مقایسه و تحلیل SSL ۲.۰ و ۳.۰

خلاصه

پروتکل SSL یک امضای دیجیتال است که به طور گسترده ای برای احراز هویت و ایجاد ارتباط امن و رمزگذاری شده بین مشتری و سرور استفاده می شود. اگرچه SSL دارای برخی ایرادات جزئی است که به راحتی از طریق لایه سطحی آن و بدون تغییر کل پایه پروتکل قابل حل است، اما ثابت کرده است که SSL در ارتباط امن مشتری/ سرور بسیار کارآمد است، خود گوگل آن را به پروتکل HTTP خود اختصاص داده است.

این گواهینامه به دلیل تطبیق پذیری و راحتی آن بسیار مورد استفاده قرار می گیرد. تقریباً در هر مرورگری استفاده می شود و کاربر برای داشتن یک اتصال امن نیازی به وارد کردن رمز عبور و شناسه ندارد. در اینجا ما به طور مفصل جنبه های اصلی این فناوری را شرح می دهیم.

کلمات کلیدی: رمزگذاری شده، داده ها، احراز هویت، سرور، گواهی، وب

۱. مقدمه

گواهی SSL[1] به زبان ساده، ارتباط بین مشتری (که می توانید خودتان باشید) و سرور را ایمن نگه می دارد و مجرمان را از خواندن و به دست آوردن اطلاعات حساس مانند شماره کارت اعتباری در درگاه های پرداخت باز می دارد. به همین دلیل شرکت ها و سازمان ها گواهی آن را به وب سایت های خود اضافه می کنند تا این نوع اطلاعات را خصوصی نگه دارند.

علاوه بر این وجود اتصال SSL در وب سایت شما دارای مزایای دیگری مانند امکان افزایش رتبه در جستجوی ارگانیک گوگل و جلب اعتماد بازدیدکنندگان است.[kasp]

نه تنها وب سایت های تجاری، بلکه وب سایت های خصوصی نیز از SSL برای جلوگیری از کپی کردن وب سایت و ایجاد نسخه جعلی از مهاجمان استفاده می کنند. بدیهی است که برای هر دو دامنه رمزگذاری ترافیک آنها یکی از اولویت‌ها است.

HTTP[2] یک پروتکل کاربردی است که نحوه انتقال اطلاعات از طریق اینترنت را تعیین می کند. "S" در انتهای HTTP در وب سایت ها نشان می دهد که ارتباط با آن سایت امن و تاریخ امن است. بدون توجه به نوع مرورگر بدون این گواهی، هنگام ورود به وب سایت یک پیام هشدار دریافت خواهید کرد. این یک سیگنال واضح است که سایت امن نیست.[kin]

در این مقاله، در بخش ۲، نگاهی به تاریخچه مختصری از SSL، ایرادات و انواع مختلف SSL می اندازیم. پس از آن در بخش ۳ ما در مورد لایه های SSL بحث خواهیم کرد. سپس در بخش ۴ در مورد روش کار SSL و روش های رمزگذاری آن صحبت می کنیم. بعد در بخش ۵ ما حملات مختلف SSL را ارزیابی می کنیم.

در پایان، در بخش ۶، نتیجه می گیریم که این نسخه ۳.۰ از SSL یکی از موثرترین راه های ارتباط امن و رمزگذاری شده با توجه به نقاط قوت و ضعف آن است.

۲. پس زمینه

نسخه SSL 1.0 اولین بار در دهه ۱۹۹۰ توسعه یافت، اما به دلیل نقص های آن هرگز منتشر و استفاده نشد. بعداً SSL 2.0 در سال ۱۹۹۵ معرفی شد، اما هنوز دارای برخی نقص‌های امنیتی بود که منجر به طراحی مجدد SSL 3.0 می‌شود که امروزه استفاده می‌شود.[kin]

امروزه SSL با نام دیگری، TLS3 استفاده می شود. TLS بعد از SSL آمد، اما از SSL امن تر و به روزتر است. در واقع اکثر وب سایت هایی که ادعا می کنند دارای گواهینامه SSL هستند، در واقع دارای TLS هستند که بسیار امن تر از SSL است.

SSL دارای دو لایه است که هر لایه از سرویس هایی استفاده می کند که توسط سرویس های پایین تر ارائه می شود و خود عملکردی را برای لایه های بالایی ارائه می دهد که بسیار شبیه پروتکل TCP است. لایه رکورد طبقه بندی و احراز هویت را برای پروتکل حمل و نقل قابل اعتماد فراهم می کند.

