مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۶۶- ۵۹

تحلیل امنیتی نسخه پروتکل بهبودیافته SPRS: یک پروتکل احراز اصالت برای سامانه‌های RFID

معصومه صفخانی[1*]

۱- استادیار، دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی

(دریافت: ۹۵/۰۱/۲۵، پذیرش: ۹۵/۱۰/۱۴)

چکیده

پروتکل‌های احراز اصالت یکی از ابزارهایی هستند که برای اطمینان از هویت طرفین ارتباط در فضای سایبری استفاده می‌شوند. اگر این چنین پروتکل‌هایی دارای ضعف باشند، امنیت فضای سایبری با تهدیدات جدی روبرو می‌شود که این تهدیدات در کاربردهای دفاعی از اهمیت فوق‌العاده‌ای برخوردار است. نویسندگان مقاله [۱]، با تحلیل یک پروتکل احراز اصالت به‌نام SPRS [۲]، توسط حملاتی مانند کشف مقادیر مخفی، جعل هویت برچسب و ردیابی برچسب، نسخه بهبودیافته این پروتکل را ارائه نموده‌اند. هم‌چنین ادعا شده که این پروتکل برخلاف نسخه پیشین خود هم در مقابل حملات وارده بر نسخه پیشین و هم در برابر دیگر حملات فعال و غیرفعال امن است. در این مقاله نشان داده می‌شود که پروتکل بهبودیافته هم در مقابل حمله کشف مقادیر مخفی و حمله ردیابی برچسب آسیب‌پذیر است و امنیت آن با دو نسخه برون‌خط و برخط از حمله کشف مقادیر مخفی به چالش کشیده می‌شود. اساس حمله‌های ارائه‌شده در این مقاله این است که با فرض $Y=PRNG(X)$ و این که تابع $PRNG$ یک تابع عمومی است و X و Y هر دو ۱۶ بیتی هستند، اجرای یک جستجوی جامع برای پیداکردن X به‌عنوان پیش‌تصویر Y با حداکثر 2^{16} ارزیابی بیرون از خط تابع $PRNG$ امکان‌پذیر می‌باشد. نسخه برون‌خط حمله با پیچیدگی یک‌بار شنود پروتکل و اجرای 2^{33} بار ارزیابی تابع $PRNG$ می‌تواند ۴ مقدار مخفی ۱۶ بیتی پروتکل یعنی مقادیر K_i، P_i، N_T و EPC_S را آشکار کند و نسخه برخط حمله با پیچیدگی دو بار جعل هویت برچسب‌خوان و اجرای 2^{17} بار ارزیابی تابع $PRNG$ می‌تواند این ۴ مقدار مخفی پروتکل را آشکار کند. با این حملات کشف مقادیر مخفی، پروتکل بهبودیافته SPRS درمقابل دیگر حملات فعال و غیرفعال دیگر هم امن نمی‌باشد. علاوه‌بر این، یک حمله ردیابی برچسب مستقل از طول تابع $PRNG$ ارائه می‌شود که با استفاده از آن حمله‌کننده قادر است برچسب را بین دو نشست با برچسب‌خوان ردیابی کند.

واژه‌های کلیدی: RFID، احراز اصالت، SPRS، محرمانگی، حمله افشای مقادیر مخفی، حمله ردیابی برچسب

۱- مقدمه

یکی از ابزارهای مورد استفاده برای تأمین امنیت فضای سایبری، پروتکل‌های احراز اصالت هستند که هویت طرفین ارتباط را برای یکدیگر اثبات می‌کنند. حال اگر این پروتکل‌های احراز اصالت دارای ضعف باشند، به‌راحتی با سوءاستفاده از این پروتکل‌ها افراد غیرمجاز و هم‌چنین مهاجمان می‌توانند امنیت فضای سایبری که از این‌گونه پروتکل‌ها استفاده می‌نمایند را با تهدید جدی مواجه نمایند. از این‌رو، تحلیل امنیتی و طراحی انواع پروتکل‌های امنیتی در حوزه سایبر به‌خصوص حوزه سایبر نیروهای نظامی و دفاعی از درجه بالای اهمیت برخوردار هستند. در این راستا، در منبع [۱] یک پروتکل احراز اصالت به نام SPRS [۲] که برای استفاده در سامانه‌های شناسایی از طریق امواج رادیویی یا همان RFID پیشنهادشده، مورد تحلیل امنیتی قرار گرفته است و حملات کشف مقادیر مخفی، جعل هویت برچسب و ردیابی برچسب به آن اعمال شده است. در همان منبع [۱]، نویسندگان نسخه بهبودیافته این پروتکل را نیز معرفی نموده و ادعا نموده‌اند که نسخه بهبودیافته ضعف‌های نسخه پیشین و دیگر ضعف‌ها را ندارد و برای اطمینان از احراز اصالت طرفین در فضای سایبری می‌تواند استفاده شود.

پروتکل SPRS بهبودیافته در چارچوب استاندارد EPC-C1G2 سامانه‌های RFID [۳] پیشنهاد شده است که در آن از PRNG به‌عنوان تابع تولید عدد شبه‌تصادفی ۱۶ بیتی، CRC و عملیات بیتی یای انحصاری $\oplus$ استفاده شده است. استاندارد EPC-C1G2 که یکی از استانداردهای مرتبط با برچسب‌های ارزان‌قیمت می‌باشد، سطح امنیتی مطلوبی ندارد و نقاط ضعف مختلفی از آن تاکنون گزارش شده است. برخی از نویسندگان طرح‌های جدیدی را برای تصحیح‌نمودن سطح امنیتی استاندارد EPC-C1G2، پیشنهاد نموده‌اند [۱۹-۴]. در بسیاری از تحقیقات اخیر سعی شده با استفاده از PRNGهای ۱۶ بیتی امنیتی فراتر از 2^{16} بیت فراهم کنند [۲-۱ و ۲۴-۲۱]. اما در مراجع [۲۶-۲۵]، نشان داده شده است که احتمالاً امکان رسیدن به امنیت لازم با تعداد محدودی فراخوانی یک PRNG ۱۶ بیتی وجود ندارد. در این

