تحلیل امنیتی پروتکل Seas: یک پروتکل احراز هویت در سیستم های RFID

معصومه صفخانی[۱]

نصور باقری[۲]، مجید نادری[۳]

چکیده

در این مقاله امنیت پروتکل SEAS[۱] که یک پروتکل احراز هویت در سیستم های RFID است، مورد تحلیل قرار می گیرد. تنها هدف امنیتی که پروتکل SEAS مطرح می نماید، احراز هویت واحد RFID برای بازخوان می باشد که ما در این مقاله نشان می دهیم که پروتکل در برآورده نمودن این هدف ناموفق بوده است. بنابراین، استفاده از پروتکل SEAS برای احراز هویت در هیچ کاربردی توصیه نمی شود.

در این مقاله یک حمله جعل واحد RFID بر علیه پروتکل SEAS مطرح می شود. حمله جعل واحد RFID، حمله ای است که موجب می شود، بازخوان حمله کننده را به عنوان یک واحد RFID معتبر و قانونی احراز هویت نماید و برای او دسترسی فراهم نماید. احتمال موفقیت حمله جعل واحد RFID ارائه شده در این مقاله که تا آنجایی که ما اطلاع داریم اولین حمله به این پروتکل است، «۱» و پیچیدگی آن تنها دو بار اجرای پروتکل SEAS می باشد.

کلید واژه

RFID، واحد RFID، بازخوان، احرازهویت، حمله جعل واحد RFID

۱- دانشجوی دکتری برق، دانشگاه علم و صنعت ایران m_safkhani@iust.ac.ir

۲- استادیار دانشکده برق، دانشگاه شهید رجایی

۳- دانشیار دانشکده برق، دانشگاه علم و صنعت ایران

تاریخ دریافت: ۹۰/۷/۱۲ تاریخ پذیرش: ۹۰/۸/۱۰

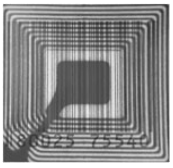
مقدمه

سیستم RFID سیستمی است که از امواج رادیویی برای شناسایی پدیده ها استفاده می نماید. این سیستم ها شامل واحد هایRFID ، امواج رادیویی و بازخوان های RFID می باشند. بازخوان های واحد RFID، سیگنال رادیویی را پخش می کنند تا بدین وسیله به داده ذخیره شده در واحد های RFID دسترسی پیدا نمایند. یکی از مهمترین تفاوت ها میان بارکدها و واحد های RFID این است که واحد های RFID یک شناسه یکتا یا یک اسم مستعار برای هر شیء فراهم می کنند. استفاده از واحدهای RFID مزایای بسیاری نسبت به بار کدها دارد. به عنوان مثال می توان به موارد زیر اشاره کرد: داده می تواند به صورت خودکار و حتی از طریق یک ماده نارسانا مانند مقوا و کاغذ خوانده شود. نرخ خواندن می تواند صدها بار در ثانیه و فاصله می تواند چندین متر باشد. شکل (۱) یک بارکد و شکل (۲) یک واحد RFID را نشان می دهد.

سیستم های RFID می توانند ابزار ارزشمندی باشند در فرآیند هایی مانند ساخت و مدیریت زنجیره تولید واحد های صنعتی و کنترل انبار. اما، فراگیرتر شدن سیستم های RFID به علت نگرانی در مورد حریم خصوصی افراد و نیز هزینه محدود شده است. از لحاظ اقتصادی می بایست هزینه واحدهای RFID بسیار اندک باشد که انگیزه کافی برای استفاده از آنها به عنوان جایگزین برای بارکدها وجود داشته باشد. علاوه بر این، برای استفاده از تمام مزایایی که واحد های RFID به صورت بالقوه پیشنهاد می نمایند، باید این شناسه در تمام طول عمر یک محصول اعم از تولید، توزیع، فروش و بازگشت دوباره به چرخه، با آن همراه شود. (شکل۳)

هزینه کم مورد انتظار برای واحدهای RFID غیر فعال که مد نظر این مقاله است، موجب می گردد که آنها منابع سخت افزاری خیلی محدودی داشته باشند. به طور معمول، آنها می توانند تنها چند صد بیت را ذخیره کنند، تقریباً بین ۵ کیلو تا ۱۰ کیلو گیت منطقی را دارا باشند و فاصله ارتباطی چند متر را داشته باشند. با این حساب، تنها میان ۲ تا ۴ کیلو گیت می تواند به توابع امنیتی اختصاص داده شود. جالب توجه است که به یاد آورده شود که برای پیاده سازی متداول رمز قطعه ای استاندارد AES بیش از ۵ کیلو گیت نیاز می باشد. بنابراین نمی توان از پیاده سازیهای متداول رمز AES در واحد های RFID استفاده نمود، اگر چه تلاشهای زیادی برای ارائه پیاده سازیهای کم حجم این الگوریتم در حال انجام است [۲]. هم چنین از هیچ کدام از این سیستم ها انتظار نمی رود که گذر واژه ها و یا دیگر مقادیر مخفی را به صورت امن ذخیره نمایند، زیرا واحدهای RFID به هیچ عنوان در مقابل حملات دستکاری فیزیکی مقاوم نیستند.

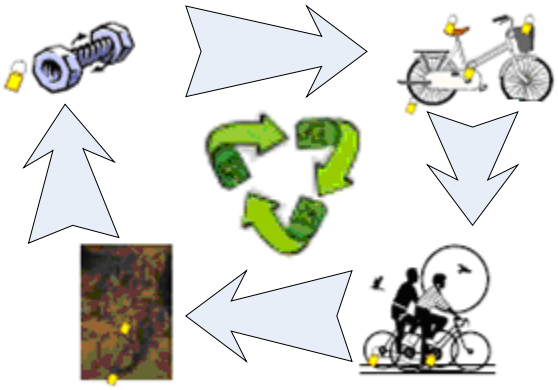
شکل ۱. بارکد [۳].



شکل ۲. واحد RFID [۳].