لایه بالای لایه رکورد لایه SSL handshake است. این یک نوع پروتکل تبادل کلید است که رمزنگاری را در دو نقطه پایانی اولیه و هماهنگ می کند. وقتی کامل شد، داده‌های محرمانه یک n برنامه را می‌توان از طریق لایه رکورد ارسال کرد.[wag]

۲.۱ معایب SSL 2.0

هدف SSL 3.0 رفع ضعف امنیتی SSL 2.0 است که در اینجا به اختصار به آن اشاره خواهیم کرد. SSL 2.0 کلیدهای احراز هویت را تا ۴۰ بیت ضعیف می کند و در زیرساخت MAC بسیار ضعیف است، اگرچه ممکن است به نظر برسد که حملات را متوقف می کند.

در MAC SSL 2.0 بایت های padding را به بلوک های رمز تبدیل می کند، اما طول padding را آشکار می کند، که می تواند منجر به شناسایی بایت ها در انتهای پیام ها توسط مهاجمان شود.

همچنین هیچ حفاظتی برای پروتکل دست دادن ندارد و مهاجم در حمله میانی می تواند شناسایی نشود. انتظار دارد گواهی دامنه ثابت و خدمات واحد و با اکثر سرورهای وب میزبانی مجازی تداخل داشته باشد.[wag]

۲.۲ انواع گواهی SSL

انواع مختلفی از گواهی SSL بسته به داده ها و زمینه کاری وب سایت وجود دارد که به شرح زیر است:

۱. گواهینامه های اعتبار سنجی توسعه یافته (EV SSL)

۲. گواهینامه های معتبر سازمان (OV SSL)

۳. گواهینامه های معتبر دامنه (DV SSL)

۴. گواهی نامه های SSL

۵. گواهی SSL چند دامنه ای (MDC)

۶. گواهینامه های ارتباطات یکپارچه (UCC)

۲.۲.۱ گواهینامه های اعتبار سنجی توسعه یافته (EV SSL)

این بالاترین رتبه و گران ترین نوع گواهی SSL است. برای وب سایت هایی که داده ها را جمع آوری می کنند و شامل پرداخت های آنلاین یا به عبارت دیگر وب سایت های تجارت الکترونیک هستند استفاده می شود. پس از نصب، این گواهی قفل، HTTPS، نام کسب و کار و کشور را در نوار آدرس مرورگر نمایش می دهد. به تصویر کشیدن اطلاعات مالک وب سایت در نوار آدرس در بالا به تشخیص سایت از جعلی کمک می کند. گواهینامه EV SSL، حقوق انحصاری را برای دامنه مالکان فراهم می کند و باید توسط تأیید هویت استاندارد اجرا شود.[kasp]

۲.۲.۲ گواهینامه های معتبر سازمان (OV SSL)

این نسخه گواهی مشابه سطح گواهینامه EV SSL است. برای به دست آوردن یکی؛ مالک وب سایت باید برخی از فرآیندهای اعتبار سنجی را تکمیل کند. این نوع گواهی همچنین اطلاعات مالک وب سایت را در نوار آدرس نمایش می دهد تا از موارد مخرب متمایز شود. گواهینامه های OV SSL دومین گواهینامه گران قیمت (بعد از EV SSL) است و هدف اصلی آنها رمزگذاری داده های حساس کاربر در طول تراکنش ها است. تجاری یا وب‌سایت‌ها باید گواهی OV SSL را نصب کنند تا مطمئن شوند که هر گونه اطلاعات مشتری به اشتراک گذاشته شده، محرمانه باقی می‌ماند.[kasp]

۲.۲.۳ گواهینامه های معتبر دامنه (DV SSL)

فرآیند اعتبار سنجی برای به دست آوردن این نوع گواهی حداقل است، در نتیجه، گواهینامه های SSL اعتبار سنجی دامنه اطمینان کمتر و حداقل رمزگذاری را ارائه می دهند. آنها برای وبلاگ ها یا وب سایت های اطلاعاتی استفاده می شوند که شامل جمع آوری داده ها یا پرداخت های آنلاین نیست. این نوع یکی از کم هزینه ترین و سریعترین است. فرآیند اعتبار سنجی فقط به صاحبان وب سایت نیاز دارد که مالکیت دامنه را با پاسخ به ایمیل یا تماس تلفنی اثبات کنند. نوار آدرس مرورگر فقط HTTPS و یک قفل بدون نام تجاری را نشان می‌دهد.[kasp]

