مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۳، پاییز ۱۳۹۴، ص ۴۸- ۳۹

ضعف‌های پروتکل احرازهویت SPRS و ارائه یک پروتکل بهبودیافته برای سامانه‌های RFID

محمد مردانی شهربابک[1*]، بهزاد عبدالملکی[2]، کریم باقری[2]
۱- استادیار، دانشگاه جامع امام حسین(ع)
۲ و ۳- کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه شاهد
(دریافت: ۹۳/۰۹/۱۱، پذیرش: ۹۴/۱۰/۲۲)

چکیده

در سال‌های اخیر حفظ امنیت سایبری تبدیل به یکی از اهداف اصلی سازمان‌های نظامی شده است. از سوی دیگر شناسایی و احراز هویت نیروها و حفظ امنیت آنها تبدیل به یکی از نیازهای اساسی سازمان‌های نظامی شده است. هرچند رمزنگاری داده‌ها از دسترسی کاربر به محتویات داده‌ها جلوگیری می‌کند، ولی مهاجم با نفوذ به کانال‌های ارتباطی انتقال اطلاعات می‌تواند داده‌ها را جعل کند. ازاین‌رو، ارائه پروتکل‌های امن جهت جلوگیری از این نوع حملات و یا همان پدافند غیرعامل در سیستم‌های احرازهویت از اهمیت فراوانی برخوردار است. در این مقاله، به تحلیل امنیتی یک پروتکل احراز هویت (SPRS) سامانه‌های RFID که در سال ۲۰۱۳ ارایه شده است، می‌پردازیم. نشان می‌دهیم بر خلاف ادعای طراحان آن همچنان ضعف‌هایی بر این پروتکل وارد است و در مقابل حمله‌های کشف کلیدهای مخفی، جعل هویت برچسب و ردیابی برچسب مقاوم نمی‌باشد. در ادامه، به منظور افزایش امنیت پروتکل SPRS نسخه بهبودیافته از آن ارائه شده است که ضعف‌های پروتکل SPRS درآن حذف شده است. همچنین، امنیت و محرمانگی پروتکل بهبودیافته با برخی از پروتکل‌های احراز هویت دوسویه که اخیرا پیشنهاد شده مقایسه شده است. . در ادامه پیچیدگی و عملکرد پروتکل پیشنهادی با پروتکل های ارایه‌شده و موجود در این زمینه مقایسه گردیده و مشاهده می‌شود که با کمترین تغییرات در پیچیدگی پروتکل تحلیل‌شده، ضعف‌های امنیتی و محرمانگی آن به‌طور کامل برطرف می‌شود.

واژه‌های کلیدی: امنیت سامانه‌های RFID، پروتکل‌های احراز هویت سامانه‌های RFID، امنیت و محرمانگی، مدل اوفی- فان

۱- مقدمه

در سازمان‌های نظامی، شناسایی و احراز هویت درست نیروهای نظامی از اهمیت بالایی برخوردار است. زیرا که اگر فرد ناشناسی وارد این سازمان‌ها شود، امنیت و محرمانگی این سازمان‌ها به خطر می‌افتد. در سال‌های اخیر، استفاده از سامانه‌های «شناسایی از طریق امواج رادیویی»[1] (RFID) رشد چشم‌گیری در این زمینه داشته است. این سامانه‌ها در سامانه‌های کنترل دست‌یابی [۱]، گذرنامه الکترونیکی [۲]، کنترل تردد [۳]، سامانه‌های ضد سرقت اتومبیل‌ها، و خیلی از موارد دیگر مورد استفاده قرار می‌گیرد [۵- ۴]. سامانه‌های RFID، قابلیت شناسایی اتوماتیک اشیا، با استفاده از یک تراشه کوچک ارزان قیمت را فراهم می‌کنند. این تراشه کوچک به اصطلاح «برچسب»[2] یا «برچسب هوشمند»[3] نامیده می‌شود. داده‌های ذخیره‌شده در این برچسب‌ها توسط دستگاه‌هایی تحت عنوان «کارت‌خوان»[4] خوانده می‌شود. در حالت کلی سامانه‌های RFID از سه بخش اصلی تشکیل شده‌اند که شامل برچسب، کارت‌خوان و «سرویس‌دهنده نهایی»[5] است. تمام اطلاعات و کلیدهای مخفی برچسب‌ها در سرویس‌دهنده نهایی ذخیره می‌شود. کارت‌خوان مابین برچسب و سرویس‌دهنده نهایی قرار می‌گیرد و وظیفه تبادل داده بین آنها را بر عهده دارد. شکل (۱) ساختار کلی از یک سامانه RFID را نمایش می‌دهد.

تاکنون استانداردهای زیادی برای سامانه‌های RFID پیشنهاد شده است. یکی از استانداردهای مهم و معتبر برای برچسب‌های فعال استاندارد «EPC C-1 G-2»[6] می‌باشد که توسط سازمان «EPCglobal»[7] ارایه شده است [۶]. در سال ۲۰۱۰ یه و همکارانش یک پروتکل احرازهویت مبتنی بر استاندارد EPC ارایه کردند [۷]. در سال ۲۰۱۲ یون و همکارانش یک تحلیل امنیتی

* رایانامه نویسنده مسئول: mmardani@ihu.ac.ir
1- Radio Frequency Identification (RFID)
2- Tag
3- Smart Tag
4- Reader
5- Back-end-server
6- EPC Class 1 Generation 2 (EPC C-1 G-2)
7- Electronic Product Code

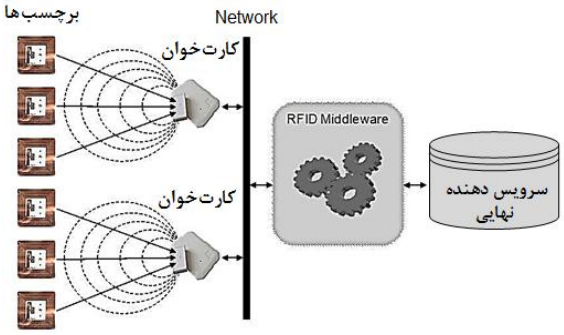
بر روی پروتکل یه و همکارانش انجام داده و نشان دادند که این پروتکل در مقابل حمله‌های ناهمزمانی و همچنین ردیابی مقاوم نسیت و سپس با اعمال تغییراتی در آن ضعف‌های آن را از بین برده و یک نسخه بهبودیافته از آن را ارایه دادند [۸]. در مارس ۲۰۱۳ فنگ خیو[1] و همکارانش پروتکل یون و همکارانش را مورد ارزیابی امنیتی و محرمانگی قرار داده و اثبات کردند که این پروتکل در مقابل حمله‌های ناهمزمانی و همچنین یکپارچگی پیام مقاومت ندارد و سپس در جهت بهبود آن «یک پروتکل احراز هویت دوسویه»[2] (SRPS) مطابق با استاندارد EPC C-1 G-2 برای سامانه‌های RFID را ارائه کردند [۹]. آنها در تحلیل امنیتی خود ادعا کرده‌اند که این پروتکل امنیت و حریم خصوصی داده‌ها را حفظ می‌کند. در این مقاله نشان می‌دهیم برخلاف ادعای طراحان این پروتکل، همچنان این پروتکل ضعف‌هایی دارد. در ادامه جهت رفع ضعف‌های پروتکل SPRS نسخه بهبود یافته‌ای از آن را ارائه می‌کنیم که ضعف‌های پروتکل SPRS در آن رفع شده است. در انتها پروتکل پیشنهادی با برخی از پروتکل‌های پیشنهادشده در سال‌های اخیر مقایسه می‌شود و نشان داده می‌شود که پروتکل پیشنهادی در مقایسه با سایر پروتکل‌ها از امنیت مناسبی برخوردار است.