* رایانامه نویسنده مسئول: Safkhani@srttu.edu

مقاله نشان داده می‌شود که تلاش انجام‌شده در مرجع [۱] برای رسیدن به امنیتی فراتر از 2^{16} بیت تنها با استفاده از تعداد محدودی فراخوانی یک PRNG ۱۶ بیتی بی‌ثمر بوده است. دلیل اصلی این امر را می‌توان سهولت وارون‌کردن یک PRNG ۱۶ بیتی دانست که می‌توان به‌راحتی یک جدول از تمام حالات ممکن ورودی به آن تشکیل داد و خروجی آن را تولید و ذخیره کرد. در این صورت با داشتن خروجی PRNG ۱۶ بیتی به‌راحتی می‌توان ورودی‌هایی که منجر به آن خروجی می‌شوند را پیدا کرده و مورد ارزیابی قرار داد. برای تحلیل پروتکل معرفی‌شده در [۱]، در این مقاله از نمادهایی استفاده می‌شود که در جدول (۱) نشان داده شده است.

جدول (۱): نمادهای مورد استفاده در مقاله

نماد	شرح
R	برچسب‌خوان
T	برچسب
EPC_s	کد ۹۶ بیتی EPC به ۶ قطعه ۱۶ بیتی تقسیم شده است و سپس این ۶ قطعه برای تشکیل EPC_s با یک‌دیگر یای‌انحصاری می‌شوند.
$DATA$	اطلاعات مربوط به برچسب که در پایگاه داده نگه‌داری می‌شود.
K_i	کلید احرازاصالت که در برچسب ذخیره شده است و در مرحله $i+1$ ام پروتکل احراز اصالت توسط پایگاه داده بررسی خواهد شد.
P_i	کلید دسترسی که برای احراز اصالت پایگاه داده در مرحله $i+1$ ام در برچسب ذخیره شده‌است.
K_{old}, K_{new}	کلیدهای احراز اصالت قدیمی و جدید که در پایگاه داده ذخیره شده‌اند.
P_{old}, P_{new}	کلیدهای دسترسی قدیمی و جدید که در پایگاه داده ذخیره شده‌اند.
C_i	نمایه[1] سابقه اطلاعات i امین برچسب در پایگاه داده که در برچسب ذخیره شده است.
C_{old}, C_{new}	نمایه‌های قدیمی و جدید پایگاه داده برای i امین برچسب که در پایگاه داده ذخیره شده‌اند.
X	متغیری‌که یکی از مقادیر new و old را می‌پذیرد و نشان می‌دهد کدام کلید قدیمی یا جدید در سابقه پایگاه داده با مقادیر موجود در برچسب تطابق دارد.
$\oplus$	عمل یای انحصاری منطقی
A	دشمن
$B \leftarrow A$	اختصاص مقدار A به B
N_T, N_R	اعداد تصادفی که به‌ترتیب توسط برچسب‌خوان و برچسب انتخاب شده‌اند.
RID	شناسه برچسب‌خوان
$PRNG$	مولد اعداد شبه‌تصادفی ۱۶ بیتی

1- Index

نوآوری مقاله: در این مقاله، ما نسخه بهبودیافته SPRS را مورد تحلیل امنیتی قرار داده و نشان می‌دهیم که این نسخه هم مانند نسخه پیشین در مقابل حمله کشف مقادیر مخفی پروتکل آسیب‌پذیر است. با این حمله کلیه مقادیر مخفی پروتکل که عبارتند از ۴ مقدار ۱۶ بیتی K_i، P_i، N_T و EPC_s، آشکار می‌شود که در حالت معمول برای پیدا کردن آن‌ها به روش جستجوی جامع به 2^{64} عملیات نیاز هست. درنتیجه آشکارشدن تمام مقادیر پروتکل در حمله ارائه‌شده در این مقاله، می‌توان انواع حملات فعال و غیرفعال دیگر را نیز به پروتکل اعمال کرد. در این مقاله دو نسخه از حمله کشف مقادیر مخفی ارائه می‌شود. اولین نسخه حمله به‌صورت برون‌خط[2] ارائه می‌شود که دارای پیچیدگی 2^{33} است. دومین نسخه حمله به‌صورت برخط[3] ارائه می‌شود که دارای پیچیدگی 2^{17} است که هردوی این پیچیدگی‌ها تفاوت زیادی با پیچیدگی‌یافتن این ۴ مقدار مخفی ۱۶ بیتی به روش جستجوی جامع که برابر 2^{64} است، دارند. علاوه بر این، دو حمله کشف مقادیر مخفی با استفاده از ضعف کوتاه‌بودن طول تابع PRNG مورداستفاده، ارائه شده‌اند. در این مقاله، مستقل از این ضعف، یک حمله ردیابی هم ارائه می‌شود که تا زمانی که برچسب اطلاعات خود را به‌هنگام‌رسانی نکرده باشد، دشمن می‌تواند برچسب را بین دو نشست موفق با برچسب‌خوان ردیابی کند. در ادامه این مقاله و در بخش ۲، پروتکل SPRS بهبودیافته شرح داده می‌شود. نسخه‌های بیرون از خط و برخط حمله کشف مقادیر مخفی و نیز حمله ردیابی برچسب برعلیه این پروتکل در بخش ۳ شرح داده می‌شوند. در بخش ۴، توصیه‌هایی برای بهبود این پروتکل و دیگر پروتکل‌هایی که در چارچوب استاندارد EPC-C1 G2 پیشنهاد می‌شوند ارائه شده است و در نهایت این مقاله در بخش ۵ با بیان جمع‌بندی و نتیجه‌گیری به اتمام می‌رسد.

