فصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۳، پاییز ۱۳۹۱، (پیاپی ۱۱): صص ۳۱-۳۹

یک پروتکل احراز اصالت دوسویه در کارت هوشمند

رسول کاظمی آشتیانی[۱]، بهروز خادم[۲]

تاریخ دریافت: ۹۱/۰۷/۱۷
تاریخ پذیرش: ۹۱/۱۰/۰۴

چکیده

یکی از شاخص‌های توسعه هرکشور، میزان رشد خدمات در شبکه‌های الکترونیکی مدیریت و کنترل (در سطح ملی و بخشی) می‌باشد. تامین امنیت اطلاعات و پیشگیری از دسترسی غیر مجاز در این‌گونه شبکه‌ها، از جمله اهداف کلان پدافند غیر عامل در حوزه فناوری اطلاعات است. یکی از فراگیرترین و حساس‌ترین نمونه‌های چنین شبکه‌هایی، شبکه بانکداری الکترونیک است که تامین امنیت اطلاعات کاربران، لازمه به‌کارگیری سامانه‌های الکترونیکی در آن می‌باشد. با توجه به اینکه پروتکل‌های احراز اصالت برای جلوگیری از دسترسی‌های غیر مجاز در چنین سامانه‌هایی به‌کار می‌روند، نقش بسیار مهمی در تامین ارتباطات امن در شبکه بانکداری الکترونیکی ایفا می‌کنند. در این مقاله ضمن معرفی یک دسته‌بندی جدید در ملزومات امنیتی و کارآیی این پروتکل‌ها، یک پروتکل احراز اصالت دوسویه مبتنی بر کلمه عبور را معرفی خواهیم کرد و نشان خواهیم داد که این پروتکل روی فناوری کارت‌های هوشمند قابل استفاده می‌باشد. همچنین نشان خواهیم داد که پروتکل پیشنهادی، هم از نظر رعایت ملزومات امنیتی در مقابل حملات متداول به پروتکل‌های احراز اصالت مقاوم است و هم از نظر رعایت ملزومات عملیاتی در مقایسه با پروتکل‌های جدید و مشابه دیگر، کارآیی بیشتری دارد.

کلیدواژه‌ها: پروتکل احراز اصالت دو سویه، کارت هوشمند، کلمه عبور

۱- کارشناس ارشد رمز- دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات- دانشگاه جامع امام حسین(ع) kazemiashtyani@gmail.com - نویسنده مسئول
۲- مربی و عضو هیئت علمی دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات- دانشگاه جامع امام حسین(ع)

۱- مقدمه

پدافند غیرعامل نقش مهمی در حفظ امنیت اطلاعات و اعتماد نسبت به پایداری و خلل‌ناپذیری شبکه‌های الکترونیکی ملی ایفا می‌کند[۱]. در هر کشوری، یکی از مهم‌ترین شبکه‌های ملی، شبکه بانکی است. انجام عملیات بانکی با استفاده از اینترنت، عابربانک‌ها و دستگاه‌های کارت‌خوان، برخی از خدمات رایج بانکداری الکترونیک است. «احراز اصالت» مفهومی است که به‌وسیله آن سرویس‌دهندگان شبکه‌های الکترونیکی از مجاز بودن کاربران این شبکه‌ها در زمان ارتباط اطمینان پیدا می‌کنند. به عبارت دیگر، احراز اصالت عبارت است از فرآیندی که در طی آن ادعای کاربر برای اثبات هویت خود از طرف سرویس‌دهنده رد یا پذیرفته می‌شود[۱۸]. یکی از فناوری‌های رایج برای انجام احراز اصالت الکترونیکی، کارت هوشمند است که استفاده روزافزون از آن در زندگی روزمره و به خصوص در بانکداری الکترونیک باعث شده است تا کاربران، سرویس‌دهندگان و سازندگان این کارت‌ها به تأمین امنیت این فناوری نگاه ویژه‌ای داشته باشند. حفظ امنیت این فناوری به دو بخش سخت‌افزاری و نرم‌افزاری تقسیم‌بندی می‌شود که ما در این مقاله فقط بخش نرم‌افزاری را مورد توجه قرار خواهیم داد؛ لذا خواننده علاقه‌مند به مطالعه ساختار کارت هوشمند و امنیت سخت‌افزاری آن را به [۱۲] ارجاع می‌دهیم.

اکنون اکثر افراد جامعه در سطوح مختلف اجتماعی از کارت هوشمند در کارهای بانکی خود استفاده می‌کنند. فراگیرتر شدن استفاده از این فناوری نیازمند آن است تا به کاربران این اطمینان داده شود که خدشه‌ای به حریم خصوصی و اطلاعات شخصی آنها وارد نمی‌شود.

به‌طور کلی پروتکل‌های احراز اصالت دارای ساختارهای متنوعی هستند که از جمله آن‌ها می‌توان به پروتکل‌های مبتنی بر رویکرد چالش و پاسخ، پروتکل‌های مبتنی بر مرکز توزیع کلید، پروتکل‌های مبتنی بر شناسه و پروتکل‌های مبتنی بر کلمه عبور که هدف ما در این مقاله می‌باشند، اشاره کرد[۱۸].

