هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
انجمن رمزایران
دانشگاه صنعتی خواجه نصیرالدین طوسی

طراحی پروتکل امنیتی جهت سامانه سیار مدیریت بلیط

شکوفه مختاری[۱]، فاطمه نوری[۲]، بهروز ترک لادانی[۳]

اصفهان، دانشگاه اصفهان، گروه مهندسی کامپیوتر
{sh_mokhtari, nouri.fatemeh}@mehr.ui.ac.ir, ladani@eng.ui.ac.ir

چکیده

امنیت یکی از مهمترین چالش های مطرح در سامانه‌های تجارت سیار می‌باشد زیرا به دلیل محدودیت منابع دستگاه‌های همراه، بسیاری از روش‌های امنیتی سنتی از قابلیت اجرایی و کارایی مناسبی برای اینگونه از سامانه‌ها برخوردار نیستند. در این مقاله پروتکل امنیتی ای را برای یکی از سرویس‌های تجارت سیار تحت عنوان سامانه سیار مدیریت بلیط، پیشنهاد می‌دهیم که علاوه بر ارضای نیازهای امنیتی مورد انتظار از کارایی مناسبی هم برخوردار می‌باشد. این پروتکل به صورت امن، انجام عملیات پرهزینه‌ی امضای دیجیتال را از جانب کاربر سیار به یک سرور کمکی واگذار کرده تا با حذف سربار ناشی از انجام این عملیات از دستگاه همراه کاربر، کارایی پروتکل را بهبود ببخشد. این پروتکل به صورت خاص برای دستگاه‌های همراه مجهز به بلوتوث طراحی شده است.

واژه های کلیدی

تجارت سیار، سامانه سیار مدیریت بلیط، پروتکل امنیتی، امضای دیجیتال، بلوتوث.

۱- مقدمه !

در طی ۱۰ سال گذشته، تجارت الکترونیک با افزایش روزافزون تعداد کاربرانی که از خریدهای اینترنتی استقبال کرده اند گسترش قابل توجهی یافته است. در عصر حاضر با توجه به پیشرفت تکنولوژی و بهبود عملکرد دستگاه‌های همراه، انتخاب تجارت سیار برای انجام معاملات، استفاده از انواع سرویس‌ها و تهیه کالاها از سوی کاربرانی که به دنبال راحتی و امکانات بیشتری هستند، گزینه مناسب‌تری است.

امنیت یکی از مهمترین چالش‌های مطرح در سامانه‌های تجارت سیار می باشد که بسیاری از محققان را به تحقیق و بررسی در این زمینه واداشته است [۴-۱]. از طرف دیگر، محدودیت منابع دستگاه‌های همراه موجب شده تا بسیاری از روش‌های امنیتی سنتی از قابلیت اجرایی و کارایی مناسبی برای اینگونه از سامانه‌ها برخوردار نباشند. از میان روش‌های شناخته شده رمزنگاری، عملیات تولید امضای دیجیتال پرهزینه‌تر و زمانگیرتر از سایر روش‌ها است [۵].

این پژوهش با هدف بررسی یکی از سرویس‌های پرطرفدار تجارت سیار، تحت عنوان سامانه سیار مدیریت بلیط[۱] انجام شده است. این سامانه، امکانی را برای کاربر فراهم می‌کند تا صرف نظر از موقعیت مکانی، با استفاده از تلفن همراه خود قادر به سفارش، پرداخت وجه و دریافت بلیط باشد. سامانه سیار مدیریت بلیط علاوه بر تسهیل فرآیند خرید و توزیع بلیط برای کاربران و سرویس‌دهندگان، با حذف هزینه‌های ناشی از تولید و توزیع بلیط‌های کاغذی از نظر اقتصادی نیز از سیستم‌های سنتی توجیه‌پذیرتر است.

سامانه‌های سیار مدیریت بلیط کنونی، دارای مشکلات و محدودیت‌هایی هستند که علیرغم تسهیلات به وجود آورنده برای مشتریان گاه تردیدهایی را در استفاده از آنها باقی می‌گذارد. اغلب

[1] mobile ticketing

SMS دارای مکانیزم امنیتی مناسبی برای ورود اطلاعات کارت‌های اعتباری نیست اینگونه پرداخت‌ها باید از طریق صفحات وب انجام شود. بلیط‌های خریداری شده در این سامانه‌ها اغلب در قالب پیام‌های متنی رمز شده یا کدهای میله‌ای به دستگاه همراه مشتری ارسال می‌شود. در مواردی که برای ارسال بلیط از پیام‌های متنی رمز شده استفاده می‌شود، سامانه از نظر امنیتی آسیب‌پذیرتر است چرا که خطر تولید بلیط‌های جعلی توسط اشخاص غیرمجاز در این سامانه‌ها بالا است. برخی دیگر از سامانه‌های کنونی، بلیط‌ها را به صورت کدهای میله‌ای به دستگاه همراه مشتری ارسال می‌کنند، هر چند که جعل این نوع بلیط‌ها کار دشوارتری است اما تأیید اعتبار آنها توسط تأییدکننده[1] در هنگام خرج کردن بلیط با چالش‌هایی روبرست. برای تشخیص صحت و اعتبار این بلیط‌ها، تأیید کننده باید مجهز به دستگاه پویشگری باشد که کدهای میله‌ای نمایش داده شده بر روی صفحه نمایش دستگاه همراه مشتری را پویش کرده و اعتبار یا عدم اعتبار آن را اعلام کند. با توجه به تنوع دستگاه‌های همراه و تفاوت چشمگیری که در نمایش و وضوح تصاویر دارند، تأیید اعتبار بلیط‌ها از طریق پویش تصاویر گاه نتایج نادرستی را در پی دارد.

در راستای حل برخی از مهمترین این مشکلات به ارائه پروتکلی برای سامانه سیار مدیریت بلیط خواهیم پرداخت. امتیاز عمده پروتکل پیشنهادی حذف سربار عملیات پرهزینه‌ی رمزنگاری کلید عمومی از دستگاه همراه مشتری و در عین حال تأمین نیازهای امنیتی مورد انتظار است. به این منظور از سرور واسطی کمک خواهیم گرفت که کاربر موبایل را قادر می‌سازد به صورت امن حق امضای خود را به آن واگذار کرده تا عملیات تولید و شناسایی امضا را از طرف او انجام دهد. به این ترتیب سربار محاسباتی ناشی از عملیات پرهزینه رمزنگاری به شخص سومی انتقال می‌یابد.

