مـز ايـــاي Kerberos

مقدمه

Kerberos نسخه ۵، پروتکل اعتبار سنجی پیش فرض شبکه برای ویندوز ۲۰۰۰ است. Kerberos پروتکل جدیدی نیست که مایکروسافت اختراع کرده باشد، بلکه از سال‌ها قبل در دنیای یونیکس مورد استفاده قرار گرفته است.

مایکروسافت اعتبار سنجی شبکه‌ای Kerberos را در ویندوز ۲۰۰۰ برای بالا بردن امنیت پیاده سازی کرده است، زیرا سرویس ها و سرورهای شبکه باید بدانند که یک سرویس گیرنده که درخواست اجازه دستیابی می کند واقعاً یک سرویس گیرنده معتبر است. Kerberos بر پایه ticket (بلیط)هایی که شامل هویت سرویس گیرنده که با کلیدهای مشترک رمزنگاری شده است، استوار می شود. Kerberos v5 بهبودهای زیر را نسبت به نسخه‌های قبلی Kerberos دارد:

- **ارسال اعتبارسنجی:** امکان می دهد که درخواست برای سرویس را از طرف یک کاربر به ارائه کننده سرویس قابل اطمینان دیگر محول کنیم.
- **سیستم های رمزنگاری قابل جایگزینی:** از چندین متد رمزنگاری پشتیبانی می کند. نسخه‌های قبلی Kerberos، فقط از رمزنگاری DES پشتیبانی می کردند.
- **کلیدهای زیر نشست (subsession):** به client و سرور امکان می دهد تا یک کلید زیر نشست کوتاه مدت را برای یک بار استفاده برای تبادل های نشست مورد مذاکره قرار دهند.

- **زمان دوام بیشتر برای بلیط:** حداکثر زمان بلیط در Kerberos v4، ۲۱/۲۵ ساعت بود. Kerberos v5 اجازه می دهد که بلیط ماه‌ها دوام بیاورد.

اعتبار سنجی در ویندوز ۲۰۰۰

ویندوز ۲۰۰۰ برای اعتبار سنجی هویت کاربر، پنج روش دارد:

- Windows NT LAN Manager (NTLM)
- Kerberos v5
- Distributed Password Authentication (DPA)
- Extensible Authentication Protocol (EAP)
- Secure Channel (Schannel)

ویندوز ۲۰۰۰، فقط از NTLM و Kerberos برای اعتبار سنجی شبکه ای استفاده می کند و سه پروتکل دیگر برای اعتبارسنجی در اتصال‌های شماره گیری یا اینترنت مورد استفاده قرار می گیرند.

ویندوز NT 4.0 از Windows NT LAN manager (NTLM) به عنوان پروتکل اعتبار سنجی شبکه ای پیش فرض استفاده می کند. به این دلیل NTLM هنوز در ویندوز ۲۰۰۰ وجود دارد تا سازگاری با نسخه های قبلی سیستم عامل های مایکروسافت حفظ شود. NTLM همچنین برای اعتبار سنجی logon به کامپیوترهای مستقل ویندوز ۲۰۰۰ به کار می رود. Kerberos، اعتبار سنجی شبکه ای پیش فرض برای ویندوز ۲۰۰۰ است.

Kerberos پروتکل اعتبارسنجی پر استفاده ای است که بر یک استاندارد باز بنا نهاده شده است. تمام کامپیوترهای ویندوز ۲۰۰۰ از Kerberos v5 در محیط شبکه ای استفاده می کنند، به غیر از شرایط زیر:

- کامپیوترهای ویندوز ۲۰۰۰ وقتی که به سرورهای ویندوز NT اعتبار سنجی می شوند از NTLM استفاده می کنند.
- وقتی که کامپیوترهای ویندوز ۲۰۰۰ به منابع domainهای ویندوز NT 4.0 دستیابی پیدا می کنند از NTLM استفاده می کنند.
- وقتی که کنترل کننده های domain ویندوز ۲۰۰۰، clientهای ویندوز NT 4.0 را اعتبار سنجی می کنند از NTLM استفاده می کنند.
- Login کردن به صورت محلی به یک کنترل کننده domain ویندوز ۲۰۰۰.
- ویندوز ۲۰۰۰.

Distributed Password Authentication (DPA) یک پروتکل اعتبارسنجی است که روی اینترنت به کار می رود تا به کاربران امکان دهد تا از یک کلمه عبور برای اتصال به هر سایت اینترنتی که به یک سازمان عضویت متعلق است، استفاده کنند. DPA توسط ویندوز ۲۰۰۰ پشتیبانی شده است ولی به همراه آن ارائه نشده است. شما باید PDA را به صورت جداگانه و به صورت یک محصول اضافی بخرید.

Extensible Authentication Protocol (EAP) یک گسترش برای پروتکل Point-to-Point است که برای اتصال های شماره گیری به اینترنت به کار می رود.

هدف EAP این است که اضافه کردن پویای ماژول های Plug-in اعتبار سنجی را هم در سمت سرور و هم در سمت سرویس گیرنده از یک اتصال اجازه دهد. اطلاعات بیشتر در مورد EAP در PPP Extensible Authentication (EAP) و Request for Comments 2284 (RFC) مورخ مارس ۱۹۹۸ یافت می شود. همچنین می توانید این RFC و RFCهای دیگر را در آدرس www.rfc-editor.org/ پیدا کنید.

Secure Channel شامل چهار پروتکل مرتبط است:

- Secure Sockets Layer (SSL) v2.0
- SSL v3.0
- Private Communication Technology (PCT) v1.0
- Transport Layer Security (TLS) v1.0

هدف اصلی استفاده از Schannel، فراهم کردن اعتبار سنجی، جامعیت داده‌ها و ارتباطات ایمن در اینترنت است. SSL معمولاً برای انتقال اطلاعات خصوصی به و از سایت های تجارت الکترونیک مورد استفاده قرار می گیرد. هر چهار پروتکل در Schannel، اعتبارسنجی را با استفاده از گواهی نامه های دیجیتال فراهم می کنند. گواهی نامه‌های دیجیتال با جزئیات بیشتر در فصل ۹، «Public Key Inftastructures. در ویندوز ۲۰۰۰» مورد بحث قرار گرفته اند.

مزایای اعتبار سنجی Kerberos

همانطور که محبوبیت و استفاده از ویندوز NT 4.0 در بازار افزایش یافت، علاقه جهان به سیستم های ویندوز NT نیز بیشتر شد. مایکروسافت با اضافه کردن اعتبار سنجی Kerberos در ویندوز ۲۰۰۰، به میزان زیادی قابلیت امنیتی سیستم عامل را

افزایش داده است. NTLM برای سازگاری با نسخه های قبلی ارائه شده است، ولی به محض اینکه تمام سرویس گیرنده های روی شبکه بتوانند با استفاده از Kerberos اعتبار سنجی شوند (که مستلزم سرورها و سرویس گیرهای ویندوز ۲۰۰۰ محض هستند) باید غیرفعال شود. تا وقتی که NTLM در شبکه موجود است، امنیت در بالاترین سطح خود قرار ندارد.

