی را تغییرخواهد داد.

۴-۲- فعال کردن کنترل NFC در دستگاه‌های کاربر

در دستگاه‌های کاربر، زمانی که رابط NFC توسط یک دستگاه NFC دیگر فعال شود، پروتکل NFC یک جلسه اتصال خودکار برقرارمی‌کند. اگر دستگاه کاربر به طور ناخودآگاه توسط شخصی دیگر فعال شود، این مسئله می‌تواند باعث ایجاد مشکل شود. برای جلوگیری از این فعال‌سازی، یک دکمه فعال‌سازی برای اتصالات تکی پیشنهاد می‌کنیم. این مورد یک ویژگی اختیاری است که توسط خود کاربرمی‌تواند کنترل شود. این تابع می تواند به شرح زیر اجرا شود:

اگر بخواهیم رابط NFC را در هر اتصال تکی فعال کنیم و همچنین اگر کاربر تصمیم به انجام این کار را دارد پروتکل NFC 18092 باید به صورت دستی شروع شود. برای این کار دستگاه NFC باید به حالت SENSE تنظیم شود. هنگامی که حالت

1 Kortvedt
2 Ozdenizci
3 Pourghomi

SENSE تنظیم می‌شود، دستگاه باید خاموش شود. این دستورالعمل باید دستورات SENS_REQ یا ALL_REQ را همان‌گونه که در استاندارد 18092 مشخص شده است شناسایی کند. با استفاده از این روش، کاربر هرگز به طور خودکار به دستگاه‌های دیگر مگر در مواقعی که از آن ها آگاهی داشته باشد متصل نمی‌شود. این یک ویژگی امنیتی اختیاری برای جلوگیری از فعال بودن و خواندن غیر ضروری است.

۴-۳- مولد هویت‌های شبه تصادفی (PRI)

PRI قادر به جایگزینی شناسه‌های فیزیکی در سیستم فعلی خواهد بود، اما باید به صورت یک تنظیم اختیاری باشد. دلیل این مورد این است که شناسه سخت افزاری در بعضی از توابع اجباری است. PRI باید در مدل OSI در لایه ی مشابه با آدرس های DiDi و DiDt موجود (لایه 2) اجرا شود تا رسانه بتواند بسته‌های داده را ارائه دهد.

شکل ۱. PRI در مدل OSI

در شکل (۱) ما PRI را در لایه دوم علاوه بر MAC موجود و LLC[1] اضافه کرده‌ایم تا سازگاری را حفظ کنیم. لایه PRI کاملاً شبیه لایه MAC است، اما طول آن ممکن است متفاوت باشد. مقدار value برای ناشناس بودن نباید هیچ چیزی را نشان دهد. استفاده از لایه PRI می‌تواند به عنوان آدرس DiDi و DiDt در نظر گرفته شود. شناسه تصادفی باید به طور تصادفی به اندازه کافی برای حفظ حریم خصوصی کاربر استفاده شود و همچنین در یک فریم زمان توانایی آن را داشته باشد که دستگاه‌های ناخواسته را مسدود کند.

در این راه حل پیشنهادی، نیازی به پیشگیری اضافی نیست، زیرا در حال حاضر در پروتکل NFC یک مقدار تصادفی در کنار شناسه منحصر به فرد استفاده می‌شود. این بدان معنی است که شناسه تصادفی می‌تواند با مقدار تصادفی یکسان باشد، اما احتمال آن بر اساس برآوردهای ما کم است. اگر این شرایط رخ دهد، collision handler در پروتکل NFC، مسئله را آغاز و حل خواهد کرد.

۴-۴- رد کردن دستگاه‌های ناخواسته

سیستم باید دستگاه‌های ناخواسته را بر اساس شناسه دستگاه رد یا به لیست سیاه اضافه کند. این می‌تواند یک شناسه دستگاه منحصر به فرد یا شناسه تصادفی تولید شده باشد که سعی در اتصال به سیستم در یک فریم زمان مشخص دارند. سیستمی که درخواست اتصال دریافت می‌کند باید شناسه آغازگر را ابتدا در لیست سیاه بررسی کند و اگر شناسه پیدا شد، اتصال را رد کند.