علیرغم تمام این محدودیت ها، نفوذ فناوری RFID به صورت آهسته و یکنواخت در حال گسترش می باشد. اعتقاد کارشناسان بر این است که هردوی این سیستم های شناسایی (RFID و بارکد ها) برای مدتی با هم وجود خواهند داشت و در نهایت واحدهای RFID به طور کامل جایگزین بارکدهای سنتی خواهند شد. بعضی از کاربردهای RFID عبارتند از :

- جایگزین مناسبی برای سیستم های قدیمی بارکد می باشد.
- ردیابی انسان، حیوان و اشیا را امکانپذیر نموده است.
- در سیستم های حمل و نقل و باجه های اخذ عوارض جاده ای کاربرد دارد.
- برای جلوگیری از دزدی امکان استفاده از آن می باشد.
- جعل اسناد مبتنی بر RFID کاری بسیار مشکلتر از اسناد سنتی می باشد.
- جهت کنترل دسترسی کاربرد دارد.
- در زنجیره تولید واحد های صنعتی قابل پیاده سازی است.
- در کنترل انبار، حمل و نقل کالا و خرده فروشی قابل استفاده است.
- جایگزین خوبی جهت نیروی انسانی نگهبان است.
- در کتابخانه ها هم برای ردیابی کتابها کاربرد دارد.
- فناوری RFID در مباحث پزشکی نیز قابل استفاده است.



شکل ۳. چرخه زندگی یک وسیله [۳].

شرح سیستم های RFID

اجزای سیستم RFID

یک سیستم RFID عموماً متشکل از دو جزء اصلی می باشد: واحد RFID و بازخوان RFID.

الف) واحد RFID

در یک سیستم RFID، هر شی با یک واحد RFID نشانه گذاری می شود. هر واحد RFID مشتمل بر

یک ریز تراشه با مقداری قابلیت های محاسباتی و ذخیره سازی و یک واحد ارتباطی مانند یک سیم پیچ آنتن می باشد. اطلاعات فراهم شده توسط واحدهای RFID معمولاً نام پایگاه اطلاعات داده را به خود می گیرند. محدودیت های جدی در پردازش و ذخیره سازی موجب می شود که اطلاعات ذخیره شده در واحد های RFID محدود باشند. واحد های RFID می توانند بر حسب دو معیار مهم تقسیم بندی شوند که عبارتند از:

۱. نوع حافظه: واحد حافظه می تواند به عنوان منبع داده خواندن و نوشتن به کار گرفته شود. واحد های RFID می توانند به صورت های فقط خواندنی ، یکبار نوشتن - بسیار خواندن و یا قابل خواندن و نوشتن برنامه ریزی شوند. بسته به نوع واحد RFID، برنامه ریزی واحد RFID می تواند در مرحله ساخت و یا مرحله استفاده انجام شود.

۲. منبع انرژی: واحد RFID می تواند انرژی را از سیگنال دریافت شده از بازخوان بدست آورد و یا منبع انرژی داخلی داشته باشد. عموماً راهی که واحد RFID، انرژی را به آن طریق بدست می آورد، دسته واحد RFID را تعریف می کند. بنابراین واحد های RFID را از نقطه نظر منبع انرژی می توان به گروه های زیر تقسیم بندی نمود:

- واحد های RFID غیر فعال : واحدهای RFID غیر فعال منبع انرژی داخلی ندارند. آنها انرژی اشان را از امواج الکترومغناطیسی که توسط بازخوان فرستاده می شود، بدست می آورند و از این انرژی هم برای به راه انداختن مدارات خود و هم برای ارتباط استفاده می نمایند.
- واحد های RFID نیمه فعال : واحدهای RFID نیمه فعال از یک باتری برای به راه انداختن مدارات خود استفاده می کنند ولی برای برقراری ارتباط از انرژی بدست آمده از سیگنال بازخوان استفاده می نمایند.
- واحد های RFID فعال : واحدهای RFID فعال دارای منبع انرژی ای می باشند که از آن هم برای به راه انداختن مدارات خود و هم برای پخش کردن سیگنال به واحد بازخوان استفاده می نمایند.

ب) بازخوان RFID

به صورت کلی، بازخوان های RFID شامل یک مجموعه RF، یک واحد کنترل و یک واحد ارتباطی برای بررسی واحد های RFID الکترونیکی از طریق ارتباط رادیویی می باشند. در مقایسه با واحدهای RFID، بازخوان ها ممکن است که قابلیت های ذخیره سازی و پردازش داخلی بهتری داشته باشند و بسیاری از اوقات به سرور وصل می شوند. محاسبات پیچیده نظیر تمام انواع عملیات رمزنگاری معمولاً توسط واحد های بازخوان انجام می شود چرا که معمولاً محدودیت های آنها کمتر از واحدهای RFID می باشد. در بیشتر سیستم های RFID به صورت کلی فرض شده است که ارتباط بین بازخوان ها و سرور امن می باشد، چرا که محدودیت های پردازش و ذخیره سازی در بازخوان ها چندان جدی نمی باشند و راه حل های معمولی مانند SSL/TLS می توانند استفاده شوند.

روش های ارتباط بازخوان و واحد RFID

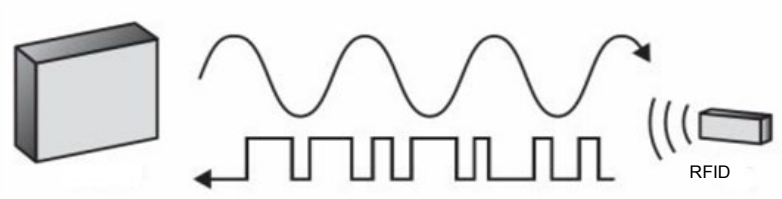
یکی از مهمترین اهداف ارتباط بازخوان با واحد های RFID، فعال نمودن واحد های RFID غیر فعال با

فراهم نمودن انرژی تماس کافی برای آنها می باشد. دو نوع روش برای انتقال انرژی به واحد های RFID غیر فعال به صورت بی سیم وجود دارد:

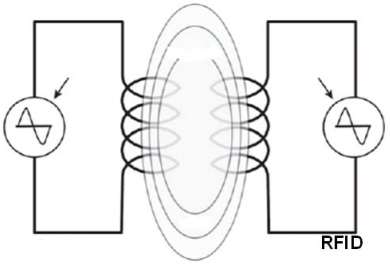
انتقال انرژی مبتنی بر تشعشع: در این روش، بازخوان یک سیگنال رادیویی منتشر می نماید. هنگامی که واحد RFID در حیطه بازخوان ظاهر شود، این سیگنال را دریافت و آن را با یک مدار یکسو کننده، به جریان مستقیم تبدیل می نماید و این انرژی را با شارژ کردن یک خازن ذخیره می کند.

