

ضعف‌های پروتکل احراز هویت SPRS و ارائه یک پروتکل بهبود یافته برای سامانه‌های RFID

محمد مردانی شهربابک^{۱*}، بهزاد عبدالملکی^۲، کریم باقری^۳

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. از این رو، ارائه پروتکل‌های امن جهت جلوگیری از این نوع حملات و یا همان پدافند غیرعامل در سیستم‌های احراز هویت از اهمیت فراوانی برخوردار است. در این مقاله، به تحلیل امنیتی یک پروتکل احراز هویت (SPRS) سامانه‌های RFID که در سال ۲۰۱۳ ارائه 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 بهبود یافته از آن ارائه شده است که ضعف‌های پروتکل SPRS در آن حذف شده است. همچنین، امنیت و محرمانگی پروتکل بهبود یافته با برخی از پروتکل‌های احراز هویت دوسویه که اخیراً پیشنهاد شده مقایسه شده است. در ادامه پیچیدگی و عملکرد پروتکل پیشنهادی با پروتکل‌های ارائه شده و موجود در این زمینه مقایسه گردیده و مشاهده می‌شود که با کمترین تغییرات در پیچیدگی پروتکل تحلیل شده، 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

ذخیره شده در این برچسب‌ها توسط دستگاه‌هایی تحت عنوان «کارت‌خوان»^۴ خوانده می‌شود. در حالت کلی سامانه‌های RFID از سه بخش اصلی تشکیل شده‌اند که شامل برچسب، کارت‌خوان و «سرویس‌دهنده نهایی»^۵ 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»^۶ می‌باشد که توسط سازمان «EPCglobal»^۷ ارائه شده است [۶]. در سال ۲۰۱۰ به و همکاری یک پروتکل احراز هویت مبتنی بر استاندارد EPC ارائه کردند [۷]. در سال ۲۰۱۲ یون و همکارانش یک تحلیل امنیتی

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»^۱ (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 [۴-۵]. سامانه‌های RFID، قابلیت شناسایی اتوماتیک اشیا، با استفاده از یک تراشه کوچک ارزان قیمت را فراهم می‌کنند. این تراشه کوچک به اصطلاح «برچسب»^۲ یا «برچسب هوشمند»^۳ نامیده می‌شود. داده‌های

4- Reader

5- Back-end-server

6- EPC Class 1 Generation 2 (EPC C-1 G-2)

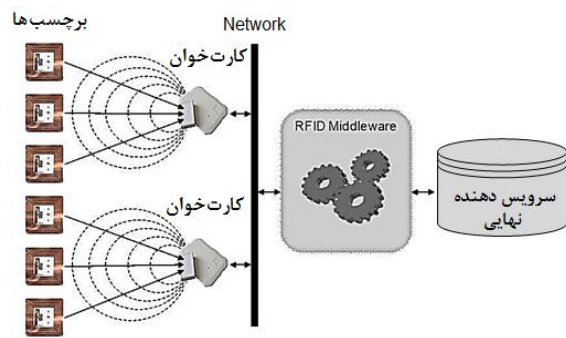
7- Electronic Product Code

* رایانامه نویسنده مسئول: mmardani@ihu.ac.ir

1- Radio Frequency Identification (RFID)

2- Tag

3- Smart Tag



شکل (۱). سامانه مدل یک سامانه 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 $(K_i = K_0, P_i = P_0, C_i = C_0)$ بر روی برچسب ذخیره می‌شود. همچنین متناظر با آن مقادیر چندتایی $K_{old} = K_{new}$ در سرویس‌دهنده $K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = C_0$ ذخیره می‌شود.