مزایای زیادی که Kerberos فراهم کرده، آن را نسبت به NTLM، انتخاب بهتری برای اعتبارسنجی نموده است. Kerberos بر پایه استانداردهای موجود بنا شده است، بنابراین به ویندوز۲۰۰۰ امکان می دهد تا روی شبکه‌های دیگری که از Kerberos v5 به عنوان مکانیزم اعتبارسنجی استفاده می کنند کار کند. NTLM نمی تواند این قابلیت را فراهم کند، زیرا خاص سیستم عامل های مایکروسافت است. اتصال به برنامه و سرورهای فایل نیز در هنگام استفاده از Kerberos سریعتر است، زیرا برای تعیین اینکه آیا اجازه دستیابی داده می شود یا خیر، سرور Kerberos فقط لازم است که هویتی که سرویس گیرنده ارائه می کند را بررسی کند. همین هویت ارائه شده توسط سرویس گیرنده می تواند برای کل نشست logon به شبکه به کار رود. وقتی که NTLM به کار می رود، برنامه و سرورهای فایل باید با یک کنترل کننده domain تماس برقرار کنند تا تعیین کنند که آیا اجازه دستیابی به سرویس گیرنده داده می شود یا خیر. اعتبارسنجی Kerberos همچنین هم برای سمت سرویس گیرنده و هم برای سمت سرور، اعتبارسنجی را فراهم می کند ولی NTLM فقط برای سرویس گیرنده،

اعتبار سنجی را فراهم می کند. سرویس گیرنده های NTLM مطمئناً نمی دانند که سروری که با آن ارتباط برقرار می کنند یک سرور نادرست است.

Kerberos همچنین برای اعتمادها (trusts) سودمند است و در واقع اساس اعتمادهای domain انتقالی است و ویندوز ۲۰۰۰، به صورت پیش فرض از اعتمادهای دو طرفه انتقالی با domain های ویندوز ۲۰۰۰ دیگر در همین مجموعه (forest)، استفاده می کند. یک اعتماد دو طرفه انتقالی از یک کلید بین ناحیه‌ای مشترک استفاده می کند. domain ها به یکدیگر اعتماد می کنند، زیرا هر دو کلید مشترک را در اختیار دارند.

استانداردهای اعتبارسنجی Kerberos

سالهاست که Kerberos ارائه شده است. مهندسانی که روی Project Athena کار می‌کردند، برای اولین بار Kerberos را در Massachusetts Institute of (MIT) Technology اختراع کردند. Project Athena در ۱۹۸۳ شروع شد، ولی اولین نمونه Kerberos تا سال ۱۹۸٦ عرضه نشد.

هدف Project Athena، ایجاد یک نسل جدید از امکانات کامپیوتری توزیع شده مبتنی بر سرویس گیرنده/ سرور در سطح دانشگاه بود. Kerberos v4، اولین نسخه عمومی پروتکل اعتبارسنجی بود. Kerberos v5، بهبودهای زیادی به پروتکل اضافه کرده است از جمله پشتیبانی از بلیط های قابل ارسال، قابل تجدید و تاریخ دار و تغییر الگوریتم key salt برای استفاده از کل اسم اصلی. دو تا از RFCهایی که Kerberos

v5 در آنها تعریف شده است، RFC 1510، Network Authentication Service، The Kerberos (v5) مورخ سپتامبر ۱۹۹۳ و RFC 1964، The Kerberos Version 5 GSS-API Mechanism، مورخ ژوئن ۱۹۹۶ است (GSS-API علامت اختصاری Generic Security Service-Application Program Interface است). مایکروسافت بیان می کند که پیاده سازی Kerberos در ویندوز ۲۰۰۰ بسیار مطابق با مشخصات تعیین شده در RFC 1510 برای پیاده سازی پروتکل و RFC 1964 برای مکانیزم و فرمت ارسال نشانه های (token) امنیت در پیغام های Kerberos است.

گسترش هایی در پروتکل Kerberos

مایکروسافت، نسخه Kerberos را در ویندوز ۲۰۰۰ گسترش داده است تا اعتبارسنجی اولیه کاربر بتواند به جای کلیدهای سری مشترک استاندارد مورد استفاده توسط Kerberos، با استفاده از گواهی نامه های کلید عمومی انجام شود. بهبود Kerberos به این طریق امکان می دهد که logon به ویندوز ۲۰۰۰ با استفاده از کارت‌های هوشمند انجام شود. بهبودهایی که مایکروسافت در Kerberos برای ویندوز ۲۰۰۰ ایجاد کرده است بر پایه مشخصات Public Key Cryptography for Initial Authentication in Kerberos که توسط چند شرکت بیرونی مثل (DEC) Digital Equipment Corporation، Novell، CyberSafe Corporation و دیگران به Internet Engineering Task Force (IETF) پیشنهاد شده است، استوار است.

نگاه کلی به پروتکل Kerberos

اسم Kerberos (با تلفظ یونانی) یا Cerberus (با تلفظ لاتین) از افسانه های یونان آمده است. Kerberos، سگ سه سری بود که از ورودی Hades محافظت می کرد. Kerberos برخلاف پروتکل های دیگر (مثل NTLM) که فقط سرویس گیرنده را اعتبارسنجی می کنند، اعتبار سنجی دو طرفه هم برای سرورها و هم برای سرویس گیرنده ها را فراهم می کند. Kerberos با این فرض کار می کند که تراکنش های اولیه بین سرویس گیرنده ها و سرورها روی یک شبکه ناامن انجام می شوند. شبکه هایی که ایمن نباشند می توانند به سادگی بوسیله افرادی که می خواهند یک سرویس گیرنده یا سرور را برای کسب دستیابی به اطلاعاتی که می تواند به آنها در رسیدن به هدفشان کمک کند (این اطلاعات هرچه می تواند باشد) تقلید کنند، تحت نظارت قرار گیرد.

مفاهیم پایه

یک کلید سری مشترک، فقط بوسیله آنهایی که نیاز دارند کلید سری (secret) را بدانند به اشتراک گذاشته می شود. کلید سری ممکن است بین دو فرد، دو کامپیوتر، سه سرور و غیره باشد. کلید سری مشترک به حداقل موجودیت های لازم برای انجام کار مورد نیاز، محدود است و به آنهایی که کلید سری مشترک را می دانند امکان می دهد تا هویت آنهایی که کلید سری مشترک را می دانند را بررسی کنند. Kerberos برای انجام اعتبارسنجی خود به کلیدهای مشترک وابسته است. Kerberos از

رمزنگاری کلید سری به عنوان مکانیزم پیاده سازی کلیدهای سری مشترک استفاده می‌کند. رمزنگاری متقارن که در آن فقط یک کلید، هم برای رمزنگاری و هم برای گشودن رمز به کار می رود، برای کلیدهای سری مشترک در Kerberos به کار می‌رود. یک موجودیت، اطلاعات را رمزنگاری می کند و موجودیت دیگر با موفقیت این اطلاعات را از حالت رمز در می آورد. این امر دانستن کلید سری مشترک بین دو موجودیت را ثابت می کند.

اعتبار سنج‌ها (Authenticators)

یک اعتبار سنج، اطلاعات یکتایی است که در کلید سری مشترک رمزنگاری شده است. Kerberos از timestampها استفاده می کند تا اعتبار سنج، یکتا باشد. اعتبار سنج ها فقط برای یک بار استفاده معتبر هستند، تا احتمال اینکه کسی سعی کند تا از هویت شخص دیگری استفاده کند را به حداقل برسانند. Replay که یک تلاش برای استفاده مجدد اعتبار سنج است، نمی تواند در Kerberos v5 انجام شود. با این احال، اعتبار سنجی دو طرفه وقتی می تواند رخ دهد که دریافت کننده اعتبار سنج، بخشی از اعتبار سنج اصلی را استخراج کند، آن را در یک اعتبار سنج جدید رمزنگاری کند و آن را به اولین اعتبار سنج بفرستد. بخشی از اعتبار سنج اصلی استخراج می شود تا ثابت شود که اعتبار سنج اصلی با موفقیت از رمز درآمده است. اگر کل اعتبار سنج اصلی بدون تغییر پس فرستاده شود، اعتبار سنج نمی داند که آیا دریافت کننده مورد نظر و یا یک مقلد آن را فرستاده است یا خیر.

