بررسی پروتکل های ایمن درلایه انتقال و کاربردی

سعید رحیمی

گروه سخت افزار ۹۱

جهاد دانشگاهی مشهد

استاد راهنما : اقای دکتر شهریاری

زمستان ۹۲

www.Prozhe.com

فهرست :

چکیده ۳
مقدمه ۳
لایه کاربردی ۴
لایه انتقال ۴
پروتکل HTTPS ۸
پروتکل SSL ۱۰
پروتکل TLS ۱۴
پروتکل SSH ۱۵
پروتکل SOCKS ۱۹
پروتکل KERBEROS ۲۲
پروتکل های FTPS/SFTP ۲۵
منابع ۲۸

www.Prozhe.com

چکیده :

در این مقاله بـــه بررسی پروتکل های ایمن در لایه انتقال[1] و کاربردی[2] از مدل TCP/IP میپردازیم.سعی شده است مطالب کامل ، ساده و قابل فهم باشد . بدیهی است که توضیح کلیه پروتکل های مربوطمبحث را بسیار طولانی نموده لذا به توضیح پروتکل های پرکاربرد میپردازیم.در ابتدا توضیح مختصری در رابطه با لایه های مذکور میدهیم . سپس به بررسی پروتکل ها میپردازیم .

مقدمه :

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. دربسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است. محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد .بادرکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. طرح امنیتیکه شما میتوانید با در نظر گرفتن میزان محرمانه بودن اطلاعات خود به کار ببندید . اگر شما تکنسینشبکه میباشید بایستی پروتکل های امنیتی در این رابطه را بلد باشد تا بتوانید امنیتی در خور توجه برای سیستم های مورد نظر را به وجود بیاورید . در ذیل به بررسی این پروتکل ها میپردازیم.

[1] Transport layer
[2] Application layer

www.Prozhe.com

لایه کاربردی[۳] :

لایه کاربرد در TCP/IP معادل ترکیب لایه های کاربرد،نمایش[۴] و جلسه[۵] در مدل مرجع OSI است. لایه کاربرد به یک کاربر اجازه میدهد به سرویسهای اینترنت خصوصی یا اینترنت سراسری دسترسی داشته باشد. بسیاری از پروتکل ها در این لایه برای فراهم کردن سرویسهایی نظیر پست الکترونیک،انتقال فایل،دسترسی به وب جهان گستر و نظایر آن تعریف شده اند.

در این لایه پروتکل های مختلف طراحی شده اند تا بتوان از طریق انـــها سرویسهای خاص را در شـبکه اینترنت یا شبکه هایی که از قرار داد IP [۶] استفاده می کنند اجرا نمود. بـــــا استفاده از این پروتکل هـا نرم افزار هایی طراحی شده و در شبکه بکار گرفته میشوند.

با توجه به اینکه تبادل اطلاعات به صورت client/server یا خادم / مخدوم انجام مـــــیشود. بر طـبق پروتکل طراحی شده برای یـــک سرویس معین نرم افزار های سرویس دهنده و سرویس گیرنده طـــراحی و تولید می شوند. ارتباط کاربران با نرم افزارهای سرویس دهنده جهت دریافت اطلاعات از طریق نرم افزار Client یا سرویس گیرنده برقرار میشود.

لایه انتقال[۷] :

در شبکه‌های رایانه‌ای، لایه انتقال سرویس‌های ارتباطی مبدأ به مقصد یا end-to-end را برای برنامه‌های کاربردی موجود در معماری لایه بندی شده پروتکل‌ها و اجزاء شبکه فراهم می‌آورد. لایه انتقال سرویس‌های مطمئنی از قبیل پشتیبانی از جریان داده اتصال گرا، قابلیت اطمینان، کنترل جریان و تسهیم یا مالتی پلکسینگ را ارائه می‌نماید.

لایه انتقال در مدل TCP/IP، که مبنا و بنیان اینترنت می‌باشد، و هم مدل OSI موجود می‌باشند. تعریف لایه انتقال در این دو مدل کمی با یکدیگر تفاوت دارد. این مقاله در اصل به تعریف لایه انتقال در مدل TCP/IP اشاره دارد.

---

[۳] Application layer
[۴] Presentation layer
[۵] Session layer
[۶] Internet protocol
[۷] Transport layer

www.Prozhe.com

معروف ترین پروتکل لایه انتقال پروتکل کنترل انتقال یا Transmission Control Protocol (TCP) می‌باشد. این پروتکل نام خود را از مجموعه پروتکل اینترنت یا همان TCP/IP گرفته‌است. از این پروتکل در انتقالات اتصال گرا استفاده می‌شود در حالیکه پروتکل بدون اتصال UDP برای انتقالات پیام ساده مورد استفاده قرار می‌گیرد. TCP پروتکل پیچیده تری است و این پیچیدگی به واسطه طراحی وضعیت محوری است که در سرویس‌های انتقالات قابل اطمینان و جریان داده تعبیه شده‌است. از دیگر پروتکل‌های عمده در این گروه می‌توان به پروتکل کنترل ازدحام دیتاگرام[۸] و پروتکل انتقال کنترل جریان[۹] اشاره نمود.

سرویس های مهم لایه انتقال:

سرویس های زیادی وجود دارد که می تواند توسط یک پروتکل در لایه انتقال ارائه شود که می توان به موارد زیر اشاره نمود:

۱- ارتباط اتصال گرا یا Connection-oriented communication: این نوع ارتباط را که می توان آنرا جریان داده نیز تفسیر کرد می تواند مزایای متعددی را برای برنامه کاربردی به ارمغان بیاورد. در حالت عادی کار کردن با آن راحتتر از کار کردن با ارتباط بدون اتصال یا Connection-less است. یکی از پروتکل هایی که این نوع سرویس را ارائه می دهد پروتکل TCP می باشد.

۲- مرتب سازی بایتی یا Byte Orientation : به جای اینکه برنامه کاربردی پیام های دریافت شده از سیستم ارتباطی را بر اساس فرمتی نامشخص پردازش کند، اغلب جریان داده را به صورت ترتیبی از بایت‌ها می خواند که این کار به مراتب آسان تر خواهد بود. این ساده سازی به برنامه کاربردی امکان می دهد که بتواند با فرمت های مختلفی از پیام ها کار کند.

۳- تحویل با ترتیب یکسان : لایه شبکه معمولاً قادر به تضمین این مسأله نیست که داده های بسته های دریافت شده دقیقاً همان ترتیبی را دارند که از سیستم ارسال کننده فرستاده شده اند. وظیفه مرتب سازی بسته معمولاً در لایه انتقال صورت می پذیرد.

۴- قابلیت اطمینان : به دلیل خطاها و تراکم های شبکه ای احتمال اینکه بسته های اطلاعاتی از بین بروند وجود دارد. با استفاده از تکنیک های کد شناسایی خطا از قبیل مجموع مقابله‌ای یا checksum، پروتکل انتقال بررسی می کند که آیا داده ها سالم هستند یا خیر. این پروتکل نتیجه بررسی خود را بوسیله

---

[۸] (DCCP) Datagram Congestion Control Protocol
[۹] (SCTP) Stream Control Transmission Protocol

www.Prozhe.com

ارسال کند ACK (به معنای صحت داده ها) و NACK (به معنای خرابی داده ها) به فرستنده اعلام می کند. ممکن است طرح های درخواست تکرار خودکار برای ارسال دوباره اطلاعات آسیب دیده و یا از بین رفته مورد استفاده قرار گیرد.

