پنجمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology

افزودن ویژگی حفاظت شناسه آغازگر در برابر حمله فعال به پروتکل IKEv2

محمد مهدی کرباسیون
دانشگاه صنعتی اصفهان
karbasioun@gmail.com

مهدی برنجکوب
دانشگاه صنعتی اصفهان
brnjkb@cc.iut.ac.ir

چکیده: دراین مقاله ضمن مطالعه و بررسی نسخه جدید پروتکل تبادل کلید در اینترنت به مشکل حفاظت شناسه آغاز گر در برابرحمله کننده فعال در آن اشاره می شود و دو روش نیز برای برطرف کردن آن ارائه می گردد. در روش اول از پروتکل احراز اصالت قابل گسترش کمک گرفته شده است و در روش دوم سعی شده است که تنها با اصلاح تبادلات آغازین در پروتکل اصلی مشکل مذکور برطرف گردد.

واژه های کلیدی: IKE ، EAP ، احراز اصالت و حفاظت شناسه

۱- مقدمه

مکانیزم IPsec[1] [1]، سرویسهای مختلفی از جمله محرمانگی، کنترل صحت داده ها، کنترل دسترسی به داده ها، مقابله با حمله تکرار، محرمانگی محدود جریان ترافیک و نیز احراز اصالت مبدأ داده ها را بین مبدا و مقصد فراهم می‌آورد. برای در اختیار قرار دادن این سرویسها لازم است که بر روی الگوریتمها رمزنگاری مناسب و به تبع آن کلیدهای متناسب با این الگوریتمها توافق گردد. بهره برداری از این الگوریتمها و کلیدهای توافق شده به صورت دستی یکی از گزینه های ممکن است. این روش دارای عیب عمده عدم مقیاس پذیری می باشد و بدین ترتیب قابلیت استفاده گسترده و متنوع برای شبکه های نوعی را ندارد؛ خصوصاً که به دلیل ملاحظات امنیتی نیاز به تازه سازی و تجدید کلیدها وجود دارد. از این رو به مکانیزم و روشی برای تبادل امن و خودکار کلید و نیزتوافق روی الگوریتمهای رمزنگاری نیاز است. آنچه برای رفع نیاز مذکور

[1] IP security

در مکانیزم IPsec به عنوان پیش فرض قلمداد شده است، استفاده از پروتکل تبادل کلید اینترنت (IKE)[۲] می باشد.

نسخه جدید پروتکل تبادل کلید اینترنت (IKEv2) [2] پس از بررسی های زیاد بر روی نتایج حاصل از مطالعاتی که روی نسخه اولیه این پروتکل (IKEv1)[3] و پیاده سازیهای مختلف آن و نیز در رقابت با سایر جایگزینهای مطرح، از جمله JFK[۳] [4]و SIGMA[۴] [5]،تحت عنوان IKEv2 ارائه گردید. مهمترین مزایای نسخه جدید نسبت به نسخه پیشین IKE عبارتند از: کاهش پیچیدگی، کاهش تعداد پیامها، افزایش انعطاف در استفاده از روشهای احراز اصالت، افزایش مقاومت در برابر حملات از کاراندازی سرویس، افزوده شدن خاصیت قابلیت اطمینان، استاندارد شدن نحوهٔ عبور بسته‌های IKE و IPsec از دروازه های NAT و همچنین استاندارد شدن روند درخواست یک آدرس داخلی از یک شبکهٔ دور [2].

درادامه ابتدا نسخه جدید پروتکل توزیع کلید اینترنت IKEv2 به اختصار معرفی می‌شود. در ادامه مشکل عدم حفاظت شناسه آغازگر در برابر حمله فعال مطرح می‌شود و برای رفع مشکل مزبور دو روش پیشنهاد خواهد شد که یکی از آنها مبتنی بر استفاده از پروتکل احراز اصالت قابل گسترش (EAP)[۵] [6] است ودیگری تنها با اصلاح تبادلات پروتکل IKEv2 حاصل شده است. سپس تحلیلی درباره روشهای پیشنهادی ارائه می‌شود و سرانجام با مروری بر مطالب مقاله نتیجه‌گیری می‌شود.