در این مقاله، در بخش ۲، به بازبینی پروتکل احراز هویت SPRS پرداخته می‌شود. در ادامه در بخش ۳، تحلیل امنیتی پروتکل SPRS و ضعف‌های آن مورد بررسی قرار می‌گیرد و حملات کشف کلیدهای مخفی، جعل هویت برچسب و حمله ردیابی را بر روی آن انجام می‌شود. سپس جهت افزایش امنیت پروتکل SPRS یک پروتکل بهبود یافته از آن را پیشنهاد می‌کنیم که در بخش ۴ آورده شده است. همچنین در بخش ۴، به تحلیل امنیتی پروتکل پیشنهادی پرداخته شده است. همچنین مقایسه تحلیل امنیتی پروتکل پیشنهاد شده با چند پروتکل مشابه در فصل ۴ آورده شده است. در نهایت نتیجه‌گیری از مقاله در بخش ۵ گزارش شده است.

۲- بازبینی پروتکل SPRS

پروتکل SRPS [۹]، دارای دو مرحله می‌باشد که در شکل (۲) نمایش داده شده است. در مرحله آغازین، برچسب‌ها مقداردهی اولیه می‌شوند و مقادیر مورد نیاز و مخفی بر روی آنها ذخیره می‌شوند. در مرحله دوم، پروتکل وارد مرحله شناسایی و احراز هویت می‌شود.

1- Feng Xiao
2- Secure Protocol for RFID System (SPRS)



شکل (۱). سامانه مدل یک سامانه‌ی RFID

۲-۱- مرحله اولیه

در این مرحله اطلاعات اولیه‌ای نظیر K_0 و P_0 و C_0 به صورت تصادفی در کارخانه تولید شده و چندتایی $(K_i = K_0, P_i = P_0, C_i = C_0)$ برروی برچسب ذخیره می‌شود. همچنین متناظر با آن مقادیر چندتایی $K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = C_0$ در سرویس‌دهنده نهایی ذخیره می‌شود.

۲-۲- مرحله احراز هویت

۱) در این مرحله ابتدا کارت‌خوان عدد تصادفی N_R را تولید کرده و آن را به برچسب ارسال می‌کند.

۲) برچسب نیز بعد از دریافت پیام، عدد تصادفی N_T را تولید کرده و سپس مقادیر زیر را محاسبه می‌کند و به کارت‌خوان می‌فرستد:

$$M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i \; D = N_T \oplus K_i, \quad E = N_T \oplus PRNG(C_i \oplus K_i) \qquad (۱)$$

۳) کارت‌خوان پیام $V = H(RID \oplus N_R \oplus t)$ محاسبه می‌کند و سپس $(M_1, D, C_i, E, N_R, V, t)$ را به سرویس‌دهنده نهایی می‌فرستد.

۴) سرویس‌دهنده نهایی بعد از دریافت چندتایی $(M_1, D, C_i, E, N_R, V, t)$ از طرف کارت‌خوان مراحل زیر را انجام می‌دهد:

- اگر $T - t > \Delta t$ برقرار باشد یعنی زمان انجام عملیات سامانه بزرگ‌تر از بیشترین مقدار زمان مورد نیاز انجام عملیات موردنظر (T) بوده است، بنابراین پروتکل متوقف می‌شود. درصورتی‌که $T - t < \Delta t$ باشد آن‌گاه سرویس‌دهنده نهایی عملیات شناسایی را ادامه می‌دهد و با استفاده از RID و اطلاعات دریافتی از کارت‌خوان، مقدار $H(RID \oplus N_R \oplus t)$ را محاسبه کرده و با V دریافتی مقایسه می‌کند، درصورت برقراری تساوی هویت کارت‌خوان تایید می‌شود.

- برای هر چندتایی $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s)$ مقادیر $I_{new} = M_1 \oplus K_{new}$ و $I_{old} = M_1 \oplus K_{old}$ محاسبه می‌کند و سپس این مقادیر را با اطلاعات دریافتی به‌صورت زیر مقایسه می‌کند.

$$I_X \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \quad (۲)$$

- درصورت برقراری یکی از روابط بالا متغیر X با نام "جدید" و یا "قدیم" متناظر با کلید K_{new} و یا K_{old} که از رابطه بالا به‌دست آمد، مقداردهی می‌کند.
- بعد از تعیین X، سرویس‌دهنده نهایی پیام $N_T \oplus PRNG(C_X \oplus K_i)$ را محاسبه می‌کند و با پیام E دریافتی مقایسه می‌کند. سپس صحت آن‌را مورد بررسی قرار می‌دهد. درصورت برقراری انجام پروتکل ادامه می‌یابد در غیر این‌صورت پروتکل متوقف می‌شود
- سرویس‌دهنده نهایی، چندتایی $(M_2, Info, MAC)$ را به‌صورت زیر محاسبه و به کارت‌خوان ارسال می‌کند:

$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X,$$

$$Info = DATA \oplus RID \oplus t,$$

$$MAC = H(DATA \oplus t) \quad (۳)$$

- اگر X = new باشد، آنگاه سرویس‌دهنده نهایی مقادیر مخفی خود را به‌صورت زیر به‌روزرسانی می‌کند:

$$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new}),$$

$$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new}),$$

$$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R) \quad (۴)$$

و اگر X = old باشد عملیات به‌روزرسانی فقط برای C_i به صورت زیر انجام می‌شود:

$$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R) \quad (۵)$$

- کارت‌خوان بعد از دریافت پیام از سرویس‌دهنده نهایی، با استفاده از RID و t، مقدار DATA دریافتی را به‌صورت $DATA = Info \oplus RID \oplus t$ به‌دست می‌آورد. در ادامه مقدار $H(DATA \oplus t)$ را محاسبه کرده و با پیام MAC دریافتی از سرویس‌دهنده نهایی مقایسه می‌کند. درصورت تساوی، کارت‌خوان هویت سرویس‌دهنده نهایی را تایید و پیام M_2 دریافتی را به برچسب ارسال می‌کند.
- برچسب پیام دریافتی را با کلید مخفی ذخیره شده در خود، XOR کرده و برقراری رابطه زیر را بررسی می‌کند:

$$M_2 \oplus P_x \stackrel{?}{=} PRNG(EPC_s \oplus N_t) \quad (۶)$$

درصورت برقراری رابطه فوق برچسب هویت سرویس‌دهنده نهایی را تایید کرده و مقادیر مخفی خود را به‌صورت زیر به‌روزرسانی می‌کند:

$$K_{i+1} \leftarrow PRNG(K_i),$$

$$P_{i+1} \leftarrow PRNG(P_i)$$

$$C_{i+1} \leftarrow PRNG(N_T \oplus N_R) \quad (۷)$$

۳- تحلیل امنیتی و محرمانگی پروتکل SPRS

در این بخش نشان داده می‌شود که اداعاهای طراحان پروتکل SPRS صحیح نبوده و پروتکل دارای برخی از ضعف‌های امنیتی و محرمانگی است. در ادامه حمله‌های کشف کلیدهای مخفی، جعل هویت برچسب و حمله ردیابی در قالب مدل اوفی- فان [۱۰] بر روی این پروتکل ارائه می‌شود. لذا در ادامه، در ابتدا به اشاره مختصری به مدل اوفی- فان می‌کنیم. سپس حملات انجام‌شده را با جزییات بیشتری ارایه می‌کنیم.

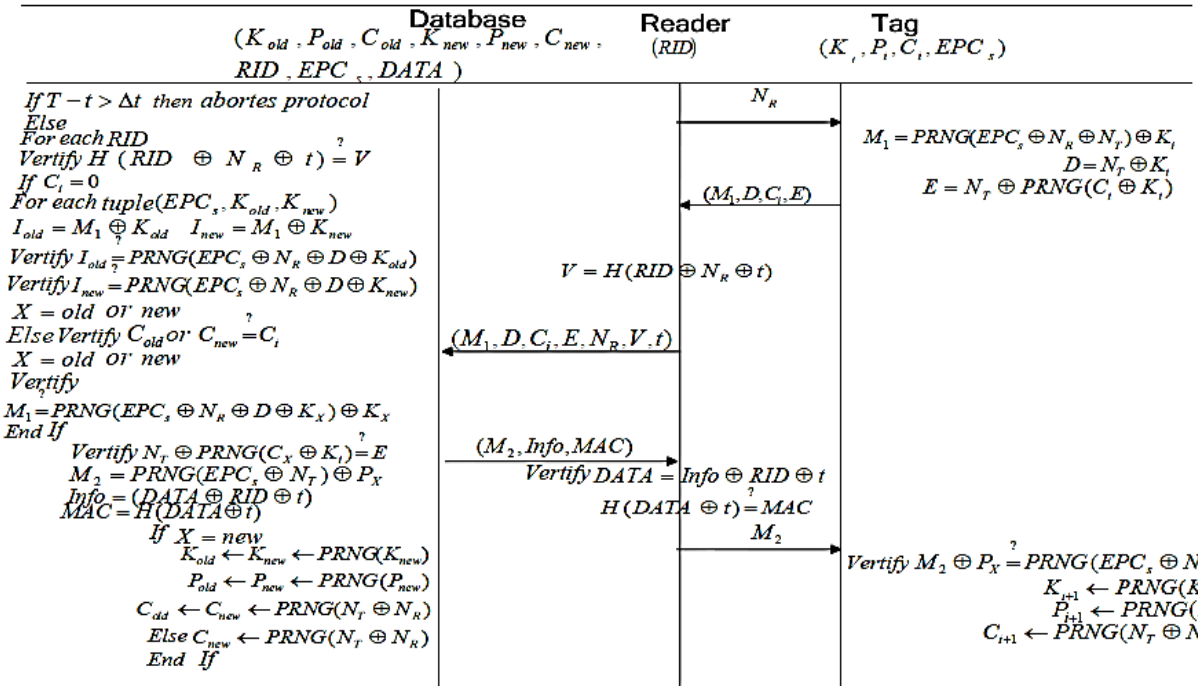
۳-۱- مدل اوفی- فان جهت ارزیابی قابلیت عدم ردیابی

مدل اوفی- فان که برای ارزیابی حمله‌های عدم ردیابی و عدم ردیابی پسرو مورد استفاده قرار می‌گیرد، به شرح زیر است [۱۰]:

در این مدل یک شریک[1] می‌تواند شامل برچسب و یا کارت‌خوان باشد. هر یک از شرکا می‌توانند فعالانه در اجرای پروتکل مشارکت کنند و پروتکل را تا پایان ادامه دهند. طرفین درگیر در پروتکل بر روی یک کانال بی‌سیم و ناامن با یکدیگر تعامل دارند که این کانال به‌طور کامل در کنترل یک مهاجم قدرتمند قرار دارد. به این مهاجم توانایی‌ها و قدرت عمل بسیاری داده می‌شود که این توانایی‌ها به طور رسمی در قالب پرسمان‌های زیر مدل می‌شوند:

- **Execute (R, T, i) query**: توسط این پرسمان به مهاجم قابلیت شنود و استراق سمع نشست‌های برگزار شده بین طرفین داده می‌شود. به بیان رسمی، هنگامی که مهاجم اقدام به ارسال Execute (R, T, i) query می‌کند، قادر می‌شود تا i-امین نشست برگزارشده بین برچسب T و کارت‌خوان R را به‌طور کامل شنود کرده و اطلاعات رد و بدل شده در آن نشست را به‌دست بیاورد. در واقع با این پرسمان مهاجم قادر است یک حمله غیرفعال[2] انجام دهد.
- **Send (U_1, U_2, i, m)query**: توسط این پرسمان به مهاجم قابلیت انجام حملات فعال داده می‌شود. به بیان رسمی، با ارسال پرسمان Send (U_1, U_2, i, m)query توسط مهاجم، به او اجاره داده می‌شود تا با جعل هویت یک کارت‌خوان $U_1 \in$ Readers (و یا برچسب $U_1 \in$ Tags)، بتواند به

1- Party
2- Passive attack



شکل (۲). پروتکل SPRS [۹].

انتخاب خودش پیام m را در نشست i-ام از پروتکل، به برچسب نمونه $U_2 \in Tags$ (و یا کارت‌خوان $U_2 \in$ Readers) ارسال کند و پاسخ او را بر طبق پروتکل دریافت کند. به علاوه توسط این پرسمان، مهاجم این قدرت را دارد تا پاسخ‌های دریافتی از طرف مقابل خود را تغییر داده و حاصل را برای طرف دیگر ارسال کند و او نیز بر طبق پروتکل به او پاسخ دهد.