۲- معرفی پروتکل SPRS بهبودیافته

پروتکل SPRS بهبودیافته شبیه به پروتکل SPRS [۲] دارای دو مرحله آغازین و مرحله احراز اصالت است و تفاوت آن با پروتکل SPRS در نحوه محاسبه پیام‌های M_1 و E است که در ادامه شرح داده می‌شوند.

۲-۱- مرحله آغازین

در این مرحله، برچسب‌ها، برچسب‌خوان و سرور پایگاه داده

2- Offline
3- Online

مقداردهی می‌شوند، بدین‌صورت که در برچسب‌ها مقادیر (K_i, C_i, P_i, EPC_s)، در برچسب‌خوان مقدار RID و در پایگاه داده مقادیر قدیمی و جدید مرتبط به برچسب‌ها و برچسب‌خوان یعنی $(K_{old}, C_{old}, P_{old}, K_{new}, C_{new}, P_{new}, RID, EPC_s, DATA)$ ذخیره می‌شود.

۲-۲- مرحله احراز اصالت

پروتکل SPRS بهبودیافته، همان‌طورکه در شکل (۱) مشاهده می‌شود به‌صورت زیر اجرا می‌شود:

۱- ابتدا برچسب‌خوان عدد تصادفی N_R را تولید کرده و برای برچسب می‌فرستد.

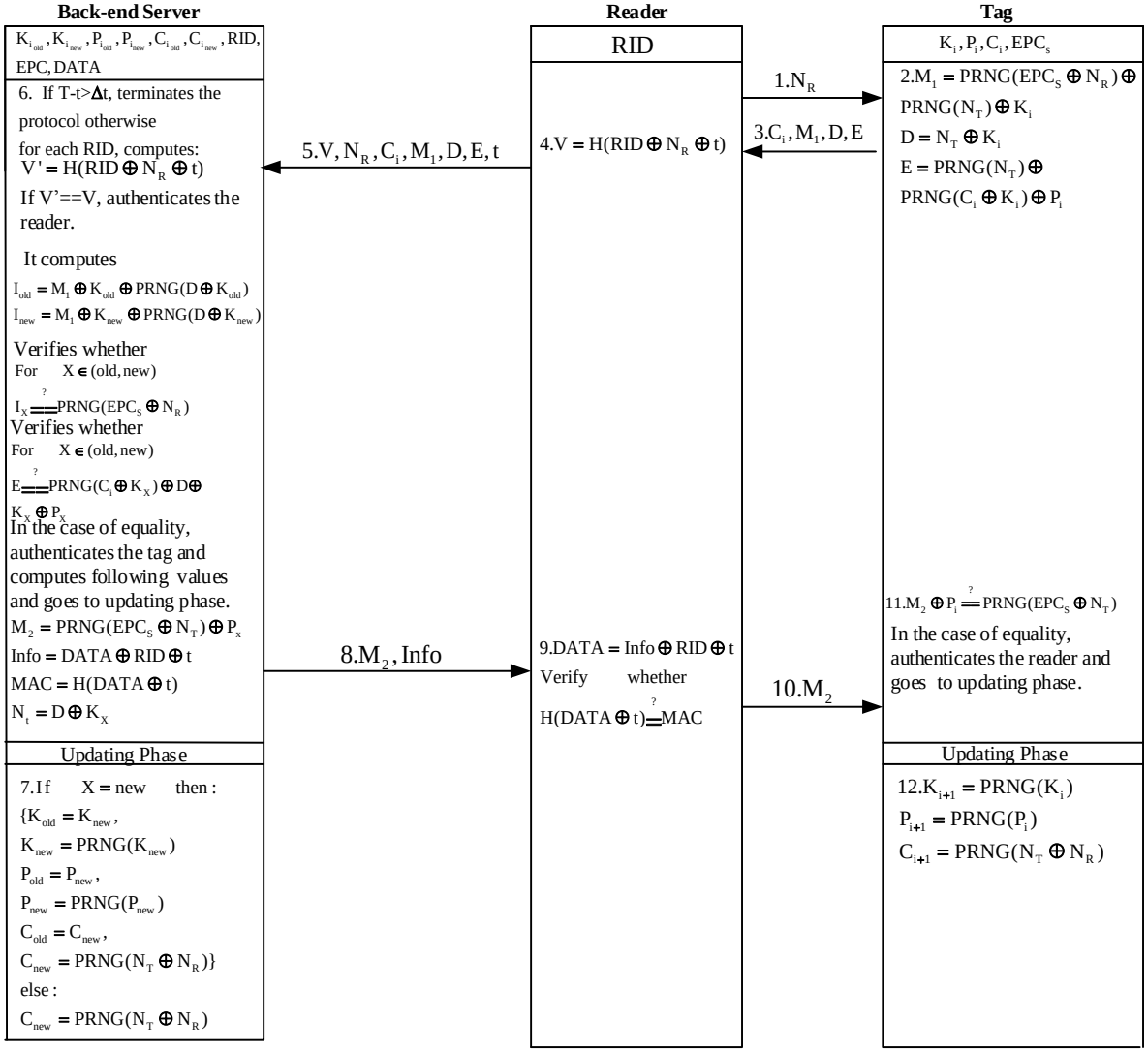
۲- برچسب به محض دریافت عدد تصادفی N_R:

- عدد تصادفی N_T را تولید می‌کند، (لازم به ذکر است که در شکل (۳) و منبع [۱]، نویسندگان یک عدد تصادفی دیگر هم به نام N_Z بیان کرده‌اند که در شرح پروتکل نیست و ما آن را یک اشتباه تایپی قلمداد کرده‌ایم چون در محاسبه پیام‌های پروتکل هم نقشی ندارد.)