۲- معرفی پروتکل تبادل کلید اینترنت (IKEv2)

IKE ضمن انجام احزار اصالت طرفین ارتباط، دوتداعی‌گر امنیتی[۶] به نامهای IKE-SA و IPsec-SA (که به آن Child-SA نیزگفته می‌شود) ایجاد می‌کند که از جمله اطلاعات محرمانه مشترک بین دو سوی ارتباط را در بر می گیرند. در واقع IKE مسؤول ایجاد، نگهداری و قطع کردن کانالهای امنی است که جلسات محرمانه IPsec به صورت مطمئن در آنها امکان برقراری داشته باشند. ایجاد این کانالها از طریق درخواست آغازگر[۷] وارائه تعدادی پیشنهاد، شامل مجموعه هایی از توابع رمزنگاری مناسب برای ایجاد آن کانال امن و در مقابل پاسخ مخاطب[۸] مورد نظر با انتخاب یکی از مجموعه های پیشنهاد شده از سوی آغازگر به صورت امن میسر می‌شود.

کلیه تبادلات IKE از زوج پیامهای «درخواست _ پاسخ» تشکیل شده اند که هر زوج پیام را یک تبادل[۹] می‌نامند. اولین پیامهای ایجاد کننده یک IKE-SA ،تبادلات IKE-SA-INIT و IKE-SA-AUTH می باشند. به دنبال آنها، تبادلات CREATE- CHILD-SA و INFORMATIONAL می‌توانند مورد استفاده قرار گیرند.در حالت معمول یک تبادل IKE -SA-INIT و یک تبادل IKE- SA-AUTH (مجموعاً ۴ پیام) برای ایجاد یک IKE-SA و اولین CHILD-SA کافی است. به مجموع این دو تبادل، تبادلات آغازین گفته می‌شود که در ادامه معرفی خواهند شد.

۲-۱- تبادلات آغازین

تمامی ارتباطات IKE، حتماً با تبادلات آغازین شامل دو تبادل IKE-SA-INIT و IKE-SA-AUTH، آغاز می‌شوند. تبادلات آغازین به طور معمول شامل ۴ پیام می باشند، هر چند که در برخی حالتها تعداد پیام های این تبادلات می‌تواند از این تعداد نیز بیشتر شوند. شکل (۱) این تبادلات را نشان می دهد.لازم به ذکر است که هر جا در این شکل و شکلهای مشابه ، عبارتی داخل نماد " [ ] " قرار داده شد، بدین معنی است که آوردن این عبارت در داخل تبادلات مذکور اختیاری است.

در دو پیام اول الگوریتمهای رمزنگاری پیشنهادی از سوی آغازگر (SAi1) و انتخاب شده از سوی مخاطب (SAr1) نانسهای هر یک از دو طرف (Ni , Nr) و نیم کلیدهای دیفی-هلمن مربوط به هر طرف (KEi , KEr) رد و بدل می‌شوند. الگوریتمهای رمزنگاری که در این مرحله بر روی آنها توافق می‌شود، برای محافظت از تبادلات IKE-SA مورد استفاده قرار

2 Internet Key Exchange
3 Just Fast Keying
4 Signature Mode of Authentication
5 Extensible Authentication Protocol
6 Security Association
7 Initiator
8 Responder
9 Exchange

می‌گیرند. از نیم‌کلیدهای دیفی- هلمن به همراه نانسها، برای تولید کلیدهای مشترک مربوط به این IKE-SA استفاده می‌شود.

در دو پیام بعدی شناسه ها رد و بدل می شوند، ضمن آنکه دو پیام مرحله قبل به همراه شناسه های مورد ادعا از سوی هر طرف، احراز اصالت می گردند.این کار به وسیلهٔ فیلد AUTH انجام می‌شود. فیلد AUTH چیزی نیست جز تبدیل یک بلوک معین از داده های رد و بدل شده در دو پیغام اول با استفاده از کلید خصوصی هر طرف(که از آن به عنوان امضا یاد می‌شود) و یا تولید یک کد احراز اصالت پیام (MAC)[10] با بهره بردن از یک کلید از پیش مشترک. بلوک داده مورد اشاره شامل مواردی چون کل پیامی که هر طرف در مرحله قبل فرستاده است، به همراه شناسه خود و نانس ارسالی طرف مقابل می‌باشد. نیز در صورت نیاز، گواهی‌های مربوط به هر طرف برای طرف مقابل ارسال می‌شود.