۲.۲.۴ گواهینامه های SSL Wildcard

گواهی نامه Wildcard SSL به شما امکان می دهد یک دامنه پایه و دامنه های فرعی نامحدود را در یک گواهی واحد ایمن کنید. گواهینامه های SSL دارای علامت * به عنوان بخشی از نام مشترک هستند، که در آن ستاره نشان دهنده هر زیر دامنه معتبری است که دامنه پایه یکسانی دارند.[kasp]

۲.۲.۵ گواهی SSL چند دامنه ای (MDC)

یک گواهی چند دامنه می تواند برای ایمن سازی بسیاری از دامنه ها و/یا نام های زیر دامنه استفاده شود. این شامل ترکیب دامنه ها و زیر دامنه های کاملا منحصر به فرد با TLD های مختلف (دامنه های سطح بالا) به جز دامنه های محلی/داخلی است.

گواهینامه های چند دامنه به طور پیش فرض از زیر دامنه ها پشتیبانی نمی کنند. اگر نیاز دارید که هر دو www.example.com و example.com را با یک گواهی چند دامنه ایمن کنید، پس هر دو نام میزبان باید هنگام دریافت گواهی مشخص شوند.[kasp]

۲.۲.۶ گواهی ارتباطات یکپارچه (UCC)

گواهی‌های ارتباطات یکپارچه (UCC) نیز گواهی‌های SSL چند دامنه‌ای در نظر گرفته می‌شوند. UCC ها در ابتدا برای ایمن سازی سرورهای Microsoft Exchange و Live Communications طراحی شدند. امروزه هر صاحب وب سایتی می تواند از این گواهی ها برای ایمن سازی دامنه های متعدد با یک گواهی استفاده کند. گواهینامه های UCC از نظر سازمانی معتبر هستند و یک قفل در مرورگر نمایش می دهند. UCC ها را می توان به عنوان گواهینامه های EV SSL استفاده کرد تا از طریق نوار آدرس سبز به بازدیدکنندگان وب سایت بالاترین اطمینان را بدهد.[kasp]

۲.۳ خلاصه

به طور خلاصه، پس از ترمیم بیشتر ایرادات، SSL راه‌های مختلفی برای حفاظت از داده‌ها در هر دو جنبه سطح امنیتی و هزینه‌ها ارائه کرده است که صاحبان سایت در انتخاب بین آن‌ها آزادند.

۳. لایه ها

۳.۱ لایه ضبط

این لایه در پایین پروتکل SSL قرار دارد و فرض می کند که پروتکل تبادل کلید به طور ایمن وضعیت جلسه و پارامترهای کلیدی را تنظیم کرده است. بلوک‌هایی از داده‌ها را بین کلاینت و سرور ارسال می‌کند و اگر پیام‌های متعددی به سرعت ارسال شوند، آن پیام‌ها به یک رکورد SSL تبدیل می‌شوند، یا در عوض به رکوردهای SSL کوچک‌تر تبدیل می‌شوند.[wag]

هر یک از این رکوردها بر اساس الگوریتم رمزگذاری فشرده و رمزگذاری می شوند. به عنوان مثال در MAC آنها با این فرمول محاسبه می شوند:

```
hash( MAC_write_secret + pad_2 +
     hash(MAC_write_secret + pad_1 + seq_num + length + content))
```

جایی که MAC_write_secret یک راز بین سرور و مشتری برای اطمینان از انتقال ایمن است.[ore]

۳.۲ لایه handshake

پروتکل Handshake برای ایجاد جلسات استفاده می شود. این پروتکل به مشتری و سرور اجازه می دهد تا با ارسال یک سری پیام به یکدیگر، یکدیگر را احراز هویت کنند. [intel]

روش برای SSL handshake

تماس: پیام مشتری از طریق مرورگر به سرور ارسال می شود. پیام حاوی اطلاعات حساسی مانند نسخه SSL مشتری، تنظیمات رمزگذاری و اطلاعات مربوط به جلسه است.

• پاسخ اولیه: به عنوان اولین پاسخ، سرور تأیید امنیتی را از طریق برخی گواهی ها، تنظیمات رمزگذاری سرور و داده های مربوط به جلسه ارسال می کند.

• احراز هویت: مرورگر گواهی امنیتی را تأیید می کند تا تأیید کند که با مرجع صحیح ارتباط برقرار کرده است.