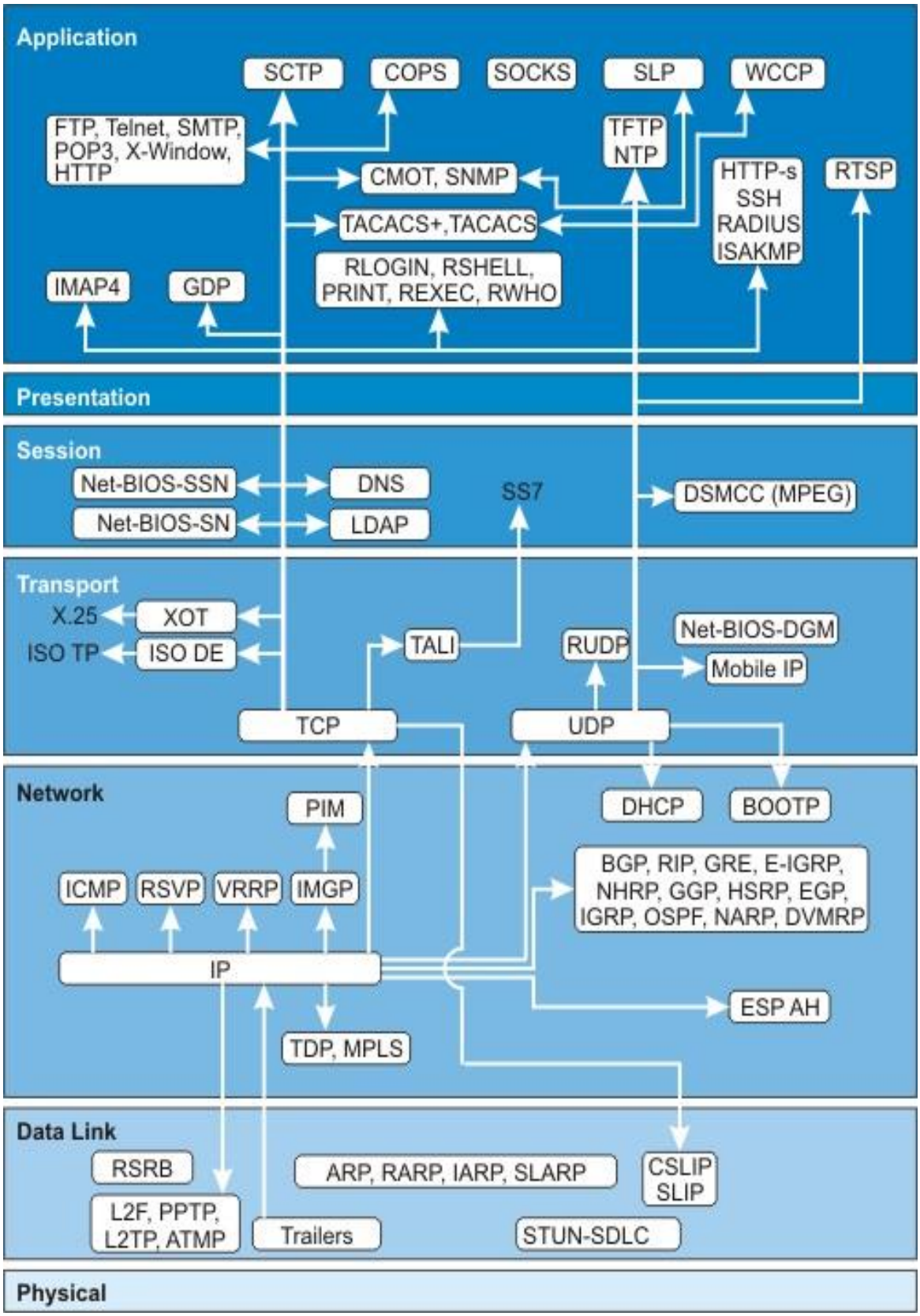
۵- کنترل جریان یا Flow Control : بعضی اوقات نرخ انتقال اطلاعات بین دو نود بایستی مدیریت شود تا از ارسال سریع تر فرستنده نسبت به گیرنده اطلاعات که می تواند منجر به سرریز بافر داده ای گیرنده شود جلوگیری به عمل آید.

۶- پیشگیری از تراکم یا Congestion Avoidance : کنترل تراکم می تواند ترافیک وارد شده به شبکه مخابراتی را مدیریت کرده و با اعمال ممنوعیت ورود هر نوع امکان ارتباطی و یا پردازشی از سوی نودهای شبکه تصادم و یا تراکم را کاهش دهد. همچنین این سرویس می تواند با در اختیار گرفتن منابع، باعث کاهش نرخ ارسال بسته های اطلاعاتی شود. برای مثال، درخواست تکرار خودکار می تواند شبکه را در حالتی متراکم نگه دارد؛ این موقعیت می تواند با اعمال پیشگیری های تراکمی به کنترل جریان به حداقل برسد. با این کار مصرف پهنای باند از همان ابتدای انتقال اطلاعات و یا بعد از ارسال مجدد بسته ها در سطحی پایین و ایمن باقی خواهد ماند.

۷- تسهیم یا مالتی پلکسینگ (Multiplexing) : پورتها می تواند چندین مقصد پایانی را بر روی یک نود فراهم آورد. برای مثال، نام موجود در آدرس پستی می تواند نمایانگر نوعی از تسهیم و تفکیک بین چندین گیرنده در یک محل باشد. برنامه های کاربردی بر روی پورت‌های مخصوص به خودشان به اطلاعات گوش می دهند که این کار این امکان را فراهم می آورد که از چندین سرویس شبکه به صورت همزمان استفاده کنیم. این سرویس بخشی از لایه انتقال در مدل TCP/IP است، اما در مدل OSI این سرویس بخشی از لایه نشست می باشد. در عکس صفحه بعد با پروتکل های مهم لایه انتقال و کاربردی اشنا میشویم که در ادامه به بررسی پروتکل های امن این دو لایه میپردازیم.

www.Prozhe.com

در این عکس به پروتکل های مهم و پراستفاده هر لایه اشاره شده است و در ادامه به توضیح پروتکلهای ایمن در لایه کاربردی و انتقال میپردازیم.



www.Prozhe.com

۱- پروتکل HTTPs[۱۰] :

یـــک پروتکل امن برای انتقال اطلاعات در شبکه‌های کامپیوتری می‌باشد که به صورت خاص برای استفاده در اینترنت توسعه یافته است. ایـن استاندارد در واقـــع به خودی خود یک پروتکل نیست.بلکه بـــا قرار گرفتن HTTP بـــر روی پروتکل TLS[۱۱] (امنیت لایه انتقال) بـــه وجود امده است.به‌این ترتیب امنیت موجود در پروتکل TLS به ارتباطات HTTP افزوده شده‌است.

در نسخه رایج پروتکل HTTPS امکان شناسایی وبگاه‌ها وجود دارد. این امر جلوی حملات مرد میانی[۱۲] را می‌گیرد. همچنین رمزگذاری ۲ طرفه بیـــــن client و server از حملات شنود و تغییر بدون اجازه جلوگیری می‌کند. در عمل، این ویژگی‌ها باعث می‌شود تا این پروتکل بتواند تا حد زیادی امنیت ارتباط کاربران را تامین نماید.

در ابتدا از این پروتکل فقط برای انجام تراکنش‌های بانکی، ارسال ای‌میل‌های مهم و کارهای حساس دیگر بر روی وب جهانی استفاده می‌شد امـا بـا گذشت زمان، استفاده از آن بیشتر و بیشتر مـــی‌شود.امـــن کردن ارتباطات کاربران ، شناسایی وبگاه‌های معتبر و مخفـی کـردن هویت کاربران از جـمله استفاده‌های نوین این پروتکل است.

البته باید توجه داشت که امنیت کامل کاربران تنها در صورتی تامین می‌شود که تمامی محتویات وبگاه از طریق همین پروتکل منتقل شود. منابعی مانند فایل‌های اسکریپت، کوکی‌ها و غیـــره نمونـــه‌هایی هستند کـه انتقال غیرامن آن‌ها تهدید امنـیتی محسوب مـــی‌شود.

وجود کلمه HTTPS در ابتدای آدرس، به مرورگر نشان می‌دهد که برای اتصال به وب‌گاه باید از امنیت لایه انتقال استفاده کند .از آنجا که در این پروتکل حتی اگر یکی از طرفین هم گواهی ثبت شده داشته بـاشد، امنیت بـرقرار خواهد شد، استفاده آن در وب بسیار مناسب اسـت. در اینترنت معمولا وب‌گـــاه‌ها گواهی ثبت شده تهیه مـی‌کنند. کاربران بـا بررسی صحت گواهی وب‌گاه، مـی‌توانند از هـــویت وب‌گاه مطمئن شده و ارتباطی امن و غیر قابل شنود داشته‌باشند.

