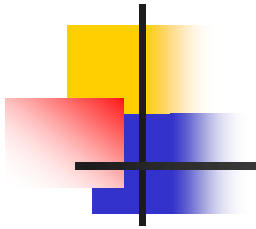
امنیت شبکه

جلسه ششم: امنیت لایه - انتقال

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393



فهرست:

- امنیت وب
- SSL
- TLS
- HTTPS
- SSH

امنیت وب

ویژگی‌های زیر از وبسایتها نیاز به ابزار امنیتی مناسب را نشان می‌دهد:

* اگرچه مرورگرهای وب برای استفاده بسیار آسان هستند، و سرویس‌دهنده‌های وب نیز نسبتا برای پیکربندی و مدیریت آسان بوده و طراحی محتوای وب سایت بطور فزاینده‌ای آسان شده است، ولی نرم-افزار زیر بنایی فوق‌العاده پیچیده است. این نرم‌افزار پیچیده ممکن است بسیاری از نفوذهای امنیتی بالقوه را مخفی نماید.

* یک سرویس‌دهنده وب می‌تواند به عنوان یک صفحه دسترسی به شرکت یا کل مجموعه کامپیوتری سازمان مورد سوء استفاده قرار گیرد.

* کاربران عادی و آموزش ندیده (در مسائل امنیتی) در اصل همانند مشتریان عادی برای خدمات مبتنی بر وب هستند.

تهدیدات امنیتی وب

اقدام متقابل	نتیجه	تهدیدات	
کنترل رمزنویسی	• گم شدن اطلاعات • خراب شدن ماشین • آسیب پذیري در برابر سایر تهدیدات	• دستکاری داده‌های کاربر • اسب تروجان • دستکاری حافظه • دستکاری جریان پیام درحال انتقال	یکپارچگی
رمزنگاری	• از دست رفتن اطلاعات • از دست رفتن محرمانگی پیام	• استراق سمع در شبکه • دزدی اطلاعات از سرویس‌دهنده • دزدی داده‌ها از شبکه • اطلاعات تنظیمات شبکه • اطلاعات در مورد مشتری که با سرویس‌دهنده صحبت می‌کند	قابلیت اعتماد
پیشگیری از مشکل	• درهم گسیختگی • جلوگیری از انجام کار کاربران	• ازکارانداختن ماشین با درخواستهای جعلی • پرکردن دیسک یا حافظه • مجزا کردن ماشین بوسیله حمله DNS	محرومیت از خدمات
تکنیک‌های رمزنگاری	• جعل هویت کاربران • باور درست بودن اطلاعات غلط	• جعل‌هویت کاربران مجاز • جعل داده	اعتبار سنجی

تهدیدات امنیتی وب

یکی از راه‌ها برای گروه‌بندی این تهدیدات دسته‌بندی از نظر حملات فعال و غیرفعال است.

حملات غیرفعال یا منفعل عبارتند از: استراق سمع ترافیک شبکه بین مرورگر و سرویس‌دهنده و دسترسی به اطلاعاتی که می‌بایست محدود شوند. در حالی که حملات فعال شامل جعل هویت یک کاربر دیگر، تغییر پیام‌ها در انتقال بین سرویس‌گیرنده و سرویس‌دهنده، و همچنین تغییر اطلاعات بر روی وب سایت است.

راه دیگر برای طبقه‌بندی، بررسی تهدیدات امنیتی وب سایت از دیدگاه محل تهدید است:

سرویس‌دهنده وب، مرورگر وب، و ترافیک شبکه بین مرورگر و سرویس‌دهنده.

مسائل مربوط به سرویس‌دهنده و امنیت مرورگر به مقوله امنیت سیستم کامپیوتری برمی‌گردد و در جلسات بعدی به آنها خواهیم پرداخت ولی مسائل مربوط به ترافیک امنیتی به گروه امنیت شبکه تعلق داشته و در این فصل به آنها پرداخته شده است.

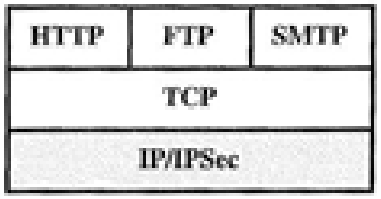
رویکردهای امنیتی ترافیک وب

یکی از راه های تامین امنیت وب در اصل استفاده از امنیت IP یا همان IPsec است (تصویر الف صفحه بعد). مزیت اصلی استفاده از IPsec در این است که برای کاربران پایانی و برنامه‌های کاربردی شفاف بوده و یک راه حل همه منظوره را فراهم می‌نماید. علاوه بر این، IPsec شامل توانایی فیلترکردن به طوری است که تنها ترافیک انتخاب شده نیاز خواهد داشت که سربار پردازش IPsec را متحمل شود.

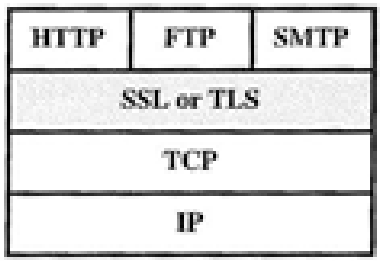
یکی دیگر از راه حلهای نسبتا همه منظوره برای امنیت در اصل پیاده‌سازی آن در لایه‌های بالایی TCP است (تصویر ب صفحه بعد). مهمترین مثال از این رویکرد همان لایه سوکت امن یا SSL و در ادامه استاندارد اینترنتی است که بنام امنیت لایه انتقال یا TLS شناخته می‌شود.

