علیرضا سلطانی نشان

تکلیف دوم

تاریخ 18 اسفند 99

آی پی سک چیست؟

منبع:

Cloud Flare

ای پی سِک[1] یا IPsec چیست؟

همان طور که گفته شد، ای پی سک نوعی پشت پروتکل [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]و یکپارچگی [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]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] 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

---

[1] Internet Protocol Security
[2] Behind Protocol
[3] Auth (Authentication)
[4] Integrity
[5] Encryption
[6] Internet Protocol Security

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]: 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.

[7] Transmission