شناسنامه مقاله

نويسنده: فرشاد فكري نجات

وب سايت: www.fekrinejat.com

ايميل: fekrinejat@yahoo.com

چاپ شده توسط: ماهنامه وب

شماره: ۳۷

صفحه: ۱۵

SSL ، مدعي تامين امنيت ارتباطات

مقدمه :

SSL مخفف Secure Socket Layer و يكي از پروتوكل هاي مهم در ايجاد امنيت ارتباطات راه دور از طريق اينترنت ميباشد. بيشتر سايتهاي كه در زمينه تجارت الكترونيكي فعاليت دارند و يا بانكهاي اينترنتي كه پولها را بواسطه كارتهاي اعتباري به سراسر اينترنت انتقال ميدهند از اين پروتوكل استفاده ميكنند. در دهه اخير و مخصوصا از سال ۱۹۹۸ به بعد، دنيا با رشد روز افزون تجارت الكترونيكي روبرو بوده و اين سرويس Online نيازمند سيستم امنيتي مناسبي ميباشد. زيرا شخصي كه با استفاده از شماره كارت اعتباري خود اقدام به خريد Online مينمايد، بايد از سيستم خريد اطمينان كامل داشته باشد. اين سيستم در محيط وب توسط پروتكلي با نام SSL فراهم ميگردد. در واقع مسئولين IT و مخصوصا ICT كه در زمينه تجارت الكترونيكي فعاليت ميكنند، ميبايست با طرز كار اين پروتكل آشنايي خوبي داشته باشند. اين پروتوكل توسط شركت Netscape ساخته شده و هم اكنون نسخه ۳ (آخرين نسخه) آن در دسترس ميباشد. با استفاده از اين پروتوكل، اطلاعاتي كه از طرف كاربر بصورت رمزگذاري شده ارسال ميشود و بعد از دريافت از طريق سرور ، رمزگشايي شده و اطلاعات اصلي بازيابي ميشود. در ضمن SSL با سيستم امنيتي مناسب خود، تضمين ميكند كه فقط شركت يا سايتي كه كاربران از آن خريد ميكنند از اطلاعات كارت اعتباري آنها باخبر هستند. به عنوان مثال شخصي كه قصد خريد Online با استفاده از Credit Card را دارد، ميبايست از طريق HTTP (پورت ۸۰) و پروتوكل TCP/IP بواسطه مرورگر وب عمل نمايد. در واقع TCP/IP قادر به انتقال اطلاعات در سراسر جهان ميباشد كه پروتكلهاي HTTP ، IMAP ، LDAP و غيره ، زير مجموعه TCP/IP ميباشند و از قوانين مربوط به آن استفاده ميكنند. ولي پروتوكل TCP/IP به تنهايي قادر به مخفي كردن داده ها بين كاربر و سرور نيست و از طرفي پورت ۸۰ مربوط به ارتباطات معمولي (غير ايمن) ميباشد و يك هكر با استفاده از Packet Sniffing قادر به بررسي و مشاهده محتواي Packet هاي پروتوكل است. از اين رو براي ارتباطات ايمن، SSL از طريق پورت ٤٤٣ ولي با پشتيباني از پروتوكل TCP/IP اقدام به ارسال و دريافت بسته هاي اين پروتوكل مينمايد. از اين رو SSL بين يك پروتوكل سطح بالا مانند HTTP يا SMTP و يك پروتوكل سطح پايين مانند TCP قرار ميگيرد و ارتباط ايمن را برقرار مينمايد. اين پروتوكل جديد در استاندارد (Transport Layer Security) TLS نيز بكار ميرود كه از معروفترين اجزاي اين

استاندار امنيتي، ميتوان به WTLS كه در براي امنيت WAP و ارتباطات بي سيم بكار برده ميشود اشاره كرد.

مشكلات تجارت الكترونيكي در ايران :

اولين نكته اينكه هيچگاه به همه سايتها اعتماد نكنيد و شماره اعتباري خود را در اختيارشان قرار ندهيد. بعضي سايتها به بهانه Adult Check و بهانه هايي از اين قبيل، شماره كارت اعتباري شما را گرفته و از آن سوء استفاده ميكنند. حتي بعضي سايتها گواهينامه هاي ديجيتالي صحيح و تثبيت شده اي به شما نشان ميدهند ولي امكان بروز مشكل همچنان وجود دارد. هميشه از سايتهاي معتبر كه سيستم هاي تست شده اي را ارائه ميدهند و مورد استفاده عموم قرار گرفته اند استفاده كنيد. در اين بين، امكان كلاهبرداري از كاربران ايراني در اينترنت چند برابر ميباشد. زيرا قوانيني براي حمايت از كشورهايي كه در اقتصاد جهاني داراي محدوديت هستند وجود ندارد و نظارتي به روي اين معاملات انجام نميگيرد. همچنين خيلي از اجناس خريداري شده به ايران ارسال نميگردد، ولي در كشورهاي خارجي در صورتي كه كالايي بعد از خريد Online به مقصد نرسد بلافاصله توسط مراجع قانوني مورد پيگيري بين المللي قرار خواهد گرفت. يكي از مشكلات مهم ديگر عدم دسترسي به كارتهاي اعتباري بين المللي است، اگرچه گامهاي موثر و مثبتي در جهت رفع اين مشكل توسط سازمانهاي خصوصي و واسطه اي انجام گرفته و حتي در بعضي معاملات از كارتهاي اعتباري داخلي استفاده ميشود ولي تجارت الكترونيكي در ايران نيازمند حمايت بيشتري از طرف مسئولين امر ميباشد.

