ایجاد اطمینان برای مشتری در اینترنت

احمد تابنده
tabandeh@idro.org

گزارش شبکه

در این مقاله درباره نیاز به امنیت بر روی اینترنت، معنای گواهینامه SSL (SECURE SOCKET LAYER CERTIFICATES) و چگونگی استفاده از این گواهینامه الکترونیکی به‌منظور دستیابی به مبادله امن و حفاظت شده بر روی شبکه جهانی اشاره خواهدشد.

چرا SSL؟

هنگامی که به فروشگاهی وارد می‌شوید، می‌دانید که با چه وضعیتی روبرو هستید. کالاها، مارک آنها و راهنمای فروشگاه را می‌بینید. می‌توانید مطمئن باشید که اگر در خرید شما اشکالی پیش بیاید، مدیر فروشگاه یا صاحب آن برای مراجعه دردسترس خواهند بود.

اما بر روی اینترنت، مراجعه‌کنندگان به پایگاههای وب هیچ راه قابل اطمینانی برای آگاهی از اینکه چه کسی صاحب پایگاه (فروشگاه مجازی) است، دردست ندارند. هنگامی که مشتریان با قصد انجام یک خرید اینترنتی، به یک پایگاه وب وارد می‌شوند، علاقه دارند بدانند که پول را به چه کسی می‌پردازند. آنها خواستار اثبات هویت صاحب پایگاه بوده، و می‌خواهند بدانند که اطلاعات شخصی ارسالی آنها به پایگاه مزبور توسط سایر کاربران اینترنتی قابل ردگیری و تداخل نیست. اینجاست که گواهینامه‌های الکترونیکی SSL به صحنه می‌آیند.

SSL پروتکلی است که توسط شرکت نت‌اسکیپ ایجاد شده و به مرورگر وب و سرویسگر وب امکان ارتباطات ایمن و حفاظت‌شده را می‌دهد. SSL به مرورگر (نت‌اسکیپ، اکسپلورر...) توان و اجازه آن را می‌دهد تا سرویسگر وب که دارای ارتباط با آن هستند را تایید کند. پروتکل SSL، سرویسگر وب را ملزم می‌کند که گواهی الکترونیک معینی را داشته باشد. پس از اطمینان از وجود آن و تایید شدنش توسط مرورگر، ارتباط پروتکلی حفاظت شده برقرار می‌شود.

در اثر وجود پروتکل SSL که دارای قابلیت عملکرد بر روی اینترنت باشد، و گواهینامه SSL که توسط یک شرکت شناخته شده (مثلاً THAWTE) که این‌گونه گواهینامه‌ها را برای تایید نقل و انتقالات بر روی اینترنت می‌دهند، مشتریان اطمینان پیدا می‌کنند که مواردی از قبیل شماره حسابهای بانکی، مراسلات الکترونیک و غیره برملا نخواهدشد. شرکتهایی که گواهینامه‌ها را صادر می‌کنند درصورت هرگونه اشکالی، هزینه‌های مربوطه را تقبل خواهند کرد. مشتری در جریان ارتباط با یک پایگاه وب حفاظت شده در سه مورد زیر اطمینان حاصل می‌کند:

- تایید (AUTHENTICATION): پایگاه وب درواقع متعلق به شرکتی است که تاییدیه مزبور را بر روی سرویسگر خود نصب کرده است؛
- خصوصی‌ماندن پیغام: SSL با استفاده از یک «کلید جلسه ارتباطی» (SESSION KEY) منحصر به فرد، کل پیام و اطلاعات ردوبدل شده میان سرویسگر وب شما (به فرض آنکه شما شرکت فراهم‌کننده کالا یا خدمات موردنیاز مشتری باشید) و مشتریانتان ازقبیل شماره حساب کارت اعتباری و سایر اطلاعات شخصی را به رمز تبدیل می‌کند. این امر تضمین می‌دهد که درصورت تداخل افراد غیرمجاز با پیام ارسالی، آنها نتوانند از اطلاعات مزبور استفاده کنند؛
- یکپارچگی پیام: داده‌های ارسالی در اینترنت دچار به‌هم‌ریختگی نخواهدشد.

مشتریان شرکت شما در موارد فوق منتفع خواهندشد زیرا ازطریق بررسی جزئیات موجود در گواهینامه متوجه می‌شوند که پایگاه اینترنتی که هم‌اکنون به آن وصل هستند درواقع همان پایگاهی است که می‌خواهند با آن معامله کنند. همچنین برای آنها مشخص است که اطلاعاتشان دردسترس شخص ثالثی قرار نخواهدگرفت.