- پیام‌های M_1، D و E را به‌صورت زیر محاسبه می‌کند:

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

- پیام (M_1, D, C_i, E) را برای برچسب‌خوان می‌فرستد.



شکل (۱): پروتکل SPRS بهبودیافته [۱]

۳- برچسب‌خوان به محض دریافت پیام، $V = H(RID \oplus N_R \oplus t)$ را محاسبه کرده و پیام $(M_1, D, C_i, E, N_R, V, t)$ را برای پایگاه داده می‌فرستد.

۴- پایگاه داده به محض دریافت پیام، اگر پیام در فاصله زمانی

مجاز دریافت نشده باشد یعنی $T-t>\Delta t$، اجرای پروتکل را متوقف می‌سازد. درغیر این‌صورت، برای هر شناسه برچسب‌خوانی یعنی RID:

- بررسی می‌کند که آیا $V \stackrel{?}{=} H(RID \oplus N_R \oplus t)$ برقرار است. درصورت برقراربودن، برچسب‌خوان را احراز اصالت می‌کند. سپس $I_{new} = M_1 \oplus K_{new} \oplus PRNG(D \oplus K_{new})$ را محاسبه می‌کند و بررسی می‌کند که آیا رابطه $I_{new} \stackrel{?}{=} PRNG(EPC_s \oplus N_R)$ برقرار است که درصورت برقراربودن، مقدار X را برابر new قرار می‌دهد.

- در غیر این‌صورت $I_{old} = M_1 \oplus K_{old} \oplus PRNG(D \oplus K_{old})$ را محاسبه می‌کند و بررسی می‌کند که آیا رابطه $I_{old} \stackrel{?}{=} PRNG(EPC_s \oplus N_R)$ برقرار است که درصورت برقراربودن، مقدار X را برابر old قرار می‌دهد.

- سپس بررسی می‌کند که آیا رابطه $PRNG(C_i \oplus K_X) \oplus D \oplus K_X \oplus P_X \stackrel{?}{=} E$ برقرار است؟ درصورت برقراربودن رابطه بالا، M_2، $Info$ و MAC را به‌صورت زیر محاسبه می‌کند و آن‌ها را برای برچسب‌خوان می‌فرستد.

$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$$
$$\inf o = DATA \oplus RID \oplus t$$
$$MAC = H(DATA \oplus t)$$
$$N_T = D \oplus K_x$$

- اگر $X = new$ باشد، پایگاه داده را به‌صورت زیر به‌هنگام می‌نماید:

$$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new})$$
$$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new})$$
$$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R)$$

- در غیر این‌صورت، پایگاه داده را به‌صورت زیر به‌هنگام می‌نماید: $C_{new} \leftarrow PRNG(N_T \oplus N_R)$

پس از این‌که برچسب‌خوان پیام را دریافت نمود، مقدار $DATA$ را به‌صورت $DATA = Info \oplus RID \oplus t$ استخراج می‌کند و بررسی می‌کند که آیا رابطه $H(DATA \oplus t) \stackrel{?}{=} MAC$ برقرار است که درصورت برقراربودن، پیام M_2 را برای برچسب ارسال می‌کند.

۶- برچسب به محض دریافت پیام، کارهای زیر را انجام می‌دهد:

بررسی می‌کند که آیا رابطه $M_2 \oplus P_i \stackrel{?}{=} PRNG(EPC_s \oplus N_T)$ برقرار است یا نه؟ اگر جواب منفی بود، پروتکل را متوقف می‌سازد.

- درصورت مثبت‌بودن پاسخ، اصالت برچسب‌خوان را احراز می‌کند و مقادیر خود را به‌صورت زیر به‌هنگام می‌نماید و به این ترتیب یک‌بار اجرای پروتکل به پایان می‌رسد.

$$K_{i+1} \rightarrow PRNG(K_i)$$
$$P_{i+1} \rightarrow PRNG(P_i)$$
$$C_{i+1} \rightarrow PRNG(N_T \oplus N_R)$$

۳- تحلیل امنیتی پروتکل SPRS بهبودیافته

در این قسمت، تحلیل امنیتی پروتکل SPRS بهبود یافته ارائه می‌شود که شامل نسخه‌های برون‌خط و بر خط حمله افشای مقادیر مخفی و حمله ردیابی است.

۳-۱- نسخه برون‌خط حمله افشای مقادیر مخفی

در این قسمت یک حمله مؤثر و برون‌خط ارائه می‌شود که می‌تواند اطلاعات مخفی برچسب مشتمل بر ۴ مقدار ۱۶ بیتی N_T، EPC_s، K_i و P_i را آشکار نماید. مشاهده اصلی که در واقع نکته مهم این حمله است این است که با فرض $Y = PRNG(X)$ و این که تابع $PRNG$ یک تابع عمومی است و X و Y هر دو ۱۶ بیتی هستند، اجرای یک جستجوی جامع و پیداکردن X به‌عنوان پیش‌تصویر Y با حداکثر 2^{16} ارزیابی برون‌خط تابع $PRNG$ امکان‌پذیر می‌باشد.