نیازهای امنیتی مورد انتظار برای سامانه سیار مدیریت بلیط را به صورت زیر تعریف می‌کنیم:

۱. غیر قابل انکار بودن: هیچ کدام از موجودیت‌ها نباید بتواند به ناحق انجام عملیات یا رخداد اتفاقی که صورت گرفته را انکار کند.

۲. صحت پیام: پروتکل باید توانایی تشخیص هرگونه تغییر در پیام امضا شده را داشته باشد.

۳. سادگی: به دلیل محدودیت منابع دستگاه‌های همراه، عملیات انجام شده توسط آنها تا حد امکان باید ساده در نظر گرفته شود.

۴. تأیید اعتبار بلیط به صورت غیر برخط: تأییدکننده باید بتواند بدون نیاز به برقراری هرگونه ارتباط با فروشنده اعتبار بلیط را تأیید یا رد کند.

۵. ممانعت از خرج کردن بلیط به سرقت رفته شده: بلیط تولید شده باید به گونه‌ای باشد که اگر توسط شخص دیگری به سرقت رفت، از هرگونه سوء استفاده از آن ممانعت به عمل آید.

ادامه مباحث این مقاله به صورت زیر دسته‌بندی شده است: کارهای مشابه انجام گرفته در زمینه سامانه سیار مدیریت بلیط در بخش ۲ مورد بحث قرار خواهند گرفت. در بخش ۳ معماری سامانه پیشنهادی را تشریح کرده، آن را از حیث تراکنش‌ها به سه فاز خرید، تحویل و خرج کردن بلیط تقسیم خواهیم کرد، همچنین موجودیت‌های درگیر در این سامانه را معرفی می‌کنیم. سپس در بخش ۴ به بررسی دقیق پروتکل امنیتی سامانه و تراکنش‌های صورت گرفته می‌پردازیم. این سامانه به طور خاص برای دستگاه‌های همراه مجهز به بلوتوث مانند اکثر گوشی‌های همراه طراحی شده است.در بخش ۵ پروتکل امنیتی ارائه شده را مورد ارزیابی قرار خواهیم داد و در بخش ۶ به جمع‌بندی و نتیجه‌گیری کار انجام گرفته خواهیم پرداخت.

۲-کارهای مرتبط

پژوهشگران در سال‌های اخیر طرح‌های مختلفی را برای سامانه سیار مدیریت بلیط ارائه کرده‌اند که هر یک دارای مزایا و معایب خاص خود است. در این بخش برخی از این طرح ها را به اختصار مورد بحث قرار می‌دهیم.

طرحی از سیستم که توسط فنگ باو[2] و سایرین[۶] ارائه شده مبتنی بر استفاده از امضای دیجیتال می‌باشد، کاربرد این طرح در مواردی است که موجودیت تایید کننده باید به صورت توزیع شده پیاده‌سازی شود. نیازهایی که در این سیستم باید به طور همزمان برآورده شود شامل تأیید صحت بلیط توسط تأییدکننده به صورت غیر بر خط، مستقل بودن تأیید کننده-های توزیع شده، صدور بلیط معتبر تنها توسط صادرکننده و تضمین صحت بلیط می‌باشد. این طرح برای تأمین نیازهای امنیتی گفته شده استفاده از امضای دیجیتال را مطرح کرده است بدون آنکه به تعریف دقیق تراکنش‌های انجام شده بپردازد. علاوه بر این، چنانکه از سامانه پرداخت آن برمی‌آید انجام عملیات رمزنگاری کلید نامتقارن بر عهده دستگاه همراه کاربر بوده که افت کارایی را به دنبال دارد.

ایده اصلی طرح دیگری که در سال ۲۰۰۱ توسط سونیا ماتاموروس[3] وسایرین[۷] ارائه شده برپایه استفاده از کارت‌های

[1] verifier

[2] Feng Bao

[3] Sonia Matamoros

هوشمند است. تأمین کارایی، تشخیص صحت بلیط به صورت غیر بر خط و فراهم آوردن قابلیت واگذاری بلیط از جمله اهداف تبیین شده ی طراحی پروتکل در این سیستم است. در این طرح، فروشنده باید از کلید عمومی کلیه اپراتورهای تلفن همراهی که قصد سرویس دهی به کاربران شان را دارد آگاهی داشته باشد. این پیش شرط از اشکالات این طرح به شمار می‌آید چراکه برای اجرایی شدن آن فروشنده نیازمند اعلام موافقت و همکاری اپراتورهای تلفن همراه است که معمولا به راحتی انجام نمی‌شود. در این طرح نیز انجام عملیات پرهزینه رمزنگاری کلید نامتقارن بر عهده دستگاه همراه کاربر می‌باشد.

پاول کولتون[1] و سایرین[۸] برای نگهداری امن بلیط‌های خریداری شده بر روی دستگاه همراه مشتری، طرحی را پیشنهاد داده‌اند که بر پایه استفاده از معماری ARM پردازنده گوشی‌های همراه هوشمند است، این طرح صرفاً برای دستگاه‌های مجهز به پردازنده با معماری ARM پیشنهاد شده و به دلیل وابستگی به سخت افزار موارد استفاده از آن محدود است.

۳- معماری سامانه پیشنهادی

در این سامانه کلیه تراکنش‌ها را می‌توان در قالب سه فاز دسته بندی کرد:

۱. فاز خرید بلیط: مشتری درخواستی را مبنی بر خرید بلیط صادر می‌کند. این امر می تواند از طریق اینترنت و یا اتصال به شبکه بی سیم فروشنده صورت گیرد.
۲. فاز تحویل بلیط: بلیط صادر شده توسط فراهم آورنده سرویس به مشتری تحویل داده می‌شود.
۳. فاز خرج کردن بلیط: مشتری پس از ارائه بلیط و تأیید صحت آن قادر خواهد بود که از سرویس یا کالای مورد نظر استفاده کند. در این بخش تکیه پروتکل پیشنهادی بر استفاده از اتصالات بلوتوث است.