بنابراین اگر برای شما مهم است که به مشتریانتان اطمینان دهید که ارسال اطلاعات آنها بر روی اینترنت با مخاطره‌ای روبرو نیست، لازم است یک گواهینامه SSL داشته باشید. اگر بیش از یک نام حوزه (DOMAIN NAME) دارید که لازم است از آن حفاظت به‌عمل آورید، آنگاه نیاز به بیش از یک گواهینامه دارید. گواهینامه‌های الکترونیکی از لحاظ نام حوزه و نام میزبان منحصربه‌فرد و ویژه‌اند. بنابراین به تعداد نام حوزه‌هایتان، نیازمند گواهینامه الکترونیکی هستید.

اطمینان، ارزش‌آور است. کسب‌وکار الکترونیک شما از داشتن سرورهای حفاظت شده توسط سیستم SSL و گواهینامه الکترونیکی منتفع خواهدشد و به‌خاطر اطمینان بیشتری که مشتریان پیدا می‌کنند، خرید بیشتری توسط افرادی که به حفاظت اطلاعات شخصی خود اهمیت می‌دهند، صورت خواهدگرفت.

اطمینان از ایمنی پایگاه وب

اگر یک پایگاه وب دارای گواهی SSL نباشد، هنگام اتصال کاربرانی که از سیستم مزبور استفاده می‌کنند، آیکونی که نمایش یک قفل باز است را در صفحه مرورگر خود خواهند دید.

تصویر ۱ - آیکون قفل باز

گواهی معتبر: اگر یک ارتباط SSL بین مرورگر و سرویسگر وب برقرار شود، «https» در آدرس وب به‌طور معمول به «https» تبدیل خواهدشد. مثلاً، «http://www.thwate.com» به «https://www.thwate.com» تبدیل می‌شود. در مرورگر نیز آیکون «قفل بسته» ظاهر خواهدشد.

تصویر ۲ - آیکون قفل بسته

اگر می‌خواهید بدانید که پایگاهی دارای گواهی تایید شده است یا خیر، به جای http از https در جایگاه آدرس مرورگر استفاده کنید.

اخطارهای مرورگر

هنگامی که اطلاعاتی را به پایگاهی ارسال می‌کنید که گواهی SSL ندارد، در مرورگر شما یک اخطار ظاهر می‌شود. اما اگر یک پایگاه وب از گواهی الکترونیکی تأییدیه استفاده می‌کند، پیامی به کاربر ارسال می‌شود که برای او مشخص می‌کند به پایگاهی وصل شده که از شرکت بخصوصی (مثلاً ITHAWTE) که به‌عنوان یک مرجع صاحب گواهی است، تأییدیه دریافت کرده است، و نیز آنکه کلیه اطلاعات به صورت رمزشده برای پایگاه مزبور ارسال می‌شود. مشتری با بررسی گواهی مزبور، می‌تواند اطمینان حاصل کند که پایگاه مربوطه موردتایید است.

گواهی SSL چیست؟

در زیر، شکل یک گواهی الکترونیکی، به صورتی که در مرورگر نت‌اسکیپ ظاهر می‌شود را می‌بینیم.

گواهی الکترونیکی برای مرورگر درخواست‌کننده، موردتایید قرار می‌دهد. این نحوه تایید، فرایند کاملاً پیچیده‌ای است که حاوی ردوبدل یک «کلید عمومی» (گذرگاه عمومی)، و به‌کارگیری یک «کلید جلسه» (گذرگاه جلسه مبادله اطلاعات میان سرویسگر و میزبان) به‌منظور رمزسازی اطلاعات درحال مبادله است. کاربر از این جریان هیچ اطلاعی نخواهدداشت. گواهی مزبور به‌عنوان اثبات این امر خواهدبود که یک شخص ثالث مورداعتماد طرفین (نظیر شرکت ITHAWTE) تأکید کرده است که سرویسگر به شرکتی تعلق دارد که مدعی ارتباط آن سوی خط با کاربر است. وجود یک گواهی معتبر، به مشتریان این اطمینان را می‌دهد که اطلاعات خود را به‌طور مطمئن و با ایمنی کامل به جای درستی ارسال می‌کنند.