انتقال انرژی مبتنی بر القاء: در این روش، آنتن بازخوان از جریان عبوری از آن برای تولید یک میدان مغناطیسی استفاده می نماید که این میدان مغناطیسی جریانی را در آنتن واحد های RFID القا می کند که همین جریان، تراشه واحد RFID را تغذیه می نماید.

بعد از تحصیل انرژی، واحد RFID شروع به پردازش درخواست بازخوان می نماید که معمولاً این کار را با دمدولاسیون دامنه موج حامل بازخوان و دیکد نمودن سیگنال باند پایه انجام می دهد. برای پاسخ دادن، واحد RFID، پیام مورد نظر را به یک رشته باینری طولانی تر کد می نماید و امپدانس بار آنتن خود را مطابق با رشته داده تطبیق می کند که موجب مدولاسیون دامنه سیگنالی می شود که بعداً باید (در انتقال انرژی مبتنی بر تشعشع) منعکس شود و یا موجب مدولاسیون میدان مغناطیسی ملحق به واحد بازخوان و واحد RFID (در انتقال انرژی مبتنی بر القا) می شود.



شکل ۴. انتقال انرژی مبتنی بر تشعشع [۳].



شکل ۵. انتقال انرژی مبتنی بر القاء [۳].

واحد های RFID معمولاً از روش کدینگی مانند کدهای منچستر استفاده می نمایند که در آن کد نمودن هر بیت داده حداقل یک بیت گذار دارد، مثلاً و دو نمونه از این کدهای منچستر را نشان می دهند. یک مزیت استفاده از کد منچستر یا گونه های آن، این است که اگر دو واحد RFID تقریباً در یک زمان به واحد بازخوان پاسخ دهند، بیت منتجه حالت گذار را از دست خواهد داد، مثلاً که به عنوان یک کد غیر عادی تعبیر می شود. بنابراین، این کد غیر عادی، به بازخوان وقوع یک برخورد را اطلاع می دهد. در واقع ساز و کار

ضد برخورد ، یک عنوان مهم تحقیق در جامعه RFID می باشد که عمومی ترین پاسخ برای آن، مبتنی بر دسترسی چندگانه تقسیم زمانی TDMA می باشد که در آن یک بازه زمانی، به بخش هایی تقسیم می شود که بازخوان در هر بخش فقط با یک واحد RFID ارتباط برقرار می کند.

روش ارتباط بازخوان با واحد RFID به صورت سئوال- پاسخ می باشد. یعنی بازخوان یک درخواست برای واحد RFID ارسال می نماید و واحد RFID مطابق دانش خود، پاسخی را محاسبه و آن را برای بازخوان می فرستد و خود را در حالت بعدی قرار می دهد. سپس اگر بازخوان پیش از این اطلاعات مطلوب را بدست آورده باشد، نشست حاضر متوقف می شود و واحد RFID حالت خود را بازنشانی می نماید. در غیر این صورت بازخوان به سئوال نمودن و واحد RFID به پاسخ دادن ادامه می دهند و حالت خود را تغییر می دهند. توجه شود که اغلب از یک پروتکل برای شرح خلاصه مبادلات بین بازخوان و واحد RFID استفاده می شود.

امنیت سیستم های RFID

امن نگهداشتن سیستم های RFID بسیار مهم می باشد، زیرا به دلیل انتقال اطلاعات به صورت بیسیم و در یک محیط غیر ایمن، در مقابل تعدادی از حملات بدخواهانه مانند استراق سمع، جعل و یا خطرهای فیزیکی (مانند دستکاری) آسیب پذیر می باشند. مسائل امنیتی برای واحد های RFID ارزان قیمت بسیار چالش برانگیز تر می باشند، چرا که در این سیستمها استفاده از بسیاری از روش های امنیتی سنتی مانند رمزگذاری / رمزگشایی متقارن و توابع درهم ساز ، به علت محدودیت منابع واحد های RFID ارزان قیمت، غیر عملی می باشد.

با گسترش کاربرد فناوری RFID، باید بیش از پیش به مسائل حریم شخصی و امنیت آن توجه نمود. امروزه مسائل امنیتی عامل های مهمی گردیده اند که مانع گسترش کاربردهای فناوری RFID در مقیاس بزرگ می شوند. حل کردن مسائل حریم خصوصی و امنیت سیستم های RFID کار تحقیقاتی چالش برانگیزی می باشد که نکته کلیدی در توسعه بیشتر فناوری RFID است. از این رو در متون علمی، پروتکل های احراز هویت بسیاری پیشنهاد شده اند [۴-۲۱] که پس از ارائه، توسط دیگر محققان تحلیل شده اند و نشان داده شده است که بیشتر این پروتکل ها در تامین اهداف امنیتی خود ناموفق بوده اند [۲۲-۳۵].

در سال ۲۰۰۹، میسرا و همکارانش در مرجع [۱] پروتکل SEAS را برای به کارگیری به منظور احراز هویت واحدهای RFID غیر فعال پیشنهاد نمودند. طراحان پروتکل SEAS ادعا کرده اند که پروتکل آنها، به واسطه تولید اعداد تصادفی و نیز به کارگیری عملیات ساده مانند یای انحصاری و انتقال حداقل بیت ها، بسیار بهینه است و از لحاظ کارایی و هزینه، در مقایسه با دیگر طرح های مطرح، بسیار بهتر از آنها است و مهم تر از همه آنکه، آنها مدعی هستند که این پروتکل در مقابل انواع حملات متداول مقاوم است.