موجودیت‌های این سامانه و ارتباط بین آنها در شکل ۱ آمده است. مبحث مربوط به روش‌های پرداخت وجه بلیط از حیطه کار فعلی این پژوهش بیرون بوده و فرض بر این است که از یکی از روش‌های موجود استفاده می‌شود. بر همین اساس موجودیت‌های سامانه را به صورت زیر در نظر گرفته و نام گذاری می‌کنیم:

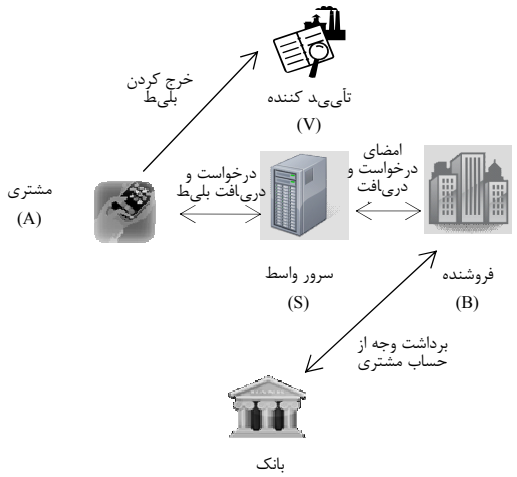
۱. صادرکننده پیام (کاربر سیار) که از این پس با نماد A به آن اشاره می‌شود.
۲. دریافت کننده پیام (فراهم آورنده سرویس اینترنتی) که با نماد B نام گذاری می‌شود.
۳. تأییدکننده بلیط که با نماد V از آن یاد می‌شود.
۴. سرور کمکی که S نامیده می‌شود.

[1] Paul Coulton

۴-شرح پروتکل ارتباطی

در این سامانه کاربر سیار پس از برقراری یک ارتباط برخط درخواست خرید بلیط را صادر کرده و فروشنده پس از تولید بلیط و طی همان ارتباط آن را برای کاربر ارسال می‌کند.

همانگونه که در بخش ۱ گفته شد به منظور حذف سربار محاسباتی ناشی از عملیات پرهزینه رمزنگاری کلید عمومی از یک سرور واسط کمک گرفته می‌شود که کاربر موبایل را قادر می‌سازد به صورت امن حق امضای خود را به آن واگذار کرده تا تولید و شناسایی امضا را از طرف او انجام دهد. لیشاهی[2] و سایرین [۹]پروتکلی را برای خریدهای اینترنتی پیشنهاد کرده-



اند که برخی از نیازهای امنیتی مورد توجه در آن مشابه نیازهای امنیتی مطرح در این پژوهش برای سامانه سیار مدیریت بلیط است. این پروتکل که IJS[3] نامگذاری شده است، حق امتیاز امضای دیجیتال کاربر سیار را به صورت امن به یک سرور واسط واگذار می‌کند. با توجه به آنچه گفته شد این پروتکل برای استفاده در فاز خرید این سامانه مناسب به نظر می‌رسد. پروتکل IJS دارای سه تراکنش است که تنها مرحله خرید کالا را پشتیبانی می‌کند و برای تحویل کالا هیچ گونه تدبیری نیاندیشده است. ما در طرح پیشنهادی با بومی‌سازی این پروتکل، آن را برای استفاده در فاز خرید بلیط در سامانه سیار مدیریت بلیط مناسب سازی می‌کنیم، اما در سامانه مورد نظر فاز تحویل بلیط نیز باید بلافاصله پس از فاز خرید و در همان ارتباط آغاز شده و پایان پذیرد. بنابراین پروتکل ویژه‌ای نیز برای فاز تحویل بلیط ارائه می‌دهیم تا کلیه نیازهای امنیتی مطرح شده را تأمین کند.

روال کار سامانه پیشنهادی با توجه به پروتکل ارتباطی آن به صورت زیر توضیح داده می‌شود: A قصد ارسال پیام m را،

[2] Lisha He

[3] Improved Joint Signature

جهت سفارش خرید بلیط، به B دارد و باید این پیام با کمک S امضا شود تا از انکار و جعل آن جلوگیری شود. بعد از دریافت پیام توسط B، او نیز باید رسید امضا شده‌ای را به S برگرداند تا از انکار دریافت پیام ممانعت به عمل آید. همراه با این امضا بلیط تولید شده نیز به S ارسال می‌شود تا پس از تأیید امضا، توسط S به A تحویل داده شود. A پس از دریافت بلیط باید پیامی به B ارسال کند تا از موفقیت‌آمیز بودن مراحل تحویل بلیط او را مطلع کند. در این پروتکل از درهم شده‌ی کد احراز اصالت صاحب پیام[1](HOAC) و درهم شده ی کد احراز اصالت پیام[2] (HMAC)استفاده شده است. HOAC به B اثبات می‌کند که A همان صادرکننده پیام است و HMAC به S ثابت می‌کند که m و HOAC هر دو، از طرف A آمده است. جزئیات این تراکنش‌ها همراه با تعریف دقیق پارامترهای ارسالی در بخش ۴-۲ آورده شده است.

۴-۱-نمادها

توضیح مختصری از علائمی که در پروتکل استفاده شده است به شرح زیر می‌باشد:

$h(x)$: تابع درهم ساز یکطرفه بدون برخورد (ایده‌آل)

K_{AB}: کلید نشست مشترک بین موجودیت A و B

Pk_A: کلید عمومی موجودیت A

Sk_A : کلید خصوصی موجودیت A

$\{X\}_K$: عملیات کلید عمومی روی X توسط کلید K

۴-۲-تراکنش ها

پروتکل پیشنهادی این طرح دارای ۷ تراکنش می باشد که کلیه فازهای خرید، تحویل و خرج کردن بلیط را پشتیبانی می‌کند. در سه تراکنش اول این پروتکل که مربوط به فاز خرید می‌باشد از پروتکل IJS استفاده شده است که پارامترهای تراکنش‌های اول و سوم آن، با توجه به نیازهای سامانه سیار مدیریت بلیط، بومی‌سازی می‌شود. تراکنش‌های سوم تا ششم مربوط به فاز تحویل بلیط از فروشنده به مشتری می‌باشد، همچنین مشتری موظف است دریافت موفقیت‌آمیز بلیط را به اطلاع فروشنده برساند. تراکنش هفتم فاز خرج کردن بلیط را پشتیبانی کرده و در ارتباطی مستقل بین مشتری و تأییدکننده صورت می‌گیرد.