• تبادل کلید: سرور و مرورگر کلیدها را مبادله می کنند و تبادل آنها را با امنیت تایید می کند.

• جمع بندی: هر دو طرف، که مرورگر و سرور هستند، تأیید می کنند که تبادل انجام شده است و کار اکنون کامل شده است.

۴ نحوه کار SSL و مفاهیم اساسی

هدف اصلی SSL این است که اطمینان حاصل شود که هر داده ای که بین کاربران و وب سایت ها یا بین دو سیستم منتقل می شود، خواندن غیرممکن باقی می ماند. از الگوریتم‌های رمزگذاری برای درهم‌کوبی داده‌ها در انتقال استفاده می‌کند، که مانع از خواندن آن‌ها هنگام ارسال از طریق اتصال توسط مهاجمان می‌شود.

فرآیند به این صورت عمل می کند:

۱. یک سرویس گیرنده تلاش می کند به یک وب سایت (به عنوان مثال، یک وب سرور) ایمن شده با گواهی SSL متصل شود.

۲. مرورگر یا سرور درخواست می کند که وب سرور خود را شناسایی کند.

۳. وب سرور در پاسخ یک کپی از گواهی SSL خود را برای مرورگر یا سرور ارسال می کند.

۴. مرورگر یا سرور بررسی می کند که آیا گواهی SSL تأیید شده است یا خیر. اگر این کار را کرد، آن را به وب سرور سیگنال می دهد.

۵. سپس وب سرور یک تأییدیه امضا شده دیجیتالی را برای شروع یک جلسه رمزگذاری شده SSL برمی گرداند.

۶. داده های رمزگذاری شده بین مرورگر یا سرور و وب سرور به اشتراک گذاشته می شود.

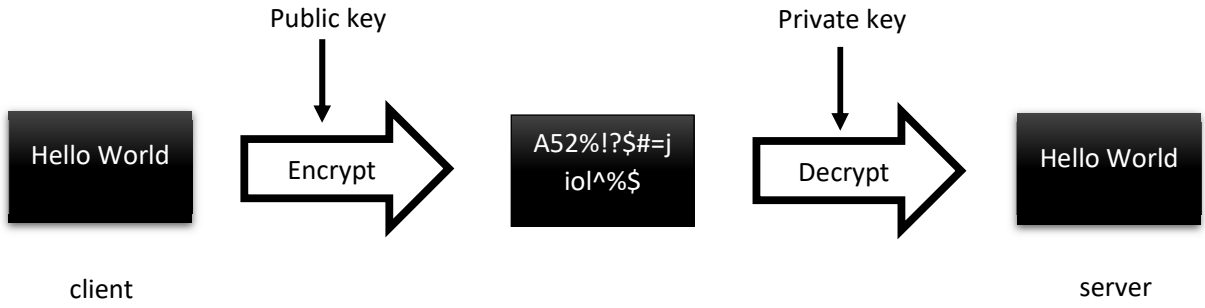
گواهی SSL از دو نوع الگوریتم برای رمزگذاری و انتقال داده ها استفاده می کند که عبارتند از رمزنگاری نامتقارن و رمزنگاری متقارن.[tut]

۴.۱ رمزنگاری نامتقارن

رمزنگاری نامتقارن (همچنین به عنوان رمزگذاری نامتقارن یا رمزنگاری کلید عمومی شناخته می شود) از یک جفت کلید مرتبط با ریاضی برای رمزگذاری و رمزگشایی داده ها استفاده می کند. در یک جفت کلید، یک کلید با هر کسی که به یک ارتباط علاقه مند است به اشتراک گذاشته می شود. این کلید عمومی نامیده می شود. کلید دیگر در جفت کلید مخفی نگه داشته می شود و کلید خصوصی نامیده می شود.

کلیدهای عمومی و خصوصی مرتبط با ریاضی هستند و با استفاده از الگوریتم های رمزنگاری که بر اساس مسائل ریاضی به نام توابع یک طرفه هستند ایجاد شده اند. از این کلیدها برای رمزگذاری یا رمزگشایی داده ها استفاده می شود.[tut]

