ایده‌ای برای افزایش مقاومت پروتکل EAP-MD5 در مقابل حمله‌ی فرهنگ لغت

بهروز خادم[1*]، عیسی سعادت یار[2]، سیاوش عابدی[3]

۱- استادیار دانشگاه امام حسین(ع) bkhadem@ihu.ac.ir

۲- دانشجوی کارشناسی ارشد دانشگاه امام حسین(ع) isasaadatyar@yahoo.com

۳- دانشجوی کارشناسی ارشد دانشگاه امام حسین(ع) sia.abedi72@gmail.com

چکیده

IEEE 802.1X یک استاندارد بین‌المللی برای کنترل دسترسی به شبکه‌های مبتنی بر درگاه[2] است که مکانیسم تأیید هویت را برای دستگاه‌هایی که متقاضی پیوستن به یک شبکه محلی[3] یا شبکه محلی بی‌سیم[4] هستند فراهم می‌کند. این استاندارد بسته‌بندی پروتکل EAP را بر روی IEEE 802 تعریف می‌کند. در این استاندارد پروتکل‌های احراز هویت تکمیل‌کننده بخشی از امنیت شبکه شده‌اند. پروتکل‌های عضو خانواده EAP ازنظر سرعت و امنیت با یکدیگر متفاوت هستند. یکی از سریع‌ترین آن‌ها EAP-MD5 است که موردتوجه این مقاله قرارگرفته است و به‌منظور بهبود امنیت، برخی از حملات انجام‌شده به آن بررسی‌شده است. در این مقاله ابتدا پروتکل EAP-MD5 به‌طور مختصر معرفی‌شده و تعدادی از حملات فرهنگ لغت[5] انجام‌شده روی آن توصیف‌شده‌اند. سپس بر اساس نقاط ضعف مشاهده‌شده درپروتکل EAP-MD5 با ارائه ایده‌ای مناسب ضمن حفظ سرعت اجرایی، امنیت آن در مقابل حمله فرهنگ لغت بهبود داده‌شده است.

کلمات کلیدی: احراز هویت، EAP-MD5، حمله فرهنگ لغت

۱. مقدمه

پروتکل احراز هویت اجرای فرآیندی روی یک کانال ارتباطی ناامن برای حصول اطمینان از هویت واقعی طرفین یک ارتباط است. یکی از متداول‌ترین روش‌ها برای این کار، احراز هویت مبتنی بر گذرواژه است. می‌توان سال ۱۹۸۱ را که لمپورت یک پروتکل احراز هویت مبتنی بر گذرواژه را ارائه کرد نقطه شروع استفاده از این پروتکل‌ها دانست [۱]. از آن سال تاکنون تعداد زیادی از این پروتکل‌ها ارائه‌شده‌اند [۲-۶]. اما هرکدام به‌نوبه خود مورد تحلیل و ارزیابی‌های متعددی قرارگرفته

*Corresponding Author E-mail: bkhadem@ihu.ac.ir

2 Port

3 LAN

4 WLAN

5 Dictionary attack

و دارای نقاط ضعفی بوده‌اند [۷-۱۱]. بنابراین تحقیقات به‌منظور رسیدن به یک پروتکل احراز هویت امن تاکنون ادامه یافته است.

یک دسته مهم از پروتکل‌های احراز هویت، پروتکل‌های خانواده EAP[۱] است. درواقع EAP یک چارچوب[۲] کلی پروتکل احراز هویت بوده و در شبکه‌های بی‌سیم و ارتباطات نقطه‌به‌نقطه[۳] رواج بسیاری دارد. این خانواده شامل بیش از ۴۰ پروتکل هست که هرکدام بنا به مقاصد کاربردی متفاوت، سرعت و امنیت متفاوتی دارند[۱۲]. یکی از پروتکل‌های این خانواده EAP-MD5 است که به دلیل سرعت زیاد موردتوجه کاربران قرارگرفته است[۱۳]. البته این پروتکل به دلیل برخوردار نبودن از احراز هویت دوطرفه و ضعف در مقابل حملات فرهنگ لغت دارای نقایص امنیتی است و به همین دلیل این مقاله با ارائه یک پیشنهاد ساده، هسته‌ی اصلی EAP-MD5 را اصلاح‌کرده تا اجرای حمله فرهنگ لغت را به‌اندازه قابل‌توجهی دشوارتر کند. ازآنجاکه بهبود پیشنهادشده در این مقاله بر روی هسته‌ی اصلی پروتکل (و نه لایه‌های شبکه‌ی پروتکل) صورت گرفته است، لذا برای سادگی از بررسی لایه‌های شبکه‌ی این پروتکل صرف‌نظر می‌شود.