---

[۱۰] Hypertext Transfer Protocol Secure

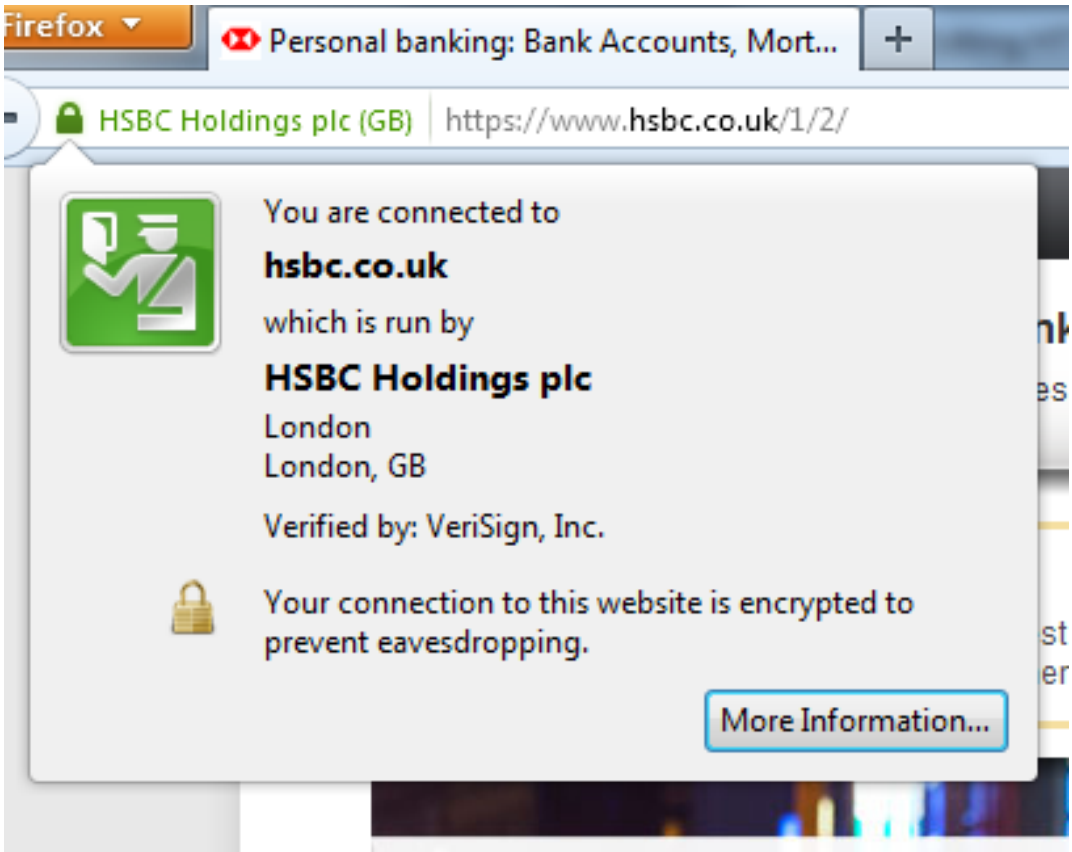
[۱۱] Transport Layer Security

[۱۲] اغلب با مخفف **MITM** و همچنین با عنوان حمله ی bucket brigade یا گاهی اوقات با عنوان حمله ی ژانوس شناخته شده‌است

www.Prozhe.com

از آنجایی که HTTPS ، پروتکل امنیت لایه انتقال را به طورکامل در لایه‌ای در زیر HTTP قرار می‌دهد، تمامی محتویات بسته HTTP به طور کامل رمزگذاری می‌گردد. این اطلاعات شامل نشانی وب (آدرس صفحه مقصد)، پارامترهای ارسالی (مانند نامِ کاربری و کلمه عبور)، سرآیندها و کوکی‌ها می‌شود. اما از آنجا که لایه TCP/IP به آدرس IP و شماره درگاه وب‌گاه نیازمند است، پروتکل HTTPS نمی‌تواند از آن‌ها محافظت کند. برای مثال در یک ارتباط امن با وب‌گاه گوگل، هیچ‌کس نمی‌تواند از روی بسته کاربر متوجه محتویات درخواست او شود. تنها از روی آدرس IP می‌توان تشخیص داد که کاربر در حال مکالمه با گوگل است.

تقریبا تمامی مرورگرهای وب در صورت دریافت یک گواهی نامعتبر به اشکال مختلف به کاربر هشدار می‌دهند .برخی از مرورگرهای قدیمی‌تر، با نمایش یک جعبه هشدار وضعیت را به کاربر گزارش داده و برای ادامه کار از او اجازه می‌گرفتند .اما مرورگرهای جدیدتر معمولا با هشدارهای واضح که تمامی صفحه را پر می‌کنند، سعی در مطلع ساختن کاربر از خطرهای احتمالی را دارند .همچنین علامت‌هایی مانند کلید و یا سبز یا قرمز شدن نوار آدرس در مرورگرهای مختلف نشانه مورد تایید یا جعلی بودن گواهی ارائه شده توسط وب‌گاه است .امروزه بسیاری از مرورگرها در صورتی که محتویات صفحه مخلوطی از پروتکل امن و غیر امن HTTP باشد، به کاربر هشدار خواهند داد.(تصویر زیر)



www.Prozhe.com

پروتکل SSL[۱۳] :

SSL راه حلی جهت برقرای ارتباط ایمن میان سرویس دهنده و یک سرویس گیرنده است که توسط شرکت Netscapeارائه شده است. در واقع SSL پروتکلی است که در لایه حمل از مدل TCP/IP عمل میکند .

مزیت استفاده از این پروتکل بهره گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل های غیرامن لایه کاربردی نظیر IMAP,LDAP,HTTP و ..... میباشد. که بر اساس آن الگوریتم های رمزنگاری بر روی داده های خام (Plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند ، اعمال میشود و محرمانه ماندن داده ها را در طول کانال انتقال تضمین میکند. به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی های دیجیتال SSL را دارد برای هر کدام از طرفی که قرار است ارتباط میان شبکه ای امن داشته باشند ، گواهی های مخصوص سرویس دهنده و سرویس گیرنده را صادر میکند و مکانیزم های احراز هویت خود ، هویت هر کدام از طرفین را برای طرف مقابل تایید میکند ، البته غیر از این کار می بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت ، برای رباینده قابل درک و استفاده نباشد که این کار را با کمک الگوریتمهای رمزنگاری و کلید های رمز نگاری نامتقارن و متقارن انجام دهد.

ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL

برای داشتن ارتباطات امن مبتنی بر SSL عموما به دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز میباشد. وظیفه CA این است که هویت طرفین ارتباط ، نشانی ها ، حساب های بانکی ، و تاریخ انقضای گواهینامه را بداند و بر اساس آن ها هویت ها را تعیین نماید.

اجزای پروتکل SSL

پروتکل SSL دارای دو زیر پروتکل تحت عناوین زیر میباشد.

۱- SSL Record Protocol که نوع قالب بندی داده های ارسالی را تعیین میکند.

---

[۱۳] Secure Sockets Layer

www.Prozhe.com

۲- SSL Handshake Protocol که بر اساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده ها میان سرویس دهنده ها و سرویس گیرنده های مبتنی بر SSL را تهیه میکند.

بخش بندی پروتکل SSL به دو زیر پروتکل دارای مزایای چندی است.

از جمله :

۱- در ابتدای کار و طی مراحل اولیه ارتباط (Handshake) هویت سرویس دهنده برای سرویس گیرنده مشخص میگردد.
۲- در همان ابتدای شروع مبادلات،سرویس دهند و سرویس گیرنده بر یر نوع الگوریتم رمز نگاری تبادلی توافق می کنند.
۳- در صورت لزوم، هویت سرویس گیرنده برای سرویس دهنده احراز میگردد.
۴- در صورت استفاده از تکنیک های رمز نگاری مبتنی بر کلید عمومی ، می توانند کلید های اشتراکی مخفی را ایجاد نمایند.
۵- ارتباطات بر مبنای SSL رمزنگاری می شوند. الگوریتمهای رمزنگاری پشتیبانی شده در SSL در استاندارد SSL ، از اغلب الگوریتمهای عمومی رمزنگاری و مبادلات کلید نظیر RSA,RC4,RC2,DES,DSA,KEA,MD5,SHA-1 پشتیبانی میشود. و بسته به این که نرم افزارهای سمت سرویس دهنده و سرویس گیرنده از موارد مذکور پشتیبانی نماید ، ارتباطات SSL می تواند بر اساس هر کدام از این الگوریتم ها صورت پذیرد.البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم می توان آن ها را در داده ها و همچنین الگوریتم SHA-1 برای مکانیزمهای تایید پیغام MD5 استفاده شود و یا اینکه اگر امنیت در این حد مورد نیاز نبود ، می توان در مواردی خاص از الگوریتم رمز نگاری RC4 با طول کلید 40 بیت و الگوریتم تایید پیغام MD5 استفاده نمود.