در این مقاله ما اثبات می نماییم که پروتکل SEAS در مقابل حمله جعل واحد RFID آسیب پذیر است. این حمله نشان می دهد که این پروتکل در برآوردن تنها هدف خود (که احراز هویت واحد های RFID است) ناموفق می باشد.

در ادامه این مقاله و در بخش ۲ پروتکل SEAS به صورت مفصل شرح داده می شود. در بخش ۳، حمله جعل واحد RFID معرفی و چگونگی اعمال آن بر پروتکل SEAS بیان می شود و نشان داده می شود که چگونه این حمله موجب می شود که بازخوان دشمن را به عنوان یک واحد RFID مجاز، احراز هویت کند

و برای او دسترسی به سیستم را فراهم آورد. این مقاله با بحث و نتیجه گیری در بخش ۴ به پایان می رسد.

پروتکل SEAS

نمادها و فرضیات پروتکل

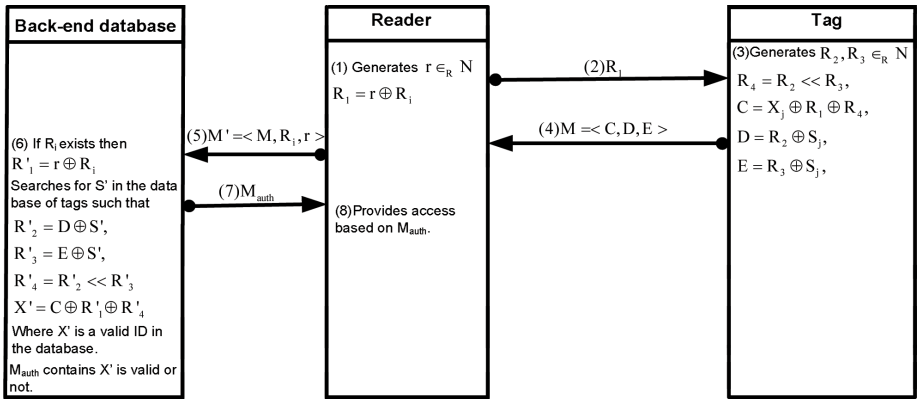
جدول ۱ نمادها و علائمی که طراحان پروتکل SEAS استفاده نموده اند و در این مقاله نیز استفاده می شوند، را به صورت خلاصه نشان می دهد. طراحان پروتکل SEAS فرض نموده اند که هر واحد RFID به نام T_j شناسه خود یعنی X_j و مقدار مخفی خود که با سرور به اشتراک نهاده است یعنی S_j را ذخیره می نماید و هر بازخوان به نام R_i نیز شناسه خود یعنی R_i را ذخیره می کند. همینطور فرض شده است که سرور، شناسه هر بازخوان (یعنی R_i) و شناسه هر واحد RFID (یعنی X_j) و مقدار مخفی متناظر با آن (یعنی S_j) را در سطرهای جداگانه ذخیره می کند.

شرح پروتکل

شکل ۶ عملیات انجام گرفته در پروتکل SEAS را نشان می دهد. این پروتکل به صورت زیر کار می کند:

علامت	شرح
R_i	شناسه بازخوان به نام R_i
X_j	شناسه واحد RFID به نام T_j
S_j	مقدار مخفی مشترک بین T_j و R_i
$\oplus$	عملیات یای انحصاری
,	عملگر الحاق (به دنبال هم قرار گرفتن)
N	مجموعه اعداد صحیح تنیه مثبتی
$x \in_R N$	انتخاب به صورت یکنواخت x از مجموعه N
$\ll$	انتقال به سمت چپ

جدول ۱. نمادها و علامت های مورد استفاده در پروتکل SEAS.



شکل ۶. پروتکل احراز هویت SEAS [۱].

۱- بازخوان اجرای پروتکل SEAS را آغاز می نماید، بدین صورت که یک عدد تصادفی r را انتخاب می نماید و شناسه خود یعنی R_i را با آن یای انحصاری می کند و متغیر $R_1 = r \oplus R_i$ را تولید می نماید. سپس R_1 را برای واحد RFID یعنی T_j ارسال می کند.

۲- واحد RFID یعنی T_j، به محض دریافت پیام، دو عدد تصادفی R_2 و R_3 را تولید می کند. سپس R_2 را به اندازه تعداد "یک" های موجود در نمایش بیتی R_3 به سمت چپ دوران می دهد که حاصل این عمل R_4 نامیده می شود. بنابراین می توان متغیر R_4 را به صورت $R_4 = R_2 << R_3$ نمایش داد. طراحان بیان کرده اند که این نحوه تولید R_4، موجب تصادفی به نظر رسیدن این متغیر می گردد. سپس T_j متغیرهای $C = X_j \oplus R_1 \oplus R_4$، $D = R_2 \oplus S_j$ و $E = R_3 \oplus S_j$ را محاسبه و از به دنبال هم قرار دادن آنها پیام $M =< C, D, E >$ را می سازد و آن را به منظور احراز هویت خود برای بازخوان می فرستد.

۳- بازخوان به محض دریافت این پیام، R_i و r را به دنبال پیام M قرار می دهد و پیام $M' =< M, R_i, r >$ را برای سرور ارسال می نماید.