در این مقاله ابتدا در قسمت دوم به‌صورت مختصر هسته‌ی اصلی پروتکل EAP-MD5 معرفی می‌شود. در قسمت سوم برخی از حملات فرهنگ لغت صورت گرفته روی این پروتکل توصیف می‌شود. سپس در قسمت چهارم یک ایده پیشنهادی برای بهبود امنیت EAP-MD5 معرفی‌شده و امنیت آن در برابر حمله فرهنگ لغت بررسی می‌شود. در قسمت پنجم خلاصه نتایج به‌دست‌آمده ارائه می‌شود.

۲. بررسی پروتکل EAP-MD5

EAP-MD5 یک پروتکل احراز هویت مبتنی بر گذرواژه و یک‌طرفه است که اغلب در شبکه‌های بی‌سیم X802.1 و اتصالات PPP استفاده می‌شود [۳]. این پروتکل شامل سه مؤلفه متقاضی، احراز کننده هویت (WAP) و سرویس‌دهنده (RADIUS) است و در آن فقط هویت متقاضی قابل‌شناسایی است (شکل ۱). توصیه‌شده که بهتر است حداقل طول گذرواژه در این پروتکل ۱۶ بایت باشد [۱۴]. اگر از لایه‌های شبکه و قالب‌بندی این پروتکل صرف‌نظر شود، این پروتکل به یک تبادل ساده اطلاعات برای بررسی هویت متقاضی تبدیل می‌شود. مراحل متوالی اجرای پروتکل شامل ۱۰ گام و به شرح زیر است.

۱. متقاضی درخواست شروع را ارسال می‌کند
۲. احراز کننده هویت یک شناسه (ID) یک بایتی برای متقاضی ارسال می‌کند.
۳. متقاضی نام کاربری خود و همان شناسه را برای احراز کننده هویت ارسال می‌کند.
۴. احراز کننده همان اطلاعات را عیناً به سرویس‌دهنده ارسال می‌کند(فقط ساختار قالب‌بندی آن متفاوت است).
۵. در این مرحله سرویس‌دهنده بررسی می‌کند که آیا این نام کاربری در پایگاه داده موجود است یا خیر؟ اگر موجود بود به‌صورت تصادفی یک چالش (Challenge) ۱۲۸ بیتی تولید کرده و در کنار ID+1 برای احراز کننده هویت می‌فرستد.
۶. احراز کننده همان اطلاعات را عیناً به متقاضی ارسال می‌کند (فقط ساختار قالب‌بندی آن متفاوت است).