قبل از شروع تراکنش‌ها لازم است که دو کلید مخفی مشترک به ترتیب، بین موجودیت‌های A وB، و بین موجودیت‌های A وS تبادل شده باشد.این کار را می‌توان با استفاده از پروتکل‌های شناخته شده برقراری کلید انجام داد و ما در این پروتکل به آن نمی‌پردازیم. بعد از اجرای این پروتکل، A و B باید دارای مقدار محرمانه مشترک K_{AB} و موجودیت های A وS دارای مقدار محرمانه مشترک K_{AS} شده باشند. تراکنش‌های این سامانه به شرح زیر می‌باشد:

مرحله۱ (درخواست خرید بلیط): موجودیت A شش پارامتر تولید می کند: پیام m، زمان[3] ts_A ، مهلت زمانی[4] dl_A ، HOAC، HMAC و یک مقدار درهم شده $h(K_{AB})$. $h(K_{AB})$ توسط S برای تأیید درستی HMAC به کار گرفته می شود. سپس A توسط تراکنش T1 این پارامترها را به S ارسال می کند.

T1. A→S: m, ts_A, dl_A, $h(K_{AB})$, HOAC, HMAC
Where HOAC=h(m, $h(K_{AS})$,dl_A, K_{AB}), and
HMAC=h(m, ts_A, dl_A, HOAC, $h(K_{AB})$, K_{AS})

پارامتر dl_A به صورت یک فاصله زمانی بین زمان شروع (t_{StartA}) و زمان پایان(t_{EndA}) تعریف می‌شود. ts_A و dl_A برای ممانعت از تکرارهای دوباره غیرمجاز امضا توسط S استفاده می-شود. یک ts_A قابل قبول بین زمان شروع و زمان پایانی که در dl_A تعریف شد در نظر گرفته می‌شود. HOAC شامل مقدار K_{AB} می‌باشد که S از آن باخبر نیست، بنابراین S نمی‌تواند یک HOAC معتبر تولید کرده و آن را به B ارسال کند. علاوه بر آن چون K_{AB} به صورت درهم شده ارسال می‌شود S قادر به کشف آن نیست. S با استفاده از HMAC می‌تواند اعتبار و صحت پیام m و HOAC دریافتی را تأیید کند.

پیام m علاوه بر اطلاعات مورد نیاز برای خرید بلیط حاوی درهم شده‌ی شماره بلوتوث دستگاه همراه خریدار می‌باشد. از این پارامتر در ممانعت از سوء استفاده از بلیط به سرقت رفته بهره خواهیم برد.

مرحله ۲ (امضای درخواست): پس از دریافت T1، S دو عمل Veri-1 و Veri-2 را برای تأیید اعتبار و تازگی[5] پیام انجام می‌دهد.

Veri-1: بررسی جدید بودن ts_A. $ts_{SA} \le ts_A \le t_E$ باشد، تراکنش قابل قبول و گرنه رد می‌شود.

Veri-2:

تأیید $HMAC=h(m', ts_A', dl_A', HOAC', h(K_{AB})', K_{AS})$ که ts_A', dl_A', $h(K_{AB})'$, HOAC و m′ پارامترهای دریافتی هستند.

هدف از Veri-1 این است که S از تازه بودن دریافت T1 اطمینان حاصل کند. هدف از Veri-2 تأیید این است که HMAC شامل پارامترهای m ، K_{AS} و HOAC است. چون HMAC با کلید K_{AS} درهم‌سازی شده است S می‌تواند

[1] HOAC : Hash Origin Authentication Code

[2] HMAC: Hash Message Authentication Code

[3] timestamp

[4] deadline

[5] freshness

مطمئن باشد که پس از تأیید، HMAC دریافتی معتبر است و هیچ کدام از مقادیر آن دستکاری نشده است. اگر هر کدام از Veri-1 یا Veri-2 با موفقیت انجام نشود S از امضای پیام خودداری کرده و پروتکل خاتمه می‌یابد (این برای تمام مراحل تراکنش‌ها صادق است). در غیر اینصورت S یک امضای مشترک (JS) روی پیام m و HOAC انجام داده و آنها را در تراکنش T2 به B ارسال می‌کند. ts_S زمان S است.

T2. S→B: m, $h(K_{AS})$, ts_S, dl_A, HOAC, JS
Where JS={h(m, $h(K_{AS})$,ts_S, dl_A, HOAC)}Sk_S

مرحله ۳ (ارسال رسید درخواست و بلیط تولید شده): بعد از تراکنش T2، B عملیات تأیید Veri-3، Veri-4 و Veri-5 را برای تأیید اعتبار، تازگی و غیر قابل انکار بودن انجام می دهد:

Veri-3: تأیید *HOAC=h(m′, $h(K_{AS})'$,dl_A', K_{AB})* که $h(K_{AS})'$، dl_A' و m′ پارامترهای دریافتی و K_{AB} کلید مشترک بین A و B است. Veri-3 تأیید می کند که HOAC شامل مقادیر درست K_{AB} ، m، $h(K_{AS})$ و dl_A است. به دلیل اینکه K_{AB} برای تولید HOAC استفاده شده، HOAC یک مقدار درهم شده است بنابراین هر دو بحث احراز اصالت A و صحت پیام m برای B قابل اثبات است.

Veri-4: بررسی جدید بودن ts_S که باید $t_{StartA} \le ts_S \le t_{EndA}$ باشد. نتیجه مثبت Veri-4 برای B تضمین می کند که T2 به تازگی دریافت شده است.