تشخيص هويت :

يكي از مباحث مهم و اصولي در ارتباطات ايمن، تشخيص هويت متقابل از هر دو طرف Client و Server ميباشد. در يك ارتباط، ميبايست هويت اصلي سرور براي كاربر و برعكس مشخص شود زيرا در غير اين صورت هر سروري قادر به ايجاد اعتماد در كاربران خواهد بود. هر سرور بايد داراي گواهينامه ديجيتالي باشد كه اين گواهينامه، نشاندهنده هويت اصلي آن است و توسط شركتهايي مانند VeriSign و Thawte ارائه ميگردد. در اين گواهينامه الكترونيكي اطلاعاتي از قبيل : كليد عمومي (براي مخفي سازي اطلاعات) ، شماره سريال ، نام دامنه ، امضاي ديجيتالي و تاريخ شروع و انقضاي اعتبار گواهينامه درج ميشود. كاربر به راحتي ميتواند مشخصات گواهينامه سرور را بررسي نمايد. به عنوان مثال فرض كنيد كه براي خريد يك كالا به صورت On-Line به يكي از سايتهاي مربوطه متصل شده ايد، در ابتدا پيغامي مبني بر ايجاد يك ارتباط با استفاده از SSL را ملاحظه ميكنيد، كه بعد از تاييد آن، اگر به پايين پنجره مرورگر خود از سمت راست (درStatus Bar) دقت نماييد، آيكوني (به شكل يك قفل) را مبني بر يك ارتباط ايمن مشاهده خواهيد كرد كه با دوبار كليك كردن بر روي آن ميتوانيد اطلاعاتي گواهينامه سرور را بطور كامل مشاهده نماييد. البته بايد توجه داشته باشيد كه حتما مرورگر وب شما قابليت پشتيباني از SSL را داشته باشد و يا آن را غير فعال نكرده باشيد. براي اطمينان از فعال بودن اين پروتوكل، در Internet Explorer از منوهاي بالا به منوي Tools > Internet Options رفته و از پنجره ظاهر شده، Tab مربوط به Advanced را انتخاب كرده و از انتخاب گزينه اي با عنوان Use SSL 3.0 اطمينان حاصل كنيد. پيشنهاد ميكنم كه حتما قبل از استفاده از Credit Card خود در اينترنت، گواهينامه سرور را از نظر تاريخ انقضا و نام دامنه مورد بررسي قرار دهيد.

تكنيكهاي امنيت در SSL :

استاندارد SSL از تكنيكهاي زيادي براي رمزگذاري و رمزگشايي بسته هاي پروتوكل TCP/IP استفاده ميكند. اين تكنيكها در نسخه هاي مختلف SSL متفاوت است و روز به روز در حال

پيشرفت و بهينه شدن ميباشد. دو تكنيك رمزگذاري كه اغلب در اين پروتوكل انجام ميگيرد روشهاي متقارن و نامتقارن است.

۱- روش متقارن :
در اين روش SSL هر دو طرف ميبايست فقط از طريق يك كليد، داده ها را رمزگذاري و يا رمزگشايي نمايند. اين روش از سرعت مناسبي برخوردار است البته اگر هكر بتواند كليد اصلي را بدست آورد امكان بروز مشكلاتي در امنيت داده ها وجود دارد. روش متقارن در الگوريتمهاي RC4 و DES (Data Encryption Standard) نيز مورد استفاده قرار گرفته است.

۲- روش نامتقارن :
در اين روش كه از سرعت كمتري نسب به روش متقارن برخوردار است، بجاي يك كليد، داراي دو كليد خصوصي و عمومي (۱ كليد خصوصي و ۱ كليد عمومي) ميباشد كه كليد عمومي در اختيار تمام SSL هايي كه اقدام به ارسال داده ها ميكنند قرار ميگيرد ولي كليد خصوصي فقط در اختيار پروتوكلي است كه اقدام به دريافت داده ها ميكند. اين روش در الگوريتمهاي مختلفي از جمله RSA و MD4 مورد استفاده قرار ميگيرد.