اطلاعات رد و بدل شده در این تبادلات تا بدینجا، برای تولید IKE-SA کفایت می‌کند. در ادامه این تبادلات اولین CHILD-SA ایجاد می‌شود. ایجاد این CHILD-SA بدین صورت است که مجموعه‌های رمزنگاری پیشنهادی برای این SA و همچنین انتخابگرهای متناظر این تداعی‌گر امنیتی از سوی آغازگر برای مخاطب ارسال می‌شود و در پاسخ مجموعه های انتخابی به همراه انتخابگرهای پذیرفته شده از سوی مخاطب برای آغازگر برگردانده می‌شود. پیام های تبادل IKE-SA-AUTH توسط الگوریتمها رمزنگاری و کلیدهای توافق شده در IKE-SA-INIT رمز و کنترل صحت می شوند. از این‌رو در نمایش آنها از نماد SK{...} استفاده شده است

	آغازگر		مخاطب
1	$HDR , SA_{i1} , KE_i , N_i$	$\longrightarrow$	
2		$\longleftarrow$	$HDR , SA_{r1} , KE_r , N_r , [CERTREQ]$
3	$HDR,SK\{ ID_i ,[CERT] , [CERTREQ] , [ID_r] , AUTH , SA_{i2} , TS_i , TS_r \}$	$\longrightarrow$	
4		$\longleftarrow$	$HDR , SK \{ ID_r , [CERT] , AUTH , SA_{r2} , TS_i , TS_r \}$

شکل ۱ : تبادلات آغازین

۳- حفاظت از شناسه آغازگر در برابر حمله‌کنندگان فعال

یکی از مشکلات IKEv1 که همچنان در IKEv2 باقی است، مسأله عدم حفاظت از شناسه آغازگر در برابر حمله کنندگان فعال است. این مسأله در محیطهای کارگزار- کارفرما[11] و خصوصاً در مواردی که کاربران را گروه‌های سیار تشکیل می‌دهند، از اهمیت ویژه ای برخوردار است. به عنوان مثال در ارتباطات سیار عوامل دشمن می‌توانند با دریافت شناسه کاربران و کارفرمایان یک کارگزار خاص، به اطلاعاتی از جمله مکان فیزیکی این نوع کاربران دست پیدا کنند و از این طریق حریم خصوصی آنها را مخدوش نمایند. دقیقاً برای جلوگیری از چنین مخاطراتی بود که طراحان پروتکل JFK برای محیطهای کارگزار- کارفرما نسخه‌ای ویژه ایجاد کردند و آنرا JFK-i نام نهادند[4] . همچنین در طراحی پروتکل SIGMA [5] نیز حفاظت از شناسه آغازگر به دلایل گفته شده، مقدم بر حفاظت شناسه مخاطب درنظر گرفته شد. همانگونه که در شکل (۱) دیده می‌شود ، در پیام سوم آغازگر لازم است شناسه خود را در اختیار مخاطبی قرار دهد که هنوز احراز اصالت نشده است. علاوه بر این آغازگر لازم است هویت خود را نیز به مخاطب اثبات کند و در عوض منتظر بماند تا مخاطب در پیام بعدی اقدامات مشابه را انجام دهد. مشکل زمانی پدید می آید که آغازگر پس از ارسال پیام سوم موفق به احراز اصالت مخاطب نشود و در عوض شناسه خود را در اختیار آن موجودیت نامعتبر قرار داده باشد. از این رو باید راهی برای برطرف کردن این نقیصه یافت. در ادامه دو روش در این رابطه ارائه خواهد شد. در روش اول از پروتکل احراز اصالت قابل گسترش (EAP) کمک گرفته شده است و در روش دوم سعی شده است که تنها با اصلاح تبادلات آغازین، مشکل مذکور برطرف گردد. برای اطلاع از جزییات بیشتر علاقه‌مندان به [۷] ارجاع داده می‌شوند.