- **Corrupt (T, K) query**: مهاجم با ارسال این پرسمان دارای این توانایی می‌شود تا برچسب را مخاطره[1] بیندازد و به همه‌ی مقادیر مخفی و محرمانه که بر روی او ذخیره شده است دسترسی پیدا کند. به بیان رسمی، هنگامی که مهاجم پرسمان Corrupt (T, K) query را ارسال می‌کند، در مقابل به او همه اطلاعات ذخیره‌شده روی برچسب $T \in Tags$ داده می‌شود که پارامتر K معرف تمام مقادیر مخفی ذخیره‌شده روی برچسب T است که این مقادیر شامل کلیدها، شناسه و سایر پارامترهای امنیتی برچسب T است.

تعریف حریم خصوصی غیرقابل ردیابی(UPriv[2]): مفهوم حریم خصوصی غیرقابل ردیابی (UPriv) با استفاده از بازی g تعریف می‌شود که این بازی بین مهاجم A و مجموعه‌ای از کارت‌خوان و برچسب‌های نمونه انجام می‌شود و دارای سه مرحله است. مهاجم A بازی g را به شرح زیر انجام می‌دهد.

مرحله یادگیری[3]: در این مرحله، ابتدا مهاجم به انتخاب خود، دو برچسب T_0 و T_1 را انتخاب می‌کند تا با آنها وارد تعامل شود. او می‌تواند در این مرحله هر نوع پرسمان Send و Execute را ارسال کند. به‌علاوه، هنگامی که انجام بازی g مربوط به ارزیابی مفاهیم عدم ردیابی پیشرو و پسرو باشد، مهاجم می‌تواند علاوه بر پرسمان‌های Send و Execute اقدام به ارسال Corrupt query نیز نماید.

مرحله چالش[4]: پس از مرحله یادگیری، مهاجم برچسب‌های انتخابی خود در مرحله یادگیری، یعنی T_0 و T_1 را به‌عنوان برچسب‌های منتخب خود به چالش‌گر معرفی می‌کند. سپس چالش‌گر برچسب $T_b \in \{T_0, T_1\}$ را به‌صورت تصادفی انتخاب و در اختیار مهاجم می‌گذارد. با در اختیار گذاشتن T_b، مهاجم باز هم مجاز است تا پرسمان‌های Send و Execute را به تعداد قابل قبولی ارسال کند که این تعداد بستگی به نوع پروتکل مورد آزمایش دارد.

مرحله حدس[5]: در نهایت مهاجم A، بازی را خاتمه داده و بیت $b' \in \{0,1\}$ را به‌عنوان حدس خود اعلام می‌کند. در واقع او باید اعلام کند که در مرحله چالش با کدام برچسب در ارتباط بوده است. هر چقدر که بیت b' اعلام شده از طرف مهاجم با احتمال بیشتری با بیت b یکسان باشد، میزان موفقیت مهاجم بیشتر می‌شود.

1- Compromise
2- Untraceable privacy
3- Learning phase
4- Challenge phase
5- Guess phase

میزان موفقیت مهاجم A در این بازی توسط یک تابع مزیت[1] و به‌صورت زیر تعریف می‌شود:

$$Adv_A^{upriv}(K) = |pr(b' = b) - pr(random\ coin\ flip)|$$

$$= \left|pr(b' = b) - \frac{1}{2}\right|,\ \ where\ \ \ 0 \le Adv_A^{upriv}(K) \le \frac{1}{2}$$

که $pr(random\ coin\ flip)$ نشان‌گر احتمال آن است که مهاجم بیت b' را به‌صورت تصادفی اتخاب کند و به‌دلیل توزیع یکنواخت، این احتمال برابر با $\frac{1}{2}$ است. هرچند مزیت به‌دست‌آمده برای مهاجم به $\frac{1}{2}$ نزدیک‌تر باشد، نشان‌دهنده قدرت مهاجم در تمایز قائل شدن بین T_0 و T_1 است و در نتیجه قابلیت عدم ردیابی پروتکل ضعیف‌تر خواهد بود.

۳-۲- حمله کشف کلیدهای مخفی

از ضعف‌های موجود در طراحی این پروتکل اعمال حمله کشف کلید می‌باشد به این‌صورت که مهاجم با یک بار شنود کردن اطلاعات مبادله شده بین برچسب و سرویس‌دهنده نهایی، و با استفاده از الگوریتم پیشنهادی در این قسمت، قادر به کشف همه کلیدهای مخفی به‌کار رفته در برچسب و سرویس‌دهنده نهایی خواهد بود. در ادامه به شرح کامل این حمله پرداخته می‌شود:

۱) ابتدا مهاجم با انجام یک حمله غیرفعال، نقش یک شنودگر را بازی می‌کند و پیام‌های مبادله شده بین برچسب و کارت‌خوان را دریافت کرده و ذخیره می‌کند که این پیام‌ها عبارتند از:

$$M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i,$$
$$D = N_T \oplus K_i,$$
$$E = N_T \oplus PRNG(C_i \oplus K_i)$$

۲) از آنجایی که کلید K_i یک دنباله ۱۶ بیتی می‌باشد پس $K_i \in U$ که $U = \{U_1, U_2, \dots, U_{2^{16}}\}$. حال مهاجم با اعمال الگوریتم (۱) و با استفاده از پیام‌های D و E شنودشده از قسمت قبل، کلید مخفی K_i و عدد تصادفی N_T را به‌دست می‌آورد.

الگوریتم ۱)

$For\ 1 \le i \le 2^{16}$

$Choose\ u_i \in U$

$N_t = u_i \oplus D$

$if\ E = N_T \oplus PRNG(C_i \oplus u_i)\ then$

$return\ u_i\ as\ K_i$ and N_t

End

۳) حال نظر به این‌که کلید EPC_i یک دنباله ۱۶ بیتی است، پس $EPC_s \in V$ که $V = \{V_1, V_2, \dots, V_{2^{16}}\}$ است. در نتیجه یک مهاجم می‌تواند از این ضعف پروتکل استفاده کند و با استفاده از مقادیر به‌دست‌آمده K_i و N_T در الگوریتم (۱)، پیام M_1 شنودشده، و الگوریتم (۲) کلید مخفی EPC_s را به‌دست می‌آورد.

