امنیت لایه انتقال

پروتکل امنیتی لایهٔ انتقال (Transport Layer Security)، بر پایه لایهٔ سوکت‌های امن (Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است و برای تأمین امنیت ارتباطات از طریق اینترنت بنا شده‌است. برای اطمینان از هویت طرف مقابل و تبادل کلید متقارن از گواهی X.509 و رمزنگاری نامتقارن استفاده می‌کند. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی 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 لایه‌های پایینی لایه کاربرد انجام می‌دهند ولی در مدل OSI در لایه جلسه مقداردهی را شده و در لایه نمایش کار می‌کنند: ابتدا لایه جلسه با استفاده از رمزنگاری نامتقارن تنظیمات لازم برای رمزنگاری را انجام می‌دهد و سپس لایه نمایش عمل رمزگذاری ارتباط را انجام می‌دهد. در هر دو مدل TLS و SSL به نمایندگی از لایه انتقال کار می‌کنند.

لایهٔ سوکت‌های امن (Secure Sockets Layer) یا **اس‌اس‌ال** (SSL) پروتکلی است که توسط شرکت Netscape برای ردّ و بدل کردن سندهای خصوصی از طریق اینترنت توسعه یافته‌است. SSL از یک کلید خصوصی برای به رمز درآوردن اطلاعاتی که بر روی یک ارتباط SSL منتقل می‌شوند استفاده می‌نماید. هر دو مرورگر Netscape Navigator و Internet Explorer (و امروزه تمام مرورگرهای مدرن) از این پروتکل پشتیبانی می‌نمایند. هم‌چنین بسیاری از وب‌سایت‌ها برای فراهم کردن بستری مناسب جهت حفظ کردن اطلاعات محرمانهٔ کاربران (مانند شمارهٔ کارت اعتباری) از این پروتکل استفاده می‌نمایند. طبق آنچه در استاندارد آمده‌است. URLهایی که نیاز به یک ارتباط از نوع SSL دارند با:https به جای:http شروع می‌شوند. SSL یک پروتکل مستقل از لایه برنامه‌است (Application Independent). بنابراین، پروتکل‌هایی مانند HTTP, FTP و شبکه راه دور قابلیت استفاده از آن را دارند. با این وجود SSL برای پروتکل‌های FTP, HTTP و آی‌پی‌سک بهینه شده‌است. درsslازدوکلیدعمومی وخصوصی استفاده می‌شودهمچنین درsslازدوحالت متقارن ونامتقارن نیز می‌توان نام بردکه می‌تواند همان بحث *کلید عمومی* واختصاصی باشد به اینصورت که دررمزنگاری متقارن ازدو کلیدعمومی توسط serverوclient استفاده می‌شود که در این صورت مطالب رمزنگاری شده ازامنیت برخوردارنخواهدشدزیراکلید مشترک مابین (سروروموشتری) توسط شخص ثالث می‌تواند استراق سمع یاهک شودبنابراین

ازحالت نامتقارن استفاده می‌شوددر رمزنگاری نامتقارن ازدوکلیدBوAاستفاده می‌شودیعنی اگر مطالب باکلیدA رمزنگاری شوددیگر باهمان کلیدرمزگشایی نخواهد شدفقط باکلیدB که متناظرباکلیدA می‌باشدرمزگشایی خواهدشد.

تعریف

پروتکل TLS به برنامه‌های Client/Server اجازه می‌دهد که در شبکه از طریقی که از eavesdropping(شنود)، message forgery(جعل پیام) جلوگیری می‌کند با یکدیگر ارتباط برقرار کنند. TLS authentication(احراز هویت) و communications confidentiality(ارتباط مطمئن) در اینترنت را از طریق استفاده از cryptography(رمز نگاری) فراهم می‌کند.