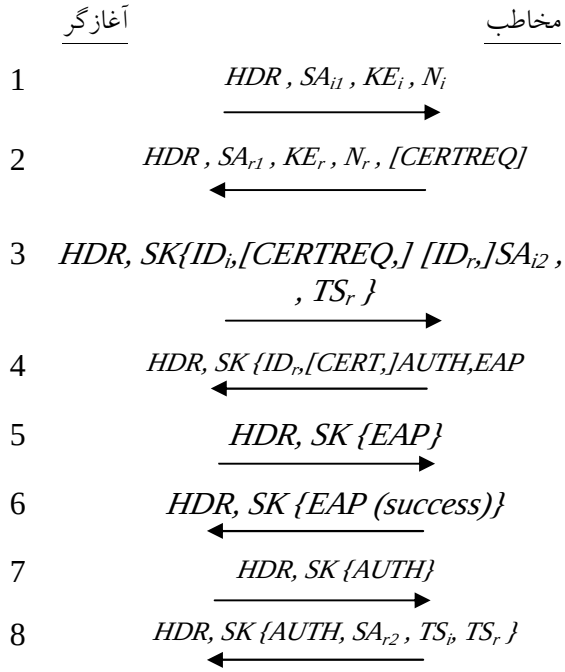
10 Message Authentication Code

11 Client - Server

۳-۱ مخفی کردن شناسه آغازگر در برابر حمله‌کنندگان فعال با استفاده از EAP

یکی دیگر از روشهایی که در IKEv2، برای انجام عملیات احراز اصالت می‌تواند مورد استفاده قرار گیرد، به کارگیریِ پروتکل احراز اصالت قابل گسترش(EAP) است. EAP یک پروتکل قابل گسترش است که با فراهم آوردن یک چارچوب کلی و بدون وابستگی به روش خاصی امکان بهره گیری از روشهای مختلف احراز اصالت را در داخل این چارچوب فراهم می‌آورد. بسیاری از روشهای به کارگرفته شده در این پروتکل نامتقارن و یک طرفه هستند و معمولاً برای احراز اصالت کارفرما به یک کارگزار کاربرد دارند. از این رو در IKEv2 نیز از EAP برای احراز اصالت آغازگر به مخاطب استفاده می‌شود و در مقابل مخاطب لازم است توسط مکانیزم امضا احراز اصالت شود.اصولاً علت مطرح شدن این روش این است که بتوان از روشهای احراز اصالت دیگر هم در آینده در IKE استفاده کرد، بدون اینکه نیازی به بازنویسی کل استاندارد مربوط به IKE باشد.

نحوه استفاده از EAP در IKEv2 بدین صورت است که در پیام سوم تبادلات آغازین، آغازگر با ارسال شناسه خود، با نیاوردن فیلد AUTH در پیام خود، اعلام می‌کند که قصد استفاده از EAP را برای احراز اصالت خود به مخاطب دارد. در مقابل اگر مخاطب مایل به استفاده از EAP باشد، یک بدنه درخواست EAP در پیام چهارم، در کنار فیلدهای دیگر این پیام قرار می‌دهد. البته مخاطب در این مرحله، روند آغاز اولین CHILD-SA را با نفرستادن بدنه SA_{r2}، TS_r و TS_i تا پایان عملیات احراز اصالت به تأخیر می‌اندازد. با اتمام موفق تبادلات EAP، باید یک بدنه حاوی پیغام موفقیت، از سوی مخاطب به آغازگر ارسال شود (یا در صورت عدم موفقیت، پیغام شکست برای آغازگر ارسال گردد). پس از آن (در صورت حصول موفقیت) در دو پیام بعدی، باید فیلد AUTH توسط آغازگر و مخاطب رد و بدل شود و بالاخره در پیام آخر مخاطب با ارسال بدنه های SA_{r2} ، TS_r و TS_i، اولین CHILD-SA را راه اندازی می‌کند.روند تبادلات آغازین در هنگام استفادهٔ آغازگر از EAP در شکل (۲) آمده است.



شکل۲: روند تبادلات آغازین در هنگام استفاده از EAP

همانگونه که در [8] هم ذکر شده است از EAP می‌توان برای حفاظت از شناسه آغازگر در برابر حمله فعال نیز بهره برد. نحوه کار بدین صورت است که در پیام سوم، آغازگر به جای ارسال شناسه کامل خود در فیلد ID_i، تنها به ارسال قسمت قلمرو از شناسه دسترسی به شبکه (NAI)[12] [9] اکتفا کند و از ذکر قسمت اسم همتا در NAI کامل خود، در این پیام بپرهیزد. در آن سو مخاطب با توجه به قسمت قلمرو در NAI، روش احراز اصالت مناسب را انتخاب می کند. روش انتخاب شده باید قادر باشد شناسه کامل آغازگر را کسب و احراز اصالت کند. نیز مخاطب می‌تواند در پیام چهارم و در کنار فیلد AUTH، به عنوان اولین درخواست EAP، درخواستی از نوع شناسه داشته باشد. بدین ترتیب تنها پس از پیام چهارم و پس از اینکه مخاطب اصالت خود را اثبات کرد، آغازگر شناسه کامل خود را با استفاده از روشها و پیامهای EAP، در اختیار مخاطب می‌گذارد و بدین وسیله شناسه خود را در برابر حمله کننده فعال مصون می‌سازد.