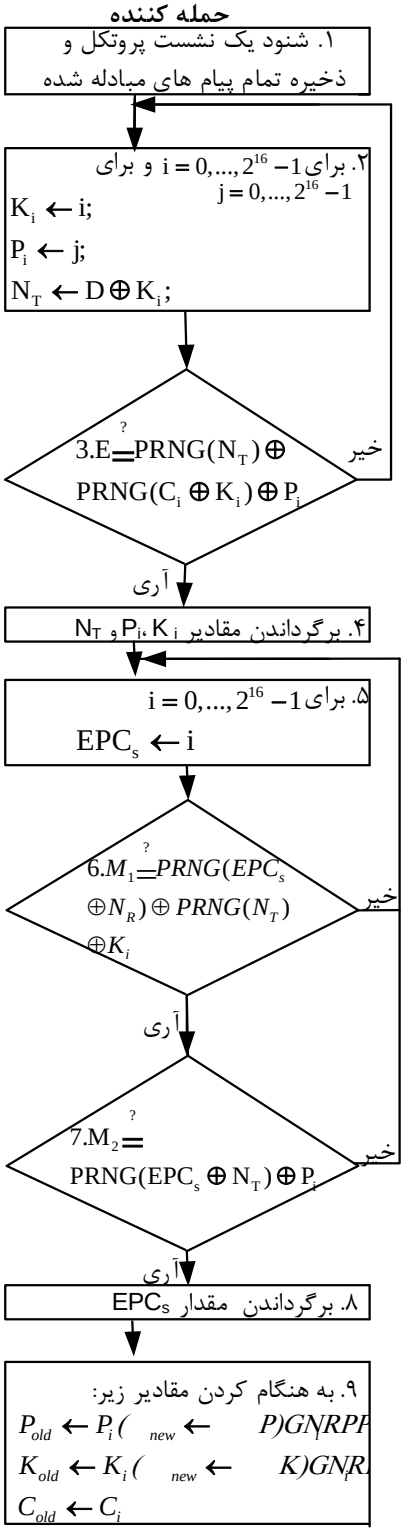
طبق مشاهده بالا و فرض این واقعیت که برچسب T_i با یک برچسب‌خوان قانونی R_i ارتباط برقرار می‌کند، دشمن می‌تواند تمام مقادیر مخفی T_i را همان‌طورکه در شکل (۲) مشاهده می‌شود، به‌صورت زیر آشکار نماید:

۱- یک نشست پروتکل را شنود می‌کند و تمام پیام‌های مبادله‌شده را ذخیره می‌نماید که در زیر نشان داده شده است.

$$M_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$$
$$D = N_T \oplus K_i$$
$$E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$$
$$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$$

۲- برای $i = 0,...,2^{16}-1$ و $j = 0,...,2^{16}-1$ به‌صورت زیر عمل می‌نماید:

- $K_i \leftarrow i$
- $P_i \leftarrow j$
- $N_T \leftarrow D \oplus K_i$



شکل (۲): نسخه بیرون از خط حمله کشف مقادیر مخفی

اگر $E \stackrel{?}{=} PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$، آن‌گاه مقادیر K_i، P_i و N_T را برمی‌گرداند.

۳- برای مقادیر برگردانده شده K_i، P_i و N_T از مرحله قبل (حدود 2^{16} سه‌تایی K_i، P_i و N_T) و برای $i = 0,...,2^{16}-1$ به‌صورت زیر عمل می‌کند:

$EPC_s \leftarrow i$ -

اگر $M_1 \stackrel{?}{=} PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$ و $M_2 \stackrel{?}{=} PRNG(EPC_s \oplus N_T) \oplus P_i$ برقرار باشند آن‌گاه مقدار EPC_s را برمی‌گرداند.

۴- مقادیر زیر را به‌هنگام می‌کند:

$P_{old} \leftarrow P_i, P_{new} \leftarrow PRNG(P_i)$
$K_{old} \leftarrow K_i, K_{new} \leftarrow PRNG(K_i)$
$C_{old} \leftarrow C_i$

پیچیدگی حمله فوق شنود یک نشست پروتکل بین برچسب و یک برچسب‌خوان قانونی و انجام $2^{32}=2^{16}\times2^{16}+2^{16}\times2^{16}+2^{32}=2^{33}$ ارزیابی تابع PRNG می‌باشد و دشمن اگر تنها یک پیش‌تصویر در هر یک از مراحل ۲ و ۳ حمله فوق بیابد، در حمله‌اش موفق می‌شود (باید توجه نمود که وجود حداقل یک پیش‌تصویر در هر مرحله ضمانت‌شده‌است). در غیر این‌صورت، باید چندین مرتبه حمله را تکرار نماید تا یک جواب یکتا بیابد. با به‌دست‌آمدن تمام مقادیر مخفی برچسب، می‌توان حملات زیر را به آسانی و با احتمال موفقیت "۱" و هزینه تنها یک‌بار اجرای پروتکل اعمال نمود:

- حمله ردیابی برچسب
- حمله جعل برچسب
- حمله جعل برچسب‌خوان
- حمله اخلال در هم‌زمانی

۳-۲- نسخه برخط حمله کشف مقادیر مخفی

در این قسمت نسخه برخط و فعال حمله کشف مقادیر مخفی ارائه می‌شود. برای این حمله، همان‌طور که در شکل (۳) مشاهده می‌شود، کافی است دشمن به‌صورت زیر عمل نماید:

گام ۱، جعل هویت برچسب‌خوان: در این مرحله، دشمن هویت یک برچسب‌خوان را جعل نموده و یک N_R را برای برچسب می‌فرستد و پاسخ‌های برچسب مشتمل بر C_i, M_1, D, E را به‌دست آورده و همان‌جا پروتکل را متوقف می‌سازد تا از به‌هنگام‌شدن مقادیر در برچسب و پایگاه داده جلوگیری نماید.

