علیرضا سلطانی نشان

تکلیف دوم

تاریخ 18 اسفند 99

آی پی سک چیست؟

منبع:

Cloud Flare

**ای پی سِک[[1]](#footnote-1) یا IPsec چیست؟**

همان طور که گفته شد، ای پی سک نوعی پشت پروتکل [[2]](#footnote-2)است، چرا که مجموعه ای از پروتکل هایی را داراست، که برای داشتن ارتباط امن و رمزنگاری شده بین دستگاه ها مورد استفاده قرار می­گیرد. این پروتکل سبب آن است، داده هایی که به شبکه عمومی (اینترنت) ارسال می­شوند به صورت امن نگه داشته شوند. ای پی سکِ غالبا برای راه اندازی فناوری های VPN که معمولا به احراز هویت [[3]](#footnote-3)و یکپارچگی [[4]](#footnote-4)و غیره مربوط است، با رمزنگری بسته های ای­پی همراه با تایید اعتبار، استفاده می­شود.

به همین ترتیب واژه های IPsec و IP مبتنی بر سرواژگان”Internet Protocol” و واژه sec بر واژه Security است، پروتکل آی­پی مسیر اصلی پروتکل استفاده شده در شبکه جهانی اینترنت است، این پروتکل تعین میکند، دیتایی که قرار است هدایت شود از چه آدرس آی­پی استفاده می­کند. IPsec امن است بخاطر این که این پروتکل رمزنگاری [[5]](#footnote-5)هایی را به فرایند احراز هویت اضافه می­کند. تمام فرایند های آی­پی سک همه در قسمت لایه کاربردی استاندارد OSI مورد استفاده قرار می­گیرند تا رد و بدل اطلاعات بین مبدا و مقصد همگی به صورت امن، انجام شود که در این بین کسی نتواند شنودی در بین دیتا هایی در حال Send و receive کند.

**ای پی سِک[[6]](#footnote-6) چگونه عمل می­کند؟**

**تعویض کلید ها:** کلید ها بسیار مورد نیاز و لازم هستند تا بتوانیم فرایند رمزنگاری را انجام دهیم. یک کلید رشته ای رندم از حروف مختلف است که برای قفل کردن یا رمزنگاری و رمزگشایی (باز کردن) پیام ها، استفاده می­شود. IPsec کلید هایی را با یک تعویض بین دستگاه های متصل، تنظیم و کنترل می­کند، به همین خاطر هر دستگاهی میتواند پیام دیگر دستگاه ها را رمزگشایی کند.

**packet** **header و trailers:** تمام دیتا هایی که در یک شبکه ارسال میشود به قطعه های کوچکی به نام پکت در لایه شبکه تقسیم می­شوند. پکت ها دارای یک پی لود یا هدر یا اطلاعاتی در مورد داده ای که کامپیوتر ها دریافت میکنند و چگونگی استفاده آنها، هستند.ای­پی سک تعدادی هدر به پکت هایی که حاوی احراز هویت و رمزنگاری داده ها هستند اضافه می­کند.

**احراز** **هویت:** ای پی سک احراز هویت هایی برای هر پکت ارائه می­دهد مانند یک مهر برای هر ایتم جمع آوری شده. این عمل باعث می­شود تا پکت ها اعتماد زیادی از مبدا داشته باشند که در طی مسیر توسط حمله کنندگان مورد نقض امنیت قرار نگیرد.

**انتقال**[[7]](#footnote-7): بسته های رمزنگاری شده IPsec با استفاده از یک پروتکل انتقال و حمل و نقل در سراسر یک یا چند شبکه خود عبور می­کنند. به خاطر این رمزنگاری ترافیک هایی که ناشی از آی­پی سک هستند با ترافیک های آی­پی که به صورت عادی می­باشد که معمولا هم از پروتکل UDP بجای TCP برای انتقال داده ها استفاده می­کنند، متفاوت هستند. پروتکل کنترل انتقال، اتصالات خصوصی بین دستگاه را فراهم می­کند و اطمینان حاصل میکند که همه بسته ها می­رسند. UDP پروتکل دیتاگرام از سمت کاربر هستن که هیچ تضمینی در ارسال و صحت دریافت آن بسته در مقصد، نمی­کند به صورت خصوصی تنظیم نمی­کند. آی­پی سک از UDP استفاده می­کند بخاطر اینکه این کار به بسته های IPsec اجازه می دهد تا از طریق فایروال ها عبور کنند.

1. Internet Protocol Security [↑](#footnote-ref-1)
2. Behind Protocol [↑](#footnote-ref-2)
3. Auth (Authentication) [↑](#footnote-ref-3)
4. Integrity [↑](#footnote-ref-4)
5. Encryption [↑](#footnote-ref-5)
6. Internet Protocol Security [↑](#footnote-ref-6)
7. Transmission [↑](#footnote-ref-7)