از سال ۱۹۸۱ که لمپورت[1] [۸] اولین پروتکل احراز اصالت مبتنی بر کلمه عبور را ارائه کرد تاکنون تکنیک‌های رمزنگاری مختلفی در طراحی پروتکل‌های مبتنی بر کلمه عبور مورد استفاده قرار گرفته است که می‌توان به [۶،۱۴RSA]، الجمال[۵]، توابع چکیده‌ساز[2][۴] و خم بیضوی [۳] اشاره کرد. برای بهبود پروتکل لمپورت[۸]، هوانگ[3] و لی [۵] در سال ۲۰۰۰ یک پروتکل مبتنی بر الجمال ارائه کردند و این پروتکل در سال ۲۰۰۳ توسط شن[4] [۱۵] بهبود یافت. آواستهی و لال[5] [۲] در سال ۲۰۰۳ یک پروتکل مبتنی بر الجمال با محرمانگی پیشرو[6] پیشنهاد کردند. یون[7] و همکارانش [۲۴] در سال ۲۰۰۴ قابلیت‌هایی نظیر تغییر کلمه عبور را به پروتکل [۲] اضافه کردند. در سال ۲۰۰۵ لی[8] و همکارانش یک پروتکل مبتنی بر الجمال و تابع چکیده‌ساز ارائه کردند [۹] اما ژو[9] و همکارانش [۲۱] حمله جعل هویت را روی [۹] اعمال کرده و یک پروتکل جدید ارائه کردند. سانگ[10] [۱۶] ضمن ارائه یک پروتکل جدید، حمله جعل هویت توسط کاربر داخلی را روی پروتکل ژو نشان داد. در سال ۲۰۱۱ چن[11] و همکارانش حمله حدس زدن کلمه عبور و نشست موازی را روی پروتکل وانگ[12][۲۰] ارائه کردند[۴]. در میان انواع پروتکل‌هایی که تاکنون ارائه شده است پروتکل‌هایی که بر پایه ترکیب پروتکل کلید عمومی الجمال و توابع چکیده‌ساز طراحی شده‌اند، همواره مورد توجه محققین بوده است. در این مقاله می‌خواهیم برای افزایش سطح امنیت و کارآیی پروتکل‌های مبتنی بر الجمال و توابع چکیده‌ساز، یک پروتکل جدید ارائه کنیم.

در ادامه مقاله، در بخش دوم بعد از معرفی پروتکل‌های مبتنی بر کلمه عبور، ملزومات اکید و غیر اکید امنیتی و کارآیی پروتکل‌های احراز اصالت مبتنی بر کلمه عبور با کارت هوشمند را مورد بررسی قرار می‌دهیم. در بخش سوم، یک پروتکل جدید پیشنهاد می‌کنیم. در بخش چهارم ضمن معرفی حملات متداول، مقاومت پروتکل پیشنهادی را در مقابل آن‌ها مورد بررسی قرار می‌دهیم. در بخش پنجم، پروتکل پیشنهادی را از نظر امنیت، کارآیی و پیچیدگی محاسباتی با برخی از پروتکل‌های مشابه دیگر مورد مقایسه قرار می‌دهیم. در بخش ششم نیز نتایج به‌دست آمده، مطرح می‌شود.

۲- پروتکل‌های مبتنی بر کلمه عبور با کارت هوشمند

در یک پروتکل احراز اصالت مبتنی بر کلمه عبور، چهار بخش: کاربر، سرویس‌دهنده، کانال امن و کانال نا امن وجود دارند و شامل سه مرحله اصلی: ثبت، ورود و احراز اصالت می‌باشد. در مرحله ثبت[13]، کاربر درخواست ثبت‌نام خود را که شامل اطلاعات ضروری و منحصر به‌فرد او است، از طریق کانال امن برای سرویس‌دهنده ارسال می‌کند. سرویس‌دهنده با استفاده از کلید خصوصی خود و اطلاعاتی که دریافت کرده است، مقادیری را تولید کرده و برخی از آنها را در کارت هوشمند ذخیره می‌کند و کارت را به‌وسیله کانال امن به کاربر تحویل می‌دهد. کاربر در مرحله ورود[14]، کارت هوشمند خود را وارد دستگاه کارت‌خوان کرده و کلمه عبورش را وارد می‌کند. کارت هوشمند با

1- Lamport
2- Hash Function
3- Huang and Li
4- Shen
5- Awasthi and Lal
6- Forward Securily
7- Yoon
8- Lee
9- Xu
10- Song
11- Chen
12- Wang
13- Registration
14- Login

استفاده از کلمه عبور و اطلاعات ذخیره شده در خودش، محاسباتی را انجام داده و در نهایت، یک پیام ورودی تولید کرده و آن را برای سرویس‌دهنده ارسال می‌کند. در مرحله احراز اصالت، سرویس‌دهنده با استفاده از کلید خصوصی و اطلاعاتی که از قبل دارد، صحت ادعای کاربر را مورد بررسی قرار می‌دهد. اگر پروتکل احراز اصالت، دوسویه باشد سرویس‌دهنده نیز پیامی را تولید کرده و برای کاربر ارسال می‌کند تا او هم هویت سرویس‌دهنده را مورد بررسی قرار دهد.

در سال ۲۰۰۶، تسای[1] و همکارانش [۱۹] بعد از بررسی و مقایسه بیش از ۵۰ پروتکل مبتنی بر کلمه عبور با کارت هوشمند، معیارهایی را برای تحلیل این پروتکل‌ها ارائه کردند و در سال ۲۰۱۲ مادهوسودهان[2] و همکارانش [۱۱] این معیارها را به‌روزرسانی کرده و معیارهای جدیدی نیز به آن افزودند. در این بخش ما با استفاده از نتایج کارهای [۱۱و۱۹] معیارهای فوق را در یک دسته‌بندی جدید به نام‌های ملزومات اکید و غیر اکید جمع‌بندی می‌کنیم.

ملزومات اکید، آن دسته از معیارهایی است که عدم رعایت آن‌ها در یک پروتکل موجب آسیب‌پذیر بودن یا غیر قابل پیاده‌سازی بودن پروتکل می‌شود. در مقابل، ملزومات غیر اکید شامل معیارهایی است که موجب ارتقای امنیت یا کارآیی پروتکل می‌گردد.

۲-۱- ملزومات امنیتی

ملزومات اکید

الف) محرمانگی پیشرو[3]: شرایطی را تصور کنید که در آن، کلید خصوصی سرویس‌دهنده سرقت شود. محرمانگی پیشرو به ما این اطمینان را می‌دهد که حتی اگر کلید خصوصی سرویس‌دهنده تصادفاً فاش یا سرقت شود، کلمات عبور پیشین که در سیستم مورد استفاده قرار گرفته‌اند، همچنان امن خواهند ماند.