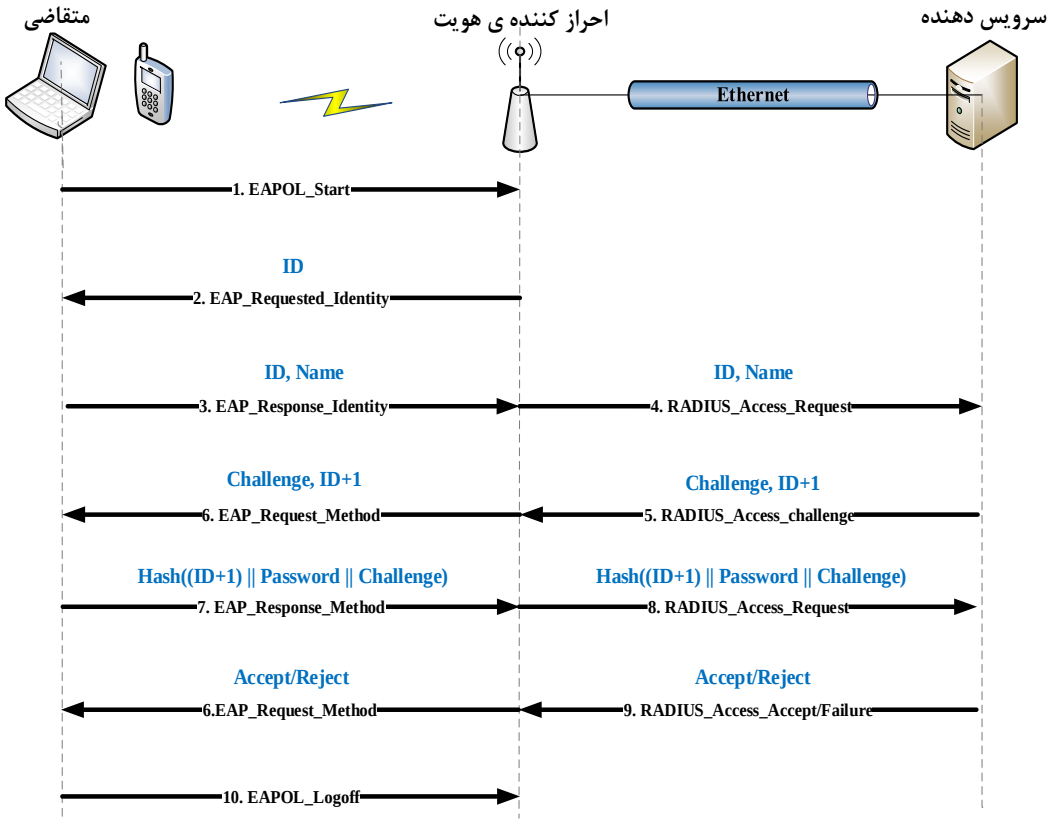
---

۱ **Extensible Authentication Protocol**

۲ **Framework**

۳ **Point to Point**

۷. در این مرحله، متقاضی سه مقدار ID+1، چالش و گذرواژه خود را در کنار هم قرار داده[۱] و از آن‌ها یک چکیده (MD5) می‌گیرد و نام آن را پاسخ به چالش (Challenge response) در نظر می‌گیرد؛ او این چکیده را به احراز کننده هویت ارسال می‌کند.
۸. احراز کننده همان اطلاعات را عیناً به سرویس‌دهنده ارسال می‌کند(فقط ساختار قالب‌بندی آن متفاوت است).
۹. در این مرحله سرویس‌دهنده محاسبات گام ۷ را انجام می‌دهد (او نیز چالش، گذرواژه و شناسه را دارد). اگر مقدار چکیده‌ی به‌دست‌آمده با مقدار دریافت شده پاسخ به چالش از متقاضی برابر بود به احراز کننده "تأیید" و در غیر این صورت "عدم‌تأیید" را اعلام می‌کند
۱۰. احراز کننده هویت همان اطلاعات را عیناً به متقاضی ارسال می‌کند (فقط ساختار قالب‌بندی آن متفاوت است).



شکل ۱ – شمای کلی گام‌های پروتکل EAP-MD5

۳. مروری بر حملات فرهنگ لغت انجام‌شده روی EAP-MD5

به‌طور مختصر در یک حمله فرهنگ لغت مهاجم ابتدا یک‌بار فرآیند احراز هویت را شنود می‌کند و از مقادیر به‌دست‌آمده برای انجام حمله به‌صورت برون‌خط[۲] استفاده می‌کند تا مقدار گذرواژه را به دست آورد. با توجه به اینکه در پروتکل مقدار