سرویسهای امنیتی مخصوص برنامه های کاربردی در خود برنامه‌های کاربردی خاص تعبیه شده‌اند (تصویر پ صفحه بعد). مزیت این روش این است که این سرویس را می‌توان متناسب با نیازهای خاص مرتبط با یک برنامه خاص، طراحی نمود.

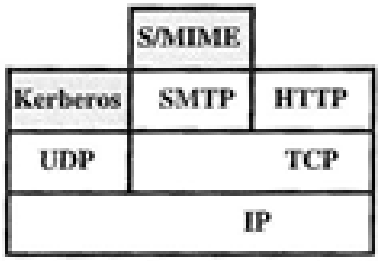
محل استقرار امکانات امنیتی در پشته پروتکل TCP/IP



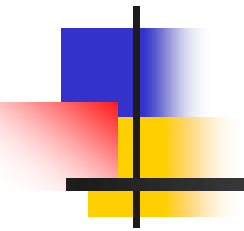
الف: سطح شبکه



ب: سطح انتقال



ب: سطح کاربردی



SSL

لایه سوکت امن SSL

یکی از سرویس‌های امنیتی که امروزه به طور گسترده استفاده می‌شود، همان لایه سوکتهای امن یا SSLاست و بعد از آن استاندارد اینترنتی که تحت عنوان امنیت لایه انتقال TLSشناخته شده است، که به تازگی در سند RFC 5246تعریف شده است.

در اصل SSL یک سرویس همه منظوره‌ای است که به عنوان مجموعه‌ای از پروتکل-هایی که بر TCP/IP تکیه دارند، پیاده‌سازی شده است.

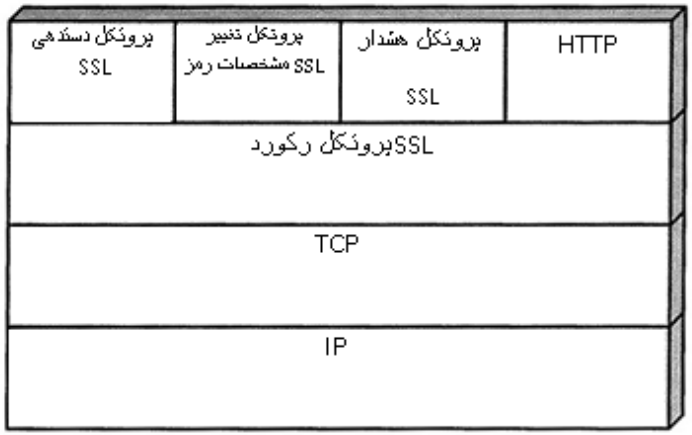
در این سطح، دو انتخاب برای پیاده سازی وجود دارد:

برای عمومیت کامل، SSL (یا TLS) می‌تواند به عنوان بخشی از مجموعه پروتکل زیر بنایی ارائه شود و در نتیجه برای برنامه‌های کاربردی فراگیر گردد.

همچنین SSL می‌تواند در بسته‌بندی‌های خاص نیز تعبیه شود، به عنوان مثال، امروزه اکثر مرورگرها به SSL مجهز شده‌اند و بسیاری از سرویس‌دهنده‌های وب نیز این پروتکل را اجرا کرده‌اند.

معماری SSL

در اصل SSLطوری طراحی شده تا از TCP استفاده نموده و بتواند خدمات قابل اعتماد امن انتها - به - انتها را فراهم نماید. یعنی SSL یک پروتکل واحد نبوده و نسبتا به دو لایه از پروتکلها همانطور که در تصویر زیرنشان داده شده است، تمایل دارد. سه پروتکل لایه بالاتر بنامهای "پروتکل دستدهی"، "پروتکل تغییر تنظیمات رمز"، و "پروتکل هشدار"، به عنوان بخشی از SSL تعریف شده‌اند که در مدیریت مبادلات SSL استفاده می‌شوند.



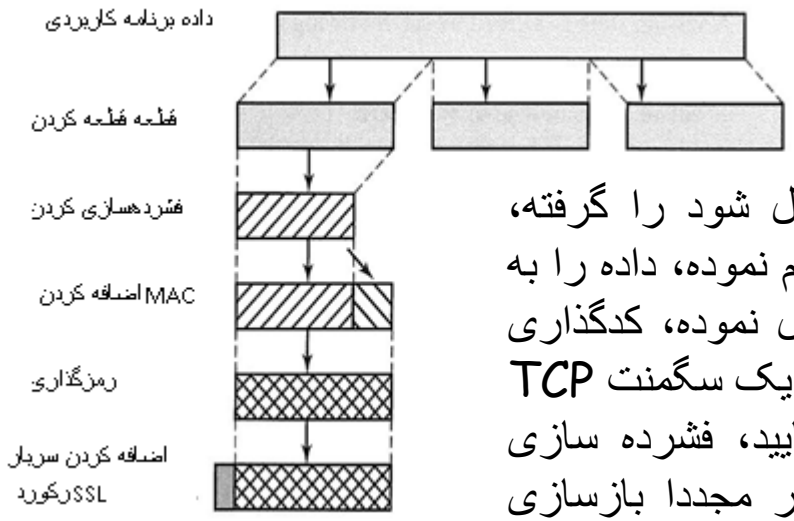
نشست و اتصال در SSL

دو مفهوم مهم در SSL همان نشست SSL و اتصال SSL هستند که مشخصاتشان به شرح زیر تعریف شده است:

* **اتصال**: یک اتصال یک نوع انتقالی (در تعریف مدل لایه بندیOSI) است که خدمات مناسبی را فراهم می‌کند. برای SSL، اتصالها بصورت نظیر - به - نظیر و گذرا هستند و هر اتصال با یک نشست در ارتباط است.