۲-۲- مرحله احراز هویت

(۱) در این مرحله ابتدا کارت خوان 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 کارت خوان می‌فرستد:

$$M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i, D = N_T \oplus K_i, E = N_T \oplus PRNG(C_i \oplus K_i) \quad (1)$$

(۳) کارت خوان پیام $V = H(RID \oplus N_R \oplus E)$ 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 کارت خوان 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 مورد نظر (T) بوده است، بنابراین پروتکل متوقف می‌شود. در صورتی که $T - t < \Delta t$ باشد آن‌گاه سرویس‌دهنده نهایی عملیات شناسایی را ادامه می‌دهد و با استفاده از RID و اطلاعات دریافتی از کارت خوان، مقدار $H(RID \oplus N_R \oplus E)$ را محاسبه کرده و با V دریافتی مقایسه می‌کند، در صورت برقراری تساوی هویت کارت خوان تایید می‌شود.

بر روی پروتکل یه و همکارانش انجام داده و نشان دادند که این پروتکل در مقابل حمله‌های ناهمزمانی و همچنین ردیابی مقاوم نسبت و سپس با اعمال تغییراتی در آن ضعف‌های آن را از بین برده و یک نسخه بهبودیافته از آن را ارائه دادند [۸]. در مارس ۲۰۱۳ فنگ خیو^۱ 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»^۲ (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)

به روزرسانی می کند:

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

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

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

۳- تحلیل امنیتی و محرمانگی پروتکل SPRS

در این بخش نشان داده می شود که ادعاهای طراحان پروتکل SPRS صحیح نبوده و پروتکل دارای برخی از ضعف های امنیتی و محرمانگی است. در ادامه حمله های کشف کلیدهای مخفی، جعل هویت برچسب و حمله ردیابی در قالب مدل اوفی-فان [۱۰] بر روی این پروتکل ارائه می شود. لذا در ادامه، در ابتدا به اشاره مختصری به مدل اوفی-فان می کنیم. سپس حملات انجام شده را با جزئیات بیشتری ارائه می کنیم.

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

ردیابی

مدل اوفی-فان که برای ارزیابی حمله های عدم ردیابی و عدم ردیابی پسر مورد استفاده قرار می گیرد، به شرح زیر است [۱۰]:

در این مدل یک شریک^۱ می تواند شامل برچسب و یا کارت خوان باشد. هر یک از شرکا می توانند فعالانه در اجرای پروتکل مشارکت کنند و پروتکل را تا پایان ادامه دهند. طرفین درگیر در پروتکل بر روی یک کانال بی سیم و ناامن با یکدیگر تعامل دارند که این کانال به طور کامل در کنترل یک مهاجم قدرتمند قرار دارد. به این مهاجم توانایی ها و قدرت عمل بسیاری داده می شود که این توانایی ها به طور رسمی در قالب پرسمان های زیر مدل می شوند:

- **Execute (R, T, i) query**: توسط این پرسمان به مهاجم قابلیت شنود و استراق سمع نشست های برگزار شده بین طرفین داده می شود. به بیان رسمی، هنگامی که مهاجم اقدام به ارسال Execute (R, T, i) query می کند، قادر می شود تا i -امین نشست برگزار شده بین برچسب T و کارت خوان R را به طور کامل شنود کرده و اطلاعات رد و بدل شده در آن نشست را به دست بیاورد. در واقع با این پرسمان مهاجم قادر است یک حمله غیرفعال^۲ انجام دهد.
- **Send (U₁, U₂, i, m) query**: توسط این پرسمان به مهاجم قابلیت انجام حملات فعال داده می شود. به بیان رسمی، با ارسال پرسمان Send (U₁, U₂, i, m) query توسط مهاجم، به او اجازه داده می شود تا با جعل هویت یک کارت خوان $U_1 \in \text{Readers}$ (و یا برچسب $U_1 \in \text{Tags}$)، بتواند به

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

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

- در صورت برقراری یکی از روابط بالا متغیر X با نام "جدید" و یا "قدیم" متنظر با کلید K_{new} و یا K_{old} که از رابطه بالا به دست آمد، مقداردهی می کند.
- بعد از تعیین X، سرویس دهنده نهایی پیام $N_T \oplus PRNG(C_X \oplus K_i)$ را محاسبه می کند و با پیام E دریافتی مقایسه می کند. سپس صحت آن را مورد بررسی قرار می دهد. در صورت برقراری انجام پروتکل ادامه می یابد در غیر این صورت پروتکل متوقف می شود
- سرویس دهنده نهایی، چندتایی $(M_2, Info, MAC)$ را به صورت زیر محاسبه و به کارت خوان ارسال می کند:

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

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

$$MAC = H(DATA \oplus t) \quad (۳)$$

- اگر $X = new$ باشد، آنگاه سرویس دهنده نهایی مقادیر مخفی خود را به صورت زیر به روزرسانی می کند:

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

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

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

و اگر $X = old$ باشد عملیات به روزرسانی فقط برای C_i به صورت زیر انجام می شود:

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

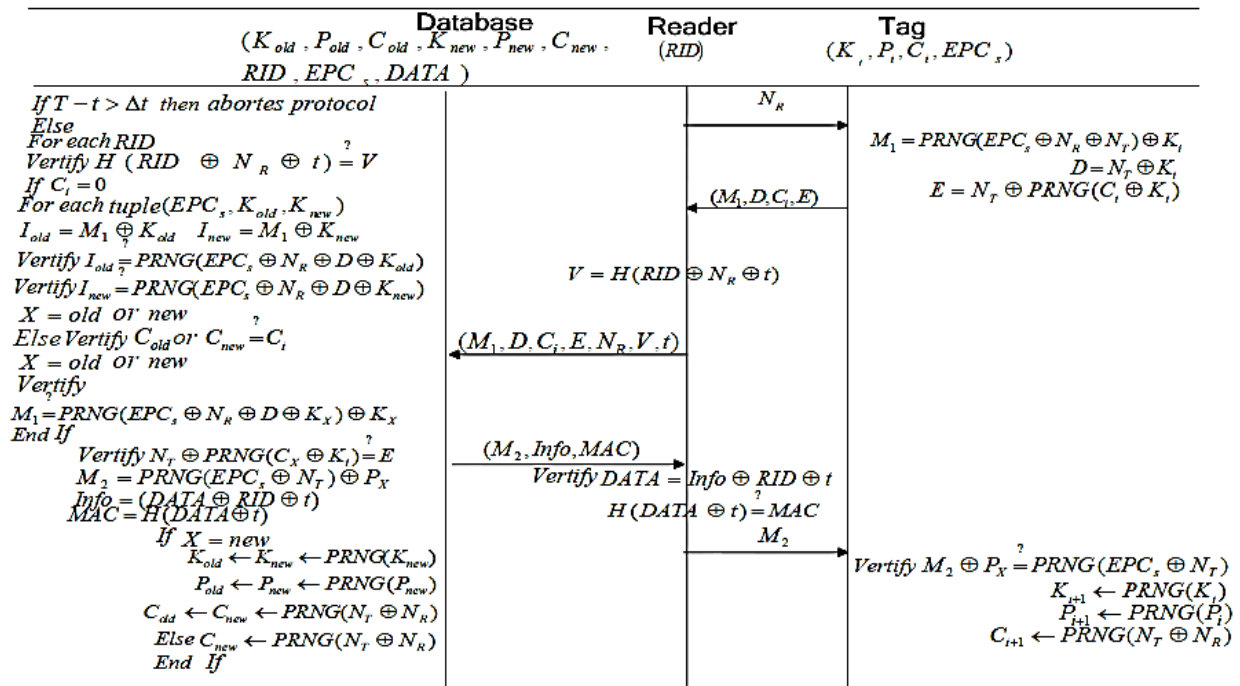
- کارت خوان بعد از دریافت پیام از سرویس دهنده نهایی، با استفاده از RID و t مقدار DATA دریافتی را به صورت $DATA = Info \oplus RID \oplus t$ به دست می آورد. در ادامه مقدار $H(DATA \oplus t)$ را محاسبه کرده و با پیام MAC دریافتی از سرویس دهنده نهایی مقایسه می کند. در صورت تساوی، کارت خوان هویت سرویس دهنده نهایی را تایید و پیام M_2 دریافتی را به برچسب ارسال می کند.
- برچسب پیام دریافتی را با کلید مخفی ذخیره شده در خود، XOR کرده و برقراری رابطه زیر را بررسی می کند:

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

در صورت برقراری رابطه فوق برچسب هویت سرویس دهنده نهایی را تایید کرده و مقادیر مخفی خود را به صورت زیر

1- Party

2- Passive attack



شکل (۲). پروتکل SPRS [۹].