۱ **Concatenate**

[2] **Offline**

شناسه و چالش به‌صورت صریح[1] برای کاربر ارسال می‌شود، مهاجم علاوه بر خروجی چکیده ساز(پاسخ به چالش)، از سه مقدار ورودی به چکیده ساز دو مقدار آن را دارد (شکل ۲) و فقط مقدار گذرواژه را ندارد. بنابراین مهاجم می‌تواند در یک حمله جستجوی کامل[2] با استفاده از یک فرهنگ لغت محدود (که معمولاً یک لیست از پیش تهیه‌شده شامل گذرواژه‌های متداول کاربر است) یک‌به‌یک مقادیر فرهنگ لغت را بجای گذرواژه قرار داده و سپس از آن چکیده بگیرد و اگر مقدار چکیده با مقداری که متقاضی در پاسخ به چالش برای احراز کننده هویت فرستاده برابر باشد آنگاه مقدار گذرواژه پیدا شده است؛ در غیر این صورت مقدار گذرواژه احتمالی بعدی را از فرهنگ لغت استخراج کرده و دوباره آن را ارزیابی می‌کند. مهاجم این روند را آن‌قدر تکرار می‌کند تا گذرواژه متقاضی را بیابد. در نظر داشته باشید هر چه گذرواژه ساده‌تر باشد آنگاه این حمله ساده‌تر خواهد بود.

در سال ۲۰۰۸ هوانگ و همکاران در محیط شبکه بی‌سیم یک حمله مردی در میان به استاندارد 802.1X و پروتکل EAP-MD5 انجام دادند و موفق شدند گذرواژه متقاضی را پیدا کنند [۸].

مجدداً در سال ۲۰۰۸ رایت و همکاران موفق شدند نشان بدهند که یک برنامه می‌تواند گذرواژه مورداستفاده در EAP-MD5 در یک شبکه بی‌سیم را پیدا کند[۱۵]. این برنامه شامل یک مرحله استراق سمع و یک مرحله حمله فرهنگ لغت بود. میزان موفقیت این حمله به نوع فرهنگ لغت بکار رفته و میزان پیچیدگی گذرواژه بستگی داشت.

همچنین در سال ۲۰۱۲ لیو و همکارانش یک حمله کارآمد برای بازیابی گذرواژه EAP-MD5 در یک شبکه IEEE X802.1 انجام دادند و موفق شدند آن را در مدتی کمتر از ۳ روز پیدا کنند [۹]. آن‌ها با انجام یک حمله برخط[3] ابتدا طول گذرواژه را پیدا کردند و سپس با استفاده از جدول رنگین‌کمان[4] بکار رفته در حمله معاوضه زمان و حافظه هلمان [۱۶] مقدار گذرواژه را نیز پیدا کردند.

پیشنهاد ارائه‌شده در این مقاله با استفاده از یک ایده مناسب امنیت پروتکل EAP-MD5 را در مقابل حملات فرهنگ لغت [۸, ۹, ۱۵] بیشتر کرده و عملاً آن‌ها را ناکارآمد می‌کند.

۴. ارائه طرح پیشنهادی برای بهبود EAP-MD5

همان‌طور که در قسمت ۳ دیده شد، یکی از موفق‌ترین حملاتی که می‌توان بر روی EAP-MD5 انجام داد، حمله‌ی فرهنگ لغت برای حدس گذرواژه است. درواقع مهاجم یک معیار برای بررسی حدس خود از گذرواژه از معیار پاسخ به چالش استفاده می‌کند. یعنی مهاجم یک گذرواژه را حدس زده و با کمی پردازش می‌تواند درستی حدس خود را بررسی کند. دلیل سادگی این فرآیند آن است که مهاجم از سه پارامتر سازنده‌ی پاسخ به چالش، دو پارامتر (شناسه متقاضی و چالش سرویس دهنده) را به دلیل صریح ارسال شدن آن‌ها بر روی کانال ناامن شنود کرده است و با حدس پارامتر سوم می‌تواند درستی حدس خود را بررسی کند. لذا اگر بتوان به طریقی از ارسال صریح یکی از این دو پارامتر (به دلیل بزرگ بودن طول چالش، این پارامتر مهم‌تر است) بر روی کانال جلوگیری کرد، آنگاه حمله مهاجم برای حدس گذرواژه سخت تر خواهد شد. در ادامه ایده‌ای ارائه‌شده است که در آن دیگر چالش سرویس دهنده به‌صورت صریح بر روی کانال ارسال نمی‌شود.