ب) عدم ذخیره جدول کلمات عبور: پروتکل باید طوری طراحی شود که در سرویس‌دهنده، جدول کلمات عبور و یا هرگونه جدول و اطلاعات مخفی دیگر هم که مهاجم از روی آن بتواند کاربران مجاز را شناسایی کند، ذخیره نشده باشد. ذخیره شدن جدول کلمات عبور نه تنها باعث بروز حملاتی همچون حمله سرقت جدول شناسایی می‌شود، بلکه هزینه نگهداری و محافظت از جدول و اطلاعات ذخیره شده در سرویس‌دهنده را نیز به دنبال خواهد داشت.

ج) عدم ارسال آشکار کلمه عبور: کاملاً بدیهی است که اگر کلمه عبور به صورت خوانا روی کانال ارسال گردد، مهاجم کار ساده‌ای پیش رو خواهد داشت؛ زیرا مهاجم بر روی کانال ارتباطی تسلط کامل دارد و هرگونه پیامی را شنود می‌کند و از این طریق به‌راحتی کلمه عبور را به دست خواهد آورد. بنابراین به‌دلیل اهمیت زیاد کلمه عبور در پروتکل‌های مبتنی بر کلمه عبور، اکیداً توصیه می‌شود که کلمه عبور روی کانال ارسال نگردد و در صورت لزوم حتی‌الامکان به صورت رمز شده ارسال شود.

د) مقاومت در برابر حملات متداول: یکی از مهم‌ترین مراحلی که یک طراح پروتکل پس از طراحی آن باید انجام دهد، بررسی مقاومت آن در برابر انواع حملات متداول (که در بخش ۴ آمده است) می‌باشد. همچنین او می‌تواند به استناد خواصی که در پروتکل خود به کار برده است، نشان دهد که طرحش در مقابل این حملات ایمن است.

ملزومات غیراکید

الف) شناسه پویا[4]: یکی از مواردی که باعث ارتقاء امنیت طرح می‌شود، استفاده از شناسه پویا در پروتکل می‌باشد؛ به‌گونه‌ای که در هر بار ورود کاربر، شناسه ارسال شده روی کانال تغییر کند. زیرا در غیر این صورت ممکن است، شناسه ثابت باعث نشت اطلاعات جزئی در رابطه با پیام ورودی کاربر شود.

ب) انتخاب کلمه عبور به‌صورت دلخواه توسط کاربر: هنگامی که کلمه عبور توسط خود کاربر انتخاب شود و در کانال امن برای سرویس‌دهنده ارسال گردد و کلمه عبور نیز در سرویس‌دهنده ذخیره نشود، طرح از امنیت بیشتری برخوردار خواهد بود؛ زیرا هنگامی که کلمه عبور توسط سرویس‌دهنده تعیین شود حتی اگر به طور مستقیم نیز در سرویس‌دهنده ذخیره نشده باشد، از آن‌جایی که نحوه محاسبه کلمه عبور در سرویس‌دهنده موجود است، احتمال آشکار شدن کلمه عبور برای مسئولین سرویس‌دهنده وجود خواهد داشت.

ج) خصوصیات بیومتریک[5]: یکی از امکانات جانبی دیگری که می‌تواند باعث افزایش امنیت پروتکل گردد، استفاده از خصوصیات منحصر به‌فرد در انسان‌ها نظیر اثرانگشت درون پروتکل می‌باشد.

۲-۲- ملزومات کارآیی

ملزومات اکید

الف) قابلیت تغییر کلمه عبور: پروتکل باید به‌گونه‌ای طراحی شود که کاربر قادر باشد در هر زمان که لازم باشد و به صورت کاملاً دلخواه، کلمه عبورش را تغییر دهد. البته این مرحله باید به‌گونه‌ای امن اجرا شود یعنی نباید کلمه عبور جدید کاربر روی کانال برای سرویس‌دهنده ارسال گردد. در مرحله تغییر کلمه عبور امن، ابتدا کاربر با کلمه عبور خود با سرویس‌دهنده ارتباط برقرار کرده و تمامی مراحل پروتکل را اجرا می‌کند و ثابت می‌کند که کاربر مجاز است، سپس درخواست تغییر کلمه عبور خود را برای سرویس‌دهنده ارسال کرده و به دنبال آن، کلمه عبور پیشنهادی خود را وارد می‌کند. از

1- Tsai
2- Madhudsaan
3- Forward Secrecy
4- Dynamic ID
5- Biometric

این جا به بعد، هیچ پیامی برای سرویس‌دهنده ارسال نمی‌گردد، بلکه با استفاده از کلمه عبور جدید، پارامترهای موجود در کارت تغییر کرده و جایگزین مقادیر قبلی در کارت می‌شود و از این به بعد کاربر می‌تواند با کلمه عبور جدید خود احراز اصالت شود.

ب) قابلیت پیاده‌سازی: یکی از مهم‌ترین مسائلی که همواره باید مورد نظر طراح باشد، کاربردی بودن پروتکل است؛ یعنی نه تنها امنیت باید یکی از دغدغه‌های طراح باشد بلکه حجم محاسبات پروتکل باید طوری باشد که اولا زمان زیادی را صرف نکند، ثانیا ویژگی‌های محاسباتی کارت هوشمند از قبیل محدودیت حافظه و محدودیت سرعت پردازشگر نیز در پروتکل لحاظ شده باشد.

ملزومات غیر اکید

توافق کلید نشست[1]: کاربر و سرویس‌دهنده، باید قادر باشند بعد از به اتمام رساندن موفقیت‌آمیز مراحل احراز اصالت، با توافق کلید نشست، یک کانال ارتباطی امن برای انتقال اطلاعات ایجاد کنند. البته این مرحله نقشی، در امنیت مراحل احراز اصالت ندارد اما وجود آن در اغلب پروتکل‌های ارتباطی متداول است.