۴- سرور به محض دریافت این پیام بررسی می کند که آیا R_i در پایگاه داده موجود می باشد یا نه؟ اگر موجود باشد، سرور بازخوان را احراز هویت می کند و در غیر این صورت بازخوان را احراز هویت نمی کند و پروتکل متوقف می شود. درصورت احراز هویت بازخوان، سرور r را با R_i یای انحصاری می نماید و بدین ترتیب R'_1 را محاسبه می کند. ($R'_1 = R_i \oplus r$) سپس در پایگاه داده به دنبال 'S می گردد به گونه ای که $R'_2 = D \oplus S'$، $R'_3 = E \oplus S'$ و $R'_4 = R'_2 << R'_3$ منجر به تولید $X' = C \oplus R'_1 \oplus R'_4$، که یک شناسه معتبر در پایگاه داده باشد، گردند. به عنوان حاصل ارزیابی، نتیجه این موضوع که آیا 'X معتبر است یا نه را در قالب پیام M_{auth} برای بازخوان ارسال می نماید. بدین ترتیب یک بار اجرای پروتکل خاتمه می یابد. به عنوان یک مثال عددی (البته با فرض طول بیت ۸ برای متغیرها)، فرض کنید مقادیر مورد نظر در یک بار اجرای پروتکل به صورت زیر باشند:

$$\left.\begin{array}{l} R_i = 11010010 \\ r = 01011101 \end{array}\right\} \Rightarrow R_1 = R_i \oplus r = 10001111$$

$$S_j = 01000110$$

$$X_j = 10101100$$

$$\left.\begin{array}{l} R_2 = 11010001 \\ R_3 = 00101100 \end{array}\right\} \Rightarrow R_4 = R_2 << R_3 = 10001110$$

آنگاه، مقادیر محاسبه شده توسط واحد RFID به صورت زیر است:

$$C = X_j \oplus R_1 \oplus R_4 = 10101100 \oplus 10001111 \oplus 10001110 = 10101101$$

$$D = R_2 \oplus S_j = 11010001 \oplus 01000110 = 10010111$$

$$E = R_3 \oplus S_j = 00101100 \oplus 01000110 = 01101010$$

$$M = \langle C, D, E \rangle = \langle 10101101, 10010111, 01101010 \rangle$$

مقادیر انتقالی از بازخوان به سرور به صورت زیر خواهد بود:

$$M' = \langle M, R_i, r \rangle = \langle 10101101, 10010111, 01101010, 11010010, 01011101 \rangle$$

محاسبات انجام گرفته توسط سرور، از قرار زیر است:

$$R'_1 = R_i \oplus r = 11010010 \oplus 01011101 = 10001111$$
$$R'_2 = D \oplus S' = 10010111 \oplus 01000110 = 11010001$$
$$R'_3 = E \oplus S' = 01101010 \oplus 01000110 = 00101100$$
$$R'_4 = R'_2 << R'_3 = 10001110$$
$$X' = C \oplus R'_1 \oplus R'_4 = 10101101 \oplus 10001111 \oplus 10001110 = 10101100$$

و از آنجایی که بازآوری شده، یک مقدار معتبر است، در نتیجه سرور، هویت واحد RFID را تأیید می کند و آن را در قالب پیام برای واحد بازخوان ارسال می کند.

طراحان پروتکل SEAS ادعا نموده اند که پروتکل آنها در مقابل حملات مختلف امن است. ولی ما در قسمت بعد نشان می دهیم که این پروتکل نه تنها امن نیست، بلکه در بر آوردن تنها هدف خود نیز که در واقع احراز هویت صحیح واحد های RFID و فراهم نمودن دسترسی برای واحد های RFID معتبر می باشد، ناموفق بوده است.

تحلیل امنیتی پروتکل SEAS

حمله جعل واحد RFID

حمله جعل واحد RFID یکی از انواع حملات جعل می باشد که موجب می شود بازخوان حمله کننده را به عنوان یک واحد RFID مجاز احراز هویت نماید. یک پروتکل احراز هویت امن باید در مقابل انواع حملات جعل، حملات اخلال در همزمانی، حملات افشای شناسه، حملات ردیابی، حملات تکرار، حملات مرد میانی و دیگر حملات فعال و غیر فعال مقاوم باشد.

آسیب پذیری پروتکل SEAS در مقابل حمله جعل واحد RFID، نشان می دهد که این پروتکل نمی تواند عملیات احراز هویت را به صورت امن انجام دهد و از این رو استفاده از آن در هیچ سیستمی توصیه نمی شود.

شرح حمله جعل واحد RFID

همانطور که در شکل ۷ نشان داده شده است، حمله جعل واحد RFID ما دارای دو مرحله می باشد: مرحله شنود و مرحله جعل.

مرحله ۱(مرحله شنود): حمله کننده ابتدا یک اجرای موفق پروتکل، میان یک بازخوان قانونی R_i و یک واحد RFID قانونی T_j را شنود می کند و پیامهای مبادله شده بین آنها یعنی R_1، C، D و E را بدست می آورد و آنها را ذخیره می نماید.

مرحله ۲(جعل): در این مرحله حمله کننده منتظر می ماند تا بازخوان احراز هویت دیگری را آغاز نماید و R_{1new} را برای واحد RFID مورد نظر ارسال کند. سپس حمله کننده R_{1new} را بدست می آورد و مانع رسیدن آن به واحد RFID می شود و خود را به عنوان واحد RFID مورد نظر یعنی T_j جا زده و به صورت

زیر عمل می نماید:

۱- حمله کننده به محض دریافت پیام R_{1new}، مقادیر C و R_1 را که در مرحله قبل شنود نموده و ذخیره کرده است را با هم یای انحصاری می کند و حاصل آن را با R_{1new} که در این مرحله دریافت نموده یای انحصاری می کند و بدین ترتیب متغیر C_{new} را محاسبه می کند ($C_{new} = C \oplus R_1 \oplus R_{1new}$). حمله کننده هم چنین از مقادیر D و E هم که در مرحله قبل شنود و ذخیره نموده است، به ترتیب به عنوان مقادیر D_{new} و E_{new} استفاده می کند ($D_{new} = D$ و $E_{new} = E$). سپس از به دنبال هم قرار دادن C_{new}، D_{new} و E_{new}، پیام M_{new} را می سازد که برابر است با $M_{new} =< C_{new}, D_{new}, E_{new} >$ و آن را به منظور احراز هویت خود برای بازخوان می فرستد.

۲- بازخوان به محض دریافت این پیام، R_i و r' را به دنبال پیام M_{new} قرار می دهد و پیام $M'_{new} =< M_{new}, R_i, r' >$ را برای سرور ارسال می کند.