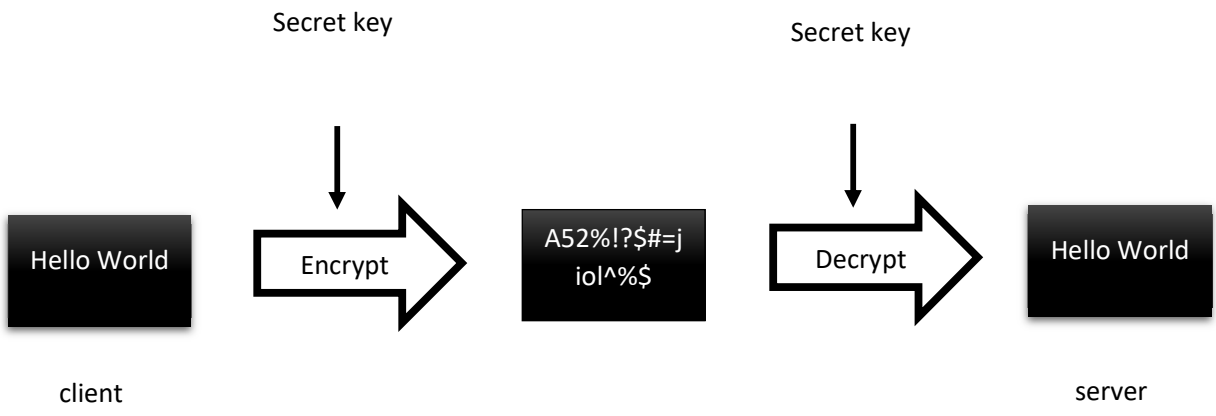
در رمزنگاری نامتقارن، فرستنده داده ها را با کلید عمومی گیرنده رمزگذاری کرده و به گیرنده ارسال می کند. گیرنده آن را با استفاده از کلید خصوصی مربوطه رمزگشایی می کند.



۴.۲ رمزنگاری متقارن

در رمزنگاری متقارن، تنها یک کلید وجود دارد که داده ها را رمزگذاری و رمزگشایی می کند. هر دو فرستنده و گیرنده باید این کلید را داشته باشند که فقط برای آنها شناخته شده است.

SSL از رمزنگاری متقارن با استفاده از کلید جلسه پس از انجام دست دادن اولیه استفاده می کند. پرکاربردترین الگوریتم های متقارن AES-128، AES-192 و AES-256 هستند.



۵. حمله SSL

درست است که SSL باید و کاملاً از داده های محرمانه در برابر حملات محافظت کند، و به نظر می رسد که رمزگذاری اساسی برای حفظ حریم خصوصی اطلاعات کافی است. با این حال مطالعات اخیر توسط IETF نشان داده است که به تنهایی کافی نیست و حملات گیج کننده برای ثبت لایه می تواند سیستم را نقض کند. برخی از این حملات عبارتند از: ۱- حملات Replay ۲-حملات Exhaustion Attacks – ۳-حملات Ciphersuite rollback.

۵.۱ تکرار حملات

این نوع حملات چندان نگران کننده نیستند زیرا به راحتی می توان از آنها محافظت کرد. SSL از داده ها در برابر این حملات با گنجاندن یک شماره دنباله در داده های MACed محافظت می کند. اطلاعات دوباره سفارش داده شده، حذف شده یا با تاخیر نیز از طریق این مکانیسم محافظت می شوند.

این اعداد دنباله‌ای ۶۴ بیتی هستند، بنابراین جمع‌بندی آن‌ها نباید سخت باشد و برای هر تعویض کلید جدید به‌روزرسانی می‌شوند، بنابراین تقریباً هیچ حساسیتی ندارند.[wag]

۵.۲ حملات خستگی

این نوع حمله SSL، پروتکل دست دادن SSL را با ارسال داده های بی ارزش به سرور SSL که منجر به مشکلات اتصال برای کاربران قانونی می شود یا با سوء استفاده از خود پروتکل دست دادن SSL هدف قرار می دهد.

بسیاری از حملات DDoS شناخته شده و بالقوه وجود دارد که از دست دادن SSL برای تخلیه منابع سرور سوء استفاده می کنند. بات نت Pushdo این کار را به راحتی با ارسال داده های زباله به یک سرور SSL هدف انجام می دهد. پروتکل SSL گران است و بار کاری اضافی روی سرور ایجاد می کند تا داده های زباله را به عنوان یک دست دادن مشروع پردازش کند. فایروال ها در این مورد کمکی نمی کنند زیرا معمولاً قادر به تمایز بین بسته

های دست دادن SSL معتبر و نامعتبر نیستند. حفاظت جامع DDoS می تواند به محافظت در برابر این نوع حملات کمک کند.