Client باید برای Server مشخص کند که آیا می‌خواهد یک اتصال TLS داشته باشد یا نه. دو راه برای رسیدن به این هدف وجود دارد: یک راه این است که از شماره پورت متفاوتی برای اتصال TLS استفاده شود (برای مثال پورت ۴۴۳ پروتکل امن انتقال ابرمتن) و دیگر اینکه اختصاص یک پورت مشخص از طریق سرور به کلاینت، که کلاینت آن را درخواست کرده باشد با استفاده از یک مکانیسم پروتکل خاص (برای مثال STARTTLS).
زمانی که کلاینت و سرور تصمیم گرفتند از اتصال TLS استفاده کنند، به مذاکره با استفاده از روش handshaking می‌پردازند. سپس سرور و کلاینت بر روی پارامترهای مختلفی که برای ایجاد امنیت اتصال استفاده می‌شود به توافق می‌رسند:

1. کلاینت اطلاعاتی را که سرور برای برقراری ارتباط با استفاده از SSL به ان نیاز دارد را ارسال می‌کند. مانند:شماره نسخه SSL کلاینت، تنظیمات رمزگذاری و سایر اطلاعاتی که سرور ممکن است به آن نیاز داشته باشد.
2. سرور اطلاعاتی را که کلاینت برای برقراری ارتباط با استفاده از SSL به ان نیاز دارد را برایش ارسال می‌کند. مانند:شماره نسخه SSL سرور، تنظیمات رمزگذاری و سایر اطلاعاتی که کلاینت به آن نیاز دارد. سرور همچنین گواهینامه خود را برای کلاینت ارسال می‌کند و اگر کلاینت درخواست منبعی از سرور داشته باشد، کلاینت باید احراز هویت شود و باید گواهینامه کلاینت برای سرور ارسال شود.
3. با اطلاعات دریافتی از سرور، کلاینت می‌تواند سرور را احرازهویت کند. اگر سرور تصدیق نشود، به کاربر هشدار داده می‌شود که عمل رمزگذاری و تصدیق نمی‌تواند انجام گیرد. اگر سرور به درستی تصدیق شد کلاینت به مرحله بعد می‌رود.
4. با استفاده از اطلاعات به دست آمده، کلاینت یک pre-master secret ایجاد کرده و آن را ب سرور ارسال می‌کند.
5. اگر سرور از کلاینت بخواهد هویتش را ثابت کند، کلاینت کلیه اطلاعات لازم و گواهی خود را برای سرور ارسال می‌کند.
6. اگر کلاینت تصدیق نشود، ارتباط قطع می‌شود اما اگر به درستی تصدیق شود، سرور از کلید خصوصی خود برای یاز کردن pre-master secret استفاده می‌کند.
7. کلاینت و سرور از master secret برای تولید کلید جلسات استفاده می‌کنندکه یک کلید متقارن است و برای رمزگذاری و رمزگشایی اطلاعات مبادله شده استفاده می‌شود.

8. وقتی کلاینت پیغامی برای سرور ارسال می‌کند با استفاده از کلید جلسه آن را رمز می‌کند.
9. وقتی سرور پیغامی برای کلاینت ارسال می‌کند با استفاده از کلید جلسه آن را رمز می‌کند.

اکنون SSL handshake کامل است و ارتباط شروع می‌شود. کلاینت و سرور از کلید جلسه برای رمزگذاری و رمزگشایی اطلاعاتی که برای هم می‌فرستند استفاده می‌کنند.
اگر یکی از قدم‌های بالا با شکست مواجه شود TLS دچار شکست شده و ارتباط برقرار نمی‌شود.
در قدم سوم مشتری باید گواهی سرور را به درستی چک کند تا باعث بروز مشکل نشود.

تاریخچه

برنامه‌نویسی امن

تلاش‌های تحقیقاتی در اوایل نسبت به امنیت در لایه انتقال شامل برنامه‌نویسی شبکه‌ای امن و رابط برنامه‌نویسی کاربردی بود. در سال ۱۹۹۳ به بررسی رویکرد داشتن یک لایه انتقال امن، به منظور تسهیل مقاوم‌سازی برنامه‌های کاربردی موجود در شبکه با اقدامات امنیتی پرداخته شد.

SSL 1.0 ،۲٫۰ ،۳٫۰

پروتکل SSL در اصل توسط Netscape توسعه داده شد. نسخه ۱٫۰ آن برای استفاده عمومی نبود. نسخه ۲٫۰ آن در سال ۱۹۹۵ منتشر شد که تعدادی نقص‌های امنیتی داشت و منجر به تولید نسخه ۳٫۰ شد. SSL 3.0 که در سال ۱۹۹۶ منتشر شد یک طراحی مجدد کامل از پروتکل‌های تولید شده بود.