* **نشست**: نشست SSL یک ارتباط بین یک مشتری و یک سرویس‌دهنده است. نشست‌ها یا جلسه‌ها با پروتکل دست دادن بوجود می‌آیند. در اصل جلسات یا نشستها مجموعه‌ای از پارامترهای امنیتی رمزنگاری را تعریف می‌کنند که می‌توانند در میان اتصالات متعدد به اشتراک گذاشته شوند و این جلسات برای جلوگیری از مذاکرات پرهزینه در مورد پارامترهای امنیتی جدید برای هر اتصال استفاده می‌شوند.

معماری SSL



پروتکل ثبت یک پیام نرم‌افزاری که باید منتقل شود را گرفته، قطعات داده‌ها را به بلوک‌های قابل مدیریت تقسیم نموده، داده را به صورت اختیاری فشرده کرده، MAC را اعمال نموده، کدگذاری کرده، سربار را افزوده، و مقدار نتیجه را درون یک سگمنت TCP انتقال می‌دهد. داده‌های دریافتی رمزگشایی، تایید، فشرده سازی شده، و پیش از تحویل به کاربران سطح بالاتر مجددا بازسازی می‌شوند.

معماری SSL

گام اول تقسیم کردن به قطعات کوچکتر است. هر پیام لایه - فوقانی به بلوکهای 2^{14} بایتی (16384 بایت) و یا کمتر تقسیم می‌شود.

سپس، فشرده‌سازی به صورت اختیاری استفاده می‌گردد. فشرده‌سازی می‌بایست بدون اتلاف بوده و نباید طول محتوا را به بیش از 1024بایت افزایش دهد. در SSLv3 (و همچنین نسخه فعلی از TLS)، هیچ الگوریتم فشرده‌سازی مشخص نشده است، به طوری که الگوریتم فشرده سازی پیش فرض صفر است.

یکی از نقاط قوت فشرده سازی این است که داده‌ها را به جای اینکه بسط داده و تفسیر نماید، کوچک می‌کند.

گام بعدی در پردازش، محاسبه یک کد تأیید هویت پیام برای داده‌های فشرده است. برای این منظور، یک کلید مخفی مشترک استفاده می‌شود. محاسبه به صورت زیر تعریف می‌گردد:

$$hash(MAC\_Write\_Secret \| Pad\_2 \| hash(MAC\_Write\_Secret \| pad\_1 \| seq\_num \| SSLCompressed.type.lenght \| SSLCompressed.fragment))$$

معماری SSL

پیام فشرده شده بعلاوه MAC با استفاده از رمزگذاری متقارن به رمز درمی‌آیند. رمزنگاری ممکن نیست طول متن را به بیش از 1024 بیت افزایش دهد، بنابراین طول کلی ممکن نیست که از $2^{14}+2048$ تجاوز نماید. الگوریتم‌های رمزنگاری زیر مجاز هستند:

الگوریتم	سایز کلید
AES	128,256
IDEA	128
RC2-40	40
DES-40	40
DES	56
3DES	168
Fortezza	80
RC4-40	40
RC4-128	128

توجه‌کنید که MAC پیش از اینکه رمزنگاری رخ دهد محاسبه می-شود و بعد از آن MAC بهمراه متن ساده یا متن فشرده شده رمزنگاری خواهد شد. طول بلوکها ثابت هستند (لایه گذاری).

مثال لایه گذاری در این مرحله:

داده برابر 58 بایت

MAC برابر 20 بایت

حاصل 79 بایت؟

لایه گذاری ؟

معماری SSL

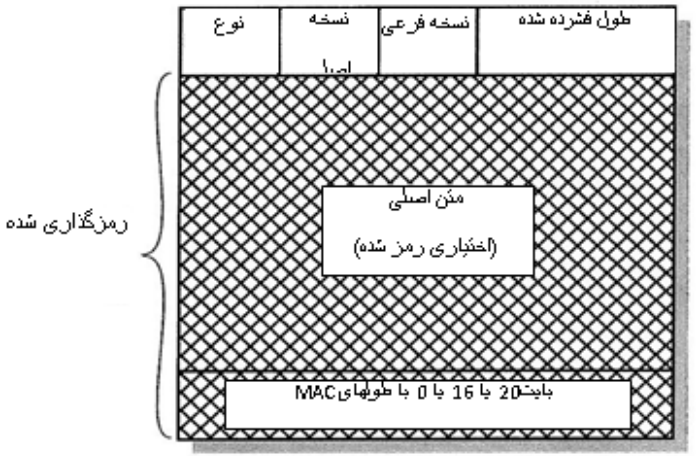
مرحله آخر پردازش پروتکل ثبت SSL همان آماده‌سازی یک سربار شامل فیلدهای زیر خواهد بود:

* **نوع محتوی** (8 بایت): پروتکل لایه بالاتر برای پردازش قطعه ضمیمه شده استفاده می‌نماید.

* **نسخه اصلی** (8 بایت): نسخه اصلی مورد استفاده در SSL را نشان می‌دهد. برای SSLv3، مقدار برابر 3 است.

* **نسخه فرعی**(8 بایت): نسخه فرعی مورد استفاده را نشان می‌دهد. برای SSLv3، مقدار برابر 0 است.