Key Distribution Center

همانطور که Kerberos در افسانه های یونانی سه سر داشت، در تکنولوژی نیز Kerberos سه قسمت دارد. پروتکل اعتبار سنجی Kerberos، یک سرویس گیرنده، یک سرور و یک مرجع مورد اعتماد دارد. Key Distribution Center (KDC) مرجع مورد اعتماد مورد استفاده در Kerberos، پایگاه داده‌ای از تمام اطلاعات مربوط به principal (موجودیت)ها در قلمرو Kerberos را نگه می دارد. یک principal (موجودیت)، یک موجودیت با اسم منحصر به فرد است که در ارتباطات شبکه شرکمت می کند. یک قلمرو یا ناحیه، سازمانی است که یک سرور Kerberos دارد. از آنجایی که سیستمی که سرویس KDC را اجرا می کند دارای پایگاه داده های با اطلاعات account های امنیتی است، باید از نظر فیزیکی ایمن باشد. بخشی از این اطلاعات امنیتی، کلید سری است که بین یک موجودیت و KDC مشترک است. هر موجودیت، کلید سری مربوط به خود را دارد که دوام زیادی دارد به همین دلیل به این کلید، کلید دراز مدت نیز می گویند. وقتی که کلید دراز مدت بر یک موجودیت کاربر انسانی استوار است، از کلمه عبور کاربر مشتق می شود. این کلید دراز مدت طبیعتاً، تقارنی است.

کلید دیگری که به همراه KDC مورد استفاده قرار می گیرد، کلید نشست است که وقتی که یک موجودیت می خواهد با موجودیت دیگر ارتباط برقرار کند، KDC آن را صادر می کند. برای مثال، اگر یک سرویس گیرنده بخواهد با یک سرور ارتباط برقرار کند، سرویس گیرنده، درخواست را به KDC می فرستد و KDC به نوبه خود، یک

کلید نشست صادر می کند تا سرویس گیرنده و سرور بتوانند با یکدیگر اعتبار سنجی شوند. هر قسمت از کلید نشست در قسمت مربوطه در کلید دراز مدت، هم برای سرویس گیرنده و هم برای سرور، رمز نگاری می شود. به عبارت دیگر، کلید دراز مدت سرویس گیرنده، شامل کپی سرور از کلید نشست است و کلید دراز مدت سرور شامل کپی سرور از کلید نشست است. کلید نشست، طول عمر محدودی دارد و به این دلیل برای یک نشست login، مناسب می باشد. بعد از اینکه نشست login به پایان رسید، کلید نشست دیگر معتبر نیست. دفعه بعدی که سرویس گیرنده نیاز داشته باشد که به همان سرور وصل شود، باید برای یک کلید نشست جدید به KDC برود.

بلیط های نشست (Session Tickets)

سرویس گیرنده یک پیغام رمزنگاری شده را از KDC دریافت می کند که شامل هم کپی سرویس گیرنده و هم کپی سرور کلید نشست است. کپی سرور کلید نشست در یک بلیط نشست قرار دارد که خود شامل اطلاعاتی درباره سرویس گیرنده است و با استفاده از کلید سری مشترک سرور و KDC رمزنگاری می شود. سرویس گیرنده نمی تواند به بلیط نشست دستیابی داشته باشد، زیرا کلید سری مشترکی که سرور و KDC به اشتراک گذاشته اند را نمی داند.

حال که سرویس گیرنده، کلید نشست سرویس گیرنده و بلیط نشست سرورها را از KDC دریافت کرده است. می تواند با موفقیت با سرور تماس بگیرد. همانطور که سرویس گیرنده یک پیغام که حاوی بلیط نشست است و یک اعتبار سنج که با استفاده

از کلید و نشست، رمزنگاری شده است به سرور می فرستد. بعد از اینکه سرور، گواهی هویت را از سرویس گیرنده دریافت می کند، بلیط نشست را با استفاده از کلید سری مشترک (مشترک بین سرور و KDC)، از رمز بیرون می آورد و کلید نشست فرستاده شده توسط KDC را استخراج می کند. سپس از کلید نشست، برای از رمز در آوردن اعتبار سنجی که سرویس گیرنده فرستاده است استفاده می کند. سرور، هویت بیان شده سرویس گیرنده را قبول دارد زیرا KDC، به عنوان مرجع مورد اعتماد، هویت سرویس گیرنده را به اطلاع سرور رسانده است. در این زمان، اگر سرویس گیرنده درخواست اعتبار سنجی دو طرفه کرده باشد، تا وقتی flag درست در پیغامی که می فرستد تنظیم شده باشد، این اعتبار سنجی دو طرفه می تواند رخ دهد.

این یکی از تفاوت های بین Kerberos و مکانیزم های اعتبارسنجی دیگر است که فقط سرویس گیرنده ها را اعتبار سنجی می کنند. اگر سرویس گیرنده، درخواست اعتبار سنجی دو طرفه کند، سرور با استفاده از کپی خود از کلید نشست، timestamp شامل میلی ثانیه های اعتبار سنج سرویس گیرنده را به رمز در می آورد و آن را به سرویس گیرنده می فرستد.

بلیط های نشست می توانند برای یک دوره مشخص زمانی که بوسیله سیاست Kerberos در محدوده تعیین می شود، مجدداً مورد استفاده قرار گیرند. KDC، دوره زمانی را در ساختار بلیط قرار می دهد. این امر نیاز موجودیت را برای اینکه هر دفعه که بخواهد با موجودیت دیگر ارتباط برقرار کند مجبور باشد که به KDC برود، کم

می کند. موجودیت سرویس گیرنده، بلیط های نشست مورد نیاز برای ارتباط با موجودیت های دیگر را در حافظه گواهی هویت خود نگه می دارد. از طرفی دیگر، موجودیت های سرور، کلیدهای نشست را در حافظه گواهی هویت خود نگه نمی‌دارند، بلکه فقط منتظر می مانند تا یک موجودیت سرویس گیرنده، یک بلیط نشست را بفرستد و با استفاده از کلید سری مشترک آن را از رمز در آورد.

بلیط هایی برای اعطای بلیط

بلیط های نشست، تنها بلیط های مورد استفاده در Kerberos نیستند. KDC با استفاده از یک بلیط که خود بلیط هایی را در اختیار می گذارد (TGT)، ارتباط برقرار می کند و بررسی می کند که موجودیت ها همانی باشند که بیان می کنند. کاربری که به یک محدود Kerberos، logon می کند، از یک کلمه عبور استفاده می کند که از یک الگوریتم در هم سازی یک طرفه عبور می کند و به یک کلید دراز مدت تبدیل می‌شود. بعد نتایج درهم سازی به KDC فرستاده می شوند که به نوبه خود یک کپی از درهم سازی را از پایگاه داده account خود دریافت می کند. وقتی که سرویس گیرنده، کلید دراز مدت را می‌فرستد، یک بلیط نشست و کلید نشست درخواست می‌کند تا بتواند از آن برای برقراری ارتباط با KDC در طی نشست logon استفاده کند. بلیطی که KDC به سرویس گیرنده بر می گرداند، TGT در کلید دراز مدت KDC، رمزنگاری می شود و کپی سرویس گیرنده از کلید نشست در کلید دراز مدت سرویس گیرنده، رمزنگاری می شود. بعد از اینکه سرویس گیرنده، پیغام پاسخ را از

KDC دریافت می کند، از کلید دراز مدت خود (که روی سیستم سرویس گیرنده ذخیره شده است) برای از رمز در آوردن کلید نشست استفاده می کند. بعد از اینکه کلید نشست، از رمز در آمد، کلید دراز مدت از حافظه نهان سرویس گیرنده بیرون کشیده می شود، زیرا دیگر برای ارتباط با KDC برای بقیه مدت نشست logon و یا تا وقتی که TGT منقضی نشود، مورد نیاز نیست. این کلید نشست، کلیدنشست logon نیز نامیده می شود.