۳- پروتکل احراز اصالت پیشنهادی

به‌منظور ارتقاء سطح امنیت پروتکل‌های احراز اصالت مبتنی بر کلمه عبور، در این بخش می‌خواهیم یک پروتکل جدید را پیشنهاد کنیم. کلیه نمادهای به‌کار رفته در این پروتکل در جدول (۱) آمده است. پروتکل پیشنهادی شامل پنج مرحله اصلی زیر می‌باشد (شکل ۱). لازم به ذکر است اندازه پارامترهای به‌کار رفته - متناسب با سخت‌افزار و کاربرد آن - قابل تغییر می‌باشند و معمولا به آن اشاره نمی‌شود.

۳-۱- مرحله اولیه

در این مرحله، سرویس‌دهنده بعد از انتخاب p و q، تابع چکیده‌ساز h(.) را انتخاب می‌کند. سپس $x_s \in z_q^*$ را به‌عنوان کلید خصوصی انتخاب کرده و نزد خود به صورت مخفی نگه می‌دارد.

۳-۲- مرحله ثبت

در این مرحله، کاربر شناسه (ID) و کلمه عبور (PW) را تعیین می‌کند و روی یک کانال امن برای سرویس‌دهنده ارسال می‌کند. بعد از آن که سرویس‌دهنده، پیام درخواست $\{ ID, PW \}$را دریافت کرد، ابتدا زمان T_R را به‌عنوان زمان ثبت درخواست کاربر انتخاب می‌کند (T_R رمز می‌شود و به صورت مخفی نزد سرویس‌دهنده باقی می‌ماند). سپس سرویس‌دهنده پارامتر A را به صورت زیر محاسبه می‌کند:

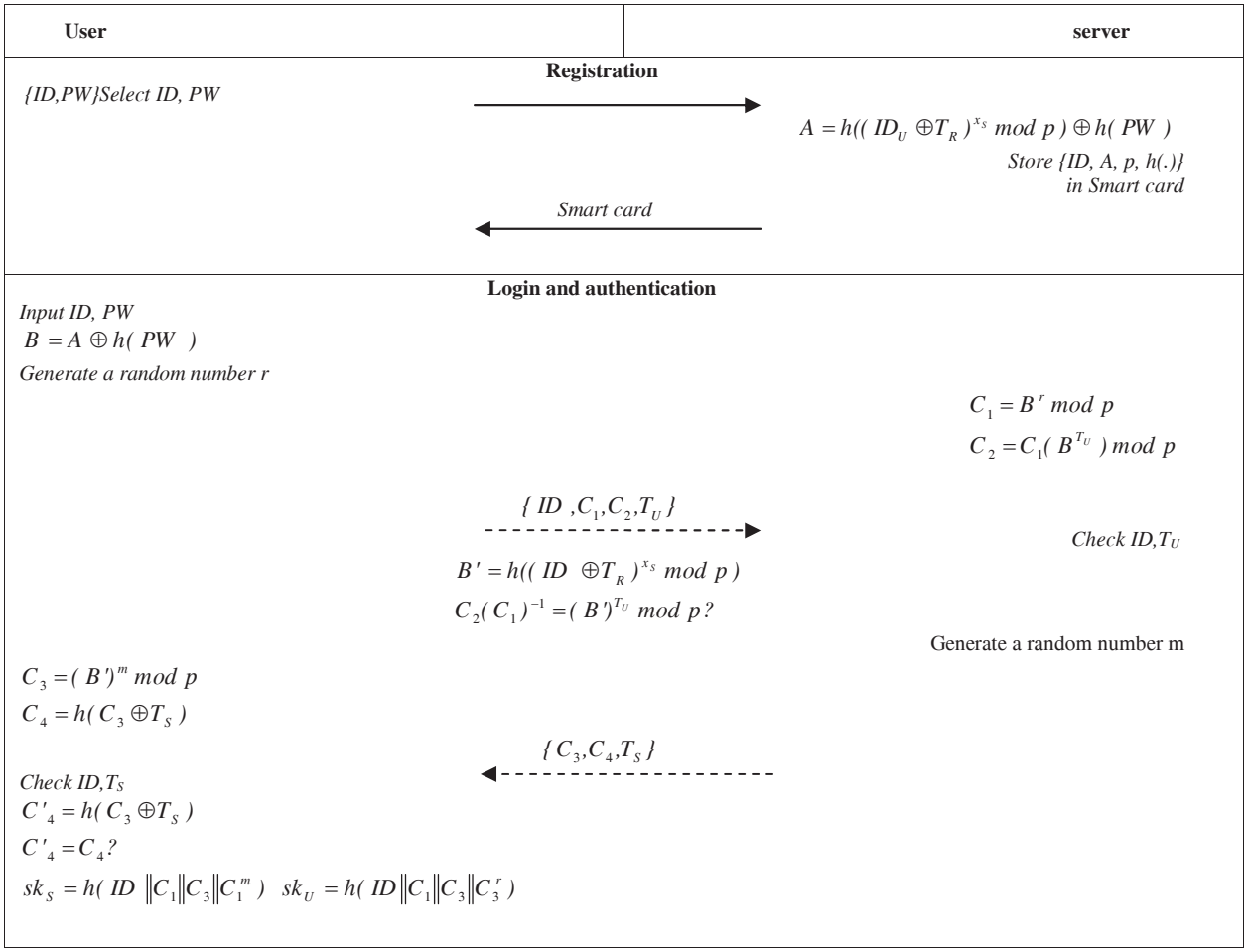
$$A = h((ID \oplus T_R)^{x_S} \bmod p) \oplus h(PW)$$

سپس پارامترهای$\{ID, A, p, h(.)\}$ را در کارت ذخیره کرده و آن را در کانال امن به کاربر تحویل می‌دهد.