۳- سرور به محض دریافت این پیام بررسی می کند که آیا R_i در پایگاه داده موجود می باشد یا نه؟ که موجود می باشد پس سرور بازخوان را احراز هویت می کند. پس از احراز هویت بازخوان، سرور با یای انحصاری نمودن R_i و r'، مقدار R'_{1new} را محاسبه می کند ($R'_{1new} = R_i \oplus r'$) سپس در پایگاه داده به دنبال یک مقدار معتبر برای X' می گردد. از آن جایی که حمله کننده پیام های D و D_{new} که در مرحله قبل بدست آورده را بدون تغییر به ترتیب به عنوان D_{new} و E_{new} برای بازخوان ارسال کرده است، پس داریم:

$$
\begin{aligned}
&R'_2 = D \oplus S' = R_2 \\
&R'_3 = E \oplus S' = R_3 \\
&R'_4 = R'_2 << R'_3 = R_2 << R_3 = R_4 \\
&X' = C_{new} \oplus R'_{1new} \oplus R'_4 = C \oplus R_1 \oplus R'_{1new} \oplus R'_{1new} \oplus R_4 = \\
&X_j \oplus R_1 \oplus R_4 \oplus R_1 \oplus R_4 = X_j
\end{aligned}
\qquad (۱)
$$

بنابراین برابر می شود که یک شناسه معتبر در پایگاه داده می باشد و بازخوان حمله کننده را به عنوان یک واحد RFID قانونی احراز هویت می کند و برای او دسترسی فراهم می کند. بدین ترتیب پروتکل SEAS در برآوردن تنها هدف خود که احراز هویت واحدهای RFID می باشد، ناموفق می باشد. احتمال موفقیت حمله ما برابر "۱" و پیچیدگی آن تنها دو بار اجرای پروتکل می باشد. همانگونه که مشاهده می شود، موفقیت حمله کننده قطعی و پیچیدگی آن تنها دو بار اجرای پروتکل است.

حال حمله را با یک مثال عددی، با فرض طول بیت ۸ برای مقادیر متغیرها، تشریح می کنیم. فرض کنید، که حمله کننده مقادیر انتقالی از طریق کانال در مرحله قبل را ذخیره کرده باشد:

فرض کنید که مقدار ارسالی توسط بازخوان در مرحله بعد به صورت زیر باشد:

$$R_{1new} = 11000110$$

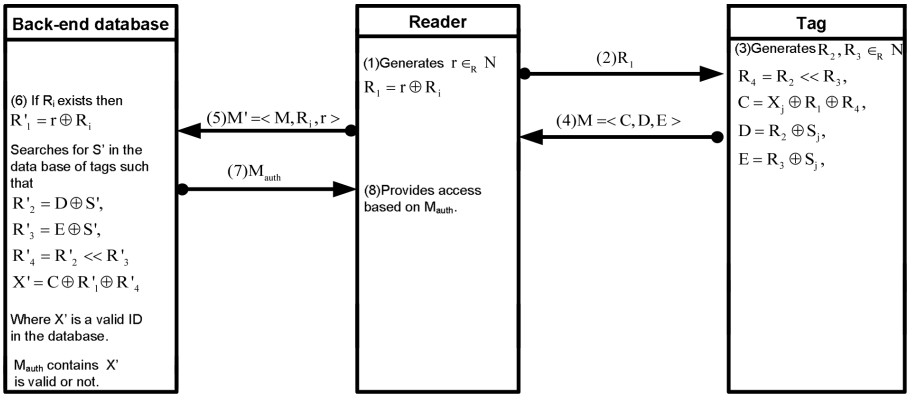
در پاسخ، حمله کننده محاسبات زیر را انجام می دهد:

$$C_{new} = C \oplus R_1 \oplus R_{1new} = 10101101 \oplus 10001111 \oplus 11000110 = 11100100$$
$$D_{new} = D = 10010111$$
$$E_{new} = E = 01101010$$

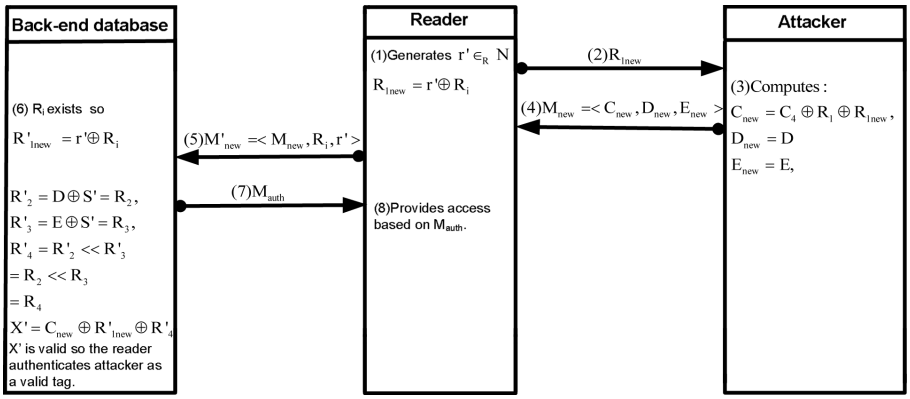
و پیام زیر را برای واحد بازخوان ارسال می کند:

$$M_{new} = \langle C_{new}, D_{new}, E_{new} \rangle = \langle 11100100, 10010111, 01101010 \rangle$$

واحد بازخوان نیز مقادیر زیر را برای سرور ارسال می کند:



حمله کننده یک اجرای موفق بین واحد RFID و بازخوان را شنود کرده و مقادیر R_1، C، D و E را بدست آورده و ذخیره کرده است. سپس منتظر می ماند که بازخوان نشست دیگری را شروع نماید و R_{1new} را بفرستد.



شکل ۷. حمله جعل واحد RFID به پروتکل احراز هویت SEAS.

$$M'_{new} = \langle M_{new}, R_i, r' \rangle = \langle 11100100, 10010111, 01101010, 11010010, 00010100 \rangle$$

حال سرور محاسبات زیر را انجام می دهد:

$$R'_{1new} = R_i \oplus r' = 11010010 \oplus 00010100 = 11000110$$
$$R'_2 = D_{new} \oplus S' = 10010111 \oplus 01000110 = 11010001$$
$$R'_3 = E_{new} \oplus S' = 01101010 \oplus 01000110 = 00101100$$
$$R'_4 = R'_2 << R'_3 = 10001110$$
$$X' = C_{new} \oplus R'_{1new} \oplus R'_4 = 11100100 \oplus 10001111 \oplus 10001110 = 10101100$$

همانگونه که مشاهده می شود، همان متناظر با واحد RFID هدف است که یک مقدار معتبر است. در نتیجه سرور هویت حمله کننده را به عنوان یک واحد RFID معتبر تأیید می کند و آن را در قالب پیام برای واحد بازخوان ارسال می کند. پس حمله کننده در حمله خود موفق بوده است.