نحوه عملکرد داخلی پروتکل SSL

همانطور که میدانید SSL میتواند از ترکیب رمزنگاری متقارت و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع تر از رمزنگاری کلی عمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک های احراز هویت قوی تری را ارایه می کند. یک جلسه SSL (SSL Session) با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع میشود. این پیغام اولیه به سرویس دهنده این امکان را میدهد تا خودش را به سرویس دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس گیرنده و سرویس دهنده این اجازه را می دهد که یک کلید متقارن را ایجاد کند که برای رمزنگاری و رمزگشایی سریع تر در جریان ادامه مبادلات مورد استفاده قرار میگیرد.

www.Prozhe.com

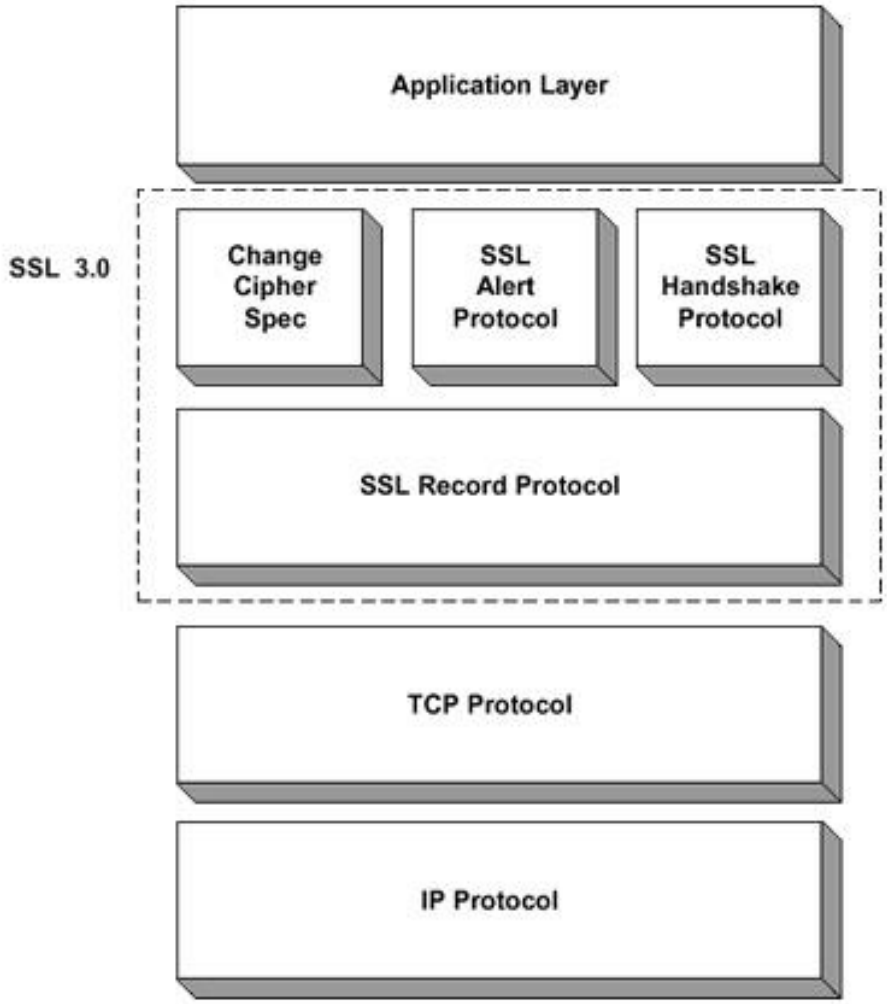
گام هایی که قبل از برگزاری این جلسه انجام میشوند براساس الگوریتم RSA Key Exchange عبارتند از:

- سرویس گیرنده ، نسخه SSL مورد استفاده خود ، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس دهنده ارسال میکند .
- سرویس دهنده نیز در پاسخ نسخه SSL مورد استفاده خود ، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس گیرنده می فریتد و همچنین سرویس دهنده گواهینامه خود را نیز برای سرویس گیرنده ارسال میکند و اگر سرویس گیرنده از سرویس دهنده ، درخواستی داشت که نیازمند احراز هویت سرویس گیرنده بود ، آن را نیز از سرویس گیرنده درخواست میکند.
- سرویس گیرنده با استفاده از اطلاعاتی که از سرویس دهنده مجاز در خود دارد ، داده ها را بررسی میکند و اگر سرویس دهنده مذکور تایید هویت شد ، وارد مرحله بعدی میشود و در غیر اینصورت با پیغام هشداری به کاربر ، ادامه عملیات قطع میگردد.
- سرویس گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد میکند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولا در سرویس دهنده موجود است) رمزنگاری می کند ، و این مقدار رمز شده را به سرویس دهنده ارسال میکند.
- اگر سرویس دهنده به گواهینامه سرویس گیرنده احتیاج داشت میبایست در این گام برای سرویس دهنده ارسال شود و اگر سرویس گیرنده نتواند هویت خود را به سرویس دهنده اثبات کند ، ارتباط در همین جا قطع میشود.
- به محض این که هویت سرویس گیرنده برای سرویس دهنده احراز شد ، سرویس دهنده با استفاده از کلید اختصاصی خودش مقدار Secret Premaster را رمز گشایی می کند و سپس اقدام به تهیه مقداری به نام Master Secret می نماید . هم سرویس دهنده و هم سرویس گیرنده با استفاده از مقدار Master Secret کلید جلسه (Session Key) را تولید می کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت داده ها بررسی می شود.
- سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد ، داده بعدی که توسط سرویس گیرنده ارسال میشود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه ، پیغام رمز شده نیز ارسال میشود تا سرویس دهنده از پایان یافتن Handshake سمت سرویس گیرنده مطلع شود.
- سرویس دهنده پیغامی را به سرویس گیرنده ارسال میکند تا او را از پایان Handshake سمت سرویس دهنده آگاه نماید و همچنین این که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز میشود.
- در این مرحله SSL Handshake تمام میشود و از این به بعد جلسه SSL شروع میشود و هر دو عضو سرویس دهنده و سرویس گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده ها می کنند.

www.Prozhe.com

حملات تاثیرگذار بر SSL

SSLنیز از حملات و نفوزهای مختلف در امان نیست. بعضی از حملات متداولی که بر این پروتکل واقع می شوند عبارتند از Traffic Analysis(تحلیل ترافیک) ،حملات Certificatio Injection و حملات از نوع Man In The Middle

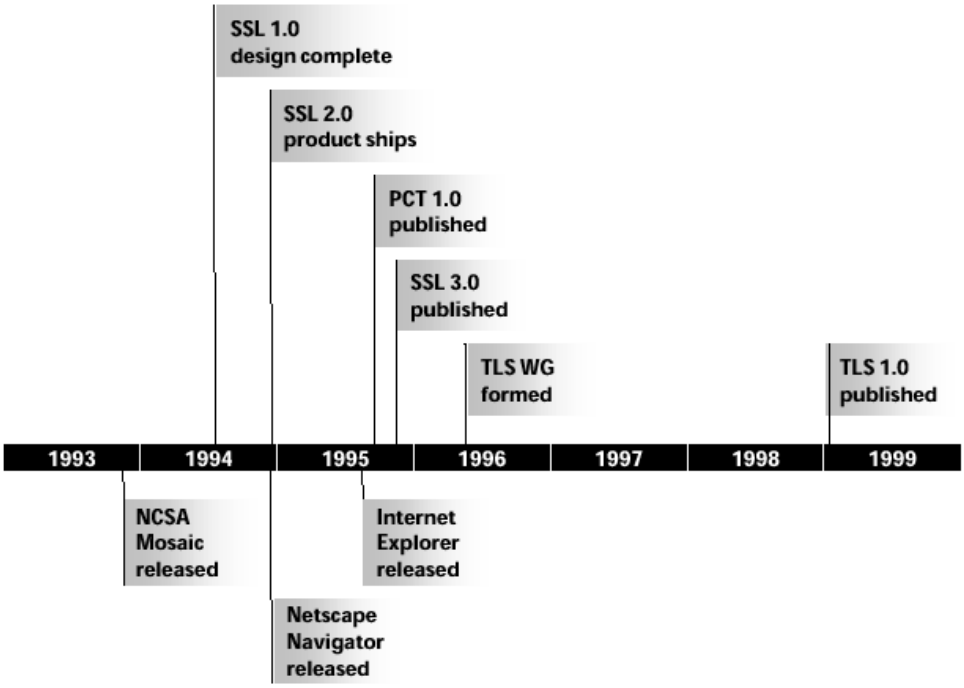


www.Prozhe.com

پروتکل TLS [۱۴]

اولین نکته که در مورد TLS باید بدانیم این است که این پروتکل نسل جدید پروتکل SSL است ، در واقع TLS بعد از SSL version3 معرفی گردیده که در حال حاضر نسخه ۱.۲ ان میباشد.