مرحله یادگیری^۳: 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. به علاوه، 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^۴: 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^۵: 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.

انتخاب خودش پیام m را در نشست i -ام از پروتکل، به برچسب نمونه $U_2 \in \text{Tags}$ (و یا کارت-خوان $U_2 \in \text{U}$) 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^۱ 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 $T \in \text{Tags}$ 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): 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.

3- Learning phase
4- Challenge phase
5- Guess phase

1- Compromise
2- Untraceable privacy

(۳) حال نظر به این که 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 می تواند از این ضعف پروتکل استفاده کند و با استفاده از مقادیر به دست آمده K_i و N_T در الگوریتم (۱)، پیام M_1 شنود شده، و الگوریتم (۲) کلید مخفی EPC_s را به دست می آورد.

الگوریتم (۲)

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

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 به صورت زیر می باشد:

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

مشاهده می شود که مهاجم با اعمال حمله کشف کلید و استفاده از روش ذکر شده قادر خواهد بود تمام کلیدهای مخفی موجود در برچسب را به دست آورد. پیچیدگی این حمله تنها 2×2^{16} محاسبه و شنود یک دور از پروتکل می باشد. توجه شود که مهاجم بعد از اعمال حمله کشف کلید، قادر خواهد بود که حمله جعل برچسب، حمله جعل کارت خوان، حمله ناهمزمانی و حمله ردیابی را با احتمال "۱" و با موفقیت کامل انجام دهد. با این وجود، علاوه بر حملات ذکر شده، در ادامه حمله جعل برچسب و حمله ردیابی را با روشی متفاوت و بدون استفاده از کلیدهای مخفی به دست آمده از حمله کشف کلید، بر روی پروتکل SPRS اعمال می کنیم.

۳-۳- حمله جعل هویت برچسب

در این حمله روشی پیشنهاد می کنیم که مهاجم حتی بدون داشتن کلیدهای مخفی برچسب قادر به جعل هویت برچسب مورد نظر خواهد بود. روند انجام این حمله به صورت زیر می باشد:

(۱) ابتدا مهاجم به عنوان یک شنودگر، پیامهای مبادله شده بین برچسب و کارت خوان شامل N_R ، M_1 ، E ، D و C_i را در یک دور موفق شنود می کند. به دلیل اتمام موفقیت آمیز دور اول، برچسب و سرویس دهنده نهایی مقادیر مخفی خود را به روزرسانی می کنند. در سرویس دهنده نهایی علاوه بر کلیدهای به روزرسانی شده K_{new} ، P_{new} و C_{new} کلیدهای مرحله قبل یعنی K_{old} ، P_{old} و C_{old} را در خود ذخیره می کند.

میزان موفقیت مهاجم A در این بازی توسط یک تابع مزیت^۱ و به صورت زیر تعریف می شود:

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

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

که $pr(\text{random coin flip})$ نشان گر احتمال آن است که مهاجم بیت b' را به صورت تصادفی انتخاب کند و به دلیل توزیع یکنواخت، این احتمال برابر با $\frac{1}{2}$ است. هر چند مزیت به دست آمده برای مهاجم به $\frac{1}{2}$ نزدیک تر باشد، نشان دهنده قدرت مهاجم در تمایز قائل شدن بین T_0 و T_1 است و در نتیجه قابلیت عدم ردیابی پروتکل ضعیف تر خواهد بود.