Veri-5: رمزگشایی امضا با کلید عمومی S
{JS}Pk_S={{h(m, $h(K_{AS})$, ts_S, dl_A, HOAC)}Sk_S}Pk_S= h(m, $h(K_{AS})$,ts_S,dl_A, HOAC)
و بررسی اینکه آیا مقدار امضای رمزگشایی شده با تابع درهم سازی که روی مقادیر دریافتی به تازگی محاسبه شده مطابقت دارد یا نه، یعنی:
h(m, $h(K_{AS})$, ts_S, dl_A, HOAC)= h(m′, $h(K_{AS})'$, ts_S', dl_A', HOAC′)
که m′، $h(K_{AS})'$، ts_S'، dl_A' و HOAC′ پارامترهای دریافتی هستند.

اگر نتیجه مثبت باشد، JS یک امضای معتبر است و بنابراین S نمی تواند انجام تراکنش T2 را انکار کند. B امضای JS و پیام m را می پذیرد.

در این مرحله بلیط مشتری (ticket) با پارامترهای زیر تولید می شود:
ticket={{M, h(blueNum), option}Sk_B}Pk_V
پارامتر M حاوی برخی از اطلاعات پیام m، شماره منحصر به فرد بلیط، قیمت، تعداد و سایر اطلاعات مورد نیاز، پارامتر h(blueNum) درهم شده ای از شماره منحصر به فرد بلوتوث دستگاه همراه موجودیت A که در تراکنش قبلی توسط B دریافت شده بود و پارامتر اختیاری option که بسته به سرویس و سرویس دهنده های مختلف مقادیر متفاوتی می گیرد. سپس بلیط تولید شده توسط کلید خصوصی B (Sk_B) امضا شده و با کلید عمومی تأیید کننده V (Pk_V) رمزنگاری می شود تا از اعمال هر گونه تغییر در بلیط بعد از تولید آن جلوگیری شود و فقط موجودیت V قادر به بازگشایی، تأیید و دریافت اطلاعات آن باشد.

B در تراکنش T3 چهار پارامتر را به S ارسال می کند:

T3. B→S: ts_B, dl_B, ticket, BS
Where BS={h(m, ticket, $h(K_{AB})$, ts_B, dl_B)}Sk_B

مرحله ۴ (تحویل بلیط): S عملیات Veri-6 و Veri-7 را برای بررسی تازه و غیر قابل انکار بودن تأیید دریافت انجام می دهد.

Veri-6: بررسی تازگی ts_B که باید $t_{SB} \le ts_B < t_{EB}$ باشد. نتیجه مثبت این مرحله نشان می دهد که BS و تراکنش T3 هر دو تازه اند.

Veri-7: امضای B روی BS را با کلید عمومی B باز کرده،
{BS}Pk_B = {{h(m, ticket, $h(K_{AB})$, ts_B, dl_B)}Sk_B}Pk_B = h(m, ticket, $h(K_{AB})$, ts_B, dl_B)
و بررسی می کند که آیا مقدار درهم شده به دست آمده از رمزگشایی امضا با تابع درهم ساز محاسبه شده از پارامترهای دریافتی مطابقت دارد یا نه، یعنی:
h(m, ticket, $h(K_{AB})$, ts_B, dl_B) = h(m′, ticket′, $h(K_{AB})'$, ts_B', dl_B')
که ts_B' و dl_B' و ticket′ پارامترهای دریافتی درتراکنش T3 و m′ و $h(k_{AB})'$ پارامترهای دریافتی از تراکنش T1 هستند.

اگر این دو مقدار مطابقت داشته باشند S اطمینان حاصل می کند که BS امضای معتبری است که توسط B و با کلید خصوصی وی تولید شده است. BS غیر قابل انکار بودن دریافت پیام m و تضمین صحت $h(K_{AB})$ را از سوی A فراهم می کند. اما در این مرحله هنوز پروتکل کامل نشده است چراکه موجودیت S وظیفه رساندن بلیط تولید شده به موجودیت A را به پایان نبرده است.

S با کلید نشست K_{AS}، کد درهم شده ی ticket، ts_{SD} زمان S ، dl_B و $h(K_{AB})$ را تولید کرده و این کد درهم شده که آن را HTC[1] می نامیم به همراه سه پارامتر دیگر در تراکنش T4 به موجودیت A ارسال می شود.

T4. S→A: ts_{SD}, dl_B, ticket, HTC
Where HTC= h(ticket, ts_{SD}, dl_B, $h(K_{AB})$, K_{AS})

مرحله ۵ (ارسال رسید دریافت بلیط): A عملیات تأیید Veri-8 و Veri-9 را برای بررسی تازگی و صحت پیام دریافت شده انجام می دهد.

[1] Hash Ticket Code

Veri-8: بررسی تازگی ts_{SD} که باید $t_{StartB} \le ts_{SD} < t_{EndB}$ باشد. نتیجه مثبت این مرحله نشان می دهد که HTC و تراکنش T4 هر دو تازه اند.

Veri-9: تأیید $HTC = h(ticket', ts_{SD}', dl_B', h(K_{AB}),$ K_{AS}) که $ticket'$، ts_{SD}'، dl'_B پارامترهای دریافتی و $h(K_{AB})$ و K_{AS} پارامترهای ذخیره شده در A هستند.

نتیجه مثبت این دو مرحله، تأیید تازگی و صحت HTC و عدم تغییر پارامترهای آن است. A بعد از تأیید این موارد در تراکنش T5 پیام ack ای مبنی بر دریافت بلیط به S می فرستد. این پیام به صورت زیر است:

T5. $A \rightarrow S$: ts_{Aack}, dl_{Aack} , ack_HOAC, ack_HMAC
Where ack_HMAC=h(ticket, ts_{Aack}, dl_{Aack}, ack_HOAC, $h(K_{AB})$, K_{AS}) , and
ack_HOAC=h(ticket, dl_{Aack}, $h(K_{AS})$, K_{AB})

مرحله ۶ (امضای رسید دریافت بلیط): S پس از دریافت T5 تازه بودن و صحت پیام ACK را در Veri-10 و Veri-11 بررسی کرده و در صورت مثبت بودن نتیجه از دریافت بلیط توسط موجودیت A مطمئن می شود.