پروتکل امنیتی لایه انتقال (TLS)، بر پایه لایه سوکت‌های امن(SSL) که یکی از پروتکل‌های رمزنگاری است و برای تامین امنیت ارتباطات از طریق اینترنت است بنا شده‌است. برای اطمینان از هویت طرف مقابل و تبادل کلید متقارن از گواهی X.509 و رمزنگاری نامتقارن استفاده می کند. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینتزنتی و پیام‌های فوری اینترنتی به کار می‌رود. اگرچه TLS و SSL با هم تفاوت‌های اندکی دارند ولی قسمت عمده‌ای از این پروتکل کم و بیش یکسان مانده‌است. TLS و SSL درمدل TCP/IP عمل رمزنگاری را در لایه های پایینی لایه کاربرد انجام می دهند ولی در مدل OSI در لایه جلسه مقداردهی شده و در لایه نمایش کار می کنند: ابتدا لایه جلسه با استفاده از رمزنگاری نامتقارن تنظیمات لازم برای رمزنگاری را انجام می دهد و سپس لایه نمایش عمل رمزگذاری ارتباط را انجام می دهد. در هر دو مدل TLS و SSL به نمایندگی از لایه انتقال کار می کنند.



[۱۴] Transport Layer Security

www.Prozhe.com

پروتکل SSH[۱۵] (پوسته امن)

تاریخچه SSH

در سال ۱۹۹۵ یک دانشجوی دانشگاه هلینسکی به نام Tatu Ylonen پس از اینکه اطلاعات مهمی مثل رمز و نام های کاربری در شبکه دانشگاه مورد شنود sniff قرار گرفت به فکر ایجاد یک شبکه امن افتاد که این فکر در نهایت منجر به ایجاد یک Shell امن شد که جایگزینی برای (FTP,Telnet rcp,rlogin,rsh) شد.

Telnetیکی از پرکاربرد ترین راه های ارتباطی بین سرور و کلاینت است. در Telnet دستورات یا کامندها بین سرویس دهنده و سرویس گیرنده مبادله میشوند. و هرچیزی که در کنسول سمت کلاینت نمایش داده میشود در طول شبکه به همان شکل به سرویس دهنده منتقل میشود و اگر نرم افزارهایی در مسیر برای شنود وجود داشته باشند این اطلاعات در اختیار افراد دیگر قرار خواهد گرفت.

SSH چیست؟

SSHیک پروتکل ارتباطی امن بر پایه TCP/IPو در لایه کاربردی عمل میکند. این پروتکل با رمزگذاری داده هاسا بین سرویس دهنده و سرویس گیرنده از افشای اطلاعات در طول مسیر جلوگیری میکند. و یک کانال ارتباطی امن در سیستم عامل سرویس دهنده برای دستیابی به خط فرمان برای کلاینت یا سرویس گیرنده ایجاد میکند.

SSHچه چیزی نیست ؟

از آنجا که کلمه shell در SSH استفاده شده ممکن است در برخورد اول تصور کنید که نوعی shellلینوکسی است که این تصور اشتباهی است و SSH مفسر فرمان نیست ، SSH یک محصول هم نیست همانطور که اشاره شد یک پروتکل است.

---

[۱۵] Secure shell

www.Prozhe.com

SSH1:

اولین ویرایش SSH در سال ۱۹۹۵ تولید شد واز انجا که نرم افزار و پروتکلی که تا کنون ایجاد شده تمام نیازها و اهداف تولید کننده و مصرف کننده را پوشش نمیدهد و دارای معایب پیش بینی نشده می باشد تا نسخه ۱.۹ به روز رسانی شد. و به صورت متن باز (رایگان) در اختیار کاربران قرار گرفت. نسخه یک این پروتکل توزیعهای مختلفی دارد که بهترین نسخه های شناخته شده ۱.۳ و ۱.۵ هستند.

SSH2:

نیاز برخی کاربران و شرکتها به خدمات پشتیبانی و همچنین نیاز به کسب درآمد از این راه Tatu Yionen تولید کننده این نرم افزار را به فکر ارائه نسخه تجاری این نرم افزار انداخت. او با تاسیس شرکت SSH communication Security محصولات SSH2 را به بازار عرضه کرد.در حالا حاضر نام این شرکت به Tectia تغییر نموده و محصولات و راه حلهای متنوعی در زمینه SSH به بازار عرضه میکند که مهمترین آن Tectia Client & Server میباشد.

لایه های پروتکل

Application Layer	ssh-connection Session multiplexing, X11 and port forwarding, remote command execution, SOCKS proxy, etc.
	ssh-userauth User authentication using public key, password, host based, etc.
	ssh-transport Initial key exchange and server authentication, setup encryption
Transport Layer	TCP
Internet Layer	IP
Network Access Layer	Ethernet

OpenSSH

با توجه به متن باز بودن نسخه یک یعنی SSH1 کاربران اینترنت که تمایل یا امکان پرداخت هزینه مجوز محصولات Tecita را نداشتند به فکر چاره افتادند و گروه OpenBSD شروع به ارائه موازی نسخه جدید

www.Prozhe.com

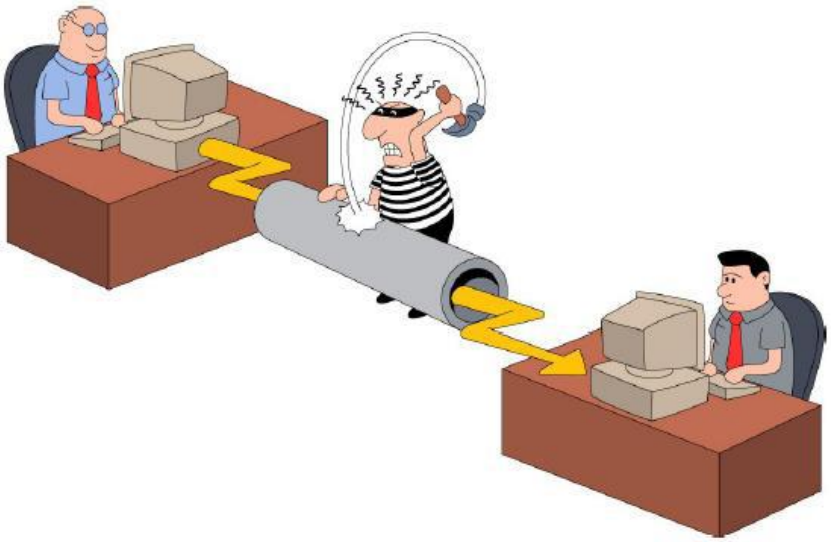
به صورت رایگان نمود که نام این محصول OpenSSH شد. در این مقاله به مقایسه نسخه تجاری و OpenSSH نمی پردازیم ولی از مزایای Tectia علاوه بر پشتیبانی از کاربران صفحه مدیریت تحت وب SSH می باشد.

مزایای SSH بر سایر روشهای قدیمی ارتباطی مثل Telnet

۱- رمزگذاری داده ها Encryption Data

همانطور که توضیح داده شد نیاز به یک اتصال امن بین کلاینت و سرور و جلوگیری از شنود اطلاعات در بین راه (sniff) مهمترین دلیل استفاده از SSH می باشد.