* **طول فشرده شده** (16 بیت): طول قطعه متن ساده را به بایت نمایش می‌دهد (یا قطعه فشرده شده اگر فشرده‌سازی استفاده شود). بیشترین مقدار $2^{14}+2048$ است.



مراحل ایجاد ارتباط SSL (دست دادن)

فاز اول

انتشار امکانات امنیتی: این مرحله برای مقدار-دهی اولیه یک ارتباط منطقی و برای انتشار امکانات امنیتی که به آن مرتبط است، استفاده خواهد شد.

فاز دوم

احراز هویت سرویس‌دهنده و تبادل کلید

سرویس‌دهنده اگر بخواهد احراز هویت شود، این مرحله را با ارسال گواهینامه خود آغاز می‌کند؛ پیام شامل یک یا زنجیره‌ای از گواهینامه‌های X.509 است.

فاز سوم

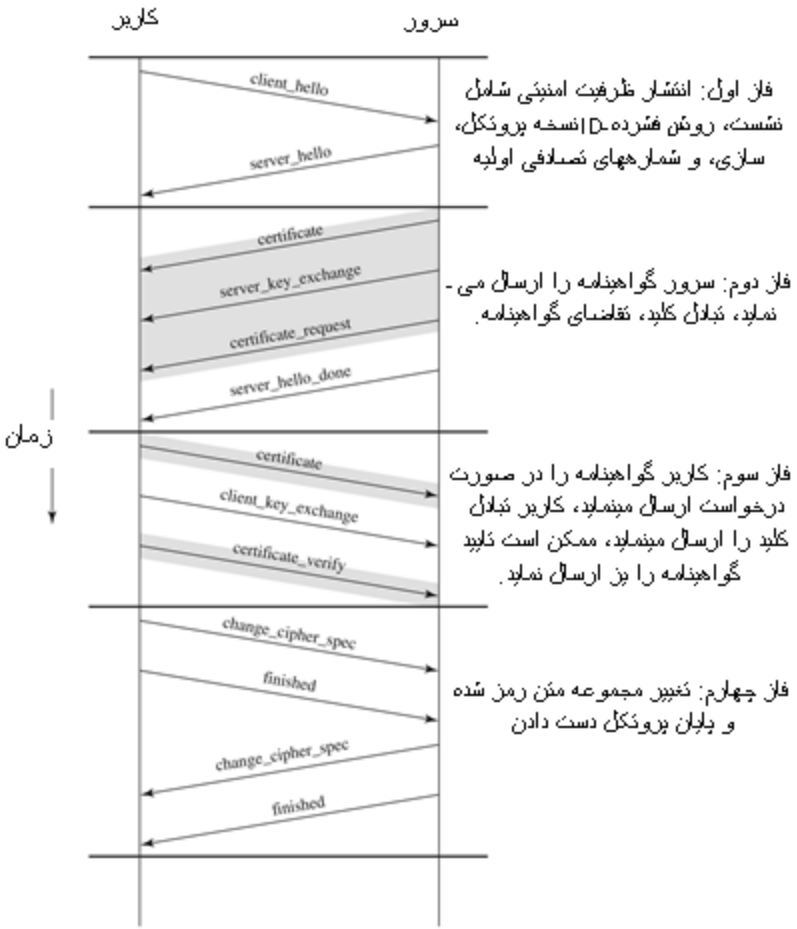
احراز هویت مشتری و مبادله کلید: بعد از دریافت پیام server_done، مشتری باید تایید نماید که سرویس‌دهنده یک گواهینامه معتبر (در صورتی که نیاز باشد) ایجاد کرده است و بررسی نماید که پارامترهای server_hello قابل قبول هستند.

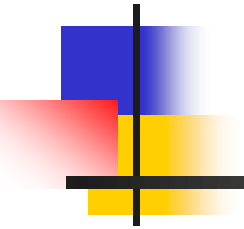
فاز چهارم

پایان: این مرحله تنظیمات یک اتصال امن را تکمیل می‌کند. مشتری یک پیام تغییر نتظیمات رمز (change_cipher_spec) را می‌فرستد و مقدار خصوصیات رمز معلق را در خصوصیات رمز فعلی کپی می‌کند.

توجه: این پیام به عنوان بخشی از پروتکل دست‌دادن در نظر گرفته نمی شود اما با استفاده از این پروتکل تغییر خصوصیات رمز فرستاده می‌شود.

مراحل ایجاد ارتباط SSL



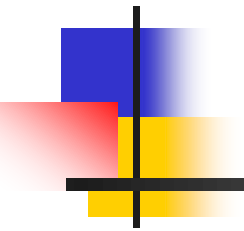


TLS

امنیت لایه انتقال TLS

در اصل TLS هدفش تولید یک نسخه استاندارد از SSL بوده و در واقع به عنوان استاندارد اینترنتی در RFC 5246 تعریف شده است که بسیار شبیه به sslv3 است ولی چندین تفاوت دارد:

- قالب رکورد TLS همانند قالب رکورد SSL است و فیلدهای سربار نیز مفهوم مشابه دارند. در نسخه فعلی TLS، شماره نسخه اصلی سه و شماره نسخه فرعی نیز سه است.
- کد احراز هویت: TLS از الگوریتم HMAC همانند ssl3 استفاده میکند با دو تفاوت : یکی الگوریتم واقعی و دیگری دامنه محاسبات MAC
- TLS از تابع شبه تصادفی که از آن به عنوان PRF یاد می‌شود، استفاده می‌کند
- تولید کدهای هشداردهنده همانند SSLv3 به استثناء no_certificate و کدهای هشداردهنده اضافی مانند Record_Overflow، Unkown_ca، Access_Denied ، ...
- تفاوتهای کوچک بسیاری بین مجوعه رمز موجود تحت SSLv3 و TLS وجود دارد:
  - تبادل کلید: همه تکنیکهای مبادله کلید SSLv3 بغیر از Fortezza
  - الگوریتم رمزنگاری متقارن: همه الگوریتم‌های رمزنگاری SSLv3 به استثنای Fortezza
- همه گواهینامه های ssl3 به غیر از rsa_empheral_dh، dss_empheral_dh و fortezza_kea
- محاسبات درهم سازی پایانی نیز کمی متفاوت است
- محاسبات رمزنگاری نیز کمی متفاوت است
- در SSL، لایه‌گذاری پیش از رمزنگاری داده‌های کاربر حداقل مقدار مورد نیاز است، ولی درTLS، می‌تواند هر مقداری باشد (مثال مشابه برای داده و MAC به حجم 79 بایت طول لایه‌گذاری می‌تواند 1، 9، 17 و مقادیر مشابه تا نهایت 249 باشد.)



HTTPS

پروتکل HTTPS

در اصل HTTPSیا همان پروتکل HTTP بر روی SSL به ترکیبی از HTTP و SSL اشاره می‌کند تا بتواند ارتباط امنی بین مرورگر وب و سرویس‌دهنده وب را برقرار نماید.

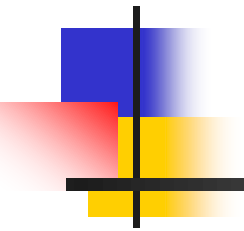
تفاوت عمده دیده شده توسط کاربر مرورگر وب، مربوط به URL یا آدرسی است (مکان جهانی منابع) که با https:// به جای http:// آغاز می‌شود.

ارتباطات معمولیHTTP از گذرگاه شماره 80 استفاده می‌کنند. اگر https تعیین شود آنگاه گذرگاه شماره 443 استفاده خواهد شد که در اصل SSL را فراخوانی خواهد نمود.

اجزاء زیر در HTTPS رمزگذاری میشوند:

* آدرس url مدارک خواسته شده
* محتوی سند
* محتوی فرمهای مرورگر (که توسط کاربر مرورگر پر شده است)
* کوکی‌هایی که از مرورگر به سرویس‌دهنده و از سرویس‌دهنده به مرورگر فرستاده می‌شوند
* محتوی سربار HTTP

برای HTTPS، عاملی که به عنوان مشتری HTTPعمل می‌کند به عنوان مشتری TLSنیز عمل می‌کند. یعنی مشتری آغاز به برقراری ارتباط با سرویس‌دهنده از طریق گذرگاه مناسب می‌کند و سپس TLC سعی می‌کند ClientHello را بفرستد تا عملیات دست‌دادن TLS آغاز گردد.



SSH

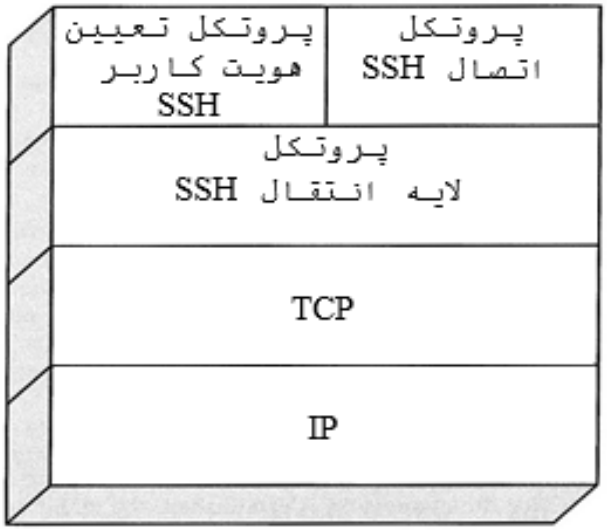
پروتکل SSH یا پوسته امن

پروتکلی است که برای ارتباطات امن شبکه‌ای طراحی شده است که پیاده سازی نسبتا ساده و ارزانی نیز دارد.

نسخه اولیه آن، SSH1 بر روی ایجاد امکانات اتصال از راه دور تمرکز کرده تا بتواند جایگزین TELNET و سایر الگوهای اتصال از راه دوری شود که امنیتی را ایجاد نمی‌کردند.

البته SSH توانایی‌های همه منظوره مشتری/ سرویس‌دهنده بیشتری را نیز فراهم نموده و همچنین می‌تواند برای توابع شبکه‌ای مانند انتقال فایل و پست الکترونیکی نیز استفاده شود.

نسخه جدید، یعنی SSH2، تعدادی از عیوب و اشکالات نسخه اصلی را رفع کرده است.