یک جفت کلید عمومی - خصوصی

موقعی که گواهی مشخصی را درخواست می‌کنید، یک جفت کلید بر روی سرویسگر خودتان ایجاد می‌کنید. هنگامی که جفت کلید موردنظر را برای کسب و کارتان (شرکت خودتان) ایجاد می‌کنید، «کلید خصوصی» شما بر روی سرویسگرتان نصب می‌شود و در این حالت هیچ کس دیگری به آن دسترسی ندارد.

شما استفاده می‌کنند تا قبل از ارسال اطلاعات برای شما، آن را به صورت رمز درآورند (البته مشتری درواقع از این فرایند بی‌خبر است). از سوی دیگر، تنها کلید عمومی است که می‌تواند این اطلاعات را رمزگشایی کند. از این رهگذر، مشتریان اطمینان می‌یابند که شخص ثالثی از این اطلاعات نمی‌تواند استفاده کند.

* برای بررسی طریقه استفاده از گواهی الکترونیک و ویژگیهای مربوطه می‌توانید به آدرس زیر مراجعه کنید.

WWW.THAWTE.COM

درعین حال یک گواهی نمونه را نیز می‌توانید تست کنید. تسهیلات دیگری از قبیل گواهی پست الکترونیک امن و ایمن‌سازی نرم‌افزارهای کاربردی نیز در این پایگاه وجود دارد که همراه با اطلاعات پرمحتوا و جالبی است.

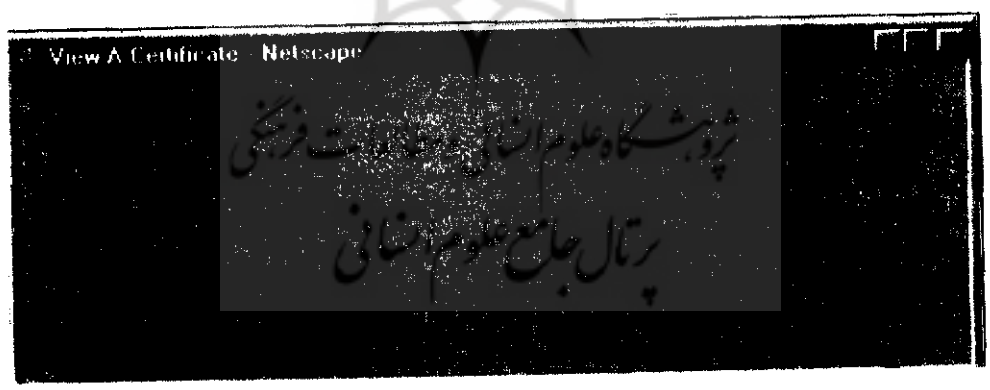
پایگاههای ماه برای مدیران

۱ - FINDARTICLES.COM حاوی مقالات بی‌شمار در زمینه‌های مختلف

۲ - QUALITY.NIST.GOV پایگاه معیارهای کیفیت مالکوم بالدریج

۳ - GOOGLE.COM حاوی چکیده‌ها و اطلاعات تخصصی علمی - فنی.

۴ - IOMA.COM پایگاهی است که در زمینه



هر گواهی SSL دارای اطلاعات زیر است:

۱ - عنوان حوزه‌ای (DOMAIN) که گواهی برای آن صادر شده؛

۲ - صاحب گواهی (همان فرد یا موجودیتی که حق استفاده از حوزه را دارد)؛

۳ - محل جغرافیایی / فیزیکی صاحب گواهی؛

۴ - تاریخهای اعتبار گواهی.

هنگامی که به یک سرویسگر ایمن وصل می‌شوید، آن سرویسگر خود را با ارائه یک «کلید عمومی» شما که با آن کلید خصوصی سازگار است نیز به‌عنوان بخشی از گواهی الکترونیک، برروی سرویسگر اینترنتی (WEB SERVER) شما نصب می‌شود. کلیدهای عمومی و خصوصی به‌طور منطقی (ریاضی) به یکدیگر مرتبط شده‌اند، لیکن همانند یکدیگر نیستند. مشتریانی که می‌خواهند به‌طور خصوصی با شما ارتباط برقرار کنند، کلید عمومی را در شناسه سرویسگر (SERVER ID)

مقالات مدیریتی برای مدیران اجرایی، حاوی منابع غنی و قابل استفاده‌ای است. مهمترین بخش این پایگاه، اتصالات آن برای معرفی سایر موسسات، جوامع و شرکتهای فعال در زمینه صنعت و خدمات و گروههای خبری مربوطه است. بدین‌منظور می‌توانید به پایگاه SCIP.ORG نیز مراجعه کنید. □

مآخذ: پایگاه www.thawte.com