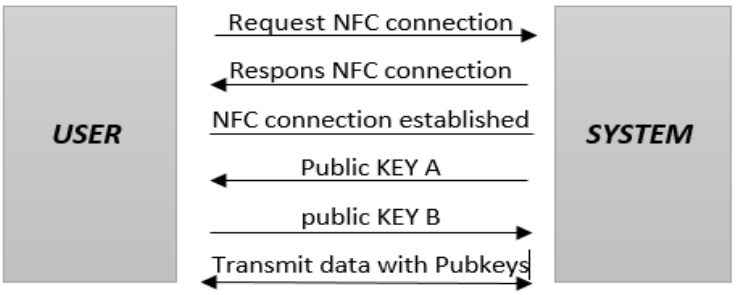
1 Logical Link Control

این سیستم همچنین می‌تواند دستگاه‌هایی را که مشکوک هستند فعال کند. یک بررسی مانند این می‌تواند در بخش نرم افزاری دستگاه سیستم اجرا شود.

۵-۴- ایمن سازی داده‌ها از طریق اتصال رادیویی NFC

هنگامی که دستگاه‌های NFC با امواج بی‌سیم رادیویی به یکدیگر متصل می‌شوند، مبادله‌های عمومی برای اطمینان از جریان اطلاعات رمز شده توسط لینک رادیویی انجام می‌شود.

همچنین مهم است که شرکت‌کنندگانی که در ارتباط هستند از شخصی که با آن ها در ارتباط هستند مطمئن باشند. پیشنهاد ما پیاده‌سازی رمزنگاری در کل روش احراز هویت بر روی کانال NFC است.



شکل ۲. جریان اطلاعات هنگام اجرای NFC به عنوان یک کانال امن

شکل (۲) یک جریان تبادل اطلاعات را نشان می‌دهد که در آن یک کاربر یک ارتباط NFC را آغاز می‌کند و پروتکل NFC را فعال می‌کند. سپس سیستم با پیام "تأیید" پاسخ می‌دهد. هنگامی که اتصال NFC برقرار می‌شود، سیستم یک session مبادله کلید عمومی را آغاز می‌کند. هنگامیکه این کار انجام می‌شود، شرکت‌کنندگان در ارتباطات می‌توانند یک ارتباط امن را از طریق کانال NFC شروع کنند. هنگامی‌که شرکت‌کنندگان داده‌های حیاتی را با NFC مبادله می‌کنند، این مبادله باید شامل استفاده از یک مقدار تصادفی، کلید عمومی و گواهینامه باشد. کاربر باید یک عدد تصادفی (Rand. r) تولید کند، امضای دیجیتالی را اضافه کند (d) و در نهایت رمزگذاری آن (e) را به سیستم ارسال کند. این سیستم باید صاحب کلید عمومی که کاربر دریافت کرده و برای رمزگذاری استفاده می‌شود باشد. اگر چنین بود، سیستم قادر به رمزگشایی داده‌های ارسال شده توسط کاربر است در غیر این صورت سیستم قادر به رمزگشایی نمی‌باشد و نمی‌تواند پاسخ صحیح را به کاربر بدهد. نهایتاً سیستم +1 را به عدد تصادفی دریافت شده (r + 1) اضافه می‌کند، امضای دیجیتال خود را (d) می‌افزاید و در نهایت آن را رمزگذاری می‌کند (e) و نهایتاً آن را به کاربر ارسال می‌کند. کاربر کسی است که ارتباط امن را آغاز کرده و کلید عمومی آن را می‌داند. اگر کاربر قادر به رمزگشایی باشد، روش پاسخ چالش صحیح است. اکنون کاربر مطمئن است که این سیستم است که با آن ارتباط برقرار می‌کند. با اضافه کردن امضای دیجیتال، می‌توان کلیدهای یکدیگر را فقط با یک پاسخ چالش تایید کرد زیرا امضای دیجیتال مربوط به کلید خصوصی است. به این ترتیب، سیستم می‌تواند ببیند که آیا کاربر کلیدی درست در پاسخ چالش را به او می‌دهد. چنین مکمل‌هایی مکانیزم‌های امنیتی را افزایش می‌دهد.