12 Network Access Identifier

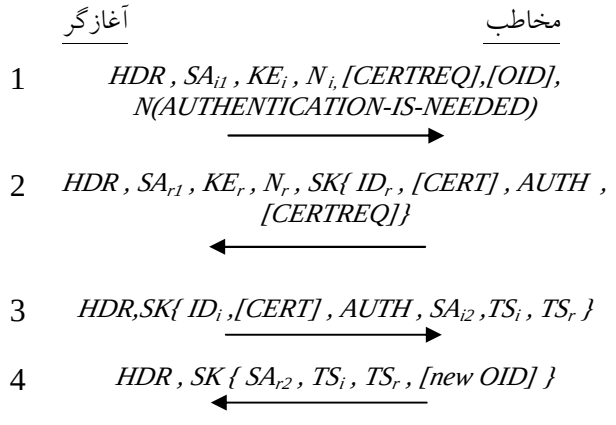
۳-۲- حفاظت از شناسه آغازگر در برابر حمله‌کنندگان فعال با اصلاح تبادلات آغازین

در این قسمت روش دیگری برای محافظت از شناسه آغازگر در برابر حمله کنندگان فعال پیشنهاد می‌شود که به اختصار آنرا IKEv2-i می‌نامیم. در این روش تبادلات آغازین به ترتیبی تغییر می‌کنند تا ابتدا این مخاطب باشد که ملزم به احراز هویت و اصالت خود برای آغازگر باشد و تنها پس از آن، آغازگر شناسه رمز شده خود را در اختیار مخاطبِ احراز اصالت شده، قرار دهد.

همانگونه که در شکل (۱) دیده می‌شود، در پیام سوم آغازگر لازم است شناسه خود را در اختیار مخاطبی قرار دهد که هنوز احراز اصالت نشده است. مشکل زمانی پدید می آید که آغازگر پس از ارسال پیام سوم موفق به احراز اصالت مخاطب نشود و در عوض شناسه خود را درا ختیار یک موجودیت نامعتبر قرار داده باشد.

بر اساس ملاحظات امنیتی، لازم است فیلد شناسه (ID) ، فیلد AUTH و فیلد گواهی (CERT)، در پیامها حتماً به صورت محافظت شده ارسال شوند تا از دید موجودیتهای دیگر شبکه پنهان نگاه داشته شوند. همانگونه که در IKEv2 بیان شده است، بدنه رمز شده باید آخرین بدنه از بدنه های یک پیام باشد[۲] و بدیهی است که این فیلد تنها پس از آنکه آغازگر و مخاطب بر روی الگوریتمهای رمزنگاری و کلیدهای مربوطه به توافق رسیدند، قابل تولید و ارائه خواهد بود. همچنین در IKEv2 ذکر شده است که اغلب بدنه رمز شده، تنها بدنه موجود در پیام های IKEv2 است ولی در عین حال هیچ کجا بیان نشده است که این امر لازم و اجباری است و در اصل همانگونه که گفته شد تنها الزامی که وجود دارد، این است که بدنه رمز شده آخرین بدنه در یک پیام IKEv2 باشد. با توجه به این نکته و نیز با توجه به روند تبادلات آغازین در IKEv2 ،پیشنهاد می‌شود این تبادلات به صورتی که در شکل (۳) نشان داده شده است، در آیند تا بدین وسیله، هدف حفاظت شناسه آغازگر در برابر حمله کنندگان برآورده شود.

در روند پیشنهاد شده در پیام اول، آغازگر ضمن ارسال مجموعه پیشنهادهای خود برای تشکیل IKE-SA و نیز نانس و نیم کلید دیفی- هلمن خود، اقدام به ارسال یک اعلان با عنوان AUTHENTICATION-IS-NEEDED و در صورت لزوم، فیلد اختیاری درخواست گواهی (CERTREQ) می کند. علاوه بر این همانگونه که در شکل (۳) نیز دیده می‌شود، آغازگر در این پیام می‌تواند از فیلد اختیاری (OID) استفاده کند. این فیلد در حالتی به کار برده می‌شود که آغازگر قصد داشته باشد از روش کلید از پیش مشترک برای انجام عملیات احراز اصالت استفاده کند. در این رابطه در ادامه توضیحات بیشتری ارائه خواهد شد.



شکل ۳: روند تبادلات آغازین در IKEv2-i

با این نحوه ارسال پیام ۱، مخاطب متوجه خواهد شد که آغازگر مایل است ابتدا مخاطب هویت خود را به او اثبات کند و سپس شناسه خود را اعلام خواهد کرد. در این حالت مخاطب در پیام ۲، ضمن ارسال مجموعه مورد قبول خود برای ایجاد IKE-SA و نیز نیم کلید دیفی- هلمن و نانس خود، به عنوان آخرین بدنه در این پیام، شناسه و فیلد AUTH همراه با فیلدهای اختیاری گواهی (CERT) و درخواست گواهی (CERTREQ) را در قالب یک بدنه محافظت شده تحت الگوریتم ها و کلیدهای توافق شده (که در این مرحله برای مخاطب مشخص هستند)، برای آغازگر ارسال می کند. آغازگر پس از دریافت شناسه مخاطب و احراز اصالت او اقدام به ارسال پیام سوم (که همانند پیام سوم در تبادلات آغازین در IKEv2 است) می کند. در انتها مخاطب در پیام چهارم، مجموعه توابع و انتخابگرهای مورد قبول خود برای تشکیل IPsec-SA را برای آغازگر می‌فرستد.