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

گام ۲، جعل مجدد هویت برچسب‌خوان: در این مرحله بار دیگر دشمن، هویت برچسب‌خوان را جعل نموده و دوباره همان N_R را برای برچسب می‌فرستد و پاسخ‌های برچسب مشتمل بر C_i, M'_1, D', E' را به‌دست آورده و همان‌جا پروتکل را متوقف می‌سازد تا از به‌هنگام‌شدن مقادیر در برچسب و پایگاه داده جلوگیری نماید. توجه نمایید که در این مرحله مقادیر مخفی مانند K_i همان مقادیر مخفی مرحله قبل هستند چون به‌هنگام نشده‌اند.

$$M'_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N'_T) \oplus K_i$$
$$D' = N'_T \oplus K_i$$
$$E' = PRNG(N'_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$$

گام ۳، حمله کشف مقادیر مخفی: در این مرحله دشمن برای کشف مقادیر مخفی به صورت زیر عمل می‌کند:

۱- مقدار $D \oplus D'$ را محاسبه می‌کند.

$$D \oplus D' = N_T \oplus K_i \oplus N'_T \oplus K_i = N_T \oplus N'_T$$

۲- مقدار $M_1 \oplus M_1'$ را به صورت زیر محاسبه می‌کند:

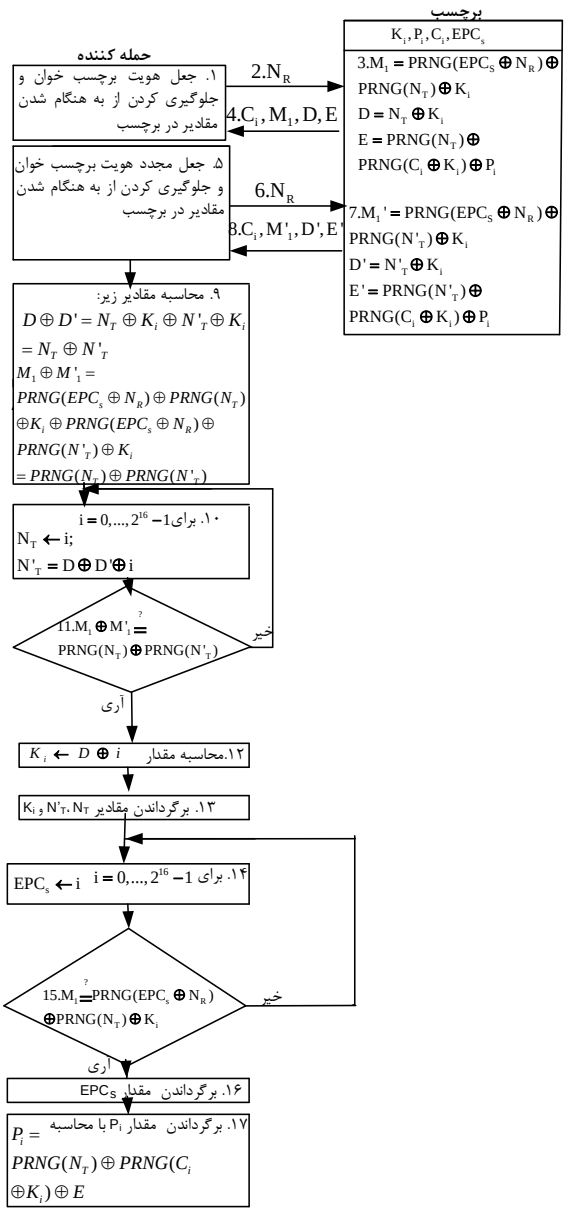
$$M_1 \oplus M'_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i \oplus PRNG(EPC_s \oplus N_R) \oplus PRNG(N'_T) \oplus K_i = PRNG(N_T) \oplus PRNG(N'_T)$$

برای $i = 0,...,2^{16}-1$ به صورت زیر عمل می‌نماید:

- $N_T \leftarrow i$
- $N'_T = D \oplus D' \oplus i$
- اگر $M_1 \oplus M'_1 \stackrel{?}{=} PRNG(N_T) \oplus PRNG(N'_T)$ آن‌گاه $K_i \leftarrow D \oplus i$ و مقادیر N_T ، N'_T و K_i را بر می‌گرداند.

۴- برای مقادیر برگردانده شده N_T، N'_T و K_i از مرحله ۳ و $i = 0,...,2^{16}-1$ به‌صورت زیر عمل می‌کند:

- $EPC_s \leftarrow i$
- اگر $M_1 \stackrel{?}{=} PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$ باشد مقدار EPC_s را بر می‌گرداند.
- مقدار $P_i = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus E$ را محاسبه و P_i را برمی‌گرداند.



شکل (۳): نسخه برخط حمله کشف مقادیر مخفی

پیچیدگی حمله فوق دو بار جعل هویت برچسب‌خوان و ارسال N_R برای برچسب، به‌دست‌آوردن و ذخیره پاسخ‌های آن‌ها و انجام $2^{17}=2\times2^{16}=2^{16}+2^{16}$ ارزیابی تابع PRNG می‌باشد و دشمن اگر تنها یک پیش‌تصویر در هر کدام از مراحل ۳ و ۴ گام ۳ حمله فوق بیابد، در حمله‌اش موفق می‌شود (باید توجه نمود که وجود حداقل یک پیش‌تصویر در هر مرحله ضمانت شده است.) در غیر این صورت، باید با مقادیر کاندیدا حمله را تکرار نماید تا یک جواب یکتا بیابد.

۳-۳- حمله ردیابی

حملات ارائه‌شده در قسمت‌های ۳-۱ و ۳-۲ وابستگی مستقیم به طول تابع PRNG دارند و اگر طول PRNG به اندازه کافی افزایش می‌یافت امکان اعمال حملات در عمل وجود نداشت. اما در این قسمت یک حمله ردیابی مستقل از طول تابع PRNG ارائه می‌شود. این حمله ضعف ساختاری در پروتکل SPRS بهبودیافته را نشان می‌دهد.