در ضمن پروتوكل SSL از دو زير پروتوكل به نامهاي SSL Record و SSL Handshake تشكيل شده است كه مسئوليت SSL Handshake برقراري ارتباط اوليه بين كاربر و سرور ميباشد و SSL Record اطلاعات مربوطه را در بسته هاي ١٦ كيلوبايتي به مقصد ارسال ميكند. در اين بسته ها اطلاعاتي از جمله الگوريتم كدگذاري ، پيغام خطا مبني بر مشكلي در شناسايي Packet و همچنين خود داده هاي اصلي قرار دارد.

چگونگي ايجاد يك ارتباط ايمن :
همانطور كه اشاره شد، يك ارتباط ايمن در پروتوكل SSL توسط SSL Handshake برقرار ميشود و مراحلي براي ايجاد يك ارتباط كامل و مطمئن از هر دو طرف (كاربر و سرور) انجام ميگيرد. شايد مراحل SSL Handshake كمي پيچيده به نظر آيد ولي با كمي تمركز و دقت به ارتباط دقيق و بي نقص دو طرف، پي خواهيد برد. مراحل مذكور عبارتند از :

۱- در مرحله اول كامپيوتر كاربر اقدام به ارسال اطلاعاتي در مورد نسخه SSL ، تنظيمات تكنيك مخفي سازي و فشرده سازي داده ها ، ID جلسه (Session) و اطلاعات ساعت و تاريخ به كامپيوتر سرور ميكند. اگر كاربر براي اولين بار از سرور مورد نظر استفاده كند، ID جلسه، صفر خواهد بود.

۲- بعد از ارسال اطلاعات از طرف كاربر ، سرور نيز اطلاعاتي از جمله نسخه SSL و تنظيمات مخفي سازي و غيره .. را به ماشين كاربر ارسال ميكند. در اين مرحله، گواهينامه سرور براي تشخص هويت نيز به كاربر ارسال ميشود.

۳- در اين مرحله ، ماشين كاربر اقدام به تشخص هويت سرور ميكند كه در صورت وجود مشكلاتي در گواهينامه سرور، ارتباط برقرار نخواهد شد.

٤- در صورتي كه مرحله قبل با موفقيت انجام گيرد و كاربر و سرور يكديگر را تايد نمايند. در اين مرحله توسط ماشين كاربر، يك كليد Premaster Secret براي جلسه تهيه ميگردد، لازم به ذكر است كه Premaster Secret با استفاده از كليد عمومي كه در مرحله دوم توسط گواهينامه سرور به ماشين كاربر ارسال شده بود، رمزگذاري (Encrypt) ميشود، در ضمن اين

كليد ٤٨ بايتي به صورت تصادفي ايجاد ميشود. در اين مرحله مشخصات ماشين كاربر نيز براي تشخيص هويت به همراه Premaster Secret به ماشين سرور انتقال داده ميشود.

٥- در اين مرحله در صورتي كه هويت كاربر براي سرور مشخص گرديد، ماشين سرور با استفاده از كليد خصوصي كه در اختيار دارد اقدام كه رمز گشايي Premaster Secret مينمايد كه در نهايت كليد Master Secret ايجاد ميشود. اين رمزگشايي را ماشين كاربر نيز انجام ميدهد. در اين مرحله هر دو طرف ارتباط داراي كليد Master Secret ميباشند. اگر توجه كرده باشيد تا اين مرحله هر دو طرف كليد Master Secret را بدون اينكه به روي خط براي يكديگر ارسال كنند در اختيار دارند، در واقع تمام اين مراحل براي امنيت بالاتر و عدم ارسال كليد اصلي به روي خط ارتباطي بود.

بعد از انجام تمام مراحل فوق ارتباط SSL Handshake بطور كامل برقرار ميگردد و هر دو طرف با استفاده از كليدهاي جلسه، اقدام به رمزگذاري و رمزگشايي بسته هاي ارسالي و دريافتي مينمايند.

مشكل امنيتي در SSL :

با وجود اينكه اين پروتوكل امروزه در سايتهاي تجارت الكترونيكي مورد استفاده گسترده قرار ميگيرد ولي نميتوان منكر معايب و نواقص آن شد. همانطور كه ميدانيد كليد اصلي مربوط به ارتباطات SSL بصورت تصادفي ايجاد ميشود، متاسفانه طراحي سيستم ايجاد كنند كليد جلسه (Session Key) اين پروتوكل كه توسط شركت NetScape ايجاد شده، ضعيف ميباشد، و يك هكر ماهر به راحتي قادر به پيدا كردن اين كليد خواهد بود. نسخه هاي قبلي SSL از كليدهاي ٤٠ بيتي استفاده ميكردند و نسخه ٣ اين پروتوكل از كليد ١٢٨ بيتي استفاده ميكند، لازم به ذكر است كه تمامي نسخه ها اين پروتوكل به غير نسخه ٣ ، توسط مهاجمان، Crack شده و ناامن است، البته هنوز نسخه ٣ كرك نشده ، ولي كارشناسان احتمال وقوع اين امر را در آينده اي نزديك ميدهند كه در اين صورت ميبايست تحولات بنيادي در زيربناي اين پروتوكل ايجاد شود.