بدین ترتیب و بر اساس روند ذکر شده، ابتدا لازم است مخاطب هویت خود را اثبات کند و سپس آغازگر بعد از آنکه از هویت مخاطب آگاه شد و از صحت ادعای او اطمینان حاصل کرد، اقدام به ارسال شناسه خود می کند و بدین صورت آنرا در برابر موجودیت های نامعتبر محافظت می کند. این مزیت در حالی حاصل شد که بر تعداد پیامهای تبادلات آغازین، پیامی اضافه نشد و در ضمن پیچیدگی خاص و محاسبات اضافی و قابل توجهی نیز به سیستم تحمیل نگردید.

در حالت استفاده از کلید از پیش مشترک، لازم است از مفهوم شناسه یکبار مصرف استفاده کرد. این مفهوم همانند مفهومی است که در پروتکل SIGMA [۵] با علامت اختصاری OID نشان داده می‌شود. نحوه استفاده از شناسه یکبار مصرف در IKEv2-i بدین صورت است که دو طرف برای اولین بار همانگونه که بر سر مقدار کلید از پیش مشترک توافق می کنند، لازم است بر سر مقدار این شناسه نیز توافق کنند. سپس هنگامی که برای اولین بار آغازگر (که معمولاً یک کارفرما یا یک گره سیار است)، قصد ایجاد یک IKE-SA با مخاطب (که معمولاً یک کارگزار است) را داشت، در درخواست خود در تبادل IKE-SA-INIT ،از شناسه یکبار مصرف شناخته شده برای آن مخاطب استفاده می کند. در مقابل مخاطب نیز با دیدن شناسه یکبار مصرف، با جستجو در جدول مربوطه در صورت یافتن آن، مقدار کلید از پیش مشترک متناظر آن را استخراج می کند و از آن در ساختن فیلد AUTH برای احراز اصالت خود به آغازگر استفاده می کند. اگر کارگزار با اجرای این نحوه پروتکل موافق نبود، در پیام دوم عدم موافقت خود را اعلام می‌کند. پس از پایان مراحل ساخت IKE-SA و IPsec-SA مخاطب در پیام چهارم، مقدار جدید شناسه یکبار مصرف آغازگر را به صورت رمز شده برای استفاده در دفعات بعدی برای آغازگر ارسال می کند(فیلد (new OID) در شکل (۳)). در نهایت نیز این شناسه در اولین درخواست بعدی IKE-SA-INIT با این مخاطب خاص استفاده می‌شود و از آن پس، دوباره در صورت موفقیت در تولید IPsec-SA و IKE-SA ، شناسه یکبار مصرف جدید تولید و مبادله می‌شود. اگر به هر دلیلی اجرای پروتکل به انتها نرسید و در نتیجه در مرحله آخر فیلد new ID صادر نشد، کماکان فیلد OID قبلی به قوت خود باقی خواهد بود و آغازگر برای برقراری ارتباط موفق با کارگزار از همان فیلد بایستی استفاده نماید.

در استفاده از شناسه‌های یکبار مصرف باید دقت داشت که هر مخاطب (که معمولاً کارگزار یک شبکه است)، در تولید این شناسه‌ها برای آغازگرهای مرتبط با خود (که معمولاً کارفرمایان و یا گره‌های سیار شبکه آن کارگزار هستند)، این نکته را رعایت کند که شناسه های کاربران متفاوت باید کاملاً از هم متمایز باشند تا بتواند از روی آنها کاربر و کلید از پیش‌مشترک متناظر آنرا به درستی تشخیص دهد. نکته دیگری که در مورد این شناسه ها لازم به ذکر است، این است که این شناسه ها باید تا حد امکان تصادفی باشند تا از سوی ناظران خارجی قابل تشخیص نباشند.

