

بهینه‌سازی IKEv2 برای استفاده در ارتباطات امن درون سازمانی

مهدی برنجکوب

استادیار دانشگاه صنعتی اصفهان
brnjkb@cc.iut.ac.ir

محمد مهدی کرباسیون

عضو هیأت علمی دانشگاه آزاد اسلامی واحد خمینی شهر
karbasian@iaukhsh.ac.ir

چکیده - در این مقاله ضمن معرفی نسخه جدید پروتکل تبادل کلید در اینترنت، به برخی مزایای آن نسبت به نسخه پیشین اشاره خواهد شد. در ادامه پس از بیان مشکلات این پروتکل برای استفاده در ارتباطات امن درون سازمانی، نسخه‌ای جدید از این پروتکل ارائه شده است که مناسب استفاده در ارتباطات مذکور می‌باشد. در پروتکل پیشنهاد شده از کارگزار سازمان در حین تبادلات پروتکل و برای انجام عملیات احراز اصالت طرفها به عنوان طرف سوم مورد اعتماد استفاده شده است و بدین صورت روشی ساده‌تر و با نیازهای کمتر برای انجام عملیات احراز اصالت ارائه شده است.

کلید واژه- IKE، احراز اصالت، تداعی‌گر امنیتی، طرف سوم قابل اعتماد و ارتباطات امن درون سازمانی.

۱- مقدمه

مختلف آن و نیز در رقابت با سایر جایگزینهای مطرح، از جمله JFK [۴] و SIGMA [۵]، تحت عنوان IKEv2 ارائه گردید. از جمله مهمترین مزایای نسخه جدید نسبت به نسخه پیشین IKE می‌توان به مواردی از جمله 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 و استاندارد شدن نحوه عبور بسته‌های IKE و IPsec از دروازه های NAT و همچنین استاندارد شدن روند درخواست یک آدرس داخلی از یک شبکه دور اشاره کرد [۲].

در ادامه ابتدا نسخه جدید پروتکل توزیع کلید اینترنت IKEv2 معرفی می‌شود. سپس با اشاره به ارتباطات درون سازمانی و نیازها و مسائل موجود در آنها، نسخه‌ای از IKEv2 ارائه خواهد شد که ضمن حفظ امکاناتی که این پروتکل در اختیار قرار می‌دهد، مناسب استفاده در ارتباطات مذکور باشد. سپس تحلیلی درباره روش پیشنهادی ارائه می‌شود و سرانجام با مروری بر مطالب مقاله نتیجه‌گیری می‌شود.

مکانیزم IPsec [۱]، 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 نیز توافق روی الگوریتمهای رمزنگاری نیاز است. آنچه در مکانیزم IPsec به عنوان پیش فرض قلمداد شده است، استفاده از پروتکل تبادل کلید اینترنت (IKE) می باشد.

۲- معرفی پروتکل تبادل کلید اینترنت (IKEv2)

IKE ضمن انجام احراز اصالت طرفین ارتباط، دوتداعی‌گر امنیتی به نامهای IKE-SA و IPsec-SA (که به آن Child-

نسخه جدید پروتکل تبادل کلید اینترنت (IKEv2) [۲] پس از بررسی های زیاد بر روی نتایج حاصل از مطالعاتی که روی نسخه اولیه این پروتکل (IKEv1) [۳] و پیاده سازیهای