جدول ۱- نمادها و اختصارات

ID	شناسه کاربر
PW	کلمه عبور کاربر
p,q	اعداد اول بزرگ که p=2q+1
h(.)	تابع چکیده‌ساز
x_S	کلید خصوصی سرویس‌دهنده
r, m	اعداد تصادفی
T_R	زمان ثبت اطلاعات کاربر در سرویس‌دهنده
T_S	مهر زمانی سرویس‌دهنده
T_U	مهر زمانی کاربر
sk_S	کلید نشست سرویس‌دهنده
sk_U	کلید نشست کاربر
T_h	زمان لازم برای محاسبه تابع چکیده‌ساز
T_{ME}	زمان لازم برای محاسبه تابع نمایی
$\oplus$	عمل جمع انحصاری
||	الحاق
⟶	کانال امن
- -▶	کانال ناامن

1- Sesssion key Agrement



شکل ۱- پروتکل پیشنهادی

۳-۳- مرحله ورود

در این مرحله، کاربر کارت را وارد کارت‌خوان کرده و سپس ID وPW را وارد می‌کند. کارت هوشمند مقدار $B = A \oplus h(PW)$ را محاسبه می‌کند، عدد تصادفی r را تولید کرده و زمان T_U را به‌عنوان مهر زمانی انتخاب می‌کند. سپس محاسبات زیر را انجام می‌دهد:

$$C_1 = B^r \bmod p$$
$$C_2 = C_1(B^{T_U}) \bmod p$$

و سپس پیام ورودی $\{ID, C_1, C_2, T_U\}$ را برای سرویس‌دهنده ارسال می‌کند.

۳-۴- مرحله احراز اصالت

این مرحله شامل دو بخش احراز اصالت کاربر و احراز اصالت سرویس‌دهنده است.

۳-۴-۱- احراز اصالت کاربر

هنگامی که سرویس‌دهنده پیام ورودی را در زمان T^* دریافت می‌کند، ابتدا اعتبار ID را بررسی می‌کند. سپس با استفاده از مقدار ثابت و معین ΔT که از قبل تعیین کرده است اعتبار T_U را با نامساوی $T^* - T_U \le \Delta T$ بررسی می‌کند. اگر شناسه و مهر زمانی معتبر بود مراحل احراز اصالت ادامه پیدا می‌کند و در غیر این صورت، ارتباط قطع می‌شود. در ادامه، سرویس‌دهنده مقدار پارامتر $B' = h((ID \oplus T_R)^{x_S} \bmod p)$ را محاسبه کرده و درستی $C_2(C_1)^{-1} = B'^{T_U} \bmod p$ را بررسی می‌کند. در صورت درستی این تساوی، سرویس‌دهنده یک عدد تصادفی m را انتخاب کرده و پارامتر $C_3 = B'^m \bmod p$ را محاسبه می‌کند. در انتها، سرویس‌دهنده T_S را به‌عنوان مهر زمانی انتخاب کرده و پارامتر $C_4 = h(C_3 \oplus T_S)$ را محاسبه و پیام $\{C_4, C_3, T_S\}$ را برای کاربر ارسال می‌کند.

۳-۴-۲- احراز اصالت سرویس‌دهنده

کاربر پس از دریافت پیام سرویس‌دهنده، ابتدا اعتبار T_S را بررسی کرده و پارامتر $C_4' = h(C_3 \oplus T_S)$ را محاسبه می‌کند. اگر تساوی $C_4' = C_4$ برقرار باشد، سرویس‌دهنده نیز با موفقیت احراز اصالت شده است.

۳-۵- استقرار کلید نشست

کاربر و سرویس‌دهنده با استفاده از اطلاعات دریافتی، به‌طور مشترک و جداگانه کلید نشست مخفی را به صورت زیر محاسبه می‌کنند:

$$sk_U = h(ID \| C_1 \| C_3 \| C_3^r)$$
$$sk_S = h(ID \| C_1 \| C_3 \| C_1^m)$$

از آن‌جایی که تساوی $C_3^r = C_1^m$ برقرار است، بنابراین تساوی $sk_U = sk_S$ نیز برقرار می‌شود.

۳-۶- تغییر کلمه عبور

در پروتکل پیشنهادی، پس از اولین احراز اصالت، کاربر می‌تواند کلمه عبور خود را تغییر دهد. برای این کار او باید مراحل احراز اصالت را با موفقیت طی کرده و سپس درخواست تغییر کلمه عبور را ارسال کند. با دریافت این درخواست، کارت هوشمند، کلمه عبور جدید PW' را از کاربر می‌گیرد و پارامتر A' را به صورت زیر محاسبه کرده و آن را جایگزین A در کارت هوشمند می‌کند.

$$A' = A \oplus h(PW) \oplus h(PW')$$

۴-تحلیل پروتکل پیشنهادی

در این بخش، انواع حملات متداول روی پروتکل پیشنهادی را مورد بررسی قرار می‌دهیم.

۴-۱- حمله جعل هویت

در این حمله مهاجم سعی می‌کند خود را به نحوی به جای کاربر مجاز جا بزند. روش‌های گوناگونی وجود دارند که یک مهاجم را قادر می‌سازند تا روی یک پروتکل، حمله جعل هویت را انجام دهد. در حمله جعل هویت، مهاجم با اطلاعاتی که از شنود ارتباط میان سرویس‌دهنده و کاربر به‌دست می‌آورد و یا به کمک تغییراتی که در پیام‌های ردوبدل‌شده در نشست‌های قبلی می‌دهد، قادر می‌شود خود را به جای یک کاربر مجاز به سرویس‌دهنده معرفی نماید. در پروتکل پیشنهادی تصور کنید مهاجم پیام $\{ID, C_1, C_2, T_U\}$ را روی کانال دریافت کند و قصد دارد با استفاده از آن یک پیام ورودی معتبر تولید کرده و خود را به جای کاربر مجاز جا بزند. در این صورت مهاجم برای موفق شدن باید B را بداند. برای محاسبه B او باید ضمن حدس r از رابطه $C_1 = B^r \bmod p$، یک مسئله لگاریتم گسسته را حل کند.

۴-۲- حمله حدس زدن کلمه عبور

این حمله به دو شکل برون‌خط و برخط قابل اجرا است.