۳-۳ تحلیل روش پیشنهادی

در مورد ارزیابی پروتکل ارائه شده باید گفت که این پروتکل از لحاظ برآورده ساختن نیازمندیهای امنیتی مختلف از قبیل پنهان‌سازی، درستی و تازگی کلید و نیز احراز حضور و اصالت طرفها از وضعیت مشابهی در مقایسه با IKEv2 برخوردار است. در واقع از آنجا که در این پروتکل در دو پیام ابتدایی ، عملیات مربوط به تولید مواد کلیدی از طریق تبادل نیم کلیدهای دیفی- هلمن و همچنین نانسها انجام می‌شود و نیز کلیهٔ این موارد به هنگام احراز اصالت طرفین و در هنگام تولید فیلدهای AUTH درستی و صحتشان به اثبات می‌رسد و همچنین از آنجا که این روش دقیقاً همانند روشی است که در IKEv2 عمل می‌شود، هر دو پروتکل از عملکرد یکسانی در موارد بیان شده برخوردارند. همچنین از آنجا که روش احراز اصالت و نیز تولید بدنه‌های AUTH در این پروتکل همانند روش به‌کاررفته در IKEv2 است، تفاوتی در احراز اصالت و حضور طرفها بین این دو پروتکل وجود ندارد. همچنین با توجه به اینکه تعداد پیامها در هر دو پروتکل یکسان است، از لحاظ تأخیر نیز هر دو از عملکرد یکسانی برخوردارند. در رابطه با طول پیامها نیز همانگونه که دیده می‌شود، بدنه‌های به کاررفته در پیامهای تبادلات آغازین در هر دو پروتکل تقریباً

یکسان هستند و از این‌رو در میزان پهنای باند مصرفی در هر دو پروتکل تفاوتی وجود ندارد. در مورد ساده‌سازی ارتباطات متعاقب نیز با توجه به اینکه در این پروتکل و نیز IKEv2 از تبادل CREAT-CHILD-SA برای تولید IPsec-SA های جدید تحت IKE-SA ی راه‌اندازی شده استفاده می‌شود، عملکرد هر دو پروتکل یاد شده در این زمینه یکسان می‌باشند و در هر دو ارتباطات متعاقب ساده‌سازی شده‌اند .

شاید مهمترین ابهام در مورد این روش، مسأله میزان مقاومت آن در برابر حملات از کار اندازی سرویس[۱۳] (DoS) باشد. خصوصاً اینکه همانگونه که ذکر شد، این روش بیشتر برای استفاده در محیطهای کارگزار- کارفرما که مسأله مقاومت در برابر حملات DoS در آنها از اهمیت خاصی برخوردار است، طراحی شده است. در این رابطه باید گفت در IKEv2-i نیز مانند IKEv2، اگر با دریافت پیام اول، مخاطب خود را در معرض حمله DoS احساس کرد، تنها به ارسال یک کوکی در پاسخ درخواست دریافت شده اکتفا می‌کند و کار بیشتری انجام نمی‌دهد و تنها زمانی پاسخی همانند پیام دوم در IKEv2-i برای آغازگر ارسال می کند که تکرار پیام اول را همراه با کوکی ارسالی دریافت دارد. پس در این زمینه تفاوتی بین IKEv2 و IKEv2-i وجود ندارد. در این روش مخاطب با دریافت پیام اول، هرگاه خود را در معرض حمله DoS احساس کرد، تنها به ارسال یک مقدار تحت عنوان کوکی در پاسخ درخواست دریافت شده اکتفا می‌کند و کار بیشتری انجام نمی‌دهد و تنها زمانی پاسخی همانند پیام دوم در IKEv2 برای آغازگر ارسال می‌کند که تکرار پیام اول را همراه با کوکی ارسالی از آغازگر دریافت دارد. مقدار این کوکی باید به گونه‌ای باشد که آغازگر بدون دریافت آن قادر به حدس زدن مقدار آن نباشد و همچنین در سوی مقابل مخاطب نیز قادر باشد با دریافت تکرار پیام اول، بدون اینکه نیازی به ذخیره‌سازی حالتی داشته باشد، بتواند کوکی متناظر آن درخواست را بازتولید کند و با کوکی دریافتی مقایسه نماید و بدین ترتیب تنها به درخواستهایی رسیدگی خواهد شد که از سوی آغازگرهای واقعی ارسال شده باشند.

آنچه در ازای دستیابی به حفاظت از شناسه آغازگر در قبال حمله فعال از دست می‌رود، عدم حفاظت از شناسه مخاطب در قبال حمله فعال است، ویژگی‌ای که در نسخه اصلی IKEv2 برقرار می‌ماند. اینکه کدامیک از این دو ویژگی از اهمیت بیشتری برخوردارند، وابسته به کاربرد و محیط بکارگیری پروتکل است. به طور مثال در بسیاری از محیطهای کارفرما – کارگزار لورفتن شناسه کارگزار تقریباً هیچ مشکلی به وجود نمی‌آورد، در حالیکه همانگونه که پیشتر اشاره شد، لورفتن شناسه آغازگر می‌تواند موجب مخدوش شدن حریم خصوصی این کاربران گردد.در مقابل در محیطهای همتا به همتا که آغازگر و مخاطب به دنبال برخورداری از سطح یکسانی از حفظ حریم خصوصی خود هستند، حفاظت از شناسه مخاطب در قبال حمله فعال از اهمیت به مراتب بیشتری برخوردار است، چرا که در واقع این آغازگر است که اجرای پروتکل را آغاز می‌کند.