عملیاتی کردن حمله جعل واحد RFID

در اینجا بحثی که ممکن است مطرح شود این است، که با وجود فاصله کم بین واحد RFID و دستگاه بازخوان، آیا می توان حمله ارائه شده در این مقاله را در عمل پیاده سازی کرد؟ باید یاد آور شدکه حملات مرد میانی در تحلیل پروتکلهای RFID کاملاً پذیرفته شده هستند و امنیت پروتکلهای زیادی با فرض وجود یک حمله کننده فعال که بین واحد RFID و دستگاه بازخوان قرار می گیرد و قابلیت کنترل، تغییر و یا قطع کردن تمامی یا بخشی از پیامهای مبادله شده را دارد، مورد ارزیابی قرار گرفته است (به عنوان مثال مراجع [۲۴، ۲۵، ۲۶، ۲۷] را مشاهده کنید). اما، حمله ذکر شده در این مقاله را می توان مطابق با روند زیر کاملاً عملیاتی کرد و حمله کننده نیازی به حضور در فاصله بین واحد RFID و دستگاه بازخوان ندارد. برای انجام حمله، کافی است که حمله کننده یک داده تصادفی که با مشخصات R_1 تطابق داشته باشد (از نظر فرکانس، طول داده، و غیره) را برای واحد RFID ارسال کند. از آنجایی که واحد RFID سازوکاری برای احراز اصالت واحد بازخوان در اختیار ندارد، بلافاصله داده مورد نیاز برای حمله کننده که برای یادگیری لازم دارد یعنی پیام های C،D و E را ارسال می کند و مرحله شنود خاتمه می یابد. حال حمله کننده یک واحد RFID جعلی می سازد که در پاسخ به R_{1new} ارسالی از طرف بازخوان واقعی، پیام $M_{new} =< C_{new}, D_{new}, E_{new} >$ را، مطابق روند بیان شده در فرایند حمله، تولید می کند و آن را برای بازخوان می فرستد. مشاهده می شود که حمله کننده برای جعل واحد RFID، عملاً تنها نیاز به ارسال یک درخواست به واحد RFID مورد نظر دارد و بعد از آن به راحتی می تواند آن را جعل نماید.

بحث و نتیجه گیری

در این مقاله امنیت پروتکل SEAS مورد بررسی قرار گرفت. طراحان پروتکل SEAS ادعا کرده بودند که پروتکل آنها در مقابل انواع حملات مختلف امن است، ولی ما در این مقاله یک حمله جعل واحد RFID بسیار کارآمد و موفق به آن اعمال نمودیم. حمله ما نشان داد که پروتکل نه تنها امن نمی باشد، بلکه در تامین تنها هدف خود که احراز هویت مطمئن و با دقت بالای واحدهای RFID می باشد، ناموفق است. موفقیت حمله ارائه شده قطعی و پیچیدگی آن تنها دو بار اجرای پروتکل می باشد. توصیه می شود که از پروتکل SEAS به هیچ عنوان در هیچ کاربردی که نیاز به احراز هویت دارد، استفاده نشود.

نتایج این مقاله نشان دهندهٔ این نکته است که طراحی یک پروتکل مناسب و امن برای واحد های RFID کار ساده ای نیست و طراحان پس از ارائه پیشنهاد خود باید با دید منتقدانه به طرح بنگرند و آسیب پذیریهای مختلف آن را شناسایی و سپس آنها را رفع نمایند. هم چنین باید به نقاط ضعف دیگر پروتکل ها نیز توجه نمایند و از تکرار دوباره آنها در پروتکل خود پرهیز نمایند.

در پایان ذکر این نکته ضروری به نظر می رسد که تمامی پروتکلهایی که تا به امروز سعی کرده اند، بدون

استفاده از توابع رمزنگاری و تنها با کمک عملیات سبک وزن، فرایند احراز هویت امن را فراهم کنند، در هدف خود ناموفق بوده اند (مشابه پروتکل بررسی شده در این مقاله و مراجع [۵، ۶، ۷، ۸]). بنابراین، به نظر می رسد استفاده از یک تابع رمزنگاری ایمن، نظیر رمزهای قطعه ای، رمزهای دنباله ای یا توابع درهم ساز در ساختار یک پروتکل ایمن اجتناب ناپذیر باشد. در غیر این صورت، تجربه نشان داده است که تلاش برای امن کردن چنین پروتکلی بدون استفاده از توابع رمزنگاری تنها معرفی یک قربانی جدید در این حوزه است که ما از آن اجتناب می کنیم.

مراجع

[1] S. Misra, M. Verma, D. Huang, G. Xue,” SEAS: A Secure and Efficient Anonymity Scheme for Low-Cost RFD tags”, in the IEEE ICC 2009 proceedings, 2009.

[2] A. Moradi, A. Poschmann, S. Ling, C. Paar, H. Wang,” Pushing the Limits: A Very Compact and a Threshold Implementation of AES”, EUROCRYPT 2011, pp 692011 ,88-.

[3] P. Peris-Lopez,” Lightweight Cryptography in Radio Frequency Identification (RFID) Systems”, PHD thesis, October 2008.

[4] B. Song and C. J. Mitchell, “RFID Authentication Protocol for Low-cost Tags”, In WiSec’ 08, pp 140–147, 2008.

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda,” M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags”, In Proc. of UIC’06, LNCS, Volume 4159, pp. 912–923, 2006.

[6] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda,” EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags”, In Proc. of IS’06, LNCS, Volume 4277, pp 352–361, 2006.

[7] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda,” LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags”, Hand. of Workshop on RFID and Lightweight Crypto, 2006.