در اصل SSH تحت عنوان سه پروتکل سازماندهی شده‌ای است که معمولا در لایه‌های بالای TCP اجرا می‌شوند:

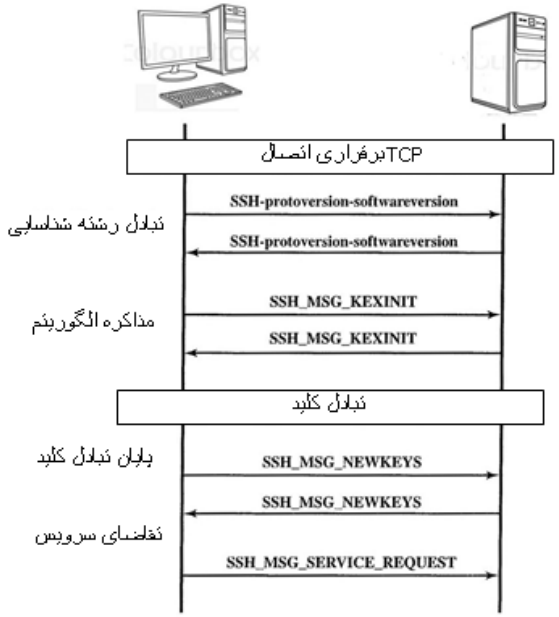
* **پروتکل لایه انتقال:** احراز هویت سرویس‌دهنده، محرمانه ماندن داده‌ها، و یکپارچگی داده‌ها را با ارسال پیام رمز میسر می‌سازد. لایه انتقال ممکن است بطور اختیاری فشرده سازی را نیز امکان پذیر نماید.

* **پروتکل احراز هویت کاربر**: کاربر را برای سرویس‌دهنده، احراز هویت می‌کند.

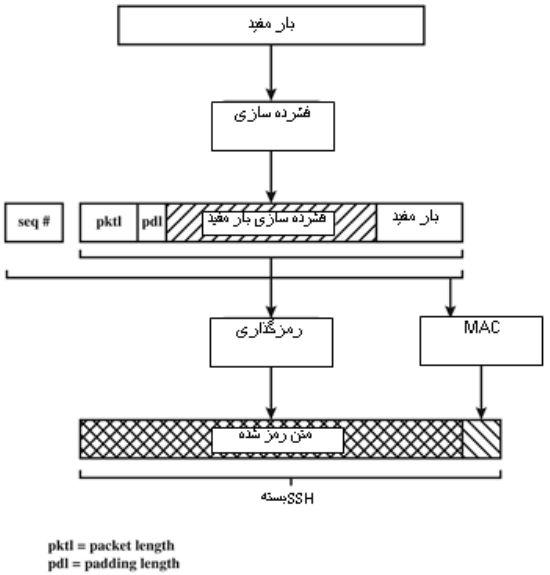
* **پروتکل اتصال**: کانالهای ارتباطی چندگانه منطقی را بر روی یک اتصال SSHزیربنایی واحد تقسیم می‌نماید.

پروتکل لایه انتقال در SSH

کلیدهای میزبان: احراز هویت سرویس‌دهنده، بسته به اینکه سرویس‌دهنده یک جفت کلید خصوصی/ عمومی را دارا باشد، در لایه انتقال اتفاق می‌افتد.



مبادله بسته‌ها: در اینجا ابتدا، مشتری ارتباط TCP را با سرویس-دهنده برقرار می‌سازد. این امر از طریق پروتکل TCP انجام شده و قسمتی از پروتکل لایه انتقال است. هنگامی که ارتباط برقرار می‌شود، با مراجعه به بسته‌ها در فیلد داده یک سگمنت TCP ، مشتری و سرویس‌دهنده داده‌ها را با یکدیگر مبادله خواهند نمود. (تصویر روبرو)



-> مراحل شکل‌گیری بسته اطلاعاتی پروتکل لایه انتقال SSH

پروتکل احراز هویت کاربر در SSH

پروتکل احراز هویت کاربر

پروتکل احراز هویت کاربر این مفهوم را ارائه می‌دهد که کدام مشتری برای سرویس‌دهنده احراز هویت شده است. سرویس‌دهنده ممکن است به یک یا چند روش احراز هویت زیر احتیاج داشته باشد:

* **کلیدعمومی**: جزییات این روش به الگوریتم کلید عمومی انتخاب شده بستگی دارد. در واقع، مشتری یک پیام به سرویس‌دهنده می‌فرستد که شامل کلید عمومی مشتری، به همراه پیامی است که با کلید خصوصی مشتری امضا شده است. زمانی که سرویس‌دهنده این پیام را دریافت می‌نماید، بررسی می‌کند که آیا کلید عرضه شده برای احراز هویت قابل قبول است یا خیر و در صورت درست بودن جواب، آنگاه بررسی می‌نماید که آیا امضاء آن نیز صحیح است یا خیر.

رمزعبور: مشتری یک پیام که شامل رمزعبور بدون رمزگذاری و بصورت متن ساده بوده و توسط رمزنگاری با پروتکل لایه انتقال حمایت خواهد شد، را ارسال می‌نماید.

* **مبتنی بر میزبان**: احراز هویت بر روی دستگاه میزبان مشتری اجرا می‌شود به جای اینکه بر روی خود مشتری اجرا شود. بنابراین، میزبانی که از مشتریهای مختلفی حمایت می‌کند باید برای همه مشتریهایش احراز هویت را مهیا نماید.

