عنوان مقاله : Protocol SSL

گروه مطالعاتی : امنیت

گروه کاری : امنیت

ارائه دهنده: افسانه کربلائي زاده

تاریخ ارائه: ۸۳/۱۱/۱۳

سرپرست گروه کاری: طیبه میرزائی

تاریخ اصلاح: ۸۳/۱۱/۱۵

اصلاح کننده : افسانه کربلائي زاده

مرجع: اینترنت

Secure Socket Layer ، یا همان SSL یک تکنولوژی استاندارد و به ثبت رسیده برای تامین ارتباطی امن مابین یک وب سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعاتی که ما بین وب سرور و مرورگر اینترنت (کاربر) انتقال میابد , محافظت میکند تا در این انتقال به صورت محرمانه و دست نخورده باقی بماند. SSL یک استاندارد صنعتی است و توسط ملیونها وب سایت در سراسر جهان برای برقراری امنتیت انتقال اطلاعات استفاده میشود. برای اینکه یک وب سایت بتواند ارتباطی امن از نوع SSL را داشته باشد نیاز به یک گواهینامه SSL دارد.

زمانیکه شما میخواهید SSL را بر روی سرور خود فعال کنید سؤالات متعددی در مورد هویت سایت شما (مانند آدرس سایت) و همین طور هویت شرکت شما (مانند نام شرکت و محل آن) از شما پرسیده میشود. آنگاه سرور دو کلید رمز را برای شما تولید میکند , یک کلید خصوصی (Private Key) و یک کلید عمومی (Public Key). کلید خصوصی به این خاطر , این نام را گرفته است , چون بایستی کاملا محرمانه و دور از دسترس دیگران قرارگیرد. اما در مقابل نیازی به حفاظت از کلید عمومی نیست و این کلید در قالب یک فایل درخواست گواهینامه یا Certificate Signing Request که به اختصار آنرا CSR مینامیم قرارداده میشود که حاوی مشخصات سرور و شرکت شما بصورت رمز است. آنگاه شما باسیتی که این کد CSR را برای صادرکننده گواهینامه ارسال کنید. در طول مراحل سفارش یک SSL مرکز صدور گواهینامه درستی اطلاعات وارد شده توسط شما را بررسی و تایید میکند و سپس یک گواهینامه SSL برای شما تولید کرده و ارسال میکند.

وب سرور شما گواهینامه SSL صادر شده را با کلید خصوصیتان در سرور و بدور از دسترس سایرین مطابقت میدهد. سرور شما آنگاه امکان برقراری ارتباط امن را با کاربران خود در هر نقطه دارد.

نمایش قفل امنیت SSL

پیچیده گیهای یک پروتکل SSL برای کاربران شما پوشیده است لیکن مرورگر اینترنت آنها در صورت برقراری ارتباط امن , وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر میشود.

و در هنگامي كه شما روي قفل كوچك زرد رنگي كه در پايين صفحه IE نمايش داده ميشود دوبار كليك ميكنيد باعث نمايش گواهينامه شما به همراه ساير جزئيات مي شود.

گواهینامه های SSL تنها برای شرکتها و اشخاص حقیقی معتبر صادر میشوند. به طور مثال یک گواهینامه SSL شامل اطلاعاتی در مورد دامین , شرکت , آدرس , شهر , استان , کشور و تاریخ ابطال گواهینامه و همینطور اطلاعاتی در مورد مرکز صدور گواهینامه که مسؤول صدور گواهینامه میباشد.

زمانیکه یک مرورگر اینترنت به یک سایت از طریق ارتباط امن متصل میشود , علاوه بر دریافت گواهینامه SSL (كليد عمومي) , پارامترهایی را نظیر تاریخ ابطال گواهینامه , معتبر بودن صادرکننده گواهینامه و مجاز بودن سایت به استفاده از این گواهینامه نیز بررسی میکند و هرکدام از موارد که مورد تایید نباشد به صورت یک پیغام اخطار به کاربر اعلام میدارد.

SSL چیست و آیا سایت شرکت ما باید به SSL مجهز باشد یا خیر ؟

بيشتر اطلاعاتي كه روي اينترنت رد و بدل ميشوند به صورت Clear Text مبادله ميشوند و به همين خاطر اطلاعات مبادله شده در بين راه از كامپيوتر شما به وب سرور قابل مشاهده هستند . به عنوان مثال شما وقتي بر روي يك سايت كه SSL نداشته باشد، يك فرمي را پر كنيد و اطلاعات شخصي خود را براي اون سايت بفرستيد اين اطلاعات به صورت Clear Text از كامپيوتر شما خارج شده و بعد از گذشتن از ISP شما و دهها گره اينترنتي ديگر به سرور ميرسند، و اين با اين خطر روبروست كه هر يك از اين گره ها ميتواند اطلاعات رد و بدل شده را به آساني مشاهده كند به عنوان مثال اگر از يك ISP ايراني استفاده ميكنيد ، هم آن ISP و

هم شركتي كه به آن ISP خط Send ميدهد و همه شركت هايي كه در مسير هستند قابليت مشاهده اطلاعات فرستاده شما را دارند .

به طور خلاصه SSL يك پروتوكل امنيتيست كه توسط نت اسكيپ ابداع شده است و در حال حاضر رايج ترين پروتوكل انتقال امن اطلاعات در وب ميباشد به شكلي كه مرورگر اينترنتي شما از وجود چنين امكاني در سرور خبر دار شده و از يك Public Key موجود در مرورگراستفاده كرده و اطلاعات شما به صورت كد شده به سرور ميفرستد و اين تنها سرور است كه با استفاده از Private Key خود اطلاعات دريافتي را ميتواند Decode كند . به علت اينكه آن Key Private تنها در سرور نصب شده است ، هيچ نرم افزار ديگري در بين راه نميتواند آن اطلاعات را مشاهده كند.

از طرف ديگر وجود SSL در سرور اين اطمينان خاطر را به شما ميدهد كه وب سايتي كه شما در حال فرستادن اطلاعات به آن هستيد يك وب سايت تقلبي يا شبيه سازي شده براي بدست آوردن اطلاعات شما نيست و از اصل بودن آن اطمينان حاصل ميكنيد .

آگر وب سايت شما اطلاعات محرمانه اي را از بازديد كننده دريافت ميكند يا داراي قسمتي است كه از بازديد كننده تان شناسه كاربري و پسورد دريافت ميكند و وارد يك User Area ميشود و در آنجا به امكانات خاصي دسترسي دارند بنا بر اهميت آن، ما توصيه به گرفتن SSL ميكنيم .