۳-۲- حمله کشف کلیدهای مخفی

از ضعف های موجود در طراحی این پروتکل اعمال حمله کشف کلید می باشد به این صورت که مهاجم با یک بار شنود کردن اطلاعات مبادله شده بین برچسب و سرویس دهنده نهایی، و با استفاده از الگوریتم پیشنهادی در این قسمت، قادر به کشف همه کلیدهای مخفی به کار رفته در برچسب و سرویس دهنده نهایی خواهد بود. در ادامه به شرح کامل این حمله پرداخته می شود:

(۱) ابتدا مهاجم با انجام یک حمله غیرفعال، نقش یک شنودگر را بازی می کند و پیامهای مبادله شده بین برچسب و کارت خوان را دریافت کرده و ذخیره می کند 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 می باشد 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 شنود شده از قسمت قبل، کلید مخفی K_i و عدد تصادفی N_T را به دست می آورد.

الگوریتم (۱)

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

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

عدد N_R یک پرسمان (R, T_0, i) *Execute query* به برچسب T_0 می فرستد و مقادیر $(E_i^{T_0}, D_i^{T_0})$ را به دست آورده و ذخیره می کند. سپس با استفاده از مقادیر به دست آمده، پیام $\Psi = D_i^{T_0} \oplus E_i^{T_0}$ محاسبه می کند.

مرحله چالش: در این مرحله، مهاجم برچسب های T_0 و T_1 را برای آزمایش انتخاب می کند تا با آنها تعامل داشته باشد. سپس برچسب $T_b \in \{T_0, T_1\}$ به تصادف انتخاب شده و در اختیار مهاجم قرار می گیرد. در این مرحله مهاجم با ارسال عدد N_R یک پرسمان $(R, T_b, i + 1)$ *Execute query* به برچسب T_b ارسال می کند و پیام های $(E_{i+1}^{T_b}, D_{i+1}^{T_b})$ را به دست می آورد.

مرحله حدس: به کمک اطلاعات به دست آمده از مراحل یادگیری و چالش، مهاجم با استفاده از قاعده ی زیر تشخیص می دهد که او در مرحله چالش با کدام برچسب در ارتباط بوده است. او بیت b' را به عنوان حدس خود به صورت زیر تولید می کند:

$$b' = \begin{cases} 0 & \text{if } D_{i+1}^{T_b} \oplus E_{i+1}^{T_b} = \Psi \\ 1 & \text{otherwise} \end{cases} \quad (11)$$

تابع مزیت به دست آمده برای مهاجم برابر است با:

$$\begin{aligned} Adv_A^{upriv}(K) &= |pr(b' = b) - pr(\text{random coin flip})| \\ &= \left| pr(b' = b) - \frac{1}{2} \right| = \left| 1 - \frac{1}{2} \right| = \frac{1}{2} \gg \end{aligned} \quad (12)$$

اثبات: با توجه به این که برچسب T_0 در مرحله یادگیری کلیدهای مخفی خود را به روزرسانی نکرده است، در نتیجه کلید K_i و C_i در مرحله یادگیری و چالش یکسان می باشند. 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 می شود با احتمال "۱" برابر با $D_i^{T_b} \oplus E_i^{T_b}$ است، در نتیجه مهاجم می تواند 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 به طور قطعی متوجه می شود که او با T_0 در ارتباط نبوده است. به بیان ریاضی می توان نوشت:

$$\begin{aligned} \text{If } T_b = T_0 &\Rightarrow \Psi = D_{i+1}^{T_b} \oplus E_{i+1}^{T_b} \\ &= N_{T,i+1}^{T_b} \oplus K_{i+1}^{T_b} \oplus N_{T,i+1}^{T_b} \oplus PRNG(C_{i+1}^{T_b} \oplus K_{i+1}^{T_b}) \\ &= K_{i+1}^{T_b} \oplus PRNG(C_{i+1}^{T_b} \oplus K_{i+1}^{T_b}) \\ &= K_i^{T_0} \oplus PRNG(C_i^{T_0} \oplus K_i^{T_0}) = D_i^{T_0} \oplus E_i^{T_0} \end{aligned} \quad (13)$$

۴- پروتکل بهبود یافته

در قسمت های قبل نقاط ضعف و رخنه های امنیتی و

(۲) سپس مهاجم با کارت خوان یک دور جدید را آغاز می کند. بعد از ارسال N'_R توسط کارت خوان، مهاجم پیام های M'_1 ، E' ، D' و C'_i را در پاسخ به کارت خوان می فرستد:

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

و کارت خوان نیز طبق روند پروتکل پیام ها را به سرویس دهنده نهایی ارسال می کند.