الگوریتم ۲)

$For\ 1 \le i \le 2^{16}$

$Choose\ v_i \in V$

$if\ M_1 = PRNG(v_i \oplus N_R \oplus N_T) \oplus K_i\ then$

$return\ v_i\ as\ EPC_s$

End

۴) در نهایت مهاجم با داشتن کلیدهای مخفی K_i، EPC_s و عدد تصادفی N_T قادر به کشف کلید مخفی P_X به‌صورت زیر می‌باشد:

$$P_X = M_2 \oplus PRNG(EPC_s \oplus N_T)$$

مشاهده می‌شود که مهاجم با اعمال حمله کشف کلید و استفاده از روش ذکر شده قادر خواهد بود تمام کلیدهای مخفی موجود در برچسب را به‌دست آورد. پیچیدگی این حمله تنها 2×2^{16} محاسبه و شنود یک دور از پروتکل می‌باشد.

توجه شود که مهاجم بعد از اعمال حمله کشف کلید، قادر خواهد بود که حمله جعل برچسب، حمله جعل کارت‌خوان، حمله ناهمزمانی و حمله ردیابی را با احتمال "۱" و با موفقیت کامل انجام دهد. با این‌وجود، علاوه بر حملات ذکرشده، در ادامه حمله جعل برچسب و حمله ردیابی را با روشی متفاوت و بدون استفاده از کلیدهای مخفی به‌دست‌آمده از حمله کشف کلید، بر روی پروتکل SPRS اعمال می‌کنیم.

۳-۳- حمله جعل هویت برچسب

در این حمله روشی پیشنهاد می‌کنیم که مهاجم حتی بدون داشتن کلیدهای مخفی برچسب قادر به جعل هویت برچسب مورد نظر خواهد بود. روند انجام این حمله به‌صورت زیر می‌باشد:

۱) ابتدا مهاجم به‌عنوان یک شنودگر، پیام‌های مبادله‌شده بین برچسب و کارت‌خوان شامل N_R، M_1، E، D و C_i را در یک دور موفق شنود می‌کند. به‌دلیل اتمام موفقیت‌آمیز دور اول، برچسب و سرویس‌دهنده نهایی مقادیر مخفی خود را به‌روزرسانی می‌کنند. در سرویس‌دهنده نهایی علاوه بر کلیدهای به‌روزرسانی‌شده K_{new}، P_{new} و C_{new} کلیدهای مرحله قبل یعنی K_{old}، P_{old} و C_{old} را در خود ذخیره می‌کند.

1- Advantage function

۲) سپس مهاجم با کارت‌خوان یک دور جدید را آغاز می‌کند. بعد از ارسال N'_R توسط کارت‌خوان، مهاجم پیام‌های M'_1، E'، D' و C'_i را در پاسخ به کارت‌خوان می‌فرستد:

$$M'_1 = M_1, \quad D' = D \oplus N_R \oplus N'_R,$$
$$C'_i = C_{old}, \quad E' = E \oplus N_R \oplus N'_R.$$

و کارت‌خوان نیز طبق روند پروتکل پیام‌ها را به سرویس‌دهنده نهایی ارسال می‌کند.

۳) در سرویس‌دهنده نهایی برای احرازهویت برچسب عملیات زیر را انجام می‌دهد:

$$PRNG(EPC_s \oplus N'_R \oplus D' \oplus K_i) \oplus K_i$$
$$= PRNG(EPC_s \oplus N'_R \oplus D \oplus N_R \oplus N'_R \oplus K_i) \oplus K_i$$
$$= PRNG(EPC_s \oplus D \oplus N_R \oplus K_i) \oplus K_i$$
$$= PRNG(EPC_s \oplus N_T \oplus K_i \oplus N_R \oplus K_i) \oplus K_i \quad (۹)$$
$$= PRNG(EPC_s \oplus N_T \oplus N_R) \oplus K_i$$
$$= M_1$$
$$= M'_1$$

$$Checks\ that: D' \oplus K_i \oplus PRNG(C_i \oplus K_i) \stackrel{?}{=} E'$$

$$D' \oplus K_i \oplus PRNG(C_i \oplus K_i) =$$
$$D \oplus N_R \oplus N'_R \oplus K_i \oplus PRNG(C_i \oplus K_i) \quad (۱۰)$$
$$= N_T \oplus K_i \oplus N_R \oplus N'_R \oplus K_i \oplus PRNG(C_i \oplus K_i)$$
$$= E \oplus N_R \oplus N'_R = E'$$

همان‌طور که مشاهده می‌شود سرویس‌دهنده نهایی هویت مهاجم را به‌عنوان برچسب مجاز تایید می‌کند و در نتیجه عملیات حمله جعل برچسب توسط مهاجم با موفقیت صورت می‌گیرد.

۳-۴- حمله ردیابی

در این بخش نشان می‌دهیم که پروتکل SPRS در برابر حمله ردیابی آسیب‌پذیر است. به‌دلیل این‌که برچسب در پیام پاسخ خود به کارت‌خوان مقدار C_i را ارسال می‌کند و این امکان وجود دارد تا یک مهاجم در نقش یک کارت‌خوان مجاز با ارسال یک عدد N_R به برچسب پاسخ او را دریافت کند و نشست را خاتمه داده تا برچسب به‌روزرسانی نکند. حال اگر مهاجم دوباره عدد N_R را برای برچسب ارسال کند، به‌دلیل به‌روز نشدن کلید، باز هم پاسخ مشابهی دریافت می‌کند و برچسب قربانی را شناسایی می‌کند. در ادامه این حمله در قالب مدل اوفی- فان نمایش می‌دهیم.

مرحله یادگیری: در این مرحله مهاجم با استفاده از ارسال عدد N_R یک پرسمان $Execute\ query\ (R, T_0, i)$ به برچسب T_0 می‌فرستد و مقادیر $(E_i^{T_0}, D_i^{T_0})$ را به‌دست‌آورده و ذخیره می‌کند. سپس با استفاده از مقادیر به‌دست‌آمده، پیام $\Psi = D_i^{T_0} \oplus E_i^{T_0}$ محاسبه می‌کند.

مرحله چالش: در این مرحله، مهاجم برچسب‌های T_0 و T_1 را برای آزمایش انتخاب می‌کند تا با آنها تعامل داشته باشد. سپس برچسب $T_b \in \{T_0, T_1\}$ به تصادف انتخاب‌شده و در اختیار مهاجم قرار می‌گیرد. در این مرحله مهاجم با ارسال عدد N_R یک پرسمان $Execute\ query\ (R, T_b, i+1)$ به برچسب T_b ارسال می‌کند و پیام‌های $(E_{i+1}^{T_b}, D_{i+1}^{T_b})$ را به دست می‌آورد.