در پروتکل SPRS بهبودیافته مقادیری که برچسب در پاسخ به مقدار تصادفی ارسالی توسط برچسب‌خوان، N_R ، برمی‌گرداند، به‌صورت زیر است:

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

همان‌گونه که مشاهده می‌شود:

$$M_1 \oplus E = PRNG(EPC_s \oplus N_R) \oplus K_i \oplus PRNG(C_i \oplus K_i) \oplus P_i$$

که مستقل از مقدار تصادفی تولیدشده توسط برچسب است. در نتیجه اگر حمله‌کننده خود را به‌جای برچسب‌خوان جا بزند و یک مقدار تصادفی دلخواه ولی ثابت N_R را برای برچسب ارسال کند، تا زمانی‌که برچسب اطلاعات خود را به‌هنگام‌رسانی نکرده باشد، با مقدار $M_1 \oplus E$ همواره ثابت، روبه‌رو خواهد بود. این ویژگی می‌تواند برای ردیابی برچسب بین دو نشست موفق با برچسب‌خوان استفاده شود.

۴- بهبود پروتکل

حمله افشای مقادیر مخفی که در این مقاله بیان شد، به‌دلیل استفاده از PRNGهای ۱۶بیتی حاصل شده است. برای مقاوم‌نمودن پروتکل‌های امنیتی در مقابل این حمله استفاده از PRNGهای با طول بیش‌تر [۲۰] و یا الگوریتم‌های رمز قطعه‌ای سبک‌وزن به‌جای PRNG توصیه می‌شود.

برای مقاوم‌نمودن پروتکل در مقابل حمله ردیابی ارائه‌شده در این مقاله، باید به‌گونه‌ای پیام‌های رد و بدل‌شده را طراحی نمود که دشمن نتواند بین دو نشست که در آن دو مقادیر مخفی به‌هنگام نشده‌اند، از ترکیب پیام‌ها به یک مقدار ثابت برسد و از آن مقدار ثابت برای ردیابی برچسب استفاده نماید.

۵- نتیجه‌گیری

در این مقاله، دو نسخه مختلف از حمله کشف مقادیر مخفی را بر علیه پروتکل SPRS بهبودیافته ارائه شد. نسخه اول حمله، یک حمله بیرون از خط است که می‌تواند مقادیر مخفی پروتکل را با 2^{33} مرتبه ارزیابی تابع PRNG آشکار نماید. نسخه دوم حمله، یک حمله برخط است که می‌تواند مقادیر مخفی پروتکل را با 2^{17} مرتبه ارزیابی تابع PRNG آشکار نماید. هر دو نسخه حمله کشف مقادیر مخفی به‌صورت خاص ادعاهای طراحان پروتکل SPRS بهبودیافته را نقض می‌کنند. علاوه بر این، در این مقاله یک حمله ردیابی برچسب ارائه شد که مستقل از طول تابع PRNG مورد استفاده می‌باشد و با استفاده از آن حمله‌کننده قادر است که برچسب را بین دو نشست با برچسب‌خوان ردیابی کند.

حملات کشف مقادیر مخفی که در این مقاله ارائه شد که تمام خواص امنیتی پروتکل (محرمانگی، یک‌پارچگی و دسترس‌پذیری) را از بین می‌برند مبتنی بر این مشاهده بودند که ورودی PRNGهای ۱۶ بیتی به‌راحتی با استفاده از 2^{16} عملیات بیرون از خط قابل به‌دست‌آوردن هستند. برای جلوگیری از چنین آسیب‌پذیری بهتر است PRNGهای طولانی‌تر نظیر [۲۰] استفاده شوند و یا از الگوریتم‌های رمز قطعه‌ای سبک‌وزن در طراحی پروتکل‌های RFID متناسب با استاندارد EPC-C1G2 استفاده شود. اما حمله ردیابی ارائه‌شده بیان‌گر ضعف ساختاری پروتکل مورد ارزیابی است و با افزایش طول تابع PRNG قابل جلوگیری نیست.

تشکر و قدردانی

این پژوهش با حمایت مالی دانشگاه تربیت دبیر شهید رجایی طبق قرارداد شماره ۲۷۷۷۰ مورخ ۹۵/۱۰/۲۵ انجام‌گردیده‌است.

۶- مراجع

[1] M. Mardani Shahrbabak, B. Abdolmaleki, and K. Baghery, "Weaknesses of SPRS Authentication Protocol and Present a Developed Protocol for RFID Systems," Journal of Electronical & Cyber Defence, vol. 3, no. 3, pp. 39-48, 2016.

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

[3] "EP Cglobal Inc.," [Online]: Available:http://www.epcglobalinc.org. [Accessed 04 06 2016].

[4] M. Burmester, B. de Medeiros, J. Munilla, and A. Peinado, "Secure EPC Gen2 Compliant Radio Frequency Identification," in ADHOC-NOW, LNCS 5793, pp. 227-240, 2009.

[5] C.-L. Chen and Y.-Y. Deng, "Conformation of EPC Class 1 Generation 2 Standards RFID System with Mutual Authentication and Privacy protection," Eng. Appl. AI, vol. 22, no. 8, pp. 1284–1291, 2009.

[6] T. C. Yeh, Y. J. Wang, T. C. Kuo, and S. S. Wang, "Securing RFID systems conforming to EPC Class-1Generation-2 standard," Expert Syst. Appl., vol. 37, no. 12, pp. 7678-7683, 2010.

[7] E.-Y. Choi, D.-H. Lee, and J.-I. Lim, "Anti-cloning Protocol Suitable to EPCglobal Class-1 Generation-2 RFID Systems," Comp. Stand. Inter., vol. 31, no. 6, pp. 1124-1130, 2009.

[8] M. H. Habibi, M. R. Alaghband, and M. R. Aref, "Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard," in WISTP, LNCS 6633, pp. 254-263, 2011.

[9] M. H. Habibi, M. Gardeshi, and M. R. Alaghband, "Practical Attacks on a RFID Authentication Protocol Conforming to EPC C-1 G-2 Standard," IJU, vol. 2, no. 1, pp. 1-13, 2011.