۲- Data Integrity بررسی یکپارچگی داده ها و جلوگیری از حمله های insertion and Replay Attackers



قابلیت فشرده سازی Compression

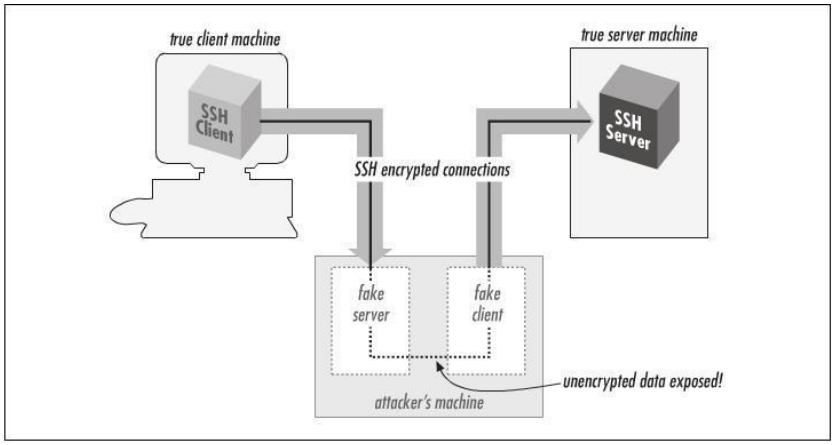
این پروتکل علاوه بر رمزگذاری اطلاعات ارسالی را فشرده نیز میکند که این کار در ارتباطهای کم سرعت بسیار مفید خواهد بود.

۳- عدم اتصال به سرور جعلی prevent Impersonation of host

www.Prozhe.com

در یک اتصال SSH هنگام اتصال به سرویس دهنده هویت سنجی انجام میگیرد و اگر یک ماشین با مشخصات سرویس دهنده در مسیر کاربر قرار گرفته باشد امکان میزبانی کلاینت یا بالعکس را ندارد. در حالی که در پروتکلهای قدیمی مثل Telnet این اتفاق اجتناب ناپذیر است.

این نوع حمله به حمله مرد میانی موسوم است : Man In The Middle Attack



۴-لاگ فایل Log Access

SSHامکان فعال یا غیر فعال شدن فرایند تهیه لاگ فایل ها را دارد با فعال شدن این امکان در مواقع بروز مشکل مدیر سیستم بعد از بروز خطا اولین موردی که برای رفع مشکل بررسی میکند لاگ فایل ها است.

۵-امکان استفاده از x11 Applications

SSHاین قابلیت را دارد که برنامه های دیگر مثل نرم افزار های گرافیکی را کد گذاری نماید به این قابلیت Port Forwardingهم میگویند. به عنوان مثال میتوان از این قابلیت برای کنترل دوربین های مدار بسته از راه دور استفاده کرد. از این قابلیت برای Tunneling هم استفاده میشود.

www.Prozhe.com

پروتکل Socks[۱۶] :

Socks یک پروتکل اینترنت است که به مسیریابی بسته های شبکه بین کلاینت و سرور از طریق یک پراکسی سرور می پردازد. ساکس در لایه چهارم مدل TCP/IP کار می کند و پورت ۱۰۸۰ برای سرویس دهنده ساکس ثبت و طراحی شده است.

ساکس در واقع یک پروتکل امنیتی است که برای اعمال مدیریت بر فایروال و دیگر محصولات امنیتی استفاده می شود. تکنولوژی بکار رفته در پراکسی Socks از برتری قابل ملاحظه ای نسبت به پراکسی HTTP برخوردار است از جمله اینکه پراکسی ساکس از تمامی پروتکل های اینترنت پشتیبانی می کند (TCP/IP) و به کامپیوترهای سرور و کلاینت اجازه ارتباطی دوطرفه از طریق تمامی پورت ها را فراهم می کند ولی پراکسی های HTTP معمولا از یک پروتکل حمایت می کنند (پروتکل HTTP) و اغلب اجازه برقراری ارتباط از طریق یک پورت را فراهم می کنند (البته این به این معنی نیست که اگر پراکسی از نوع ساکس باشد می توان توسط پورت دلخواه با سرور ارتباط برقرار کرد بلکه این امکان معمولا توسط مدیران سرور محدود شده و در نهایت از طریق پورتهای محدودی می توان با سرور ارتباط برقرار کرد)

از آنجایی که پراکسی ساکس در عین پشتیبانی از تمامی پروتکل ها امکان دسترسی امن کامپیوترهای داخل شبکه به اینترنت و امکان مدیریت شبکه برای جلوگیری از دسترسی های غیر مجاز و اعمال محدودیت های امنیتی به شبکه برخوردار است پراکسی ساکس بطور متداول به عنوان فایروال استفاده می شود

Socks دارای دو ورژن ۴ و ۵ می باشد که ورژن ۵ دارای برتری هایی نظیر پشتیبانی از پروتکل UDP و امنیت بالاتر نسبت به ورژن قبلی (ورژن ۴) می باشد

---

[۱۶] Socket Secure

www.Prozhe.com

مزایای Socks :

پروکسیهای ساکس نسبت به پروکسیهای HTTP مزیتهای زیادی دارند، از جمله:

سرور ساکس از کل پروتکلهای اینترنت (TCP/IP) پشتیبانی میکند و به کامپیوترهایی که در دو سمت آن قرار گرفته‌اند اجازه میدهد به طور کامل و از طریق تمام پورتها با همدیگر ارتباط برقرار کنند. پروکسیهای HTTP غالباً از یک پروتکل اینترنتی یعنی همان HTTP حمایت میکنند و تنها اجازه برقراری ارتباط بر روی یک پورت را میدهند.

از آنجایی که پروکسیهای HTTP فقط از یک پروتکل حمایت میکنند، با نرم‌افزارهای معدودی مانند مرورگرهای وب سازگاری دارند. پروکسیهای ساکس به خاطر تطابقشان با کلیه پروتکلهای اینترنتی تقریباً با همه نرم‌افزارهای شبکه سازگاری دارند.

بیشترین کاربرد پروکسیهای HTTP، کنترل و تسهیل دسترسی به صفحات وب در یک شبکه است. در حالیکه از پروکسیهای ساکس به طور رایج به عنوان فایروال در شبکه استفاده میشود. زیرا ساکس میتواند به کامپیوترهای داخل شبکه امکان دسترسی کامل به اینترنت را بدهد و در عین حال جلوی دسترسی‌های غیر مجاز از اینترنت به داخل شبکه را بگیرد.

ساکس اجازه یک ارتباط دو طرفه بین کامپیوترهای دو سوی سرور ساکس را میدهد. سایر پروکسی‌ها فقط از ارتباط یک طرفه از داخل شبکه به اینترنت پشتیبانی میکنند. این مسئله خصوصاً در مورد برنامه‌های مولتی‌مدیا و مسنجرها که نیاز به ارتباط دو طرفه دارند حائز اهمیت است.

تفاوت VPN و Proxy چیست؟

ما در کل دو نوع VPN داریم هم از نظر ساختار ارتباطی و هم تکنولوژی ارتباطی که عبارتند از :

Site 2 Site VPN

Client Side-Vpn

Site 2 Site VPN: فرض میکنیم دو شبکه ی LAN را به هم وصل میکنیم که برای وصل شدن باید از Tunnel ها استفاده کنیم، مثل GRE و IpSec ، هر کدام از اینها در واقع یکسری عملیات را دوباره روی Packet انجام می دهند که به این عملیات کپسوله سازی یا همون Encapsulate گفته می شود.

www.Prozhe.com

Client Side-Vpn : در این روش ما کلاینت ها را به شبکه ی VPN وصل میکنم، مثلا سازمانی را در نظر بگیرید که برای هر کارمندش ۱۰ ساعت اینترنت رایگان ارائه می دهد، یکی از روش پیاده سازی استفاده از همین تکنولوژی می باشد که ما کلاینت را اعتبار سنجی کرده و به شبکه VPN وصل می کنیم

در واقع هسته ی VPN با استفاده از تانل ها می باشد، هر کدام از VPN Protocol ها یک پورت مخصوص برای این کار دارند، برای پیاده سازی امنیت هم از رمز نگاری با SHA1 گرفته تا MD5 را هم داریم. در VPN ها تمام ترافیک ما تحت سرور رمزنگاری می شود و بعد انتقال داده می شود که از لحاظ امنیت بسیار مناسب می باشد.

اما پروکسی سرور در واقع یک سروری می باشد که مابین ارتباطات WAN و Local شبکه قرار می گیرد، از یک نظر هم میتوانیم ان را یک نوع مدل از Firewall دانست چون تمام محتوای پکت توسط این سرور برسی می شود و بعد به درخواست جواب داده می شود. چندین نوع Proxy Server وجود دارد که هر کدام کاری خاصی را انجام می دهند مثل : IP Nat -Web Proxy- SNMP Proxy و ....