موجودیت سرویس گیرنده با KDC تماس حاصل می کند تا یک بلیط نشست برای برقراری ارتباط با موجودیت دیگر، مثل یک سرور بدست آورد. سرویس گیرنده از کلید نشست logon برای راه اندازی یک اعتبار سنج استفاده می کند و بعد اعتبار سنج TGT را به همراه یک درخواست برای یک بلیط نشست برای سروری که می‌خواهد به آن دستیابی پیدا کند، به KDC می فرستد. وقتی که KDC، پیغام را از سرویس گیرنده دریافت می کند، TGT را با استفاده از کلید دراز مدت خود از رمز در می آورد تا کلید نشست logon را استخراج کند و از آن اطلاعات برای صحت سنجی اعتبار سنج فرستاده شده به سرویس گیرنده استفاده می کند. هر زمان که سرویس گیرنده، TGT را به KDC می فرستد، باید یک اعتبارسنج جدید بفرستد.

سرویس های ارائه شده توسط Key Distribution Center

KDC وظایف خود را بین دو سرویس تقسیم می کند. Authentication (AS) Service که برای انتشار TGT ها به کار می رود و سرویس اعطای ticket (TGS) که

برای صادر کردن بلیط های نشست به کار می رود. این بدان معناست که وقتی که سرویس گیرنده برای اولین بار با KDC تماس برقرار می کند، با AS ارتباط برقرار می کند و وقتی که نیاز داشته باشد که با یک سرور ارتباط برقرار کند، بلیط اعطای بلیط صادر شده بوسیله طرف AS از KDC را به طرف TGS از KDC می فرستد تا بتواند یک بلیط نشست برای ارتباطات به سرور بفرستد.

اعتبار سنجی بین محدوده ای

KDC به دو سرویس مختلف تقسیم شده است، اگرچه یک سرویس از KDC می‌تواند هر دو کار را انجام دهد تا Kerberos بتواند از اعتبار سنجی در چند محدوده پشتیبانی کند. یک دلیل برای اینکه چندین محدوده بتوانند در یک سازمان به کار روند این است که بار روی یک KDC کم شود. بدون توجه به دلیل، محدوده های چندگانه فقط هنگامی وجود دارند که یک کلید بین محدوده ای بین KDCها به اشتراک گذاشته شده باشد. بعد از اینکه کلید بین محدوده ای به اشتراک گذاشته شد، TGS مربوط به هر محدوده، یک موجودیت امنیتی در KDC دیگر می شود.

وقتی که یک سرویس گیرنده در Realm 1 بخواهد به یک سرور در Realm 2 دستیابی داشته باشد، مستقیماً به KDC مربوط به Realm 2 نمی رود. بلکه ابتدا باید به AS در Realm 1، logon کند. AS در Realm 1، یک TGT به سرویس گیرنده پس می فرستد. سرویس گیرنده می داند که باید با سرور Realm 2 تماس برقرار کند. بنابراین از TGS در Realm 1، یک بلیط نشست برای سرور درخواست می کند.

TGS می فهمد که سرور در محدوده آن نیست و بنابراین یک بلیط ارجاعی به سرویس گیرنده صادر می کند. بلیط ارجاعی یک TGT است که با کلید بین محدوده‌ای مشترک بین Realm 1 و Realm 2 رمزنگاری می شود. سرویس گیرنده از بلیط ارجاعی استفاده می کند و یک پیغام به TGS در Realm 2 می فرستد. TGS در Realm 2، از کپی کلید بین محدوده ای خود برای از رمز در آوردن بلیط ارجاعی استفاده می کند و اگر این موفقیت آمیز باشد، یک بلیط نشست برای سرور Realm 2 به سرویس گیرنده Realm 1 می فرستد.

زیر پروتکل‌ها

Kerberos، سه زیر پروتکل دارد که exchange (تبادل) نیز نامیده می شوند. این سه زیر پروتکل عبارتند از:

- Authentication Service (AS) Exchange
- Ticket-Granting Service (TGS) Exchange
- Client/Server (CS) Exchange

As Exchange

As Exchange زیر پروتکلی است که KDC برای صادر کردن یک کلید نشست logon و یک TGT برای سرویس گیرنده از آن استفاده می کند. وقتی که یک کاربر به شبکه login می‌کند، یک پیغام بنام Kerberos Authentication Service Request (KRB_AS_REQ) به سمت سرویس اعتبار سنجی KDC فرستاده می شود.

بعد از اینکه سمت سرویس اعتبار سنجی KDC، پیغام KRB_AS_REQ را دریافت کرد، کاربر و نیز اطلاعات دیگر موجود در پیغام را صحت سنجی می کند. اگر

این صحت سنجی با موفقیت انجام نشود، KDC، یک KDC_ERROR ایجاد می کند و آن را به سرویس گیرنده می فرستد. بعد از این صحت سنجی موفقیت آمیز، KDC کلید نشست logon و TGT را ایجاد می کند و هر دو را در یک پیغام Kerberos Authentication Service Reply (KRB_AS_REP)، به سرویس گیرنده می‌فرستد. سرویس گیرنده برای از رمز در آوردن کلید نشست logon و TGT، از کلید دراز مدت استفاده می کند و آنها را در حافظه نهان گواهی هویت خود که یک ناحیه از حافظه فرار سرویس گیرنده‌هاست، ذخیره می کند.

TGS Exchange

TGS Exchange، زیر پروتکلی است که KDC برای صادر کردن یک کلید نشست سرور و یک بلیط نشست مربوط به سرور برای سرویس گیرنده مورد استفاده قرار می‌دهد. سرویس گیرنده با فرستادن یک پیغام Kerberos Ticket-Granting Service Request (KRB_TGS_REQ) به KDC، یک بلیط نشست برای سرور درخواست می کند. ساختار پیغام KRB_TGS_REQ، درست مثل ساختار نشان داده شده برای پیغام KRB_AS_REQ می باشد، ولی KRB_TGS_REQ، از فیلدهایی نیز استفاده می کند که بوسیله پیغام KRB_AS_REQ مورد استفاده قرار نمی گیرد. وقتی که KDC، پیغام KRB_TG_REQ را دریافت می کند، با استفاده از کلید سری مشترک، آن را از رمز در می آورد. KDC، کلید نشست logon مربوط به سرویس گیرنده ها را استخراج می‌کند که به نوبه خود برای از رمز در آوردن اعتبار سنج از آن استفاده می کند. اگر اعتبار سنج معتبر باشد، KDC داده های اختیار دهی را از بلیط استخراج می

کند و بعد یک کلید نشست ایجاد می کند تا بین سرویس گیرنده سرور به اشتراک گذاشته شود.

KDC یک کپی از کلید نشست را با استفاده از کلید نشست logon مربوط به سرویس گیرنده به رمز در می آورد. یک کپی از کلید نشست به همراه داده های اختیار دهی سرویس گیرنده در یک بلیط قرار داده می شود و بعد بلیط با استفاده از کلید دراز مدت سرور به رمز در می آید. تمام این داده‌ها در یک Kerberos Ticket-Granting Service Reply (KRB_TGS_REP) به سرویس گیرنده فرستاده می شود. ساختار پیغام (KRB_TGS_REP)، درست مثل ساختار نشان داده شده

بعد از اینکه سرویس گیرنده، پیغام KRB_TGS_REP را دریافت می کند، آن را با استفاده از کلید نشست logon برای از رمز در آوردن کلید نشست، از رمز در می‌آورد. بعد از، از رمز در آوردن کلید نشست، سرویس گیرنده آن را در حافظه نهان گواهی هویت خود ذخیره می کند. بعد سرویس گیرنده، ticket مربوط به سرور را استخراج می کند و آن را در حافظه نهان گواهی هویت خود ذخیره می کند.