Veri-10: بررسی تازگی ts_{Aack}

Veri-11: تأیید $ack\_HMAC=h(ticket', ts_{Aack}', dl_{Aack}', ack\_HOAC', h(K_{AB})', K_{AS})$ که ts_{Aack}'، dl_{Aack}' پارامترهای دریافتی هستند و سایر پارامترها هم در تراکنش های قبلی تبادل شده و در S ذخیره شده اند.

با مثبت بودن نتیجه S از دریافت بلیط توسط A و صحت آن اطمینان حاصل می کند، سپس در تراکنش T6 پیامی را با امضای خود به B ارسال کرده و از تحویل موفقیت آمیز بلیط خبر می دهد که به عنوان رسید برای B تلقی می شود.

T6. $S \rightarrow B$: ts_{Sack}, dl_{Aack},ack_HOAC, SACK
Where SACK= { h(ticket, ts_{Sack} , dl_{Aack} , $h(K_{AB})$, ack_HOAC) }Sk_S

ts_{Sack} زمان S می باشد.

مرحله ۷ (تأیید رسید دریافتی): B پس از دریافت و تأیید تراکنش T6 از تحویل صحیح بلیط به موجودیت A و غیرقابل انکار بودن فعالیت S در این روند (دریافت بلیط از B و ارسال آن برای A) اطمینان حاصل می کند.

Veri-12: تأیید *$ack\_HOAC=h(ticket', dl_{Aack}', h(K_{AS})', K_{AB})$* که dl_{Aack}' پارامتر دریافتی، $ticket'$ و $h(K_{AS})'$ پارامترهایی هستند که قبلا در B ذخیره شده و K_{AB} کلید مشترک بین A و B است. Veri-12 تأیید می‌کند که ack_HOAC شامل مقادیر درستی است. بنابراین به B اثبات می شود که رسید دریافتی از جانب A است و صحت رسید و بلیط تحویل داده شده نیز برای B قابل اثبات است.

Veri-13: تأیید کردن تازگی ts_{Sack} اگر $t_{StartA} \le ts_{Sack} < t_{EndA}$

Veri-14: امضای S را با کلید عمومی آن باز کرده،

$\{SACK\}Pk_S = \{\{h(ticket, ts_{Sack}, dl_{Aack,} h(K_{AB}), ack\_HOAC\}Sk_S\}Pk_S = h(ticket, ts_{Sack}, dl_{Aack}, h(K_{AB}), ack\_HOAC)$

و مطابقت مقدار درهم به دست آمده از رمزگشایی امضا با مقدار درهم محاسبه شده از پارامترهای دریافتی را بررسی می کند، یعنی:

$h(ticket, h(K_{AB}), ts_{Sack}, dl_{Aack}, ack\_HOAC) = h(ticket', h(K_{AB})', ts_{Sack}', dl_{Aack}', ack\_HOAC')$

که ts_{Sack}'، dl_{Aack}' و ack_HOAC' پارامترهای دریافتی درتراکنش T6 و $ticket'$ و $h(k_{AB})'$ مقادیر ذخیره شده در B هستند. اگر این دو مقدار مطابقت داشته باشند S اطمینان حاصل می کند که SACK امضای معتبری است که توسط S و با کلید خصوصی وی تولید شده است.

بعد از این مراحل و در صورت انجام درست تمامی تراکنش ها پروتکل خاتمه می یابد. حال موجودیت A دارای بلیط معتبری است که می تواند آن را پس از گرفتن تأیید از تأییدکننده خرج کند.

در فاز خرج کردن بلیط، مشتری پس از برقراری ارتباط با تأییدکننده از طریق پروتکل بلوتوث، بلیطی که قبلاً خریداری کرده را ارسال می کند که در صورت تأیید اعتبار و صحت بلیط، اجازه دسترسی به سرویس مورد نظر را دریافت می کند. در این مرحله علاوه بر تأیید اعتبار بلیط لازم است که تأیید کننده شماره منحصر به فرد بلوتوث گوشی همراه مشتری را با شماره بلوتوث موجود در بلیط تأیید شده مطابقت دهد تا در صورت عدم تطابق، از خرج شدن آن جلوگیری کند و راه هر گونه سوء استفاده از بلیط توسط فرد غیر مجاز مسدود خواهد شد.

مرحله ۸ (تأیید صحت بلیط): برای خرج کردن بلیط، مشتری اطلاعات بلیط خود را برای تأیید کننده ارسال می‌کند.

T7. $A \rightarrow V$: ticket

Veri-15: تأییدکننده ابتدا بلیط را توسط کلید خصوصی خود از رمز خارج می‌کند، یعنی:

$\{ticket\}Sk_V = \{\{M, h(blueNum), option\}Sk_B\}Pk_V\}Sk_V$

سپس اعتبار امضای B روی بلیط را بررسی کرده و برای این کار آن را با کلید عمومی B باز می کند،

$\{\{M, h(blueNum), option\}Sk_B\}Pk_B = (M, h(blueNum), option)$

در صورتی که صحت هر دوی این مراحل به تأیید تأییدکننده برسد، بلیط مشتری معتبر تشخیص داده شده و اجازه دسترسی به سرویس مورد نظر را به دست می‌آورد.

۵-تحلیل امنیتی پروتکل پیشنهادی

در این بخش پروتکل پیشنهادی را در مقابل نیازهای امنیتی مطرح شده ارزیابی می کنیم:

۵-۱- غیرقابل انکار بودن

در این قسمت پروتکل پیشنهادی را در مقابل غیر قابل انکار بودن صدور درخواست بلیط از جانب مشتری، نقش واسط در انجام تراکنش ها، دریافت درخواست بلیط توسط فروشنده و دریافت بلیط توسط مشتری بررسی می کنیم.