TLS 1.0

این پروتکل در سال ۱۹۹۹ به عنوان ارتقا یافتهٔ نسخه SSL 3.0 تعریف شد. تفاوت چشمگیری بین این پروتکل و SSL 3.0 وجود ندارد و می‌توان گفت این پروتکل SSL 3.0 را کامل کرده‌است.

TLS 1.1

این پروتکل در سال ۲۰۰۶ تعریف شد و توسعه یافته TLS 1.0 بود.
تفاوت‌های قابل توجهی که در این نسخه وجود دارد:

- حفاظت دربرابر حملات Cipher block chaining (CBC) اضافه شده‌است.
- IV implicit با IV explicit جایگزین شده‌است.

TLS 1.2

در سال ۲۰۰۸ تولید شد. مشخصات TLS 1.1 را دارد. تفاوتی که این پروتکل دارد این است که MD5-SHA-1 با SHA-256 جایگزین شده‌است.

برنامه‌های کاربردی

در طراحی برنامه‌های کاربردی، TLS معمولاً در بالای تمامی پروتکل‌های لایه انتقال پیاده‌سازی می‌شود و پروتکل‌های برنامه‌های کاربردی مانند HTTP, FTP, SMTP, NNTP, XMPP، را کپسوله می‌کند. با استفاده از پروتکل‌های انتقال داده گرام مانند UDP و پروتکل کنترل ازدحام داده(DCCP)استفاده می‌شود.

وب سایت‌ها

یک استفاده برجسته از TLS این است که برای امن کردن ترافیک بین وب سایت‌ها و مرورگرها استفاده می‌شود.

تبادل کلید

در پیاده‌سازی‌های نخستین لایهٔ سوکت‌های امن، به علّت محدودیت‌های اعمال شده بر روی صادرات تکنولوژی رمزنگاری از طرف دولت ایالات متحده، از کلیدهای متقارن با طول ۴۰ استفاده می‌شد. قبل از اینکه کلاینت و سرور به تبادل اطلاعات حفاظت شده توسط TLS بپردازند باید بر روی یک کلید رمزگذاری و یک روش رمزگذاری توافق کنندتا مبادلهٔ امنی داشته باشند.
متدهایی که برای مبادله کلید استفاده می‌شود:
تولید کلیدهای عمومی خصوصی باRSA, Diffie-Hellman, ephemeral Diffie-Hellman, ECDH, ephemeral Elliptic Curve Diffie-Hellman, anonymous Diffie-Hellman و PSK.
روش توافق کلید TLS_DH_anon سرور و کلاینت را احراز هویت نمی‌کند به همین دلیل به ندرت استفاده می‌شود.

SSL

لایه سوکت امن (SSL) توسط Netscape طراحی شد و نسخه ۳ آن به صورت استاندارد اینترنت درآمد. معماری SSL به صورت دولایه‌ای است که روی TCP قرار گرفته‌است. لایه اول بالای لایه حمل قرار گرفته‌است و لایه دوم در لایه کاربرد است. قسمتی از SSL که در لایه دوم قرار می‌گیرد مربوط به سرویس‌های مدیریتی است و شامل پروتکل دست دادن، پروتکل تغییر مشخصات رمزکننده و پروتکل هشدار است. SSL اجازه می‌دهد که بین کلاینت و سرور یک جلسه ایجاد شود و از آن طریق هر تعداد اتصال امن امکان‌پذیر باشد. از نظر تئوری بین یک کلاینت و یک سرور می‌تواند بیش از یک جلسه وجود داشته باشد و در عمل فقط یک جلسه به وجود می‌آید.
یک جلسه توسط پروتکل دست دادن ایجاد می‌شود و مجموعه‌ای از پارامترهای امنیتی را تعریف می‌کند که به صورت اشتراکی در اتصالات مربوط به آن جلسه استفاده می‌شوند. برای هر جلسه و هر اتصال به یک سری پارامترها نیاز است.