۴-۲-۱- حمله حدس زدن کلمه عبور برون‌خط

در این حمله، مهاجم مابین ارتباط بین کاربر و سرویس‌دهنده قرار می‌گیرد و پیام‌های مبادله‌شده را در جایی ذخیره می‌کند. سپس درستی حدس‌های خود را با استفاده از پیام‌هایی که به‌دست آورده است، مورد بررسی قرار می‌دهد. البته در حالتی که مهاجم کارت هوشمند را نیز در دسترس داشته باشد، می‌تواند از اطلاعاتی که از کارت استخراج می‌کند نیز استفاده کند تا درستی حدس‌های خود را مورد بررسی قرار دهد. در پروتکل پیشنهادی، کلمه عبور روی کانال ارسال نشده است؛ بنابراین پروتکل در مقابل این حمله مقاوم است.

۴-۲-۲- حمله حدس زدن کلمه عبور برخط

اکثر کاربران از کلمات عبور قابل پیش‌بینی مانند سال تولد و شماره شناسنامه استفاده می‌کنند که متاسفانه باعث پیاده‌سازی این حمله می‌شود. به این صورت که مهاجم کارت هوشمند کاربر را سرقت کرده و سپس لیستی از کلمات عبور محتمل تهیه می‌کند و مانند کاربر با استفاده از حدس‌های خود سعی می‌کند وارد سیستم شود. برای جلوگیری از این حمله باید تعداد دفعاتی که کاربر می‌تواند کلمه عبور غلط وارد کند، محدود شود؛ مثلاً بعد از اینکه سه بار کلمه عبور به اشتباه وارد شد (عمداً یا سهواً) کارت‌خوان کارت را به کاربر باز نگرداند و در نتیجه، شانس مهاجم در موفق شدن بسیار کمتر خواهد شد.

۴-۳- حمله نشست موازی

پیاده‌سازی حمله نشست موازی مهاجم بدون هیچ‌گونه اطلاعی از کلمه عبور در میان ارتباط بین سرویس‌دهنده و کاربر قرار می‌گیرد. مهاجم قادر است اطلاعات ردوبدل شده بین طرفین را مشاهده کند و تغییرات مورد نظر خود را در آن‌ها ایجاد کند؛ سپس یک پیام معتبر تولید کرده و برای سرویس‌دهنده ارسال کند. البته مهاجم در طراحی پیام‌ها باید به‌گونه‌ای عمل کند که طرف مقابلش پی به هویت واقعی او نبرد. از آن‌جایی که در پروتکل پیشنهادی از اعداد تصادفی و مهر زمانی استفاده می‌شود، این حمله کارساز نخواهد بود.

۴-۴- حمله تکرار

از این حمله معمولا برای جعل هویت یکی از طرفین پروتکل استفاده می‌شود. به این صورت که مهاجم پیام‌های ردوبدل شده در چندین نشست قبلی را شنود می‌کند و سپس در زمانی دیگر نشستی را با سرویس‌دهنده آغاز کرده و از پیام‌های معتبری که قبلا به دست آورده است به‌عنوان پاسخ استفاده می‌کند. در پروتکل پیشنهادی، مهاجم از هیچ‌یک از پیام‌های قبلی نمی‌تواند استفاده کند؛ زیرا در پیام مربوط به درخواست ورود از مهر زمانی استفاده شده است و بعد از بازه زمانی از قبل مشخص‌شده ΔT، دیگر پیام‌های قبلی اعتبار ندارند.

۴-۵- حمله جعل هویت سرویس‌دهنده

این حمله دقیقاً مشابه حمله جعل هویت پیاده‌سازی می‌گردد، با این تفاوت که هدف مهاجم در این حمله، آن است که خود را به جای سرویس‌دهنده جا بزند و از این طریق اطلاعات مفیدی از کاربر به‌دست آورد و با سوء استفاده از آنها وارد نشست‌های بعدی بشود. تنها راه جلوگیری از حمله جعل هویت سرویس‌دهنده، برقراری احراز اصالت دو سویه می‌باشد. به این ترتیب، کاربر هم از هویت سرویس‌دهنده اطمینان پیدا خواهد کرد. در پروتکل پیشنهادی بعد از آن‌که کاربر توسط سرویس‌دهنده احراز اصالت شد، سرویس‌دهنده و پیام $\{ID, C_4, C_3, T_S\}$ را برای کاربر ارسال می‌کند تا کاربر هم سرویس‌دهنده را احراز اصالت کند. ایجاد احراز اصالت دوسویه، طرح را در برابر حمله جعل هویت سرویس‌دهنده مقاوم می‌سازد.

جدول ۲- مقایسه پروتکل پیشنهادی با شش پروتکل دیگر از نظر رعایت ملزومات امنیتی و کارآیی

	پروتکل پیشنهادی	[۱۰]	[۱۳]	[۲۳]	[۱۷]	[۷]	[۲]
محرمانگی پیشرو	بله	بله	بله	خیر	خیر	بله	بله
عدم ذخیره جدول کلمات عبور	بله	بله	بله	بله	بله	بله	بله
عدم ارسال آشکار کلمه عبور	بله	بله	بله	بله	بله	بله	بله
انتخاب کلمه عبور به صورت دلخواه توسط کاربر	بله	بله	خیر	بله	بله	خیر	خیر
قابلیت تغییر کلمه عبور	بله	بله	خیر	بله	بله	خیر	خیر
قابلیت پیاده‌سازی	بله	بله	بله	بله	بله	بله	بله
توافق کلید نشست	بله	خیر	خیر	خیر	خیر	خیر	خیر
شناسه پویا	خیر	خیر	خیر	خیر	خیر	خیر	خیر
خصوصیات بیومتریک	خیر	بله	خیر	خیر	خیر	خیر	خیر

جدول ۳- مقایسه پروتکل پیشنهادی با شش پروتکل دیگر از نظر مقاومت در برابر حملات متداول