بنابراین با توجه به نیازهای امنیتی متفاوتی که بین این دو محیط وجود دارد، استفاده یکسان از IKEv2 در هر دو آنها توصیه نمی‌شود و در عوض پیشنهاد می‌شود که بسته به محیط به‌کارگیری از IKEv2 و یا IKEv2-i استفاده گردد.

در رابطه با مقایسه IKEv2-i با روش بیان شده در (۳-۱) که در آن از پروتکل EAP بهره برده می‌شد، باید گفت که IKEv2-i از تعداد پیامهای کمتر و در نتیجه تأخیر کمتری برخوردار است، ضمن آنکه در IKEv2-i نیز همچنان این امکان برای آغازگر وجود دارد که به منظور احراز اصالت خود به مخاطب، از پروتکل EAP استفاده کند و بدین ترتیب از مزایای آن بهره‌مند گردد. از این‌رو برای استفاده از EAP نیز مشکلی در IKEv2-i وجود ندارد و از این منظر نیز تفاوتی با IKEv2 ندارد.

٤- نتیجه‌گیری

در این مقاله ابتدا ضمن معرفی نسخه جدید پروتکل تبادل کلید در اینترنت به برخی از مزایای آن نسبت به نسخه پیشین اشاره شد. در ادامه با اشاره به مشکل عدم حفاظت از شناسه آغازگر در برابر حمله فعال در IKEv2 که خصوصاً در محیطهای کارفرما – کارگزار از اهمیت به سزایی برخوردار است، دو

13 Denial of Service

پیشنهاد برای رفع آن ارائه شد که یکی مبتنی بر استفاده از پروتکل احراز اصالت قابل گسترش (EAP) بود ودیگری تنها با اصلاح تبادلات آغازین در IKEv2 بدست آمد. پیشنهادهای ارائه شده در هر دو نحوه احراز اصالت در IKEv2 (یعنی نحوه مبتنی بر امضا و نحوه کلید از پیش مشترک) قابل بکارگیری هستند. با استفاده از این پیشنهاد ها می توان مزیت امنیتی حفاظت شناسه آغاز گر در برابر حمله فعال را که خصوصاً برای کاربران شبکه های خصوصی مجازی (VPN) وکاربران سیار بسیار حائز اهمیت است، به مجموعه خصوصیات مثبت IKEv2 افزود. پیشنهادات ارائه شده در قالب کلی پروتکل IKEv2 ارائه شدند. در نتیجه هرگاه آغازگر احساس نیاز کند، قادر به استفاده از گونه‌های مذکور خواهد بود و همانطور که در تحلیل روش پیشنهادی تبیین گردید ، هزینه خاصی برای نیل به ویژگی حفاظت شناسه آغازگر در قبال حملات فعال، پرداخت نخواهد شد.

مراجع

[1] Kent, S. and K. Seo, Security *Architecture for the Internet Protocol*, RFC 4301, December 2005.

[2] Kaufman, C., *Internet Key Exchange (IKEv2) Protocol*, RFC 4306, December 2005.

[3] Harkins, D. and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.

[4] Aiello, W., Bellovin, S. M., Blaze, M., Canetti, R. Ioannidis, J., Keromytis, A. D. and Reingld, O., *Just Fast Keying (JFK)*, Available at http://www.ietf.org/internet-drafts/draft-ietf-ipsec-jfk-04.txt, 2002.

[5] Krawczyk, H., *The IKE-SIGMA Protocol*, Internet draft available at http://www.ietf.org/internet-drafts/draft- Krawczyk-ipsec-ike-sigms-00.txt, November 2001.

[6] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, RFC 3748, June 2004.

[7] کرباسیون،م، تحلیل و ارتقای پروتکل تبادل کلید برای امنیت لایه IP همراه با قابلیت جابجایی و چندخانگی در آن. ،دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، پایان نامه کارشناسی ارشد، ۱۳۸۶.

[8] Eronen, P. and Tschofenig, H., *Extension for EAP Authentication in IKEv2*, Internet draft Available at http://www.ietf.org/internet-drafts/draft-eronen-ipsec-ikev2-eap-auth-05.txt, June 2006.

[9] Aboba, B. and M. Beadles, *The Network Access Identifier*, RFC 2486, January 1999.