پروتکل رکورد در SSL

این پروتکل مربوط به لایه اول SSL است که دو سرویس محرمانگی و احرازهویت را بواسطهٔ کلیدهایی که در پروتکل دست دادن ساخته می‌شوند فراهم می‌کندو در این پروتکل محرمانگی توسط الگوریتم رمز متقارن و احرازاصالت توسط MAC فراهم می‌شود. این پروتکل شامل مراحل زیر است:

- قطعه قطعه کردن: داده کاربر تقسیم‌بندی می‌شود.
- فشرده سازی: SSL دارای یک الگوریتم فشرده سازیست که در نسخه ۳٫۰ اختیاری است.
- کد احرازاصالت پیام
- رمزگذاری: قطعه فشرده شده به همراه MAC رمز می‌شوند.
- سرآیند: سرآیند به ابتدای قطعه رمزشده می چسپد.

پروتکل تغییر مشخصات رمز در SSL

این پروتکل ساده‌ترین پروتکل مربوط به لایه دوم است که تنها یک بایت با مقدار یک دارد. هدف از این پیام یک بایتی تغییر اطلاعات رمزگذاری مربوط به ارتباط موجود است که در واقع وضعیت معلق را به وضعیت جاری کپی می‌کند.

پروتکل هشدار در SSL

این پروتکل به منظور اعلام هشدارهای SSL به طرفین اتصال استفاده می‌شود. مربوط به لایه دوم است و از ۲ بایت تشکیل شده‌است. این ۲ بایت عبارتنداز:

1. نوع خطا که می‌تواند Warning یا Fatal باشد.
2. کد خطا مانند پیغام غیرمنتظره، خطا در بازگشایی، خطا در گواهی و ...

اگر خطا ز نوع Fatal باشد، اتصال مذکور فوراً قطع می‌شود و اجازه ایجاد اتصال جدید در جلسه فوق داده نمی‌شود، اما ارتباطات دیگر موجود در این جلسه می‌توانند ادامه پیدا کنند.

پروتکل دست دادن در SSL

این عمل به منظور احرازاصالت دوطرف و توافق روی الگوریتم‌ها و کلیدهای رمزگذاری است و به لایه دوم مربوط است و قبل از هر انتقال داده بین دو طرف این پروتکل صورت می‌گیرد. این پروتکل پیچیده‌ترین پروتکل SSL است که یکسری پیام دارد که بین دوطرف ارتباط مبادله می‌شود. هر پیام شامل نوع پیام، طول پیام به بایت و محتوای پیام است. این پروتکل دارای ۴ مرحله است.

مرحله ۱: برقراری قابلیت‌های امنیتی

این مرحله به منظور آغاز یک اتصال منطقی برای معین کردن قابلیت‌های امنیتی مربوط به آن اتصال است.

مرحله ۲: احراز اصالت و تبادل کلید سرور

در این مرحله حداکثر ۴ پیام از طرف سرور به کلاینت ارسال می‌شود که ۳ تا از آن‌ها اختیاری است. پیام اول شامل گواهی سرور است. پیام دوم مربوط به تبادل کلید از طرف سرور است. پیام سوم در صورتی که سرور مخفی نباشد ممکن است از سرور به کلاینت ارسال می‌شود. پیام چهارم که حتماً باید ارسال شود پارامتری ندارد و بیان‌کننده پایان ارسال پیام مرحله دوم است.

مرحله ۳: احرازاصالت و تبادل کلید کلاینت

در این مرحله ۳ پیام از کلاینت به سرور ارسال می‌شودکه فقط یکی از آن‌ها اجباری است.

مرحله ۴: پایان

در این مرحله طرفین با ارسال مشخصات رمزکننده وضعیت جدید رمز خود را اطلاع می‌دهند و سپس با ارسال پیام پایانی، پروتکل دست دادن را پایان می‌دهند.

امنیت

برای بهره‌مندی از این پروتکل، سرویس‌دهنده و سرویس‌گیرنده با یکدیگر یک قرارداد تبادلی اطلاعات را مذاکره می‌کنند. در این مذاکرات، سرویس‌دهنده و سرویس‌گیرنده بر سر پارامترهای مختلفی که برای برقراری امنیت مورد نیاز است، به توافق می‌رسند.

منابع

- وبوپدیا (http://www.webopedia.com/TERM/S/SSL.html)
- نسخه انگلیسی همین موضوع در ویکی‌پدیا
- ابزار بررسی تنظیمات اس اس ال (https://www.ssllabs.ir/)

آخرین ویرایش ۵ ماه پیش توسط Mahdy Saffar انجام شده

ویکی‌پدیا