	پروتکل پیشنهادی	[۱۰]	[۱۳]	[۲۳]	[۱۷]	[۷]	[۲]
حمله جعل هویت	√	√	√	×	×	√	√
حمله حدس زدن کلمه عبور	√	√	√	√	√	√	√
حمله نشست موازی	√	√	√	√	×	√	√
حمله تکرار	√	×	√	√	√	√	√
حمله جعل هویت سرویس‌دهنده	√	√	√	√	×	×	×
حمله سرقت کارت هوشمند	√	√	√	×	√	√	√
حمله سرقت جدول شناسایی	√	√	×	√	×	√	√
حمله منع خدمت	√	×	√	√	√	√	√

√: مقاوم، ×: آسیب‌پذیر

جدول ۴- مقایسه پروتکل پیشنهادی با شش پروتکل دیگر از نظر پیچیدگی محاسباتی

	مرحله ورود	مرحله احراز اصالت
پروتکل پیشنهادی	$2T_{ME}+T_h$	$3T_{ME}+2T_h$
پروتکل لی [۱۰]	$2T_h$	$5T_h$
پروتکل یه [۲۳]	$4T_h$	$5T_h$
پروتکل سود [۱۷]	$7T_h$	$5T_h$
پروتکل راماسامی[۱۳]	$3T_{ME}+T_h$	$3T_{ME}+T_h$
پروتکل کومار [۷]	$3T_{ME}+T_h$	$3T_{ME}+T_h$
پروتکل آواستهی [۲]	$3T_{ME}+T_h$	$3T_{ME}+T_h$

۴-۶- حمله سرقت کارت هوشمند

در این حمله، فرض اولیه بر آن است که مهاجم توانسته است کارت هوشمند را سرقت کند، لذا او می‌تواند تمامی پارامترهای ذخیره‌شده در کارت را به کمک حملات فیزیکی استخراج کند و سپس با استفاده از آن‌ها به طریقی حمله حدس کلمه عبور را پیاده‌سازی کند و یا این‌که با استفاده از پارامترهایی که به‌دست آورده است، یک پیام ورودی معتبر تولید کرده و حمله جعل هویت را پیاده‌سازی کند. البته در حالتی که مهاجم از قبل پیام‌های ردوبدل‌شده روی کانال را شنود کرده باشد می‌تواند از آن‌ها نیز در حدس زدن کلمه عبور و یا ساخت یک پیام معتبر استفاده کند. در پروتکل پیشنهادی اگر مهاجم پس از سرقت کارت هوشمند، اطلاعات ذخیره شده در آن را استخراج کند، نباید قادر به حدس کلمه عبور باشد؛ چون مهاجم در پروتکل پیشنهادی با استخراج پارامتر B از کارت هوشمند نیاز به حل مسئله لگاریتم گسسته و پیدا کردن تصادم دارد. بنابراین، پیاده‌سازی این حمله برای مهاجم کار سختی است.

۴-۷- حمله سرقت جدول شناسایی

در این حمله ،مهاجم با سرقت جدول شناسایی (همان چکیده کلمات عبور) از سرویس‌دهنده سعی در جعل هویت کاربر مجاز خواهد داشت. بنابراین اساس این حمله، ذخیره کلمه عبور توسط سرویس‌دهنده است. از آن‌جایی که هیچ‌گونه جدول شناسایی یا کلمات عبور در سرویس‌دهنده ذخیره نشده است، پیاده‌سازی این حمله برای مهاجم امکان‌پذیر نیست.

۴-۸- حمله منع خدمت

در این حمله، مهاجم اطلاعات شناسایی غلط یک کاربر مجاز را به‌روزرسانی می‌کند و با استفاده از آنها پیام ورود معتبر تولید می‌کند. بعد از آن دیگر کاربر مجاز، قادر به ورود موفقیت‌آمیز نخواهد بود. در پروتکل پیشنهادی، هر پیام ورودی شامل مهر زمانی T_U است که در تولید پارامتر C_2 به کار رفته است. بنابراین مهاجم نمی‌تواند اطلاعات قبلی را برای ورود به سیستم مورد سوء استفاده قرار دهد.

۵- مقایسه امنیت و کارآیی پروتکل پیشنهادی

نتایج مقایسه‌های انجام شده با شش پروتکل دیگر از نظر ملزومات امنیتی، مقاومت در برابر حملات متداول و پیچیدگی محاسباتی، در جداول (۲-۴) ارائه شده است. نتاج ارائه شده در جداول (۲) و (۳) نشان می‌دهد که در طراحی پروتکل پیشنهادی، تمامی ملزومات امنیتی در نظر گرفته شده است. در نتیجه، پروتکل جدید در برابر حملات متداول مقاوم است و در مقایسه با پروتکل‌های دیگر، امنیت بیشتری دارد. از نظر پیچیدگی‌های محاسباتی نیز با $2T_{ME}+T_h$ زمان محاسبه در مرحله ورود و $3T_{ME}+2T_h$ زمان محاسبه در مرحله احراز اصالت نیز در وضعیت مطلوبی قرار دارد. البته پروتکل جدید نسبت به پروتکل لی [۱۰]، یه[1] [۲۳] و سود[2] [۱۷] به‌دلیل استفاده از تابع‌نمایی سرعت کمتری دارد اما بر اساس جداول (۲) و (۳) سطح امنیت بسیار بالاتر از آن‌ها است.

۶- نتیجه‌گیری

در حوزه فناوری‌های ارتباطات و اطلاعات، نقش دولت الکترونیک و پدافند غیر عامل در تامین امنیت اطلاعات و در پیشگیری از دسترسی‌های غیر مجاز، اهمیتی غیر قابل انکار دارد. در این خصوص، پروتکل‌های احراز اصالت، نقش مهمی در تأمین امنیت شبکه‌های الکترونیکی ایفا می‌کنند. در این مقاله پس از مرور و دسته‌بندی ملزومات اکید و غیر اکید امنیتی و کارآیی پروتکل‌های احراز اصالت مبتنی بر کلمه عبور با کارت هوشمند، یک پروتکل جدید پیشنهاد شد. همچنین نشان دادیم که پروتکل پیشنهادی در مقابل اکثر حملات متداول مقاوم است. در انتها نیز پروتکل پیشنهادی با شش پروتکل مشابه دیگر از نظر امنیت، کارآیی و پیچیدگی محاسباتی مورد مقایسه قرار گرفت. نتایج به‌دست آمده نشان می‌دهند در هر سه معیار نامبرده، پروتکل پیشنهادی برتری آشکاری دارد.