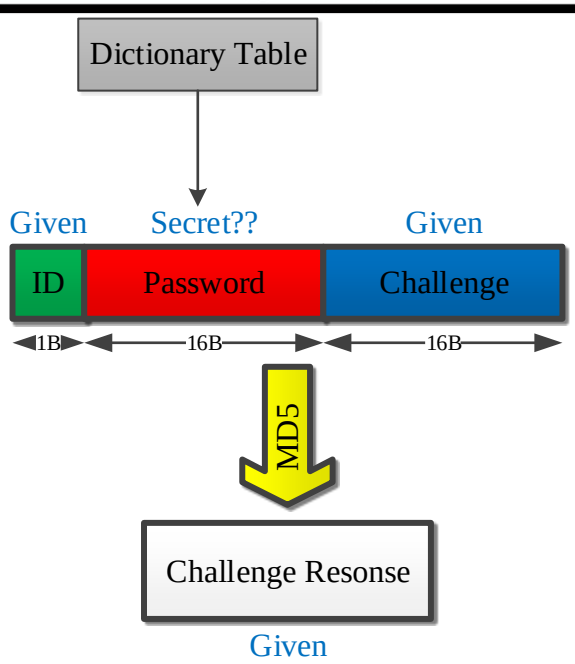
---

[1] **Plaintext**

[2] **Brute Force attack**

[3] **Online**

[4] **Rainbow Table**



شکل ۲ – نمایی از حمله‌ی فرهنگ لغت برای یافت گذرواژه

به‌منظور بهبود، روال پروتکل به صورت زیر تغییر می‌یابد:

۱. متقاضی درخواست شروع را ارسال می‌کند
۲. احراز کننده هویت یک شناسه(ID) یک بایتی برای متقاضی ارسال می‌کند.
۳. متقاضی نام کاربری خود و همان شناسه را برای احراز کننده هویت ارسال می‌کند.
۴. احراز کننده همان اطلاعات را عیناً به سرویس‌دهنده ارسال می‌کند(فقط ساختار قالب‌بندی آن متفاوت است).
۵. در این مرحله سرویس‌دهنده بررسی می‌کند که آیا این نام کاربری در پایگاه داده موجود است یا خیر؟ اگر موجود بود، گذرواژه او را استخراج کرده و سپس یک چالش(Challenge) ۱۲۸ بیتی را به‌صورت تصادفی تولید کرده و مقدار Request را مطابق رابطه‌ی(۱) محاسبه کرده و برای احراز کننده ارسال می‌کند:

$$Request = hash(ID \oplus Challenge) \oplus Password \quad (1)$$

۶. احراز کننده همان اطلاعات را عیناً به متقاضی ارسال می‌کند (فقط ساختار قالب‌بندی آن متفاوت است).
۷. در این مرحله، متقاضی یک مهر زمانی[۱] تولید کرده و Response را مطابق روابط (۲) و (۳) محاسبه کرده و به همراه مهر زمانی برای احراز کننده هویت ارسال می‌کند:

$$C = Request \oplus Password = hash(ID \oplus Challenge) \quad (2)$$
$$Response = hash(C \oplus Time\ Stamp) \quad (3)$$

۸. احراز کننده همان اطلاعات را عیناً به سرویس‌دهنده ارسال می‌کند(فقط ساختار قالب‌بندی آن متفاوت است).
۹. در این مرحله سرویس‌دهنده ابتدا مهر زمانی را بررسی می‌کند و در صورت قدیمی بودن آن "عدم‌تأیید" را ارسال می‌کند؛ اگر مهر زمانی به‌روز بود، آنگاه سرویس‌دهنده C' را مطابق رابطه‌ی(۴) محاسبه می‌کند (او نیز چالش و شناسه را دارد)؛ سپس با استفاده از آن $Response'$ را مطابق رابطه‌ی(۵) محاسبه می‌کند؛ اگر مقدار $Response'$ با مقدار دریافت شده (Response) برابر بود به احراز کننده "تأیید" و در غیر این صورت "عدم‌تأیید" را اعلام می‌کند (شکل ۳).