پروتکل ارتباط در SSH

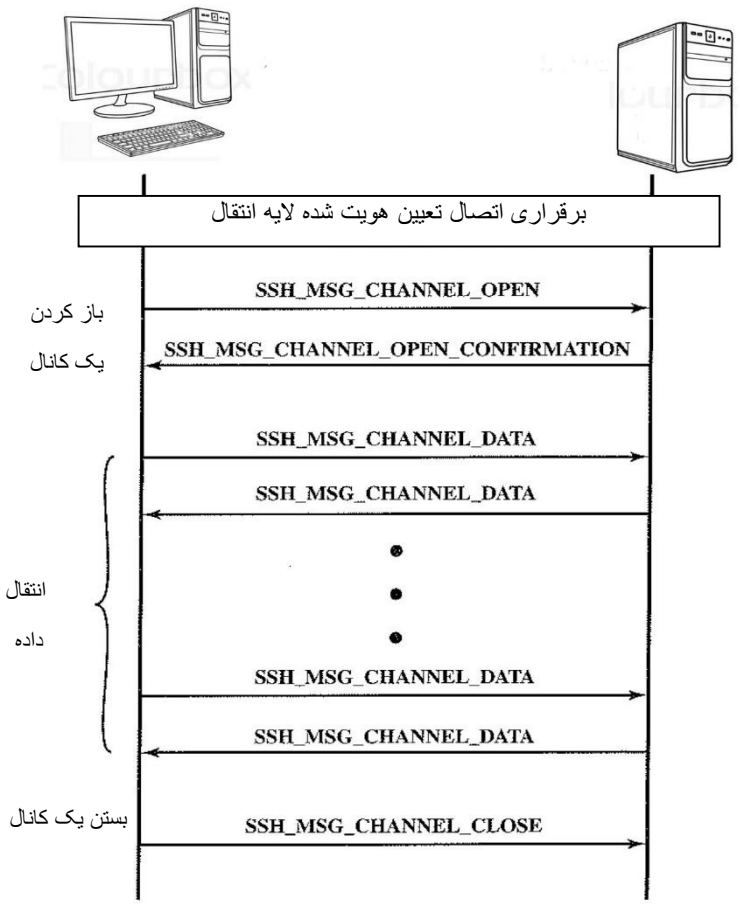
پروتکل ارتباط SSH در بالای پروتکل لایه انتقال اجرا می‌شود و فرض می‌کند که از یک ارتباط احراز هویت امن استفاده می‌کند. این اتصال احراز هویت امن، که از آن به عنوان تونل یا tunnel نیز یاد می-شود، بوسیله پروتکل اتصال برای تسهیم تعدادی از کانالهای منطقی استفاده می‌شود.

مکانیزم کانال: همه انواع ارتباطات که از SSH استفاده می‌کنند، همانند یک نشست ترمینال، با استفاده از کانالهای متفاوت پشتیبانی می‌شوند. هر طرف در این ارتباط ممکن است یک کانال را بازنماید. برای هر کانال، هر طرف به یک شماره کانال منحصر بفرد مرتبط است، که لازم نیست این شماره کانالها در هر دو انتها مشابه باشند.

نوع کانال: چهار نوع کانال در مشخصات پروتکل اتصال SSH در نظر گرفته شده است: نشست یا Session، x11، Forwarded_Tcpip ، Direct_tcpip

ارسال گذرگاه: یکی از مهمترین خصیصه‌های کاربردی SSH ارسال گذرگاه است. در واقع، ارسال گذرگاه امکان تبدیل هرگونه ارتباط غیر امن TCP را به یک ارتباط امن SSH بوجود می‌آورد. از این امر همچنین با عنوان تونل SSH یا SSH Tunnling نیز یاد می‌شود. (مثال، برای پروتکل ساده انتقال پست الکترونیکی یا SMTP، طرف سرویس‌دهنده معمولا به گذرگاه شماره 25 گوش می‌دهد. لذا TCP متوجه خواهد شد که این آدرس سرویس‌دهنده SMTPاست و داده‌ها را به برنامه سرویس‌دهنده SMTP خواهد فرستاد.)

تبادل پیام پروتکل ارتباط در SSH



در اینجا یک برنامه کاربردی مشتری داریم که بوسیله شماره گذرگاه X تشخیص داده می‌شود و یک برنامه کاربردی مربوط به سرویس‌دهنده داریم که با شماره گذرگاه yمشخص می‌شود. موجودیت TCP محلی با موجودیت TCPمتحرک در یک اتصال TCP مذاکره می‌نماید، و بدین ترتیب گذرگاه محلی x را به گذرگاه متحرک y مرتبط می‌سازد.

برای ایمن نمودن این اتصال، تنظیمات SSH تنظیم خواهند شد، لذا پروتکل لایه انتقال SSH یک اتصال TCP بین مشتری و موجودیت‌های سرویس‌دهنده با شماره-های گذرگاههای TCP بترتیب a و b ایجاد می‌نماید. لذا یک تونل SSHامن روی این اتصال TCP ساخته می-شود. ترافیک از مشتری در گذرگاه x به موجودیت محلی SSH راهنمایی می‌شود و از طریق تونل به جایی که موجودیت SSH داده‌ها را به برنامه سرویس‌دهنده روی گذرگاه y ارسال می‌نماید، فرستاده می‌شود. ترافیک در جهت دیگر نیز به طور مشابهی عمل هدایت داده‌ها را انجام می‌دهد. در اصل SSH دو نوع ارسال گذرگاه را پشتیبانی می‌نماید: ارسال محلی و ارسال از راه دور.