مراجع

۱. یزدان‌پناه، محمود؛ خادم، بهروز. شبیه‌سازی و پیاده‌سازی یک رمز جریانی خودهمزمان بومی (CPSA3) جهت تأمین امنیت داده‌ها در شبکه‌های الکترونیکی کشور؛ فصلنامه علمی- ترویجی پدافند غیرعامل، سال دوم، شماره ۴، صص ۱۹-۲۳، (**۱۳۹۰**).

2. A. K. Awasthi and S. Lal, A remote user authentication scheme using smart cards with forward secrecy, IEEE Transactions on Consumer electronics, Vol. 49, No. 4, PP.1246-1248, (**2003**).
3. M. Bayat, M. Sabzinejad and S. Movahed, A novel secure bilinear pairing based remote authentication scheme with smart card, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, (**2010**).
4. T. H. Chen, H. C. Hsiang and W. K. Shih, Security enhancement on an improvement on two remote user authentication schemes using smart cards, Future Generation Computer Systems, Vol. 27, No.4, PP.377-380, (**2011**).
5. M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on consumer Electronics, Vol. 46, PP.28-30, (**2000**).

1- Yeh
2- Sood

6. W. C. Ku, S. M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron, Vol. 50, PP.204-207, (**2004**)
7. M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer electronics, Vol. 50, No. 2, PP.597-600, (2004).
8. L. Lamport, Password authentication with insecure communication, Commun.ACM, Vol. 24, No. 11, PP.770-772, (**1981**).
9. N. Y. Lee, Y. C. Chiu, Improved remote authentication scheme with smart cards, Computer standards & Interfaces, Vol. 27, No. 8, PP. 177-180, (**2005**).
10. C. T. Li, M. S. Hwang, An efficient biometrics based remote user authentication scheme using smart cards, Computer standards & Interfaces, Vol. 27, PP.1-5, (**2010**).
11. R. Madhusudhan and R.C.Mittal, Dynamic ID-based remote user password authentication schemes using smart cards: A review, Journal of Network and Computer Applications, Vol. 35, PP.1235-1248, (**2012**).
12. W. Rankl," Smart card applications: Design models for using and programming smrt cards", (**2007**).
13. R. Ramasamy A.P. Muniyandi, New remote mutual authentication scheme using smart cards, Transactions on data privacy, Vol. 2, PP.141-152, (**2009**).
14. R. Ramasamy A.P. Muniyandi, An efficient password authentication scheme for smartcard, International journal of Network Security, Vol. 14, PP.180-186, (**2012**).
15. J. J. Shen, C. W. Lin and M. S. Hwang, A modified remote user authentication scheme using smartcard, IEEE Transactions on Consumer electronics, Vol. 49, PP.414-416, (**2003**).
16. R. Song, Advanced smart card based password authentication protocol, Computer standards & Interfaces, Vol. 32, PP.321-325, (**2010**).
17. S. K. Sood, A.K. Sarjee and K. Singh, An improvement of Liao et al.'s authentication scheme using smart card, IEEE 2 nd International Advance Computing Conference (IACC 2010), PP.240-245, (**2010**).
18. R. Stinson, "Cryptography theory and practice", CRC Press, Third edition, (**2006**).
19. C. S. Tsai, C. C. Lee, M. S. Hwang, Password authentication schemes: Current Status and Key Issues, International journal of Network Security, Vol. 3, No. 2, PP.101-115, (**2006**).
20. X. M. Wang, W.F. Zhang, J. S. Zhang, Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer standards & Interfaces, Vol. 29, PP.507-512, (**2006**).
21. J. Xu, W. T. Zhu, D. G. Feng, An improved smart card password authentication scheme with provable security, Computer standards & Interfaces, Vol. 31, No.4, PP.723-728, (**2009**).
22. C. C. Yang, R. C. Wang and T. Y. Chang, An improvement of the Yang-Shieh password authentication schemes, Applied Mathematics and Computation, Vol. 162, PP.1391-1396, (**2005**).
23. K. H. Yeh, C. Su, N. W Lo, Y. Li, Y. X. Hung, Two robust remote user authentication protocols using smart cards, The Journal of Systems and Software, Vol. 83, No.12, PP.2556-2565, (**2010**).
24. E. J. Yoon, E. K. Ryu, and K. Y. Yoo, Further Improvement of an Efficient password based Remote Authentication Scheme using smart cards, IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 612–614, (**2004**).
25. H. Zhang, M. Li, Security vulnerabilities of an remote password authentication scheme with smart card, IEEE International on Communications and Networks , PP.698-701, (**2011**).

A Mutual Authentication Protocol with Smart Cards

R. Kazemi Ashtyani[1]

B. Khadem[2]

Abstract

One of the main development criteria in each country is the growth of national or sub-national electronic systems of management and control. Preserving information security and trust in un-trusted access to such networks, is one of the main purposes of passive defense. One of the most common samples of such networks is E-banking where providing the user's information security is a very essential goal. Since the authentication protocols are crucial in any electronic system, they perform a very important role in providing secure communication. In this paper, while introducing a password-based mutual authentication protocol, we will demonstrate that such a protocol is applicable in smart card technology. Also we will show that the proposed scheme regarding resistance to common attacks, has better behavior in the view of both security and performance requirements

Key Words: *Authentication Protocol, Smart Card, Password*

1- Imam Hosein University-Faculty of Communication and Information Technology - Writer in Charge (kazemiashtyani@gmail.com)
2- Imam Hossein University-Faculty of Communication and Information Technology- Instructor and Academic Member