---

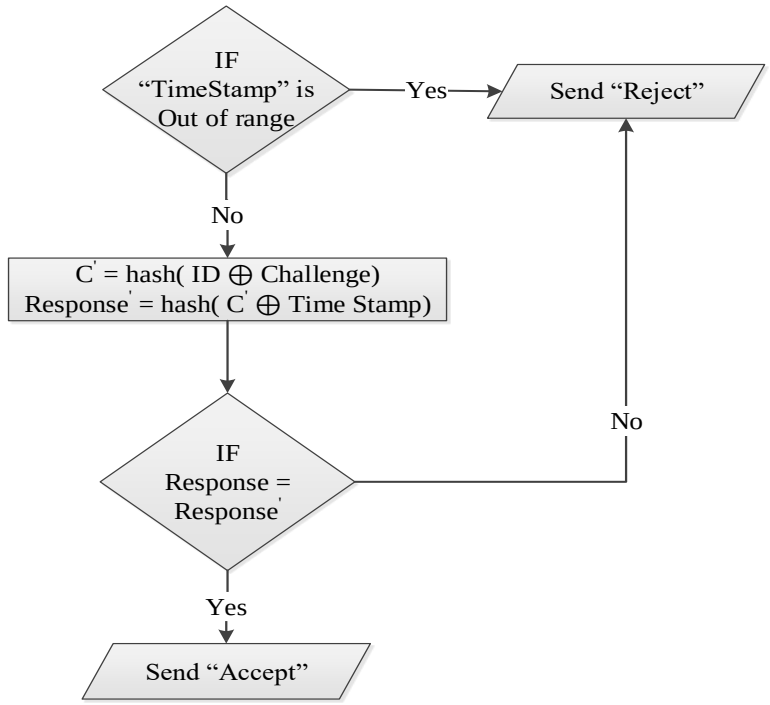
۱ **Time Stamp**

$C' = hash(ID \oplus Challenge)$ (4)

$Response' = hash(C' \oplus Time\ Stamp)$ (5)

۱۰. احراز کننده همان اطلاعات را عیناً به متقاضی ارسال می‌کند (فقط ساختار قالب‌بندی آن متفاوت است).

همان‌طور که (در شکل ۴) مشاهده می‌شود، در این بهبود، چالش سرویس‌دهنده به‌صورت صریح بر روی کانال قرار نگرفته و همین امر پیچیدگی حمله‌ی فرهنگ لغت را افزایش داده است.