مرحله حدس: به کمک اطلاعات به‌دست آمده از مراحل یادگیری و چالش، مهاجم با استفاده از قاعده‌ی زیر تشخیص می‌دهد که او در مرحله چالش با کدام برچسب در ارتباط بوده است. او بیت b' را به‌عنوان حدس خود به‌صورت زیر تولید می‌کند:

$$b' = \begin{cases} 0 & if \quad D_{i+1}^{T_b} \oplus E_{i+1}^{T_b} = \Psi \\ 1 & otherwise \end{cases} \quad (۱۱)$$

تابع مزیت به‌دست آمده برای مهاجم برابر است با:

$$Adv_A^{upriv}(K) =$$
$$|pr(b' = b) - pr(random\ coin\ flip)|$$
$$= \left|pr(b' = b) - \frac{1}{2}\right| = \left|1 - \frac{1}{2}\right| = \frac{1}{2} \gg \quad (۱۲)$$

اثبات: با توجه به این‌که برچسب T_0 در مرحله یادگیری کلیدهای مخفی خود را به‌روزرسانی نکرده است، در نتیجه کلید K_i و C_i در مرحله یادگیری و چالش یکسان می‌باشند. پس اگر در مرحله چالش $T_0 = T_b$، مقدار $D_{i+1}^{T_b} \oplus E_{i+1}^{T_b}$ که توسط او تولید می‌شود با احتمال "۱" برابر با $D_i^{T_b} \oplus E_i^{T_b}$ است، در نتیجه مهاجم می‌تواند با احتمال "۱" بگوید که اگر $D_{i+1}^{T_b} \oplus E_{i+1}^{T_b} = D_i^{T_0} \oplus E_i^{T_0}$، او با برچسب T_0 در ارتباط بوده است. از طرف دیگر در صورتی که $D_{i+1}^{T_b} \oplus E_{i+1}^{T_b} \neq D_i^{T_0} \oplus E_i^{T_0}$، مهاجم به‌طور قطعی متوجه می‌شود که او با T_0 در ارتباط نبوده است. به بیان ریاضی می‌توان نوشت:

$$If\ T_b = T_0 \implies \Psi = D_{i+1}^{T_b} \oplus E_{i+1}^{T_b}$$
$$= N_{T,i+1}^{T_b} \oplus K_{i+1}^{T_b} \oplus N_{T,i+1}^{T_b} \oplus PRNG\left(C_{i+1}^{T_b} \oplus K_{i+1}^{T_b}\right)$$
$$= K_{i+1}^{T_b} \oplus PRNG\left(C_{i+1}^{T_b} \oplus K_{i+1}^{T_b}\right)$$
$$= K_i^{T_0} \oplus PRNG\left(C_i^{T_0} \oplus K_i^{T_0}\right) = D_i^{T_0} \oplus E_i^{T_0} \quad (۱۳)$$

۴- پروتکل بهبود یافته

در قسمت‌های قبل نقاط ضعف و رخنه‌های امنیتی و

محرمانگی در پروتکل SPRS بیان شد. در ادامه برای بهبود این پروتکل، ابتدا دلایل ایجاد رخنه‌های امنیتی و محرمانگی را در طراحی پروتکل SPRS بیان می‌کنیم و سپس پروتکل پیشنهادی خود را ارائه می‌دهیم.

۴-۱- بررسی ضعف‌های پروتکل SPRS

ضعف اول: اولین نقطه آسیب‌پذیری پروتکل مورد نظر در وابستگی در ساختار پیام E و پیام D می‌باشد که در این پیام‌ها از دو مقدار مخفی K_i و C_i استفاده شده است و از آنجایی‌که در پیام‌های E و D عدد تصادفی N_T بدون هیچ‌گونه اعمال توابع رمزنگاری می‌باشد، در نتیجه مهاجم می‌تواند از این نقطه ضعف برای اعمال حمله کشف کلید و همچنین حمله ردیابی استفاده نماید.

ضعف دوم: ضعف دیگر این پروتکل از ساختار پیام M_1 ناشی می‌شود که این پیام یکی از مقیاس‌هایی است که سرویس‌دهنده نهایی از آن برای احرازهویت برچسب استفاده می‌کند. بنابراین ساختار آن از اهمیت بالایی برخوردار می‌باشد، ولی در پروتکل SPRS وجود رخنه امنیتی در ساختار این پیام، زمینه را برای اعمال حمله جعل برچسب برای مهاجم فراهم می‌کند.

۴-۲- ارائه پروتکل پیشنهادی

در پروتکل پیشنهادی نقاط ضعف موجود در پروتکل SPRS برطرف شده است. در طراحی این پروتکل پیشنهادی برای جلوگیری از حمله کشف کلید و حمله جعل برچسب تغییراتی در ساختار پیام M_1 داده شده است و همچنین برای جلوگیری از حمله ردیابی و حمله جعل برچسب تغیراتی در ساختار پیام E اعمال شده است که به طبع آن نحوه احراز هویت در سرویس‌دهنده نهایی نیز تغییر یافته است. با تمهیدات امنیتی و محرمانگی صورت گرفته در طراحی پروتکل پیشنهادی، این پروتکل را در مقابل همه حملات مقاوم کرده است. فرایند انجام پروتکل پیشنهادی به‌صورت زیر می‌باشد که ساختار کلی آن در شکل (۳) نمایش داده شده است.

۴-۲-۱- مرحله آغازین

در این مرحله اطلاعات اولیه‌ای نظیر K_0 و P_0 و C_0 به صورت تصادفی در کارخانه تولید شده و چندتایی $(K_i = K_0, P_i = P_0, C_i = C_0)$ در برچسب ذخیره می‌شود. همچنین متناظر با آن چندتایی $K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = C_0$ در سرویس‌دهنده نهایی ذخیره می‌شود.

۴-۲-۲- مرحله احراز هویت

۱) در این مرحله ابتدا کارت‌خوان عدد تصادفی N_R را تولید کرده و آن‌را به برچسب ارسال می‌کند.

۲) برچسب نیز بعد از دریافت پیام، عدد تصادفی N_T را تولید کرده و سپس مقادیر زیر را محاسبه می‌کند و به کارت‌خوان می‌فرستد:

$$M_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i,$$
$$D = N_T \oplus K_i, \quad (۱۴)$$
$$E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$$

۳) کارت‌خوان پیام $V = H(RID \oplus N_R \oplus t)$ محاسبه می‌کند و سپس $(M_1, D, C_i, E, N_R, V, t)$ را به سرویس‌دهنده نهایی می‌فرستد.