(۳) در سرویس دهنده نهایی برای احراز هویت برچسب عملیات زیر را انجام می دهد:

$$\begin{aligned} &PRNG(EPC_s \oplus N'_R \oplus D' \oplus K_i) \oplus K_i \\ &= PRNG(EPC_s \oplus N'_R \oplus D \oplus N_R \oplus N'_R \oplus K_i) \oplus K_i \\ &= PRNG(EPC_s \oplus D \oplus N_R \oplus K_i) \oplus K_i \\ &= PRNG(EPC_s \oplus N_T \oplus K_i \oplus N_R \oplus K_i) \oplus K_i \end{aligned} \quad (9)$$

$$\begin{aligned} &= PRNG(EPC_s \oplus N_T \oplus N_R) \oplus K_i \\ &= M_1 \end{aligned}$$

$$= M'_1$$

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

$$D' \oplus K_i \oplus PRNG(C_i \oplus K_i) =$$

$$D \oplus N_R \oplus N'_R \oplus K_i \oplus PRNG(C_i \oplus K_i) \quad (10)$$

$$= N_T \oplus K_i \oplus N_R \oplus N'_R \oplus K_i \oplus PRNG(C_i \oplus K_i)$$

$$= E \oplus N_R \oplus N'_R = E'$$

همان طور که مشاهده می شود سرویس دهنده نهایی هویت مهاجم را به عنوان برچسب مجاز تایید می کند و در نتیجه عملیات حمله جعل برچسب توسط مهاجم با موفقیت صورت می گیرد.

۳-۴- حمله ردیابی

در این بخش نشان می دهیم که پروتکل SPRS در برابر حمله ردیابی آسیب پذیر است. به دلیل این که برچسب در پیام پاسخ خود به کارت خوان مقدار C_i را ارسال می کند و این امکان وجود دارد تا یک مهاجم در نقش یک کارت خوان مجاز با ارسال یک عدد N_R به برچسب پاسخ او را دریافت کند و نشست را خاتمه داده تا برچسب به روزرسانی نکند. حال اگر مهاجم دوباره عدد N_R را برای برچسب ارسال کند، به دلیل به روز نشدن کلید، باز هم پاسخ مشابهی دریافت می کند و برچسب قربانی را شناسایی می کند. در ادامه این حمله در قالب مدل اوفی- فان نمایش می دهیم.

مرحله یادگیری: در این مرحله مهاجم با استفاده از ارسال

۴-۲-۲- 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:

$$\begin{aligned} M_1 &= PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i, \\ D &= N_T \oplus K_i, \\ E &= PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i \end{aligned} \quad (14)$$

- (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 مورد نظر (T) بوده است، بنابراین پروتکل متوقف می‌شود. در صورتی که $T - t < \Delta t$ 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. در صورت 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 $I_{old} = M_1 \oplus K_{old}$ و $I_{new} = M_1 \oplus K_{new}$ محاسبه می‌کند و سپس این مقادیر را با اطلاعات دریافتی به صورت زیر مقایسه می‌کند.

$$I_X = PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \oplus PRNG(D \oplus K_X) \quad (15)$$

- در صورت 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 به دست آمد، مقداردهی می‌کند.

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

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

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

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 آنجایی که 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 احراز هویت 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 تغییراتی 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 به صورت 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.