Socks مشهورترین پراکسی در زمینه وب می باشد و کار این پراکسی به این صورت است که تمام ترافیک مربوط به پورت ۸۰ را دریافت کرده و مودر بررسی قرار می دهد و بعد در اختیار کاربران قرار میدهد، معمولا پراکسی سرور را روی پورت ۱۰۸۰ یا ۸۰۸۰ ارائه میدهد. این شماره پورت در واقع ادرس پورت سرور پراکسی می باشد که ترافیک مروبوط به پورت ۸۰ یا همون WWW را گرفته و مورد پردازش قرار میدهد.

اما پورت ۴۴۳ در واقع همون HTTP می باشد،پروتکل SSL که پروتکلی جهت پیاده سازی امنیت در TCP/IP می باشد تمام ترافیک WWW را با الگوریتم های با طول رمز نگاری متفاوت انکریپت می کند و با HTTPS معرفی می کند. شما میتوانید SSL را بر روی هر Application اجرا کنید و از ان استفاده کنید.

www.Prozhe.com

پروتکل Kerberos

کربروس (Kerberos) یک پروتکل اعتبار سنجی در شبکه است و برای انجام اعتبار سنجی های قوی ، در برنامه های سرویس دهنده و سرویس گیرنده تعبیه شده است . این پروتکل توسط دانشگاه MIT طراحی و پیاده سازی شده است.

کربروس یک پروتکل رایگان است (مانند BSDها) و تحت قانون حق مؤلف (Copyright) می توانید از آن استفاده کنید. نکته جالبی که در مورد کربروس وجود دارد این است که کربروس یک سگ سه سر است که از دروازه ی جهنم محافظت می کند. البته کمی املای آن فرق دارد (Cerberus) ولی همان مفهوم مدنظر بوده است.

آخرین نسخه آن نیز، نسخه ۵ است.

کربروس بر مبنای این تئوری بنا شده است که شبکه یک مکان ناامن و خطرناک است و اطلاعات ارسالی در شبکه قابل تغییر و دستکاری هستند.

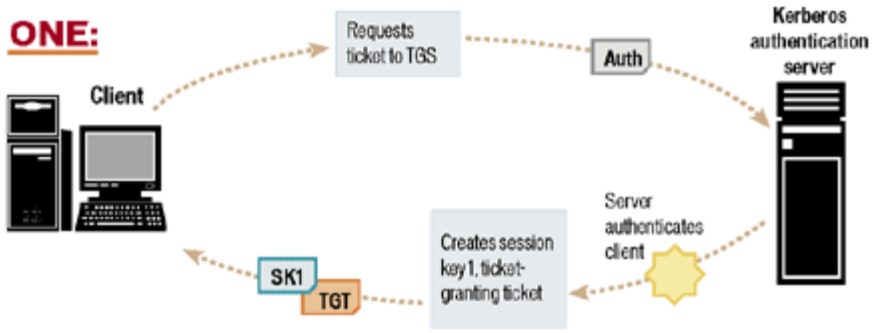
کربروس یک سرویس thrid-party و تأیید شده است. این بدان معنی است که یک کارگزار کربروس در شبکه وجود دارد که مورد اعتماد Principal ها (Principal ها اجزایی هستند که هویت آنها در سیستم تأیید شده است مانند کاربران و سرویس ها) است. Principal ها یک کلید عمومی را بین خود و کارگزار به رسمیت می شناسند و بدین ترتیب principal ها قادر خواهند بود پیام هایی که از کارگزار می آید را درک کنند. Principal ها به رد و بدل کردن بلیط می پردازند و با همین بلیط ها هویت principal ها معلوم می شود.

جزییات بیشتر در مورد نحوه عملکرد kerberos را با یک مثال و شکل نشان می دهیم.

۱-کاربر (Clinet) از متصدی اعتبارسنجی (Kerberos Authentication Server) یک بلیط درخواست می کند که بعداً آن را به متصدی صدور بلیط(Ticket Granting Server) بدهد. متصدی اعتبارسنجی، در پایگاه داده خود جستجو می کند و در صورت یافتن کاربر در فهرست خود، یک کلید (Session Key 1 - SK1) می سازد که برای استفاده بین کاربر و متصدی بلیط بکار خواهد رفت. متصدی اعتبارسنجی، بلیط را که شامل SK1 است را با کلید A کد کرده و برای کاربر ارسال می کند.

www.Prozhe.com

متصدی اعتبارسنجی، همچنین از کد مخفی متصدیان بلیط که فقط بین متصدی اعتبارسنجی و متصدیان بلیط معتبر است، استفاده کرده و یک بلیط صدورِ بلیط (Ticket Granting Ticket) برای کاربر می سازد و برای کاربر می فرستد.



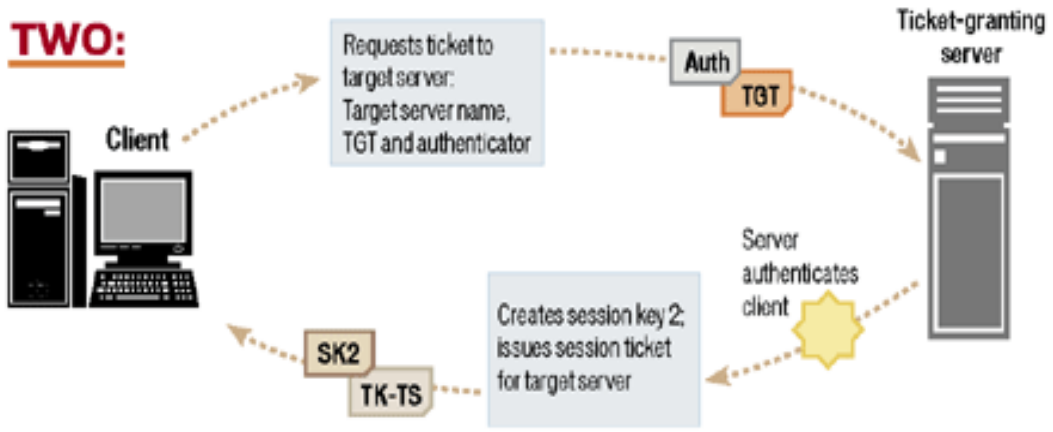
۲- کاربر پس از دریافت پیام، آن را رمزگشایی کرده و SK1 را بدست می آورد. سپس یک Authenticator می سازد (شامل نام کاربر، آدرس و تاریخ و زمان فعلی)و آن را به همراه بلیط صدورِ بلیط (TGT) ، برای دریافت اجازه دسترسی به کارگزار موردنظر به متصدی صدور بلیط (TGS) می فرستند.

متصدی صدور بلیط (TGS) ، بلیط صدورِ بلیط (TGT) را می گیرد و آن را رمزگشایی می کند. پس از بدست آوردن SK1 که از رمزگشایی بلیط صدورِ بلیط (TGT) بدست آمده است، Authenticator را نیز رمزگشایی می کند. اگر زمان و نام A معتبر بود، روند کار ادامه پیدا می کند.

متصدی صدور بلیط (TGS) یک کلید جدید (Session Key 2 – SK2) تولید کرده و آن را با SK1 کد می کند و برای کاربر می فرستد تا بین کاربر و کارگزار استفاده شود.

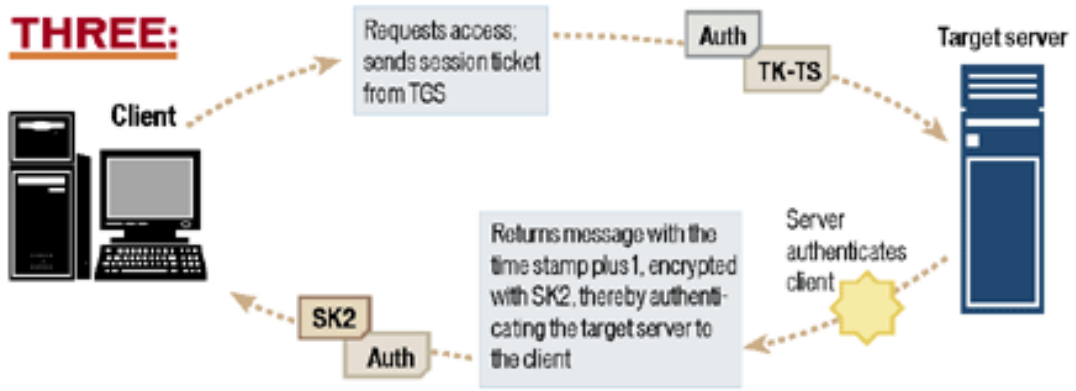
همچنین متصدی صدور بلیط (TGS) یک بلیط جدید شامل نام کاربر، IP(آدرس)، تاریخ و زمان، زمان اعتبار (که همه با کلید کارگزار کد شده اند) و نام کارگزار می سازد و برای کاربر می فرستد.

www.Prozhe.com



۳- کاربر پس از گرفتن بلیط آن را رمزگشایی کرده SK2 را بدست می آورد. حال کاربر آماده است تا با کارگزار ارتباط برقرار کند. کاربر یک Authenticator جدید می سازد و با SK2 آن را کد می کند. سپس کاربر، Authenticator را به همراه بلیطی که با کلید کارگزار کد شده بود را به کارگزار می فرستد.