CS Exchange

CS Exchange، زیر پروتکلی است که وقتی که سرویس گیرنده بلیط نشست را به سرور می فرستد به کار می رود. سرویس گیرنده یک پیغام Kerberos Application Request (KRB_AP_REQ) به سرور می فرستد.

بعد از اینکه سرور، بلیط را دریافت می کند، آن را از رمز در می آورد و داده های اختیار دهی سرویس گیرنده و کلید نشست را استخراج می کند. سرور از کلید نشست برای از رمز در آوردن اعتبار سنج سرویس گیرنده استفاده می کند. اگر اعتبار سنج معتبر باشد، سرور نگاه می کند که آیا flag اعتبار سنجی دو طرفه تنظیم شده است یا خیر. Flag بوسیله سیاست Kerberos برای محدوده و نه به صورت تکی توسط سرویس گیرنده، تنظیم می شود. اگرflag تنظیم شده باشد، سرور از کلید نشست برای به رمز در آوردن timestamp در اعتبار سنج سرویس گیرنده استفاده می کند و آن را در یک پیغام Kerberos Application Reply (KRB_AP_REP) به سرویس گیرنده می فرستد. بعد از اینکه سرویس گیرنده، پیغام KRB_AP_REP را دریافت می کند، اعتبار سنج سرور را با استفاده از کلید نشست از رمز در می آورد و زمان فرستاده شده بوسیله سرور را با زمان موجود در اعتبار سنجی که سرویس گیرنده در ابتدا به سرور فرستاده است مقایسه می کند. اگر این زمان ها یکی بودند، ارتباط بین سرویس گیرنده و سرور ادامه می یابد.

flagهای Option برای پیغامهای KRB_AS_REQ و KRB_TGS_REQ

flagها برای TGT می توانند در فیلد KDC Options مربوط به پیغام KRB_AS_REQ مورد درخواست قرار گیرند. این فیلد در پیغام KRB_TGS_REQ نیز وجود دارد. طول فیلد ۳۲ بیت است و هر گزینه به یکی از این بیت ها مربوط است.

بلیط ها (Tickets)

بلیط ها، قلب سیستم اعتبار سنجی Kerberos هستند. پیغام های مختلفی برای درخواست کردن و فرستادن بلیط ها بین موجودیت ها به کار می روند. اجزایی که یک بلیط را تشکیل می دهند شبیه اجزایی هستند در این فصل مورد بحث قرار گرفتند.

بلیط ها مثل پیغام های KRB_AS_REQ و KRB_TGS_REQ، یک فیلد falg دارند که ۳۲ بیتی است. برخی از این فیلدها شبیه فیلدهای پیغام های بالاست، ولی برخی دیگر متفاوت است.

تا وقتی که بلیط در فاصله زمانی بین زمان شروع و زمان پایان قرار داشته باشد، می‌تواند بوسیله موجودیتی که بلیط را نگه می دارد به هر تعداد لازم، مورد استفاده قرار گیرد. KDC، زمان یک بلیط را براساس زمان جاری تنظیم می کند، مگر اینکه سرویس گیرنده یک زمان شروع متفاوت، درخواست کند. سرویس گیرنده ها مجبور نیستند که یک زمان شروع را درخواست کنند، ولی زمانی که می خواهند در آن بلیط منقضی شود را الصاق می کنند. KDC از سیاست محدوده Kerberos کمک می گیرد و زمان مشخص شده در سیاست را به زمان شروع اضافه می کند. اگر سرویس گیرنده، یک زمان پایان خاص را درخواست کند، KDC، زمان پایان درخواست شده را به زمان شروع اضافه می کند. هر زمانی که کوتاهتر باشد (زمان محاسبه شده با استفاده از سیاست Kerberos یا زمان محاسبه شده با استفاده از زمان درخواست شده سرویس گیرنده)، زمان مورد استفاده برای زمان پایان است.

اگر یک سرویس گیرنده، یک بلیط نشست منقضی شده به یک سرور بفرستد، سرور آن را نمی پذیرد. بعد به عهده سرویس گیرنده است که به KDC برگردد و یک بلیط نشست جدید درخواست کند. با این حال، اگر سرویس گیرنده در حال ارتباط با سرور باشد و بلیط نشست منقضی شود، ارتباط ادامه پیدا می کند. بلیط های نشست برای اعتبارسنجی اتصال به سرور به کار می روند. بعد از اینکه اعتبارسنجی رخ داد، بلیط نشست می تواند منقضی شود، ولی اتصال قطع نمی شود.

بلیط های اعطای بلیط نیز براساس زمان تنظیم شده در سیاست محدوده Kerberos منقضی می شوند. اگر سرویس گیرنده ای سعی کند تا از یک TGT منقضی شده با KDC استفاده کند، KDC آن را نمی پذیرد. در این زمان، سرویس گیرنده باید با استفاده از کلید دراز مدت کاربر، از KDC یک TGT جدید درخواست کند.

می توان تنظیمات flag و بلیط ها را تجدید کرد. سیاست محدوده Kerberos دیکته می کند که آیا بلیط ها قابل تجدید هستند یا خیر. اگر سیاست به بلیط ها اجازه دهد که تجدید شوند، renewable flag در هر بلیط صادر شده توسط KDC، تنظیم می شود. در این شرایط، KDC یک زمان در فیلد End Time و یک زمان دیگر در فیلد Renew Till Time قرار می دهد. زمان تنظیم شده در فیلد Renew Till Time معادل زمان تنظیم شده در فیلد Start Time بعلاوه حداکثر طول دوام تجمعی تنظیم شده در سیاست محدوده Kerberos است. سرویس گیرنده باید قبل از زمان انقضای اولیه (اصلی) که در فیلد End Time نشان داده شده است، بلیط را به KDC بفرستد.

هر زمانی که سرویس گیرنده، یک بلیط را به KDC می فرستد، باید یک اعتبار سنج جدید نیز بفرستد. وقتی که KDC، بلیط را از سرویس گیرنده دریافت می کند، زمان تنظیم شده در فیلد Renew Till Time را بررسی می کند. اگر زمان قبلاً فرستاده نشده باشد، KDC یک کپی جدید از بلیط ایجاد می کند که یک زمان جدید در فیلد End Time آن و یک کلید نشست، تنظیم شده است. KDC با صادر کردن یک کلید نشست جدید، احتمال اینکه کلیدها به خطر بیافتند را کم می کند.

بلیط‌های پروکسی و بلیط های ارسال شده

در بلیط ها، flagهای proxy و forwarded برای شرایطی به کار می روند که در آنها یک سرویس گیرنده به یک سرور وصل می شود و آن سرور به سرور دیگری وصل می شود تا تراکنش را برای سرویس گیرنده کامل کند. این روند، محول کردن اعتبارسنجی (delegation of authentication) نامیده می شود. Kerberos با استفاده از بلیط ها کار می کند. بنابراین، سرور اول باید یک بلیط داشته باشد تا به سرور دوم وصل شود. flagهای Proxy و Forwarded بر پایه اصول متفاوتی کار می کنند و باید در سیاست محدوده Kerberos مجاز باشند.

بلیط های پروکسی بر این اصل کار می کنند که سرویس گیرنده، اسم سرور دوم را بکه باید به آن وصل شود را می داند. اگر سیاست محدوده Kerberos به بلیطهای پروکسی اجازه دهد، KDC و Proxiable flag را در TGT که به سرویس گیرنده می‌فرستد، تنظیم می کند. وقتی که سرویس گیرنده، یک بلیط را برای سرور دوم

درخواست می کند، flag را تنظیم می کند، به این معنی که یک بلیط پروکسی می‌خواهد و اسم Server1 را نیز شامل کرده است که این سرور از طرف سرویس گیرنده عمل می کند. KDC، بلیط را برای Server2 ایجاد می کند، Proxy flag را تنظیم می کند و آن را به سرویس گیرنده می فرستد. بعد سرویس گیرنده، بلیط را به Server1 می فرستد، Server1 از بلیط برای دستیابی به Server2 از طرف سرویس گیرنده استفاده می کند.