[8] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda,” Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol,” In Proc. of WISA’08, LNCS, Volume 5379, pp 562008 ,68-.

[9] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda,'' An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks'', In EUC Workshops: SecUbiq Workshop, LNCS, Volume 4809, pp. 781–794, 2007.
[10] G. Tsudik,'' YA-TRAP: Yet Another Trivial RFID Authentication Protocol'', In Proc. of PERCOM'06. IEEE Computer Society, 2006.
[11] T. Li and G.Wang,'' SLMAP – A Secure Ultra-Lightweight RFID Mutual Authentication Protocol'', In Proc. of Chinacrypt'07, 2007.
[12] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, T.-C. Chen,'' A New Ultralightweight RFID Protocol with Mutual Authentication'', In Proc. of WASE'09, Volume 2 of ICIE, pp. 582009 ,61-.
[13] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, Volume 4, Number 4, pp. 337–340, December 2007.
[14] C. C. Tan, B. Sheng and Q. Li ,''Secure and Serverless RFID Authentication and Search Protocols'', IEEE Transactions on Wireless Communications, Volume 7, Number 4, pp. 14002008 ,1407-.
[15] R. Xueping and X. Xianghua,'' A Mutual Authentication Protocol For Low-cost RFID System'', In 2010 IEEE Asia-Pacific Services Computing Conference, pp. 632–636, 2010.
[16] H.-M. Sun and W.-C. Ting. "A Gen2-Based RFID Authentication Protocol for Security and Privacy", In IEEE Transactions On Mobile Computing, Volume 8, pp. 1052–1062, 2009.
[17] J.-S. Cho, S.-S. Yeo and S. K. Kim, "Securing Against Brute-Force Attack: A Hash-Based RFID Mutual Authentication Protocol Using a Secret Value", In Comput.Commun., doi:10.1016/j.comcom.2010.02.029, 2010.
[18] Y. Gu and W. Wu, "A Light-Weight Mutual Authentication Protocol for ISO 180006-B Standard RFID System," In Proceedings of ICCTA 2009, pp. 21–25, 2009.
[19] A. Sadighian and R. Jalili, "FLMAP: A Fast Lightweight Mutual Authentication Protocol for RFID Systems", In ICON 2008, pp. 1–6, 2008.
[20] A. Sadighian and R. Jalili. "AFMAP: Anonymous Forward-Secure Mutual Authentication Protocols for RFID systems", The Third IEEE

International Conference on Emerging Security Information, Systems and Technologies(SECURWARE 2009), pp 31–36, Athens, Greece, 2009.
[21] G. Avoine, X. Carpent and B. Martin,"Privacy-Friendly Synchronized Ultralightweight Authentication Protocols in the Storm", J. Network and Computer Applications, Volume 35, Number 2, pp 8262012 ,843-.
[22] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", In Proc. of IFIP-SEC'07, 2007.
[23] H.-Y. Chien and C.-W. Huang," Security of Ultra-Lightweight RFID Authentication Protocols and its Improvements", SIGOPS Oper. Syst. Rev., Volume 41, Number 4, pp. 83–86, 2007.
[24] T. Li, "Security Analysis on a Family of Ultra-Lightweight RFID Authentication Protocols", Jornal of Software, Volume 3, Number 3, pp. 110-, March 2008.
[25] G. Kapoor and S. Piramuthu," Vulnerabilities in Some Recently Proposed RFID Ownership Transfer Protocols", In IEEE Communications Letters, Volume 14, Number 3, pp. 260- 262, March 2010.
[26] P. Rizomiliotis, E. Rekleitis and S. Gritzalis," Security Analysis of the Song Mitchell Authentication Protocol for Low-Cost RFID Tags", In IEEE Communications Letters, Volume 13, Number 4, pp. 274–276, 2009.
[27] R. C. Phan," Cryptanalysis of a New Ultralightweight RFID Authentication Protocol-SASI", In IEEE Transactions on Dependable and secure Computing, Volume 6, Number 4, pp. 3162009 ,320-.
[28] T. Li and R. H. Deng. "Vulnerability analysis of EMAP-an Efficient RFID Mutual Authentication Protocol". In ARES, pp 238–245, 2007.
[29] M. Safkhani and M. Naderi, "Cryptanalysis and Improvement of a Lightweight Mutual Authentication Protocol for RFID Systems", In 7th International ISC Conference on Information Security and Cryptology 2010(ISCISC'10), pp 57–59, 2010.
[30] M. Safkhani, M. Naderi and N. Bagheri, " Cryptanalysis of AFMAP", IEICE Electronics Express, Volume 7, Number 17, pp. 1240–1245, 2010.
[31] M. Safkhani, N. Bagheri, S.K. Sanadhya, M. Naderi and H. Behnam, "On the Security of Mutual Authentication Protocols for RFID Systems: The Case of Wei et al.'s Protocol", J. Garcia-Alfaro et al. (Eds.): DPM 2011 and SETOP 2011, LNCS, Volume 7122, pp. 902012 ,103-.

[32] M. Safkhani, M. Naderi and H. F.Rashvand, “Cryptanalysis of the Fast Lightweight Mutual Authentication Protocol (FLMAP)”. International Journal of Computer & Communication Technology (JCCT), Volume 2, Number 2, pp. 182–186, 2010.
[33] M. Safkhani, N. Bagheri, M. Naderi, Y. Luo, and Q. Chai,” Tag Impersonation Attack on Two RFID Mutual Authentication Protocols”, Sixth International Conference on Availability, Reliability and Security, pp. 581584-, Vienna, Austria, August, 2011.
[34] P. Rizomiliotis, E. Rekleitis and S. Gritzalis, “Security Analysis of the Song Mitchell Authentication Protocol for Low-Cost RFID Tags”, In IEEE Communications Letters, Volume 13, pp. 274–276, 2009.
[35] J. César Hernández Castro, P. Peris-Lopez, M. Safkhani, N. Bagheri, M. Naderi,” Another Fallen Hash-Based RFID Authentication Protocol”, WISTP 2012, pp. 2937-, London, 2012.