۴) سرویس‌دهنده نهایی بعد از دریافت چندتایی $(M_1, D, C_i, E, N_R, V, t)$ از طرف کارت‌خوان مراحل زیر را انجام می‌دهد:

- اگر $T - t > \Delta t$ برقرار باشد یعنی زمان انجام عملیات سامانه بزرگ‌تر از بیشترین مقدار زمان مورد نیاز انجام عملیات موردنظر (T) بوده است، بنابراین پروتکل متوقف می‌شود. درصورتی‌که $T - t < \Delta t$ باشد آن‌گاه سرویس‌دهنده نهایی عملیات شناسایی را ادامه می‌دهد و با استفاده از RID و اطلاعات دریافتی از کارت‌خوان، مقدار $H(RID \oplus N_R \oplus t)$ را محاسبه کرده و با V دریافتی مقایسه می‌کند. درصورت برقراری تساوی هویت کارت‌خوان تایید می‌شود.
- سرویس‌دهنده نهایی برای هر چندتایی $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s)$ مقادیر $I_{new} = M_1 \oplus K_{new}$ و $I_{old} = M_1 \oplus K_{old}$ محاسبه می‌کند و سپس این مقادیر را با اطلاعات دریافتی به‌صورت زیر مقایسه می‌کند.

$$I_X \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \oplus PRNG(D \oplus K_X) \quad (۱۵)$$

درصورت برقراری یکی از روابط بالا متغیر X با نام "جدید" و یا "قدیم" متناظر با کلید K_{new} و یا K_{old} که از رابطه بالا به‌دست آمد، مقداردهی می‌کند.

- بعد از تعیین X، سرویس‌دهنده نهایی پیام $PRNG(N_T) \oplus PRNG(C_X \oplus K_i) \oplus P_i$ را محاسبه می‌کند و با پیام E دریافتی مقایسه می‌کند. سپس صحت آن را مورد بررسی قرار می‌دهد. درصورت برقراری رویه پروتکل ادامه می‌یابد، در غیر این‌صورت پروتکل متوقف می‌شود.
- سرویس‌دهنده نهایی چندتایی $(M_2, Info, MAC)$ را به‌صورت زیر محاسبه می‌کند و به کارت‌خوان ارسال می‌کند:

$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X,$$
$$Info = (DATA \oplus RID \oplus t),$$

Database $(K_{old}, C_{old}, P_{old}, K_{new}, C_{new}, P_{new}, RID, EPC, DATA)$	Reader (RID)	Tag (K_i, C_i, P_i, EPC_s)
If $T - t > \Delta t$ *then abortes protocol* *Else* *For each RID* *Verify* $H(RID \oplus N_R \oplus t) \stackrel{?}{=} V$ *If* $I_{new} = M_1 \oplus K_{new} \oplus PRNG(D \oplus K_{new})$ $I_{new} \stackrel{?}{=} PRNG(EPC_s \oplus N_R)$ $X = new$ Else: $I_{old} = M_1 \oplus K_{old} \oplus PRNG(D \oplus K_{old})$ $I_{old} \stackrel{?}{=} PRNG(EPC_s \oplus N_R)$ $X = old$ End *Verify* $PRNG(C_i \oplus K_x) \oplus D \oplus K_x \oplus P_x \stackrel{?}{=} E$ Then computes values below: $M_2 = PRNG(EPC_s \oplus N_T) \oplus P_x$ $info = DATA \oplus RID \oplus t$ $MAC = H(DATA \oplus t)$ $N_T = D \oplus K_x$ *If* $X = new$ $K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new})$ $P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new})$ $C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R)$ *Else* $C_{new} \leftarrow PRNG(N_T \oplus N_R)$ *End*	**(1)** $N_R \rightarrow$	Generates N_T and N_2 as random numbers $M_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$ $D = N_T \oplus K_i$ $E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$
	(2) $\leftarrow (M_1, D, C_i, E)$	
$V = H(RID \oplus N_R \oplus t)$		
(3) $\leftarrow (M_2, D, C_i, E, N_R, V, t)$		
(4) $(M_2, Info, MAC) \rightarrow$		
Verify $DATA = Info \oplus RID \oplus t$ $H(DATA \oplus t) \stackrel{?}{=} MAC$		
	(5) $M_2 \rightarrow$	*Verify* $M_2 \oplus P_i \stackrel{?}{=} PRNG(EPC_s \oplus N_T)$ $K_{i+1} \leftarrow PRNG(K_i)$ $P_{i+1} \leftarrow PRNG(P_i)$ $C_{i+1} \leftarrow PRNG(N_T \oplus N_R)$

شکل (۳). پروتکل پیشنهادی

$$MAC = H(DATA \oplus t) \quad (۱۶)$$

اگر X = new باشد، آنگاه سرویس‌دهنده نهایی مقادیر مخفی خود را به‌صورت زیر به‌روزرسانی می‌کند:

$$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new}),$$

$$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new}),$$

$$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R) \quad (۱۷)$$

و اگر X = old باشد عملیات به‌روزرسانی فقط برای C_i به‌صورت زیر انجام می‌شود:

$$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R) \quad (۱۸)$$

- کارت‌خوان بعد از دریافت پیام از سرویس‌دهنده نهایی، با استفاده از RID و t، مقدار DATA دریافتی را به صورت $DATA = Info \oplus RID \oplus t)$ به‌دست می‌آورد. در ادامه مقدار $H(DATA \oplus t)$ را محاسبه کرده و با پیام MAC دریافتی از سرویس‌دهنده نهایی مقایسه می‌کند. درصورت تساوی، کارت‌خوان هویت سرویس‌دهنده نهایی را تایید می‌کند و پیام M_2 دریافتی را به برچسب ارسال می‌کند.
- برچسب پیام دریافتی را با کلید مخفی ذخیره‌شده در خود، XOR کرده و برقراری رابطه زیر را بررسی می‌کند:

$$M_2 \oplus P_x \stackrel{?}{=} PRNG(EPC_S \oplus N_T) \quad (۱۹)$$

درصورت برقراری رابطه فوق برچسب هویت سرویس‌دهنده نهایی را تایید کرده و مقادیر مخفی خود را به‌صورت زیر به‌روزرسانی می‌کند:

$$K_{i+1} \leftarrow PRNG(K_i),$$

$$P_{i+1} \leftarrow PRNG(P_i),$$

$$C_{i+1} \leftarrow PRNG(N_T \oplus N_R). \quad (۲۰)$$

۴-۳- تحلیل امنیتی پروتکل پیشنهادی

در این بخش پروتکل پیشنهاد شده در مقابل حملات کشف کلید شناسه، حمله جعل برچسب و حمله ردیابی مورد تحلیل امنیتی واقع شده است.

حمله کشف کلید: از آنجایی که در پروتکل بهبودیافته با استفاده از تابع $PRNG(N_T)$، بین پیام‌های D و E از یکدیگر

مستقل شده‌اند. لذا مهاجم نمی‌تواند با استفاده از این دو پیام و حتی با استفاده از الگوریتم ذکر شده در قسمت ۳-۲ کلیدهای مخفی را کشف کند.

حمله جعل برچسب: در پروتکل بهبود یافته برای جلوگیری از حمله جعل برچسب، تمهیداتی در ساختار پیام M_1 و E اندیشده شده است. استفاده از کلید مخفی P_i و $PRNG(N_T)$ در ساختار پیام E و همچنین تغییر پیام M_1 به‌صورت $M_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$ مانع از انجام حمله جعل برچسب می‌شود.