اگر سرویس گیرنده، اسم Server2 را ندارند، نمی تواند یک بلیط پروکسی درخواست کند. اینجاست که بلیط های ارسال شده (محول شده) به کار می روند. بلیط های محول شده بر این اساس کار می کنند که سرویس گیرنده Server1، یک TGT می دهد که هر وقت لازم باشد می تواند از آن برای درخواست کردن بلیط برای سرورهای دیگر استفاده کند. سرویس گیرنده، یک TGT قابل ارسال را از KDC می‌گیرد و اسم سرور (در اینجا Server1) را که اجازه دارد تا از طرف سرویس گیرنده عمل کند، به اطلاع KDC می رساند. KDC، TGT قابل ارسال برای Server1 را ایجاد می کند و آن را به سرویس گیرنده می فرستد. بعد سرویس گیرنده، TGT قابل ارسال را به Server1 می فرستد. وقتی که Server1 بخواهد با سرور دیگری مثل Server2 تماس حاصل کند، TGT مربوط به سرویس گیرنده را به KDC می فرستد. KDC تشخیص می دهد که TGT قابل ارسال است، بنابراین یک بلیط قابل ارسال

برای Server2 ایجاد می کند و بلیط را به Server1 می فرستد. Server1 سپس می‌تواند از ان بلیط برای دستیابی Server2 از طرف سرویس گیرنده استفاده کند.

Kerberos و ویندوز ۲۰۰۰

پیاده سازی Kerberos در ویندوز ۲۰۰۰، Microsoft Kerberos نامیده می شود، زیرا مایکروسافت گسترش های خود را اضافه کرده است. Microsoft Kerberos فقط هویت کاربر را اعتبار سنجی می کند و در مورد دادن اجازه دستیابی کاری نمی‌کند. بعد از اینکه Microsoft Kerberos هویت کاربر را بررسی کرد، Local Security Authority (LSA)، اجازه دستیابی به منبع را می دهد و یا این اجازه را نمی‌دهد.

Key Distribution Center

KDC در عملیات Kerberos گنجانده شده است و ویندوز ۲۰۰۰ KDC را به صورت یک سرویس domain پیاده‌سازی می کند. KDC از Active Directory به عنوان منبع پایگاه داده accountهای خود استفاده می کند. سرویس KDC، به همراه Active Dorectory، روی هر کنترل کننده domain ویندوز ۲۰۰۰ قرار دارد. این امر به هر کنترل کننده domain امکان می‌دهد تا به‌جای اینکه فقط به یکKDC وابسته باشد، درخواست‌های بلیط و اعتبارسنجی را قبول کند.

هر Kerberos KDC، اسم موجودیت خاص خود را دارد. اسم مورد استفاده در ویندوز ۲۰۰۰، krtbtgt است که برطبق راهنمایی های RFC 1510 می باشد. وقتی کهم یک domain در ویندوز ۲۰۰۰ ایجاد می شود، یک account کاربری بنام krbtgt

برای موجودیت KDC ایجاد می‌شود. این account، یک account نهادین است و بنابراین نمی توان آن را حذف کرد، تغییر نام داد و یا برای استفاده کاربر معمولی فعال کرد. اگرچه به نظر می رسد که این account غیرفعال است، در واقع بوسیله KDC مورد استفاده قرار می گیرد. اگر مدیری سعی کند تا آین account را فعال کند.

ویندوز ۲۰۰۰ به صورت خودکار برای account، یک کلمه عبور ایجاد می کند که سیستم به صورت خودکار و به صورت منظم آن را تغییر دهد. کلید مورد استفاده بوسیله krbtgt account، درست مثل یک کلید دراز مدت کاربر معمولی، بر کلمه عبور آن بنا نهاده شده است. کلید دراز مدت krbtgt برای به رمز در آوردن و از رمز در آوردن TGTهایی که صادر می کند به کار می رود. krbtgt account به وسیله همه KDCها در یک domainبه کار می رود. برای مثال، یک domain ویندوز ۲۰۰۰ می‌تواند پنج کنترل کننده domain داشته باشد که هر کدام از آنها KDC در حال کار خود را دارد، ولی هر کدام از KDCها از krbtgt account استفاده می کند. این به هر KDC اجازه می دهد تا TGT ها را با استفاده از یک کلید دراز مدت به رمز درآورند و از رمز درآورند. سرویس گیرنده می داند که با کدام KDC ارتباط برقرار کند، زیرا کامپیوتر سرویس گیرنده از Domain Name System (DNS) به دنبال یک کنترل کننده کمک می گیرد (سئوال می کند). بعد از اینکه سرویس گیرنده، کنترل کننده domain را پیدا کرد، پیغام KRB_AS_REQ را به سرویس KDC روی آن کنترل کننده domain می فرستد.

سیاست Kerberos در ویندوز ۲۰۰۰، در سطح domain تنظیم می شود. در حقیقت، وقتی که مایکروسافت به سیاست Kerberos اشاره می کند به جای کلمه محدوده (realm) از کلمه domain استفاده می کند. سیاست Kerberos درون Active Directory ذخیره می شود و فقط اعضای گروه Domain Admins مجاز هستند که این سیاست را تغییر دهند.

تنظیمات موجود در سیاست domain متعلق به Kerberos عبارتند از:

- Enforce user logon restrictions
- Maximum lifetime that a user ticker can be renewed
- Maximum service ticket lifetime
- Maximum tolerance for synchronization of computer clocks
- Maximum user ticket lifetime

تنظیمات «Enforce user logon restrictions» به صورت پیش فرض فعال است و برای اعتبار سنجی هر درخواست برای بلیط‌های نشست با اطمینان از اینکه سرویس گیرنده، حقوق کاربری مناسب برای logon کردن به سرور مقصد را دارد به کار می‌رود. این تنظیمات می تواند غیرفعال شود. این تنظیمات برای اجرا شدن نیاز به زمان اضافی دارد و می تواند کارآیی شبکه را پایین بیاورد.

تنظیمات «Maximum lifetime that a user ticker can be renewed» برحسب روز تنظیم می شود. تنظیمات پیش فرض برای این صفت، هفت روز است.

«Maximum service ticket lifetime» برحسب دقیقه تنظیم می شود، نگذارید که اصطلاح بلیط سرویس شما را گیج کند. این فقط اسمی است که مایکروسافت برای

بلیط های نشست انتخاب کرده است. تنظیمات برای طول عمر بلیط سرویس نمی‌تواند بیشتر از زمان مشخص شده در «Maximum user ticket lifetime » یا کمتر از ۱۰ دقیقه باشد. این تنظیمات می تواند طوری Set شود که هرگز منقضی نشود. تنظیمات منطقی برای این گزینه این است که آن را مثل «Maximum user ticket lifetime » تنظیم کنیم. تنظیمات پیش فرض برای این صفت، ۱۰ ساعت است.

«Maximum tolerance for synchronization of computer clocks» تعیین می‌کند که چقدر تفاوت در Clock ها مورد قبول است. این تنظیمات برحسب دقیقه است و به صورت پیش فرض، ۵ دقیقه است.