یکی دیگر از ابزارهای حمله DDoS مبتنی بر SSL، ابزار THC-SSL-DOS است که با تکمیل یک دست دادن معمولی SSL کار می کند اما بلافاصله درخواست مذاکره مجدد در مورد روش رمزگذاری را می کند. به محض اتمام مذاکره مجدد درخواست مذاکره مجدد می کند و غیره. اگر سرور مذاکره مجدد SSL را غیرفعال کرده باشد (بهترین روش امنیتی استاندارد)، آنگاه ابزار به سادگی اتصال SSL را به محض تکمیل مذاکره می بندد و یک اتصال جدید را برای شروع مجدد فرآیند مذاکره باز می کند. این از نظر محاسباتی بسیار گران است و در غیرقابل دسترس کردن خدمات برای کاربران قانونی به دلیل فرسودگی منابع مؤثر است.[net]

۵.۳ حملات بازگشتی Ciphersuite

این نوع حمله عمدتاً مربوط به SSL 2.0 است که یک مهاجم فعال می‌تواند در سکوت از رمزگذاری ضعیف استفاده کند و می‌تواند با ویرایش فهرست متن شفاف مجموعه‌های رمزی ارسال شده در پیام‌ها انجام شود.[wag]

SSL این مشکل را با احراز هویت همه پیام ها توسط master_secret برطرف می کند، که در آن، مهاجم را می توان در پایان handshake تعیین کرد و جلسه را می توان خاتمه داد.

۵.۴ خلاصه

همانطور که بحث شد، راه‌های متعددی برای حمله و نقض امنیت SSL وجود دارد، حتی با اینکه دارای ویژگی‌های داخلی زیادی برای جلوگیری از این تهدیدات و قرار گرفتن در معرض داده‌ها باشد. اما با کمک TLS در کنار SSL، اکثر این حملات بیهوده هستند.

۶. نتیجه گیری

هدف این مقاله نشان دادن مزایا و معایب پروتکل SSL و روش این مکانیزم است که امروزه تقریباً در هر صفحه وب مورد استفاده قرار می‌گیرد و تمامی داده‌های موجود در اینترنت فرآیند آن را طی می‌کنند.

به طور کلی با مقایسه SSL 3.0 و ۲.۰ نشان داده شد که SSL 3.0 مسیرها و ویژگی های بسیار ایمن تری دارد و ما نقاط ضعف SSL 2.0 را دیدیم و متوجه شدیم که چرا هرگز منتشر نشد.

این مقاله انواع مختلف پروتکل‌های SSL و حوزه استفاده از آن‌ها و نحوه دست‌یابی به آن‌ها برای وب‌سایت یا میزان امنیت هر گواهی را نشان می‌دهد.

این مقاله همچنین الگوریتم‌های مختلف SSL را نشان داد و دیدیم که مشتری و سرور چگونه با یکدیگر تعامل دارند. هر فرآیند برای داده ها در هر یک از این الگوریتم ها نیز بیان شد.

حملات مختلفی که می‌توانند پروتکل SSL را تهدید کنند نیز مورد بحث قرار گرفت و دیدیم که SSL از راه‌های خاصی برای مقابله با هر حمله استفاده می‌کند که می‌تواند از از دست دادن یا افشای داده‌ها جلوگیری کند.

به طور کلی ثابت شد که پروتکل SSL امروزه پرکاربردترین و امن ترین راه انتقال داده از طریق اینترنت است.

۷ قدردانی

بدینوسیله بیان می شود که این مقاله از مراجع مختلف گردآوری شده است و هر اعتباری به آن مقالات خواهد رسید. هر گونه اشتباه، البته، تنها مسئولیت من است.

منابع

[kin] https://kinsta.com/knowledgebase/how-ssl-works/

[kasp] https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

[ore] https://www.oreilly.com/library/view/web-security-and/1565922697/apcs02.html

[intel] https://intellipaat.com/blog/what-is-ssl-handshake/

[geek] https://www.geeksforgeeks.org/secure-socket-layer-ssl/

[tut] https://www.tutorialsteacher.com/https/how-ssl-works

[net] https://www.netscout.com/what-is-ddos/ssl-tls-exhaustion

[seek] https://www.seekahost.com/flaws-in-ssl-version-2/

[wag] https://www.usenix.org/legacy/publications/library/proceedings/ec96/full_papers/wagner/wagner.pdf

[bbl] https://bblfish.net/tmp/2009/05/spot2009_submission_15.pdf

[rfc] https://www.rfc-editor.org/rfc/rfc6101.html