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

شکل (۳). پروتکل پیشنهادی

- برچسب پیام دریافتی را با کلید مخفی ذخیره شده در خود، XOR کرده و برقراری رابطه زیر را بررسی می کند:

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

در صورت برقراری رابطه فوق برچسب هويت سرویس دهنده نهایی را تایید کرده و مقادیر مخفی خود را به صورت زیر به روزرسانی می کند:

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

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

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

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 بهبود یافته با استفاده از تابع $PRNG(N_T)$ ، بین پیام های D و E از یکدیگر

$$MAC = H(DATA \oplus t) \quad (۱۶)$$

اگر $X = new$ باشد، آنگاه سرویس دهنده نهایی مقادیر مخفی خود را به صورت زیر به روزرسانی می کند:

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

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

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

و اگر $X = old$ باشد عملیات به روزرسانی فقط برای C_i به صورت زیر انجام می شود:

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

- کارت خوان بعد از دریافت پیام از سرویس دهنده نهایی، با استفاده از RID و t مقدار $DATA$ دریافتی را به صورت $DATA = Info \oplus RID \oplus t$ به دست می آورد. در ادامه مقدار $H(DATA \oplus t)$ را محاسبه کرده و با پیام MAC دریافتی از سرویس دهنده نهایی مقایسه می کند. در صورت تساوی، کارت خوان هويت سرویس دهنده نهایی را تایید می کند و پیام M_2 دریافتی را به برچسب ارسال می کند.

۵- نتیجه گیری

در این مقاله، به تحلیل امنیت و محرمانگی یک پروتکل احراز هویت دوسویه در سامانه های RFID پرداخته شد. این پروتکل در سال ۲۰۱۳ ارائه شده است. نشان داده شد که برخلاف ادعای طراحان پروتکل، این پروتکل در مقابل حمله هایی نظیر کشف کلیدهای مخفی، جعل برچسب و ردیابی آسیب پذیر است. لذا این پروتکل نمی تواند امنیت و محرمانگی کاربران RFID را فراهم کند. در این مقاله، حمله ردیابی در قالب مدل اوفی- فان انجام شد. در ادامه، جهت رفع ضعف های 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 پروتکل های احراز هویت دوسویه که در سال های اخیر پیشنهاد شده است مورد مقایسه قرار گرفت و مشاهده شد که پروتکل پیشنهاد شده، در مقایسه با سایر پروتکل ها از امنیت و محرمانگی کاملی برخوردار است. در نهایت پیچیدگی و عملکرد پروتکل پیشنهادی با پروتکل های ارائه شده و موجود در این زمینه مقایسه گردیده است و مشاهده شد که با کمترین تغییرات در پیچیدگی پروتکل قادر به رفع ضعف های 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.

مستقل شده اند. لذا مهاجم نمی تواند 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 اندیشیده شده است. استفاده از کلید مخفی P_i و $PRNG(N_T)$ در ساختار پیام E و همچنین تغییر پیام M_1 به صورت $M_1 = PRNG(EPC_S \oplus N_R) \oplus PRNG(N_T) \oplus K_i$ مانع از انجام حمله جعل برچسب می شود.

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

در جدول های (۱ و ۲) به ترتیب مقایسه ای از تحلیل امنیتی و عملکردی پروتکل بهبود یافته با برخی از پروتکل های مشابه موجود آورده شده است. مشاهده می شود بر خلاف سایر پروتکل ها، امنیت و محرمانگی پروتکل بهبود یافته تأمین است.

جدول (۱). تحلیل امنیتی پروتکل ها

پروتکل بهبود داده شده	پروتکل SPRS [9]	پروتکل یون و همکارانش [8]	پروتکل یه و همکارانش [7]	پروتکل ها حمله ها
✓	×	×	✓	حمله کشف مقادیر مخفی
✓	×	×	×	حمله تکرار
✓	×	✓	✓	حمله جعل
✓	×	×	×	حمله ردیابی
✓	✓	✓	✓	حمله ناهمزمانی

امن: ✓ نامن: ×

جدول (۲). تحلیل عملکردی پروتکل ها: H تابع چکیده ساز، PRNG

تابع شبه عدد 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 کارت خوان	$2H + 10 \times PRNG$	$4H + 10 \times PRNG$	$4H + 10 \times PRNG$	$4H + 12 \times PRNG$

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.

Archive of SID

Archive of SID

Archive of SID

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

M. Mardani Shahrabak*, 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