«Maximum user ticket lifetime » برحسب ساعت تنظیم می شود. مایکروسافت تصمیم گرفته است که از اصطلاح بلیط کاربری (user ticket) استفاده کند، ولی در اصطلاحات Kerberos، این TGT نامیده می شود. تنظیمات پیش فرض برای این صفت، ۱۰ ساعت است. تغییر صفت با دو بار کلیک کردن صفت و تغییرات تنظیمات، آسان است.

توجه: مایکروسافت از اصطلاحات بلیط سرویس و بلیط کاربری استفاده می کند. Kerberos استاندارد از اصطلاحات بلیط نشست و بلیط اعطای بلیط (TGT) استفاده می کند. یک راه ساده برای اینکه به یاد بسپاریم که چگونه اسم های مایکروسافت با اسم های Kerberos استاندارد مطابقت می کنند این است:

- مایکروسافت بلیط های نشست را بلیط سرویس می نامد، زیرا آنها اتصال به سرویس‌ها را اعتبارسنجی می کنند.
- مایکروسافت TGT ها را بلیط کاربری می نامد، زیرا آنها کاربران را اعتبار سنجی می کنند.

محتویات یک بلیط متعلق به Microsoft Kerberos

بلیط های Microsoft Kerberos شامل قسمت های اضافی هستند که در بلیط های پیاده سازی شده دیگر Kerberos موجود نیستند. ویندوز ۲۰۰۰، مثل نسخه های قبلی ویندوز NT، از شناسه‌های امنیتی (SID) استفاده می کند. SIDها به عنوان نماینده accountهای کاربری و گروه‌ها به کار می روند. SID برای یک کاربر به همراه هر SID برای گروه هایی که کاربر به آنها تعلق دارد، در بلیط هایی که سرویس گیرنده استفاده می کند قرار می گیرند و به Privilege Attribute Certificate (PAC) معروف هستند. PAC مشابه گواهی نامه کلید عمومی نیست. اسم کاربر که User Principal Name نامیده می‌شود به صورت UPN:name@domain به بلیط اضافه می شود. برای مثال، UPN:stace@sdc.biloxi.ms.us برای شناسایی کاربری بنام Stace در یک بلیط قرار داده می شود.

محول کردن اعتبارسنجی

Kerberos از دو روش محول کردن پشتیبانی می کند: بلیط های قبال پروکسی شدن و بلیط های قابل ارسال (قابل محول کردن). Microsoft Kerberos فقط از

بلیط‌های قابل ارسال پشتیبانی می کمند و سیاست پیش فرض Kerberos برای domainهای ویندوز ۲۰۰۰ این مجوز را فقط به اعضای Domain Admins اختصاص می دهد. این سیاست می تواند با تغییر account کاربری از طریق Active Directory Users and Computers در اختیار یک کاربر قرار گیرد. برای دستیابی به accountهای‌کاربری‌در Start|Programs|Administrative Tools Active Directory را انتخاب کنید و بعد Active Directory Users and Computers را انتخاب کنید. گزینه account برای فعال کردن عمل محول کردن، در برگه account کادر محاوره‌ای properties مربوط به یک کاربر موجود است یک گزینه برای account نیز موجود است که پذیرش گواهی های هویت محول شده را مجاز نمی داند.

پیش اعتبار سنجی

در اعتبار سنجی Kerberos، برخی از پیغام ها یک فیلد پیش اعتبار سنجی دارند. Microsoft Kerberos به صورت پیش فرض از پیش اعتبار سنجی در domainها استفاده می کند. داده های موجود در این فیلد، timestamp به رمز در آمده مربوط به سرویس گیرنده است. اگر لازم باشد، می توانید به صورت فردی و شخص به شخص، پیش اعتبار سنجی را برای accountهای کاربری غیرفعال کنید. اگر Microsoft Kerberos را با شکل های دیگر پروتکل Kerberos ترکیب می کنید، ممکن است احتیاج داشته باشید که پیش اعتبار سنجی را غیرفعال کنید.

ارائه کنندگان پشتیبانی امنیتی (Security Support Providers)

وقتی که یک سیستم بوت می شود، ویندوز ۲۰۰۰ سرور به صورت خودکار دو ارائه کننده پشتیبانی امنیتی (SSP) را راه اندازی می کند: SSP مربوط به Kerberos و SSP مربوط به NTLM. هر دو SSP توسط LSA راه اندازی می شوند و هر دو برای اعتبارسنجی logonهای شبکه ای و اتصال ها بین سرویس گیرنده ها و سرورها موجودند. ویندوز ۲۰۰۰ سرور به صورت پیش فرض از Kerberos SSP استفاده می‌کند، مگر اینکه مثل ویندوز 9x، سرویس گیرنده نتواند از Kerberos استفاده کند. در این صورت، NTLM SSP به کار می رود. SSP مربوط به NTLM همچنین برای سرورهای ویندوز ۲۰۰۰ مورد استفاده قرار می گیرد که به صورت سرورهای عضو و یا سرورهای مستقل و برای logon کردن روی یک کنترل کننده domain به صورت محلی به جای یک domain تنظیم شده اند.

Kerberos SSP در ابتدا برای اعتبار سنجی به کار می رود، زیرا پیش فرض برای ویندوز ۲۰۰۰ است. با این حال، اگر کاربر به صورت محلی logon کند، یک خطا به Security Support Provieder Interface (SSPI) فرستاده می شود و بعد SSPI، درخواست logon را به NTLM SSP می فرستد.

حافظه نهان گواهی هویت

سرویس گیرنده از یک ناحیه از حافظه فرار بنام حافظه نهان گواهی هویت (Credentials Cache) استفاده می کند. این ناحیه از حافظه بوسیله LSA محافظت

می شود و هرگز نمی توان آن را در Pagefile روی درایو دیسک سخت قرار داد.

وقتی که کاربر از سیستم log off می کند، هر چیزی در ناحیه حافظه که برای حافظه نهان گواهی هویت به کار می رود، بیرون کشیده می شود.

Kerberos SSP، حافظه نهان گواهی هویت را کنترل می کند و برای بدست آوردن بلیطها و کلیدهای جدید، تا حد ممکن به کار می رود. وقتی که این کارها باید انجام شوند، LSA مسئول اطلاع دادن به Kerberos SSP است.

LSA همچنین وقتی که کاربر logon کرده است، یک کپی از کلمه عبور درهم شده کاربر را در یک ناحیه امن از registry حفظ می کند. وقتی که کاربر log off کند، کلمه عبور درهم سازی شده به دور انداخته می شود. LSA یک کپی از کلمه عبور درهم سازی شده نگهداری می کند، چون شاید TGT منقضی شود. بعد LSA یک روش برای بدست آوردن یک TGT دیگر بدون درخواست کلمه عبور از کاربر، در اختیار Kerberos SSP قرار می دهد. این باعث می شود که این کار بدون مشکل در پس زمینه انجام شود.

تبدیل اسم DNS

Microsoft Kerberos برای پیدا کردن یک KDC موجود برای فرستادن درخواست اعتبار سنجی اولیه به Domain Name System (DNS) وابسته است. تمام کنترل کننده های domain ویندوز ۲۰۰۰، KDC هستند و KDC به صورت _kerberos ._udp.nameofDNSdomain در رکورد محل سرویس DNS (که در رکورد SRV نیز نامیده می شود) ثبت می شود. سرویس گیرنده ها می توانند به دنبال این رکورد SRV بگردند تا آدرس IP کامپیوتری که سرویس KDC را اجرا می کند را پیدا کنند. سرویس گیرنده ای که نتواند رکورد SRV را پیدا کند می تواند با استفاده از اسم domain، به دنبال یک رکورد میزبان (یک رکورد A) بگردد.

