Kerberos

Arash TaherKalateh ۸۸۲۹۸۰

Kerberosیک روش امن برای تایید هویت به منظور استفاده از یک سرویس تحت شبکه تعریف میشود. آغاز این پروژه در MIT بود و نام آن از یک افسانه یونانی، مربوط به سگ سه سر نگهبان گرفته شده است و در دو نسخه رایگان و تجاری عرضه شده است.

بیشتر پروتکل‌هایی که در اینترنت پیاده سازی شده اند امن نیستند و به اسانی امکان Sniff شدن را به مهاجم میدهند. پسوردهایی که بدون رمزنگاری روی اینترنت فرستاده میشوند به راحتی دیده میشوند. ضعف‌های دیگری نیز وجود دارد، مثلا برنامه‌های Client/Server انتظار دارند که کاربر آنها درباره هویت خود صادق باشد و یا از او انتظار دارند فقط کارهایی را انجام دهد که مجاز به انجام دادن آنهاست.

یکی از را حل‌های ارائه شده استفاده از Firewall است. اما مشکل در اینجاست که فایروال جلوی نفوذ خارجی‌ها را می‌گیرید، در حالی که بسیاری از آسیب‌های اساسی از سمت افراد داخلی تحمیل میشوند . Kerberos protocolراه حلی است برای حل این مشکلات امنیتی در شبکه.

Kereberosبه کاربر اجازه میدهد که از Kerberos Key Distribution Center (kdc) درخواست یک "بلیط" رمز شده کند تا بعدا از این بلیط برای درخواست خدمات از سرور استفاده نماید. در اینجا نیازی نیست پسورد کاربر روی شبکه فرستاده شود.

این روش مانع از eavesdropping و replay attacks میشود. منطق آن از رمزنگاری کلید متقارن استفاده می‌کند و نیازمند به فرد ثالث معتمد است. پورت پیش فرض در پیاده سازی این پروتکل ۸۸ است.

به صورت خلاصه این پروتکل به صورت زیر کار می‌کند:

۱ .فرض کنید می‌خواهید به یک سرور توسط Telnet یا روش‌های دیگر ورود متصل شوید. میدانید برای اینکه این سرور به درخواست شما پاسخ دهد نیاز به Kereberos ticket دارید.

۲ .برای گرفتن بلیت یک درخواست تصدیق برای Authentication server (as) ارسال می‌کنیم . ASبا توجه به رمز عبور کربر (که از نام کاربری آن به دست میاورد) و یک مقدار تصادفی که برای سرویس درخواستی است، یک Session-key که رمز شده هم هست می‌سازد. این session-key در در واقع

یک "بلیت اعطا بلیت" است.

۳ .در مرحله بعد "ticket-granting ticket" تولید شده را برای یک ticket-granting server (tgs)می‌فرستیم. این سرور میتواند از نظر فیزیکی همان سرور قبلی باشد، اما کاری که الان انجام میدهد برگرداندن بلیتی است که بتوان آن را برای استفاده از سرویس به سرور فرستد.

۴ .سرویس یا بلیت را رد می‌کند و یا آن را می‌پذیرد و سرویس مورد نظر را انجام میدهد.

۵ .بلیت دریافتی از TGS برچسب زمان خورده است، این موضوع اجازه میدهد که در یک بازه زمانی مشخص بتوان از همین بلیت برای درخواست‌های متوالی استفاده کرد. به این صورت هم می‌توان بدون نیاز به تصدیق هویت مجدد از سرویس‌ها استفاده کرد، و هم اینکه با نقض شدن آن پس از گذشت زمان، امکان سوٗ استفاده از کاهش می‌یابد.