ارسال محلی در SSH

مثال: فرض کنید که شما یک برنامه پست الکترونیکی برای کاربران بر روی کامپیوتر شخصی خود دارید و از آن برای دریافت پست الکترونیکی از سرویس-دهنده پست الکترونیکی خود براساس پروتکل POP استفاده می‌نمایید. شماره گذرگاهی که به POP3اختصاص داده شده است برابر 110خواهد بود. حال می‌توانیم ترافیک را به روش زیر ایمن سازیم:

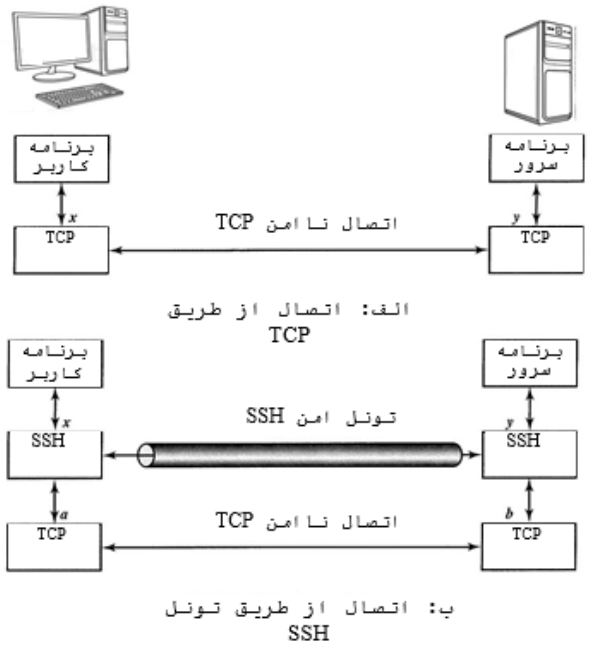
1. مشتری SSHیک اتصال با سرویس‌دهنده متحرک راه دور برقرار می‌سازد

2. یک شماره گذرگاه استفاده نشده محلی مانند 9999را انتخاب نموده و تنظیمات SSH را تنظیم می‌نماید تا ترافیک ارسالی از سرویس‌دهنده به گذرگاه 110 را روی این گذرگاه دریافت نماید.

3. مشتری SSHبه سرویس‌دهنده SSHاطلاع می‌دهد تا یک اتصال با مقصد، در این مورد گذرگاه 110 سرویس‌دهنده پست الکترونیکی ایجاد نماید.

4. مشتری کلیه بیتهای ارسالی به گذرگاه محلی 9999را دریافت نموده و آنها را به سرویس‌دهنده با نشست رمزگذاری شده SSH ارسال می‌نماید. سرویس-دهنده SSH بیتهای ورودی را رمزگذاری نموده و متن رمزگشایی شده را به گذرگاه 110 ارسال می‌نماید.

5. در طرف دیگر، سرویس‌دهنده SSHکلیه بیتهای رسیده به گذرگاه 110 را گرفته و از داخل نشست SSH به مشتری برمی‌گرداند که مشتری آن را رمزگشایی نموده و آنها را به پردازش متصل به گذرگاه 9999 ارسال می‌نماید.



ارسال راه دور در SSH

با ارسال از راه دور، برنامه SSH مشتری به جای سرویس‌دهنده عمل می‌کند. مشتری ترافیک را با یک شماره گذرگاه داده شده دریافت می‌نماید، ترافیک را روی گذرگاه درست قرار داده و به مقصدی که کاربر انتخاب نموده است، ارسال می‌نماید. بعنوان آخرین نمونه نیز یک نمونه بارز از اتصال راه دور در اینجا آورده شده است.

فرض کنید شما می‌خواهید به سرویس‌دهنده خود در محل کارتان از کامپیوتر شخصی خود در خانه دسترسی پیدا کنید. از آنجایی که سرویس‌دهنده کاری در پشت دیوار آتش قرار دارد، لذا یک درخواست SSH از کامپیوتر خانگی شما مورد قبول نخواهد بود. با این حال، شما می‌توانید یک تونل SSH با استفاده از ارسال از راه دور ایجاد نمایید. گامهای زیر در این کار مشارکت خواهند داشت:

1. از طریق کامپیوتر محل کار، یک اتصال SSH به کامپیوتر خانه ایجاد نمایید. دیوارآتش ازآنجایی که این اتصال محافظت شده خارجی است، اجازه را صادر خواهد نمود.

2. سرویس‌دهنده SSHرا برای گوش دادن به یک گذرگاه محلی، بعنوان مثال 22، تنظیم نموده بطوری که داده-ها را بر پایه یک اتصال SSH به گذرگاه راه‌دور، بعنوان مثال 2222، ارسال نماید.

3. حال می‌توانید به کامپیوتر خانگی خود مراجعه نموده و SSHرا طوری تنظیم نمایید که ترافیک روی گذرگاه 2222 را بپذیرد.

4. اکنون یک تونل SSH دارید که می‌تواند برای اتصال از راه دور به سرویس‌دهنده محل کار خود از آن استفاده نمایید.

سوالات مرتبط

1. چه پروتکلهایی دارای SSL هستند؟
2. تفاوت بین یک اتصال SSL و یک جلسه SSLچیست؟
3. پارامترهایی که حالت یک جلسه SSL رو تعریف می‌کنند را نام برده و مختصر شرح دهید.
4. پارامترهایی که یک اتصال SSL رو تعریف می‌کنند را نام برده و مختصر شرح دهید.
5. چه سرویسهایی توسط پروتکل ثبت SSL ارائه می‌شوند؟
6. چه مراحلی در انتقال پروتکل ثبت SSL تاثیرگذار هستند؟
7. هدف پروتکل HTTPS چیست؟
8. SSHچیست و در چه برنامه‌های کاربردی می‌توان از آن بهره‌مند شد؟
9. پروتکلهای SSH را نام برده و مختصری شرح دهید.

خلاصه: امنیت وب، SSL، TLS، TTPS، SSH

جلسه بعدی: امنیت شبکه های بی سیم

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

ترجمه: دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.