اگر کامپیوتر ویندوز ۲۰۰۰، عضو یک محدوده Kerberos متفاوت (نه یک domain ویندوز ۲۰۰۰) باشد، نمی تواند به دنبال رکورد SRV بگردد. در این صورت، اسم سرور KDC در registry کامپیوتر ویندوز ۲۰۰۰، ذخیره می شود. وقتی که کامپیوتر لازم داشته باشد که KDC را پیدا کند، SSP مربوط به Microsoft Kerberos، اسم domain مربوط به سرور KDC را از registry پیدا می‌کند و بعد از DNS برای پیدا کردن آدرس IP مربوط به سیستم استفاده می کند. کلید registry زیرا را برای اضافه کردن اسم domain مربوط به Kerberos ویرایش کنید:

HKEY_LOCAL_MACHINE\System\CurrentcontrolSet\Control\LSA\Kerberos\Domains

توجه: رکوردهای پیدا کننده سرویس (SRV) یک سرویس را به اسم میزبان کامپیوتری که آن سرویس را ارائه می کند، نگاشت می کنند. رکوردهای میزبان (که رکوردهای A نیز نامیده می شوند) یک اسم میزبان را به یک آدرس IP نگاشت می‌کنند. سرورهای DNS ویندوز ۲۰۰۰ و سرورهای DNS ویندوز NT 4.0 که Service Pack 4 یا بالاتر را اجرا می کنند، از رکوردهای SRV پشتیبانی می کنند. اگر از یک سرور BIND DNS استفاده می نمایید، این سرور حداقل باید نسخه 4.9.6 باشد، تا از رکوردهای SRV پشتیبانی کند.

پورت های UDP و TCP

وقتی که یک سرویس گیرنده، پیغام های Kerberos را به KDC می فرستد، یا وقتی که برخی معیارها تحقق می یابند، به صورت پیش فرض از (UDP) User Datagram Protocol پورت ۸۸ استفاده می کند. روی یک شبکه اترنت، حداکثر واحد انتقال (MTU) که می توان منتقل کرد، ۱۵۰۰ بایت است. اگر پیغام Kerberos از ۱٤۷۲ بایت کوچکتر باشد، Microsoft Kerberos از UDP به عنوان مکانیزم انتقال استفاده می کند. اگر پیغام بین ۱٤۷۳ بایت و ۲۰۰۰ بایت باشد، IP، قاب (frame) را روی UDP پورت ۸۸ تقسیم می کند (می کشند)، اگر پیغام Kerberos بیش از ۲۰۰۰ بایت باشد، بوسیله Transmission Control Protocol (TCP) روی پورت ۸۸ فرستاده میشود.RFC 1510 بیان میکند که پورت ۸۸ UDP باید برای تمام پیغام‌های Kerberos بکاررود،ولی از آنجایی که پیغام‌های Microsoft Kerberos می

توانند بیشتر از ۲۰۰۰ بایت باشند زیرا SID های کاربری و گروهی در آنها بکار برده می شود، مایکروسافت از پورت ۸۸ TCP نیز استفاده می‌کند. یک بازنگری اولیه برای RFC 1510 به Internet Engineering Task Force (IETF) ارسال شده است که استفاده از پورت ۸۸ TCP را پیشنهاد کرده است، ولی این بازنگری هنوز در RFC رسمی قرار داده نشده است. قابلیت کار با محدوده‌های دیگر Kerberos نباید تحت تأثیر قرار گیرد و ارتباطات فقط بین کامپیوترهای ویندوز ۲۰۰۰ رخ می دهد.

داده های اجازه دهی (Authorization Data)

Kerberos فقط هویت موجودیتها را بررسی می کند و به منابعی که می تواند مورد استفاده قرار دهد اجازه می دهد. یک فیلد برای داده های اجازه دهی در بلیط های Kerberos موجود است، ولی Kerberos اطلاعات موجود در فیلد و یا آنچه که باید با اطلاعات انجام شود را کنترل نمی کند.

KDC و Authorization Data

فیلد Authorization Data در یک بلیط مربوط به Microsoft Kerberos از یک لیست از SIDها برای کاربر، از جمله SID مربوط به گروه‌ها تشکیل شده است. KDC این اطلاعات را از Active Directory بدست می آورد و آن را در TGT داده شده به سرویس گیرنده قرار می دهد. وقتی که سرویس گیرنده یک بلیط نشست (یا به اصطلاح مایکروسافت، یک بلیط سرویس) را درخواست می کند، KDC داده‌ها را از فیلد Authorization Data متعلق به TGT به بلیط نشست کپی می کند. KDC، داده

های اجازه دهی را قبل از اینکه داده‌ها در بلیط نشست ذخیره شود امضاء می کند تا LSA بتواند تشخیص دهد که آیا داده‌ها تغییر کرده اند یا خیر. LSA، هر بلیط نشست را بررسی می کند تا مطمئن شود که امضاء معتبر است.

سرویس ها و داده های اجازه دهی

بعد از اینکه گواهی های هویت در یک بلیط نشست بوسیله سرور شبکه ای که سرویس روی آن قرار دارد صحت سنجی شد، یک نشانه (token) دستیابی ایجاد می‌شود. PAC از بلیط نشست استخراج می شود و برای ایجاد یک نشانه تقلید به کار می رود که برای دستیابی به سرویس روی سرور مورد استفاده قرار می گیرد و تا وقتی که اطلاعات موجود در PAC با داده های موجود در Access Control List (ACL) برای سرویس مطابقت می کند، اجازه دستیابی داده می شود.

در Microsoft Kerberos یک بلیط نشست برای دستیابی به سرویس ها روی سیستم های محلی نیز لازم است. همین روند برای دستیابی به منابع محلی رخ می‌دهد. LSA یک نشانه دستیابی محلی، از PAC موجود در بلیط نشست می سازد.

ابزارهای Kerberos

مایکروسافت دو ابزار به ما ارائه کرده است تا بتوانیم گواهی نامه های Kerberos را مدیریت کنیم. این دو ابزار، Kerberos List و Kerberos Tray هستند. این ابزارها به ما امکان می دهند تا مشخصات گواهی نامه های خود را مشاهده کنید. همچنین می‌توانید بلیط هایی را که دیگر مورد نیاز نیستند، حذف کنید. با استفاده از این ابزارها

می توانیم بلیط‌های Kerberos را از طریق خط فرمان و از داخل یک واسط گرافیکی مدیریت کنیم. این دو ابزار در Windows 2000 Server Resource Kit موجودند. فصل ۱۲ «استفاده از ابزارهای مرتبط با امنیت»، شرح می‌دهد که چگونه Resource Kit را نصب کنید.

Kerberos List

Kerberos List به شما امکان می دهد تا بلیط های Kerberos را از طریق خط فرمان مدیریت کنید. می توانید بلیط های اختصاص داده شده به نشست logon جاری را مشاهده و حذف کنید. تنها فایل مورد نیاز برای استفاده از Kerberos List، Klist.exe است. Kerberos List باید به صورت محلی روی ماشینی که می خواهید بلیط ها را برای آن مدیریت کنید اجرا شود.

Kerberos Tray

Kerberos Tray، درست مثل Kerberos List به شما امکان می دهد تا بلیط‌های Kerberos اختصاص داده شده به نشست logon فعلی را مشاهده و حذف کنید. Kerberos Tray یک ابزار گرافیکی است که اسم خود را از آنجا گرفته است که روی System Tray می نشیند و منتظر می ماند تا مورد استفاده قرار گیرد. وقتی که فایل قابل اجرای Kerbtray.exe را اجرا می کنید، یک آیکون مستطیلی سبز رنگ روی System Tray ظاهر خواهد شد. با حرکت دادن اشاره گر به روی این آیکون، می توانید زمان باقی مانده تا انقضای TGT خود را ببینید. با دوبار کلیک کردن روی این آیکون، پنجره Kerberos Tickets باز می شود. این پنجره چهار برگه دارد.