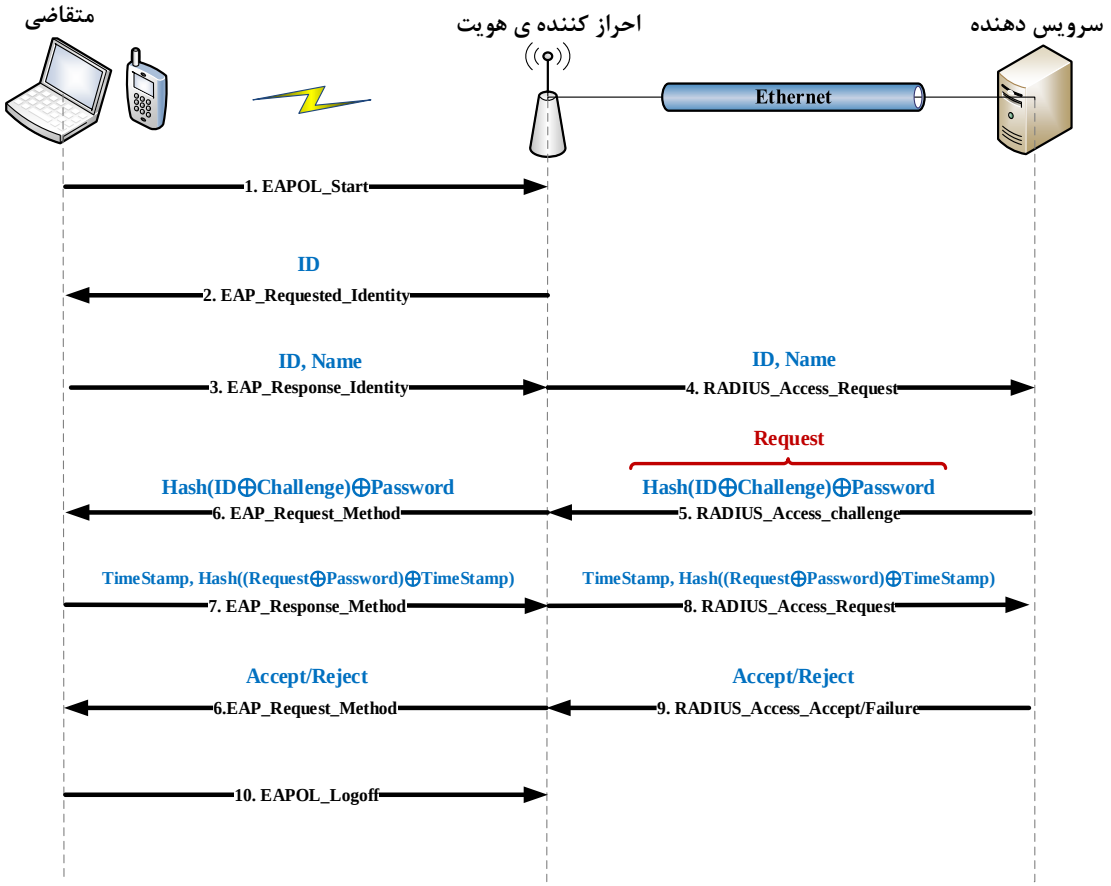
شکل ۳– فلوچارت رویه تصمیم‌گیری سرویس‌دهنده در پروتکل پیشنهادی

همان‌گونه که (در شکل ۴) مشاهده شد در پروتکل پیشنهادی دیگر چالش به‌صورت صریح ارسال نمی‌شود و لذا مهاجم از سه پارامتر سازنده‌ی پاسخ چالش دیگر دو پارامتر آن را نداشته و عملاً حدس گذرواژه با حمله‌ی بیان‌شده ناکارآمد است.

۵. نتیجه‌گیری

پروتکل EAP-MD5 بااینکه سریع و سبک بوده، اما متأسفانه دارای مشکلات امنیتی نیز است. یکی از مشکلات امنیتی آن آسیب‌پذیری در مقابل حمله فرهنگ لغت و جستجوی سریع فضای گذرواژه توسط مهاجم است. علت اصلی این آسیب‌پذیری آن است که در مراحل ۵ و ۶ پروتکل اصلی، مقدار چالش سرویس‌دهنده به‌صورت صریح ارسال می‌شود که مهاجم با شنود آن می‌تواند مقدار گذرواژه را به‌طور مؤثری حدس بزند. در این مقاله طرحی پیشنهادشده است که ضمن حفظ سرعت اجرای پروتکل (به دلیل استفاده از یک تابع چکیده ساز مشابه)، مانع از ارسال صریح چالش روی کانال می‌شود و به همین دلیل مانع از اجرای عملیات استراق سمع توسط مهاجم شده و به دنبال آن به‌طور مؤثری پیچیدگی اجرای حمله فرهنگ لغت را برای مهاجم بسیار زیاد می‌کند. ازآنجاکه چالش عددی تصادفی است، اگر مهاجم بخواهد بر روی پروتکل