کارگزار با دریافت Authenticator که با SK2 رمز شده است، می فهمد که کاربر، SK2 را دارد. زمان و تاریخ تعبیه شده در بلیط، این امکان را شنودگرها می گیرد که این بلیط ها را ذخیره کنند و بعدها دوباره آن را برای کارگزار بفرستند و خود را جای کاربر جا بزنند. برای برنامه های که نیاز به اعتبارسنجی دوطرفه دارند، یک بلیط دیگر از طرف کارگزار به کاربر فرستاده می شود که با SK2 کد شده است. که انجام این عمل به کاربر نیز اطمینان کامل را می دهد.



www.Prozhe.com

۴- اطلاعات بین کاربر و کارگزار با استفاده از SK2 رد و بدل می شود.

پروتکل های FTPS/SFTP

ابتدا به مباحث جزیی برای درک بهتر FTPS و SFTP میپردازیم.

AS2

AS2 (Applicability Statement 2) گونه ای EDI (Electronic Date Exchange) یا تبادل دیتای الکترونیکی (اگرچه به قالبهای EDI محدود نشده) برای استفاده های تجاری با استفاده از HTTP است. AS2 در حقیقت بسط یافته نسخه قبلی یعنی AS1 است. AS2 چگونگی تبادل دیتای تجاری را بصورت امن و مطمئن با استفاده از HTTP بعنوان پروتکل انتقال توصیف می کند. دیتا با استفاده از انواع محتوایی MIME استاندارد که XML، EDI ، دیتای باینری و هر گونه دیتایی را که قابل توصیف در MIME باشد، پشتیبانی می کند، بسته بندی می شود. امنیت پیام (تایید هویت و محرمانگی) با استفاده از S/MIME پیاده سازی می شود. AS1 در عوض از SMTP استفاده می کند. با AS2 و استفاده از HTTP یا (SSL با HTTP)HTTPS برای انتقال، ارتباط بصورت زمان حقیقی ممکن می شود تا اینکه از طریق ایمیل انجام گیرد. امنیت، تایید هویت، جامعیت پیام، و خصوصی بودن با استفاده از رمزنگاری و امضاهای دیجیتال تضمین می شود، که برپایه S/MIME هستند و نه SSL. استفاده از HTTP/S بجای HTTP استاندارد بدلیل امنیت ایجادشده توسط S/MIME کاملاً انتخابی است. استفاده از S/MIME اساس ویژگی دیگری یعنی انکارناپذیری را شکل می دهد، که امکان انکار پیام های ایجادشده یا فرستاده شده توسط کاربران را مشکل می سازد، یعنی یک شخص نمی تواند منکر پیامی شود که خود فرستاده است.

www.Prozhe.com

: FT

(انتقال فایل یا File Transfer)

AS2 مشخصاً برای درکنارهم قراردادن و یژگیهای امنیتی با انتقال فایل یعنی تایید هویت، رمزنگاری، انکارناپذیری توسط S/MIME و SSL انتخابی ، طراحی شده است. از آنجا که AS2 یک پروتکل در حال ظهور است، سازمانها باید تولید کنندگان را به پشتیبانی سریع از آن تشویق کنند. قابلیت وجود انکارناپذیری در تراکنش های برپایه AS2 از اهمیت خاصی برای سازمانهایی برخوردار است که می خواهند پروسه های تجاری بسیار مهم را به سمت اینترنت سوق دهند. وجود قابلیت برای ثبت تراکنش پایدار و قابل اجراء برای پشتبانی از عملکردهای بسیار مهم مورد نیاز است. AS2 ازMDN (Message Disposition Notification) بر پایه RFC 2298 استفاده می کند. MDN (که می تواند در اتصال به سایر پروتکل ها نیز استفاده شود) بر اساس محتوای MIME است که قابل خواندن توسط ماشین است و قابلیت آگاه سازی و اعلام وصول پیام را بوجود می آورد، که به این ترتیب اساس یک ردگیری نظارتی پایدار را فراهم می سازد.

FTP (File Transfer Protocol)

FTP یا پروتکل انتقال فایل به منظور انتقال فایل از طریق شبکه ایجاد گشته است، اما هیچ نوع رمزنگاری را پشتیبانی نمی کند. FTP حتی کلمات عبور را نیز بصورت رمزنشده انتقال می دهد، و به این ترتیب اجازه سوءاستفاده آسان از سیستم را می دهد. بسیاری سرویس ها FTP بی نام را اجراء می کنند که حتی نیاز به کلمه عبور را نیز مرتفع می سازد (اگرچه در این صورت کلمات عبور نمی توانند شنیده یا دزدیده شوند)

www.Prozhe.com

برای FT:

FTP بعنوان یک روش امن مورد توجه نیست، مگر اینکه درون یک کانال امن مانند SSL یا IPSec قرار گیرد.

گرایش زیادی به FTP امن یا FTP بر اساس SSL وجود دارد.

FTPS و SFTP

SFTP به استفاده از FT بر روی یک کانال که با SSH امن شده، اشاره دارد، در حالیکه منظور از FTPS استفاده از FT بر روی SSL است. اگرچه SFTP دارای استفاده محدودی است، FTPS (که هر دو شکل FTP روی SSL و FTP روی TLS را بخود می گیرد) نوید کارایی بیشتری را می دهد. (FTPS) رمزنگاری کانالهای دیتا را که برای ارسال تمام دیتا و کلمات عبور استفاده شده اند، ممکن می سازد اما کانالهای فرمان را بدون رمزنگاری باقی می گذارد (بعنوان کانال فرمان شفاف شناخته می شود). مزیتی که دارد این است که به فایروالهای شبکه های مداخله کننده اجازه آگاهی یافتن از برقراری نشست ها و مذاکره پورتها را می دهد. این امر به فایروال امکان تخصیص پورت پویا را می دهد، بنابراین امکان ارتباطات رمزشده فراهم می شود بدون اینکه نیاز به این باشد که تعداد زیادی از شکاف های دائمی در فایروال پیکربندی شوند.

اگرچه معمول ترین کاربردهای FTP (مخصوصاً بسته های نرم افزاری کلاینت) هنوز کاملاً FTPS را پشتیبانی نمی کنند و پشتیبانی مرورگر برای SSL، برای استفاده کامل از مجموعه کامل فانکشن های FTPS کافی نیست، اما این امر در حال پیشرفت است. بسیاری از تولیدکنندگان برنامه های کاربردی در حال استفاده از SSL استاندارد در کنار FTP استاندارد هستند. بنابراین، گرچه در بعضی موارد مسائل تعامل همچنان وجود دارند، اما امیدواری برای پشتیبانی گسترده از FT امن در ترکیب با SSL وجود دارد.(اطلاعات بیشتر در RFC 2228)

www.Prozhe.com

منابع :

- ✓ www.fa.wikipedia.org
- ✓ www.wikipedia.org
- ✓ http://www.ircert.com/articles/SecureFTP.htm
- ✓ http://www.protocols.com
- ✓ http://www.webkaran.com/essay/SSL.html
- ✓ مبانی امنیت شبکه (ویلیام استالینگز) ترجمه جعفری نژاد قمی
- ✓ مجموعه پروتکلTCP/IP(بهروزفروزان) ترجمه محمدحسین یغمایی مقدم
- ✓ اصول مهندسی اینترنت (احسان ملکیان)
- ✓ مروری بر SSH دانشگاه شریف(امیر عباس جاویدان)

www.Prozhe.com