غیرقابل انکار بودن صدور پیام m از جانب A: HMAC و HOAC اعتباری غیر قابل انکار از صدور پیام m از جانب A را برای B فراهم می‌کنند زیرا اولا فقط A و S می‌توانند یک HMAC معتبر تولید کنند، ثانیا فقط A و B هستند که می‌توانند یک HOAC معتبر تولید کنند. در نهایت تنها S (صرفنظر از A) می‌تواند یک HMAC معتبر را تولید کند وتنها B (صرفنظر از A) می‌تواند یک HOAC معتبر تولید کند. به عبارت دیگر هیچ یک از S یا B نمی‌توانند هر دوی HMAC و HOAC را تولید کنند. اگر نتیجه Veri-2 و Veri-3 مثبت باشد، A تنها کسی است که می‌توانسته هر دوی HMAC و HOAC را تولید کرده باشد و نمی‌تواند صدور پیام از جانب خود را انکار کند.

غیرقابل انکار بودن نقش واسط در انجام تراکنش‌ها: غیرقابل انکار بودن نقش واسط در انجام تراکنش‌ها نیز به وسیله امضای دیجیتال مربوط به S بر روی پیام‌های ارسالی فراهم می‌شود.

غیرقابل انکار بودن دریافت درخواست خرید بلیط توسط B: این مورد نیز به وسیله امضای دیجیتال موجودیت B روی رسید ارسالی به S تأمین می‌شود.

غیرقابل انکار بودن دریافت بلیط توسط A: اثبات این مورد به وسیله رسید ارسالی از سوی A به B فراهم می‌شود. این رسید از دو پارامتر ack_HMAC و ack_HOAC تشکیل شده که ابتدا به S ارسال می‌شود و در صورت تأیید صحت ack_HMAC موجودیت S رسید را امضا کرده و به B می‌فرستد. دقیقاً همانند آنچه در اثبات غیرقابل انکار بودن صدور پیام m از جانب A گفته شد، غیرقابل انکار بودن صدور رسید دریافت بلیط توسط A نیز اثبات می‌شود.

۵-۲-صحت پیام

به کار بردن m در HMAC و HOAC به ترتیب این اطمینان را برای S و B فراهم می‌کند که m تغییری نکرده است، بنابراین صحت پیام تضمین می‌شود. به طریق مشابه، استفاده از پارامتر ticket در تراکنش‌های T3 و T4 توسط HTC صحت پیام را برای A و S تأمین می‌کند.

۵-۳-سادگی

تنها عملیات مورد نیاز که توسط دستگاه همراه مشتری باید انجام شود درهم‌سازی چند پارامتر دریافتی در طی تراکنش‌ها به منظور بررسی صحت پیام است که با توجه به حداقل قابلیت‌های دستگاه‌های همراه فعلی از سادگی و کارایی مناسبی برخوردار است.

۵-۴-تأیید اعتبار بلیط به صورت غیر بر خط

مشتری قبل از دستیابی به سرویس یا کالای مورد نظر باید اعتبار بلیط خود را به تأیید موجودیت تأییدکننده برساند. به این منظور پس از برقراری ارتباط و ارسال بلیط، تأییدکننده موظف است تا ابتدا بلیط را که با کلید عمومی او رمز شده است از رمز خارج کرده، سپس امضای آن را بررسی کند. در صورت تأیید این دو مرحله اعتبار بلیط به اثبات می‌رسد.

۵-۵-ممانعت از خرج کردن بلیط به سرقت رفته

پس از تأیید اعتبار بلیط، تأییدکننده شماره بلوتوث دستگاه همراه مشتری را که در طی ارتباط با وی به دست آورده است توسط تابع درهم ساز، در هم ریخته و آن را با پارامتر h(blueNum) موجود در بلیط مقایسه می کند، در صورت تطبیق این دو مقدار مشخص می‌شود که مشتری واقعی اقدام به خرج کردن بلیط نموده است و بلیط به سرقت نرفته است.

۵-۶-مقاومت در برابر حمله DoS

اگر حمله کننده بتواند با صدور درخواست‌های معتبر به موجودیت‌های سامانه آنها را به انجام تعداد زیادی از عملیات امضای دیجیتال وادار کند، موجودیت‌ها از پاسخ به درخواست-های کاربران واقعی در زمان معین بازمانده و حمله DoS صورت می‌گیرد.

پروتکل پیشنهادی از موجودیت‌های S و B در برابر حمله DoS حفاظت می‌کند. موجودیت S با بررسی HMAC مبادله شده در تراکنش اول و یا ack_HMAC در تراکنش پنجم و موجودیت B با بررسی HOAC درتراکنش دوم و یا ack_HOAC در تراکنش ششم، می‌تواند حمله DoS را تشخیص دهد. زیرا دو پارامتر اول شامل کلید مخفی K_{AS} و پارامترهای بعدی شامل کلید مخفی K_{AB} می‌باشند که حمله کننده از آن اطلاعی ندارد و همین امر تولید پارامترهای معتبر جعلی را دشوار می‌سازد. بنابراین حمله کننده قادر به عبور از Veri-2 یا Veri-11 به منظور حمله به S و Veri-3 یا Veri-

12 برای حمله به B نبوده و این موجودیت ها از انجام عملیات امضای دیجیتال روی پیام‌های حمله کننده سرباز زده و پروتکل خاتمه می‌یابد.

۶-سایر مسائل مربوط به سامانه سیار مدیریت بلیط

سامانه سیار مدیریت بلیط را از دو جنبه کلی می‌توان مورد بحث و بررسی قرار داد: الف) مسائل سطح بالا مانند تعریف قالب استانداردی برای نمایش بلیط‌ها [۱۰]، ب) مسائل سطح پایین شامل پروتکل ارتباطی سامانه که موضوع اصلی مورد بحث این پژوهش بود. پرداختن به مسائل سطح بالا در حیطه کار فعلی ما قرار نمی‌گیرد اما به اختصار به مواردی از این دست که ذکر آنها ضروری به نظر می رسد اشاره می‌کنیم.