بهبودیافته پیشنهادی حمله‌ی موردنظر را اجرا کند، علاوه بر اجرای عملیات حمله‌ی فرهنگ لغت، برای هر گذرواژه‌ی حدس زده‌شده باید کل فضای چالش را نیز جستجو کند. با توجه به آنکه طول چالش ۱۲۸ بیت است لذا فضای جستجوی آن برابر با $۲^{۱۲۸}$ است. درواقع پروتکل پیشنهادی به پیچیدگی حمله مقدار $۲^{۱۲۸}$ گام محاسباتی اضافی را افزوده است. به عبارت دیگر اگر پیچیدگی حمله به پروتکل اصلی با یک گذرواژه خاص مقدار 2^c باشد (مقدار c وابسته به ابزار محاسباتی مهاجم است) آنگاه پیچیدگی حمله به پروتکل پیشنهادی با فرض همان شرایط 2^{128+c} خواهد بود. بنابراین اگر فرض شود که مقدار 2^c برابر یک باشد، آنگاه بازهم پیچیدگی محاسباتی $2^{128}\times 1$ نیز عددی بزرگ بوده و انجام حمله برای مهاجم به زمان و توان پردازشی بسیار زیادی نیاز دارد. جدول ۱ نتایج مقایسه دو روش را با یکدیگر نشان می دهد.



شکل ۴ – شمای کلی گام‌های پروتکل پیشنهادی برای بهبود EAP-MD5

جدول ۱- مقایسه‌ی پروتکل اصلی و پیشنهادی

	پیچیدگی محاسباتی حمله فرهنگ لغت	مقاومت در برابر حمله تکرار	سرعت اجرای پروتکل
پروتکل اصلی	2^c	ندارد	زیاد
پروتکل پیشنهادی	2^{128+c}	دارد	زیاد

ازجمله مزایای دیگر طرح پیشنهادی، چکیده‌سازی مضاعف اطلاعات است که باعث پیچیدگی بیشتر اطلاعات تبادل شده می‌شود. به‌علاوه در طرح پیشنهادی از مهر زمانی نیز استفاده‌شده است که به‌خودی‌خود مانع از انجام حمله تکرار [1] نیز می‌شود.

۶. منابع

[1] Lamport, L., *Password authentication with insecure communication.* Communications of the ACM, 1981. **24**(11): p. 770-772.
[2] Wu, T.D. *The Secure Remote Password Protocol*. in *NDSS* .۱۹۹۸ .Citeseer.
[3] Aboba, B., et al., *Extensible authentication protocol (EAP)*. 2004.
[4] Aboba, B., D. Simon, and P. Eronen, *Extensible authentication protocol (EAP) key management framework*. 2008.
[5] Kumari, S., et al., *An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement.* Security and Communication Networks, 2014. **7**(11): p. 1921-1932.
[6] Ruoti, S., J. Andersen, and K.E. Seamons. *Strengthening Password-based Authentication*. in *Way@ Soups*. 2016.
[7] Han, L ,.*A threat analysis of the extensible authentication protocol.* Honors Project Report, 2006.
[8] Hwang, H., et al. *A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1 X and EAP*. in *Information Science and Security, 2008. ICISS. International Conference on*. 2008. IEEE.
[9] Liu, F. and T. Xie. *How to break EAP-MD5*. in *IFIP International Workshop on Information Security Theory and Practice*. 2012. Springer.
[10] Chaudhry, S.A., et al., *Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems.* Journal of Medical Systems, 2015. **39**(6): p. 66.
[11] Rajeswari, S.R. and V. Seenivasagam, *Comparative study on various authentication protocols in wireless sensor networks.* The Scientific World Journal, 2016. **2016**.
[12] Chiorniţă, A., L. Gheorghe, and D. Rosner. *A practical analysis of EAP authentication methods*. in *Roedunet International Conference (RoEduNet), 2010 9th*. 2010. IEEE.
[13] Youm, H.Y., *Extensible authentication protocol overview and its applications.* IEICE transactions on information and systems, 2009. **92**(5): p. 766-776.

[1] **Replay attack**

[14] Aboba, B. and P. Calhoun, *RFC 3579-RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).* Internet Society, September, 2003.
[15] Wright, J. and B. Antoniewicz, *PEAP: Pwned extensible authentication protocol*. 2008, ShmooCon.
[16] Hellman, M., *A cryptanalytic time-memory trade-off* .IEEE transactions on Information Theory, 1980. **26**(4): p. 401-406.