حمله ردیابی: وجود $PRNG(N_T)$ در پیام E وابستگی بین پیام E و D را از بین می‌برد و مهاجم با استفاده از این دو پیام قادر به ردیابی برچسب نمی‌باشد.

در جدول‌های (۱ و ۲) به ترتیب مقایسه‌ای از تحلیل امنیتی و عملکردی پروتکل بهبود یافته با برخی از پروتکل‌های مشابه موجود آورده شده است.مشاهده می‌شود بر خلاف سایر پروتکل‌ها، امنیت و محرمانگی پروتکل بهبود یافته تأمین است.

جدول (۱). تحلیل امنیتی پروتکل‌ها

پروتکل‌ها / حمله‌ها	پروتکل یه و همکارانش[7]	پروتکل یون و همکارانش [8]	پروتکل SPRS [9]	پروتکل بهبود داده شده
حمله کشف مقادیرمخفی	✓	×	×	✓
حمله تکرار	×	×	×	✓
حمله جعل	✓	✓	×	✓
حمله ردیابی	×	×	×	✓
حمله ناهمزمانی	✓	✓	✓	✓

امن: ✓ ناامن: ×

جدول (۲). تحلیل عملکردی پروتکل‌ها: H تابع چکیده‌ساز، PRNG: تابع شبه‌عدد تصادفی

عملکرد	پروتکل یه و همکارانش [7]	پروتکل یون و همکارانش [8]	پروتکل SPRS [9]	پروتکل پیشنهادی
هزینه محاسبات در برچسب	$0H + 6 \times PRNG$	$0H + 6 \times PRNG$	$0H + 6 \times PRNG$	$0H + 8 \times PRNG$
هزینه محاسبات در سرور و کارت‌خوان	$2H + 10 \times PRNG$	$4H + 10 \times PRNG$	$4H + 10 \times PRNG$	$4H + 12 \times PRNG$

۵- نتیجه‌گیری

در این مقاله، به تحلیل امنیت و محرمانگی یک پروتکل احراز هویت دوسویه در سامانه‌های RFID پرداخته شد. این پروتکل در سال ۲۰۱۳ ارایه شده است. نشان داده شد که برخلاف ادعای طراحان پروتکل، این پروتکل در مقابل حمله‌هایی نظیر کشف کلیدهای مخفی، جعل برچسب و ردیابی آسیب‌پذیر است. لذا این پروتکل نمی‌تواند امنیت و محرمانگی کاربران RFID را فراهم کند. در این مقاله، حمله ردیابی در قالب مدل اوفی- فان انجام شد. در ادامه، جهت رفع ضعف‌های پروتکل SPRS یک پروتکل احراز هویت دوسویه جدید پیشنهاد شد که در واقع نسخه بهبود یافته از پروتکل SPRS است. در نهایت، تحلیل امنیتی پروتکل پیشنهاد شده با برخی از پروتکل‌های احراز هویت دوسویه که در سال‌های اخیر پیشنهاد شده است مورد مقایسه قرار گرفت و مشاهده شد که پروتکل پیشنهاد شده، در مقایسه با سایر پروتکل‌ها از امنیت و محرمانگی کاملی برخوردار است. در نهایت پیچیدگی و عملکرد پروتکل پیشنهادی با پروتکل های ارایه‌شده و موجود در این زمینه مقایسه گردیده است و مشاهده شد که با کمترین تغییرات در پیچیدگی پروتکل قادر به رفع ضعف‌های موجود شده است.

۶- مراجع

[1] E.-C. Australia, “Access control, sensor control, and trans-ponders,” Available on: http://www.rfid.com.au/rfid uhf.htm, 2008.

[2] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. W. Scherer, “Crossing borders: Security and privacy issues of the European e-passport,” in IWSEC, Springer-Heidelberg, pp. 152-167, 2006.

[3] “Transport for London, Oyster,” [Online]: Available: http://www.tfl.gov.uk/tickets/27298.aspx. [Accessed 01 02 2014].

[4] D. C. Wyld, “24-Karat protection: RFID and retail jewelry marketing,” International Journal of UbiComp (IJU), vol. 1, no. 1, 2010.

[5] K. Khedo, D. Sathan, R. Elaheebocus, R. K. Subramanian, and S. D. V. Rughooputh, “Overlapping zone partitioning localization technique for RFID,” International Journal of UbiComp (IJU), vol. 1, no. 2, 2010.

[6] “EP Cglobal Inc.,” [Online]: Available: http://www.epcglobalinc.org. [Accessed 02 01 2014].

[7] T. C. Yeh, Y. J. Wang, T. C. Kuo, and S. S. Wang, “Securing RFID systems conforming to EPC Class-1 Generation-2 standard,” Expert Systems with Applications, vol. 37, no. 12, pp. 7678-7683, 2010.

[8] E.-J. Yoon, “Improvement of the securing rfid systems conforming to EPC Class 1 Generation 2 standard,” Expert Syst. Appl., vol. 39, no. 11, pp.

1589-1594, 2012.

[9] F. Xiao, Y. Zhou, J. Zhou, H. Zhu, and X. Niu, "Security Protocol for RFID System Conforming to EPC-C1G2 Standard," Journal of Computers, vol. 8, no. 3, pp. 605-612, 2013.

[10] K. Ouafi and R. C.-W. Phan, "Traceable privacy of recent provably-secure RFID protocols," in ACNS 2008, LNCS 5037, pp. 479–489, 2008.

Journal Of Electronical & Cyber Defence
Vol. 3, No. 3, 2016, Serial No.11

Weaknesses of SPRS Authentication Protocol and Present a Developed Protocol for RFID Systems

M. Mardani Shahrbabak*, B. Abdolmaleki, K. Baghery

* Imam Hossein University

(Received: 02/12/2014, Accepted: 12/01/2016)

ABSTRACT

In recent years, cyber security has become one of the main objectives of military organizations. On the other hand, forces identification, authentication and their security have become one of the basic needs of military centers. Although data encryption prevents user access to data contents, an attacker can forges exchanged data by access to communications channels. As a result, providing secure protocols for authentication systems, to prevent different attacks is very important. In this paper, we cryptanalyze a mutual RFID authentication protocol (SPRS) that presented in 2013. Unlike climes of the designers of protocol, we show that their protocol has some weaknesses yet and does not secure against some attacks such as rival secret values, tag impersonation and tractability. Then, an improved version of SPRS protocol is proposed that eliminates SPRS weaknesses. Also, the security and the privacy of proposed protocol are compared with some mutual authentication protocols that proposed recently.

Keywords: RFID Authentication Protocols, Security and Privacy, Attacks, SPRS Protocol

* Corresponding Author Email: mmardani@ihu.ac.ir