در این پروتکل به منظور جلوگیری از خرج کردن بلیط دزدیده شده توسط سارق، استفاده از بلیط را به وسیله درهم شده‌ی شماره بلوتوث دستگاه همراه خریدار اصلی منحصراً به او اختصاص دادیم. حال ممکن است این ابهام به وجود آید که آیا بلیط‌های تولید شده به هیچ وجه قابل انتقال به غیر نیستند؟ همانگونه که در بخش ۴-۲ گفته شد بلیط تولید شده دارای پارامتری به نام option است که می‌تواند بر حسب کاربردها و سرویس‌های مختلف، مقادیر متفاوتی بپذیرد. در مواردی که نیاز است به خریدار اختیار انتقال بلیط به غیر داده شود باید پارامتر option طوری تنظیم شود که تأییدکننده پس از باز کردن بلیط متوجه آن شده و در صورت عدم تطابق درهم شده‌ی شماره بلوتوث درج شده در بلیط با آن چه در طی ارتباط با مشتری به دست آورده و درهم شده‌ی آن را محاسبه کرده است، از خرج کردن آن ممانعت نکند. به منظور امنیت بیشتر و جلوگیری از خرج شدن بلیط‌های دزدیده شده در این گونه از کاربردها، تأییدکننده می‌تواند درهم شده‌ی شماره بلوتوث دستگاه همراه خریدار اصلی را درخواست و در صورت مطابقت، اعتبار بلیط را تأیید کند. بدیهی است که پیش از این و در هنگام انتقال بلیط از خریدار اصلی به شخص دیگر باید این مقدار درهم شده مبادله و نگهداری شده باشد.

مسئله دیگر جلوگیری از خرج کردن دوباره بلیط است که یکی از راه‌حل‌های موجود برای آن، ذخیره شماره منحصر به فرد بلیط‌های خرج شده در پایگاه داده تأییدکننده و بررسی وجود این شماره در پایگاه داده برای هر بلیطی که در انتظار تأیید اعتبار است، می‌باشد. بدیهی است که در صورت وجود این شماره در پایگاه داده و در صورتی که بلیط فقط برای یک بار استفاده صادر شده باشد، اعتبار آن تأیید نمی‌شود. در مواردی که نیاز است تأییدکننده به صورت توزیع شده پیاده‌سازی شود و امکان همگام سازی پایگاه داده تمام تأییدکننده ها ممکن نیست می‌توان از ترکیبی از شماره منحصر به فرد بلیط و زمان استفاده کرد. زمان دار کردن بلیط ها از طریق پارامتر option تعبیه شده در بلیط می تواند انجام گیرد.

۷- جمع بندی

در این مقاله به بررسی یکی از سرویس‌های پرطرف دار تجارت سیار تحت عنوان سامانه سیار مدیریت بلیط پرداختیم و برخی از چالش‌ها و نیازهای امنیتی مطرح در این زمینه را مورد بحث قرار دادیم. پس از آن پروتکلی را پیشنهاد دادیم که از یک سو، غیرقابل انکار بودن، صحت پیام، سادگی، تأیید اعتبار بلیط به صورت غیر بر خط، ممانعت از خرج کردن بلیط دزدیده شده و مقاومت در برابر حمله‌های DOS را تضمین می‌کند و از سوی دیگر، محدودیت منابع دستگاه‌های همراه را در نظر گرفته و از کارایی مناسبی برخوردار است. این پروتکل به جای انجام عملیات پرهزینه و زمان بر امضای دیجیتال تنها نیازمند انجام چند عمل کم هزینه درهم‌سازی بر روی دستگاه همراه مشتری است.

تمرکز ما در این پژوهش بر روی پروتکل‌های ارتباطی این سامانه و جزئیات تراکنش‌ها بوده است، اما مسائل دیگری مانند انواع روش‌های پرداخت، تعریف قالب استانداردی برای تولید و نمایش بلیط‌ها و دسته‌بندی بلیط‌ها برای کاربردهای مختلف از جمله کارهایی است که در حیطه کار فعلی نبوده و در آینده به آن خواهیم پرداخت.

۸- سپاسگزاری

از استاد ارجمند، جناب آقای مهندس بهروز شاهقلی، به خاطر حمایت‌ها و نظرات ارزشمندشان در طی این پژوهش سپاسگزاری می‌کنیم.

مراجع

[1] S. S. Grosche and H. Knospe, Secure Mobile Commerce, Electronics & Communication Engineering Journal, (2002), pp.228-238.

[2] A. Tsalgatidou and E. Pitoura, Business Models and Transactions in Mobile Electronic Commerce: Requirements and Properties, Computer Networks, 37, (2001), pp.221-236.

[3] A. Tsalgatidou, J. Veijalainen and E. Pitoura, Challenge in Mobile Electronic Commerce, Proceeding of IeC 2000, 3rd Int. Conf. On Innovation through E-Commerce, UK, Nov. 14th-16th, 2000.

[4] J. Veijalainen, V. Terziyan and H. Tirri, Transaction Management for M-Commerce at a Mobile Terminal, URL: http://cosco.hiit.fi/Articles/hiccs36.pdf.

[5] L. He, and N. Zhang, A new signature scheme: Joint signature, Proceedings of the 2004 ACM symposium on Applied computing , Cyprus, 2004, pp. 807-828.

[6] F. Bao, L. Anantharaman, and R. Deng. Design of portable mobile devices based e-payment system and e-ticketing system with digital signature. In Proceedings of 1st International Conferences on Info-tech and Info-net, volume 6, pages 7–12. IEEE, 2001.

[7] Antonio Maña, Jesús Martínez, Sonia Matamoros, José M. Troya . GSM-Ticket: Generic Secure Mobile Ticketing Service. In proceedings of the International Graduate Consortium and Educational Symposium, 2001.

[8] Wan Huzaini Wan Hussin, Paul Coulton, Reuben Edwards. "Mobile Ticketing System Employing TrustZone Technology," In Proceedings of IEEE Fourth International Conference on Mobile Business, Sydney Australia, July 2005 pp. 651-654.

[9] Lisha He, Ning Zhang, Lirong He, Ian Rogers. Secure M-commerce Transaction :A Third Party Based Protocol. In Proceedings of Third International Symposium on Information Assurance and Security(IAS07), Manchester, UK, 29-31 August 2007.

[10] MeT Ticketing Requirements. Proposed Specification. Version 1.0, September 2002, http://www.openmobilealliance.org/.