۵- نتیجه گیری:

با رشد روزافزون فناوری NFCو ضریب نفوذ این فناوری در زندگی عمومی مردم در آینده نزدیک شاهد استفاده و کاربردهای بیشتر آن خواهیم بود. پیشرفت‌های بسیاری در این زمینه صورت گرفته اما با این وجود این فناوری باز هم نیازبه تلاش‌های بیشتری در زمینه‌ی امنیت است. دراین مقاله تکنولوژی NFC و مسائل مربوط به امنیت آن به صورت اجمالی مورد بررسی

قرارگرفت و راه حل‌هایی به منظور بهبود امنیت ارائه شد در پایان این موضوع مطرح است که این تکنولوژی علاوه بر برخی مشکلات امنیتی که با آن مواجه بوده باز هم توانسته است بسیاری از انتظارات را برآورده کند.

منابع

۱. حیاتی، شجاع الدین؛ کیومرث بحرینی و مهدی اصلانی دویچ، ۱۳۹۶، بررسی استفاده از NFC در جهت رفاه کاربران تلفن همراه، اولین کنفرانس بین المللی دستاوردهای نوین در علوم و تکنولوژی، تهران شرکت بین المللی کوشا، https://www.civilica.com/Paper-ASTCONF01-ASTCONF01_071.html

2. Kortvedt, H., &Mjolsnes, S. (2009, November). Eavesdropping near field communication. In The Norwegian Information Security Conference (NISK) (Vol. 27).
3. Leinonen, A. P., Tuikka, T., &Siira, E. (2012, March). Implementing Open Authentication for Web Services with a Secure Memory Card. In Near Field Communication (NFC), 2012 4th International Workshop on (pp. 31-35). IEEE.
4. Madlmayr, G., Langer, J., Kantner, C., &Scharinger, J. (2008, March). NFC devices: Security and privacy. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on (pp. 642-647). IEEE.
5. Ozdenizci, B., Alsadi, M., Ok, K., &Coskun, V. (2013). Classification of NFC applications in diverse service domains. International Journal of Computer and Communication Engineering, 2(5), 614.
6. Pourghomi, P., &Ghinea, G. (2012, December). Challenges of managing secure elements within the NFC ecosystem. In Internet Technology And Secured Transactions, 2012 International Conference for (pp. 720-725). IEEE.
7. Strommer, E., Jurvansuu, M., Tuikka, T., Ylisaukko-oja, A., Rapakko, H., &Vesterinen, J. (2012, March). NFC-enabled wireless charging. In Near Field Communication (NFC), 2012 4th International Workshop on (pp. 36-41). IEEE.
8. Timalsina, S. K., Bhusal, R. (2012, June). NFC and its application to mobile payment: Overview and comparison. In Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference on (Vol. 1, pp. 203-206). IEEE.

مطالعات علوم کاربردی در مهندسی

دوره ۳، شماره ۴، زمستان ۱۳۹۶، صفحات ۴۷-۳۹

A summary on security in NFC and presenting some methods for improving the security in it

Omid Movaghar

Student of Masters in computer engineering, Tabriz University, Tabriz, Iran

Abstract

NFC which is short term for Near-Field Communication is a type of wireless communication that works on short ranges and it's also a set of standards that are designed for managing radio communications between small mobile devices. The idea of NFC technology was formed for the first time in 2004. In fact this technology was created for smart phones and other similar tools, in order to define a simple connection. Devices Equipped by NFC technology can operate as smart cards with no contact and also are able to read and write data. Because the NFC is a wireless standard, it would be obvious that the security has a great importance in this field. In this article, problems related to security in NFC will be studied and a set of solutions will be presented for improving security in NFC.

Keywords: NFC, Security, Attacks, Electronic Payments