[10] G. Jin, E.-Y. Jeong, H.-Y. Jung, and K.-D. Lee, "RFID Authentication Protocol Conforming to EPC Class-1 Generation-2 standard," Arabnia HR, Daimi K (eds) Security and Management, CSREA Press, USA, pp. 227–231, 2009.

[11] 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.

[12] N.-W. Lo and K.-H. Yeh, "A Secure Communication Protocol for EPCglobal Class 1 Generation 2 RFID Systems," in IEEE 24th international conference on advanced information networking and applications workshops, pp. 562–566, 2010.

[13] P. Peris-Lopez, J. C. H. Castro, J. M. Este´vez-Tapiador, and A. Ribagorda, "Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard," Comp. Stand. Inter., vol. 31, no. 2, pp. 372-380, 2009.

[14] P. Peris-Lopez, J. C. H. Castro, J. M. Este´vez-Tapiador, and A. Ribagorda, "RFID Specification Revisited," The internet of things: from RFID to the next-generation pervasive networked systems, Taylor& Francis Group, London, pp. 311-346, 2008.

[15] P. Peris-Lopez, J. C. Hernandez-Castro, J. E. Tapiador, and J. C. A. van der Lubbe, "Cryptanalysis of an EPC Class-1 Generation-2 Standard Compliant Authentication Protocol," Eng. Appl. AI, vol. 24, no. 6, pp. 1061-1069, 2011.

[16] P. Peris-Lopez, T. Li, and J. C. Hernandez-Castro, "Lightweight Props on the Weak Security of EPC Class-1 Generation-2 Standard," IEICE Trans., vol. 93-D, no. 3, pp. 518-527, 2010.

[17] P. Peris-Lopez, T. Li, J. C. Hernandez-Castro, and J. E. Tapiador, "Practical Attacks on a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard," Comput. Commun., vol. 32, no. 7-10, pp. 1185-1193, 2009.

[18] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA (extended abstract)," in Biryukov A(ed) FSE, LNCS 4593, pp. 181-195, 2007.

[19] K.-H. Yeh and N.-W. Lo, "Improvement of an EPC Gen2 Compliant RFID Authentication Protocol," in IAS. IEEE Computer Society, pp. 532-535, 2009.

[20] H. Martin, E. S. Millán, L. Entrena, J. C. H. Castro, and P. Peris-Lopez, "\Akari-x: A Pseudorandom Number Generator for Secure Lightweight Systems," in IOLTS, pp. 228-233, IEEE, 2011.

[21] H. Niu, E. Taqieddin, and S. Jagannathan, "EPC Gen2v2 RFID Standard Authentication and Ownership Management Protocol," IEEE Trans. Mob. Comput., vol. 15, no. 1, pp. 137-149, 2016.

[22] W. I. Khedr, "On the Security of Moessner's and Khan's Authentication Scheme for Passive EPCglobal C1G2 RFID Tags," I. J. Network Security, vol. 16, no. 5, pp. 369-375, 2014.

[23] S. Wang, S. Liu, and D. Chen, "Security Analysis and Improvement on Two RFID Authentication Protocols," Wireless Pers. Commun., vol. 82, no. 1, pp. 21-33, 2015.

[24] F. Moradi, H. Mala, and B. T. Ladani, "Cryptanalysis and Strengthening of SRP+ Protocol," ISCISC 2015, pp. 91-97, 2015.

[25] M. Safkhani, N. Bagheri, M. Hosseinzadeh, M. Eslamnezhad Namin, and S. Rostampour, "On the (im)possibility of receiving security beyond 2l using an l-bit PRNG: the case of Wang et. al. protocol," Wireless Pers. Commun., 2016. doi:10.1007/s11277-016-3623-z

[26] N. Bagheri, M. Safkhani, and H. Jannati, "Security Analysis of Niu et al. Authentication and Ownership Management Protocol," IACR Cryptology ePrint Archive 2015: 615 , 2015.

Cryptanalysis of the Improved SPRS Protocol: an Authentication Protocol for RFID Systems

M. Safkhani*
Shahid Rajaee Teacher Training University

(Received: 13/04/2016, Accepted: 03/01/2017)

ABSTRACT

Authentication protocols are tools used to ensure the identity of the parties in cyberspace. If these protocols are compromised, the cyber security is threatened. These threats are of paramount importance in military applications. Recently, in [1] *an authentication protocol, called SPRS has been considered and several attacks such as secret disclosure attack, tag impersonation attack and tag traceability attack have been applied on it. In addition, authors of that paper, presented the improved version of the protocol and claimed the improved protocol, unlike its predecessor, is secure against the attacks applied on the predecessor version and also other active and passive attacks.In this paper, we show that unfortunately, the security claims of authors do not hold and the improved protocol is also vulnerable against secret disclosure attack and tag traceability attack. We offer two versions of the secret disclosure attack which are offline and online versions. The basis of the attacks presented in this paper is that given Y=PRNG(X) and PRNG function is a public function and X and Y are 16 bits, performing an exhaustive search to find X as a pre-image of Y with a maximum of* 2^{16} *off-line evaluations of PRNG function is possible. The offline version of the attack with the complexity of one run of protocol eavesdropping and doing* 2^{33} *evaluations of PRNG function can disclose* 4 *secret values of protocol i.e.* K_i, P_i, N_T *and* EPC_S *which are 16 bits and the online version of the attack with the complexity of two times impersonating the reader and doing* 2^{17} *evaluations of PRNG function can disclose these 4 secret values of protocol. Given these secret disclosure attacks, the improved protocol is not secure against other active and passive attacks as well. In addition, we propose a tag traceability attack to trace a given tag which does not depend on the length of the output of the PRNG function. Given this attack, an adversary can trace a given tag between any two sessions with the reader.*

Keywords: RFID, Authentication, SPRS, Privacy, Secret Disclosure Attack, Tag Traceability Attack

* Corresponding Author Email: Safkhani@srttu.edu