امینت اطلاعات در بزرگراه های الکترونیکی ✱

نوشته: اس. اچ. فن سلمز
ترجمه: علی اکبر پور احمد
کارشناس اشد کتابداری و اطلاع رسانی

کلید واژه ها
پروتکال های امنیتی / ینترنت/ WWW/ SSL/ SHTTP/ SEPP

چکیده
این مقاله تعدادی از پروتکال های امنیتی اینترنت و WWW **را مورد بررسی قرار می دهد. از این میان** SSL **و** SHTTP **تأیید اصالت، محرمانه بودن یکپارچگی را ارائه می کنند. در حالی که** SEPP **پروتکال پرداخت است، و مخصوصا" برای استفاده در خرید الکترونیکی طراحی شده است.**

هرگاه در بارهٔ اینترنت مقاله ای می خوانید یا با کسی صحبت می کنید، تقریبا" تردیدی نیست که هر مؤسسه ای که نتواند برنامه ریزی خاصی برای استفاده اینترنت / WWW برای خودش داشته باشد در نهایت ازبین می رود. به هر حال، در محتوای همین مقالات و سخنان، به طور واضح نسبت به خطرات امنیت اطلاعات و آنچه که باید انجام شود، هشدار داده می شود. داده های مختلفی برای یک مؤسسه وجود دارد تا بتواند خود را بر روی اینترنت عرضه کند. اما به طور کلی، الگوی قابل قبولی در این مورد وجود دارد. معمولا" مراحل زیر کلا" می تواند ملاک باشد، ولی نه لزوما" به ترتیبی که در اینجا پیشنهاد شده است.

مرحله یک: اجازه دادن به کارمندان برای بازیابی اطلاعات از اینترنت و WWW(۱). بنابراین مشتریان(۲) مؤسسه می توانند به پردازشگرهای(۳) WWW دسترسی داشته باشند، اما مؤسسه نمی تواند پردازشگرهای قابل دسترس را در خارج از مؤسسه فراهم نماید.

مرحله دوم: حرکت به سوی استفاده از اینترنت و WWWبرای ارائه اطلاعات دربارهٔ تولیدات مؤسسه و قیمت های آن که در برگیرندهٔ اطلاعات محرمانهٔ گزینش شده برای مشتریان مخصوص است. در این مرحله مؤسسه می تواند پردازشگری فراهم نماید که هر کدام از مشتریان خارج از مؤسسه بتوانند به آن دسترسی داشته باشند. این مسئله غالبا" نقطهٔ آغاز استفاده از اینترنت برای بازاریابی است.

مرحله سوم: حرکت به سوی استفاده از اینترنت و WWW برای خرید الکترونیکی در یک وحیط بسته، که در آن قبلا" مشتری باید پذیرش شود و معامله فقط به صورت پذیرشی(۴) انجام می گیرد.

✱-
systems security, 1996 edited by sodratis K. Katsikas. Lindan, chapmman & Hall, pp. 153- 166.

مرحله چهار: خرید الکترونیکی به صورت باز، که در آن، معاملات را می توان با ارائه شمارهٔ کارت اعتباری توسط هر مشتری انجام داد.

این مقله ماهیتا" بسیار آزموده است و هدف ازآن، مشخص کردن بعضی از خطراتی است که در این مراحل با آن درگیر هستیم. ضمنا" بعضی از راه حل های موجود ارائه می شود. ما عمدتا" به راه حل های امنیتی مربوط بخ مراحل ۲و ۴ می پردازیم و همچنین تعدادی از پروتکال هایی را که به نظر می رسد نقش مهمی در این حوزه داشته باشند بررسی خواهیم کرد.

مرحلهٔ یک- هیچ مقدار از اطلاعاتی که توسط مؤسسه فراهم می گردد به خارج از مؤسسه درز پیدا نمی کند. معمولا" در این مرحله روش هایی به کار برده می شود. این روش ها به گونه های مختلفی ظاهر می شوند. در این مرحله نحوهٔ به کار گرفتن این روش ها شرط اصلی است.

مرحلهٔ دوم- در این مرحله محیط بازتری ایجاد می شود، طوری که داده های مؤسسه از پردازشگر مؤسسه به دنیای خارج راه پیدا می کند. خطرات افزایش می یابد، زیرا آلودگی ناشی از مؤسسات دیگر، همچنین احتمال ارائه اطلاعات محرمانه به دلالال غیر قانونی(۵)، ممکن است انجام شود.

در بخش های بعدی راه حل های مرتبط با مرحلهٔ ۲ بررسی خواهدشد. برای این کار تسهیلاتی لازم است:

توانایی تأیید(۶) مشتریان برای انجام معاملات، یعنی مشتری باید مطمئن باشد که با یک نظام قانونی در ارتباط است؛

توانایی محافظت و امنیت داده های ارسال شده بین مشتری و پردازشگر، یعنی نگهداری آن به طور محرمانه؛

توانایی جلوگیری از تکرار معاملات؛

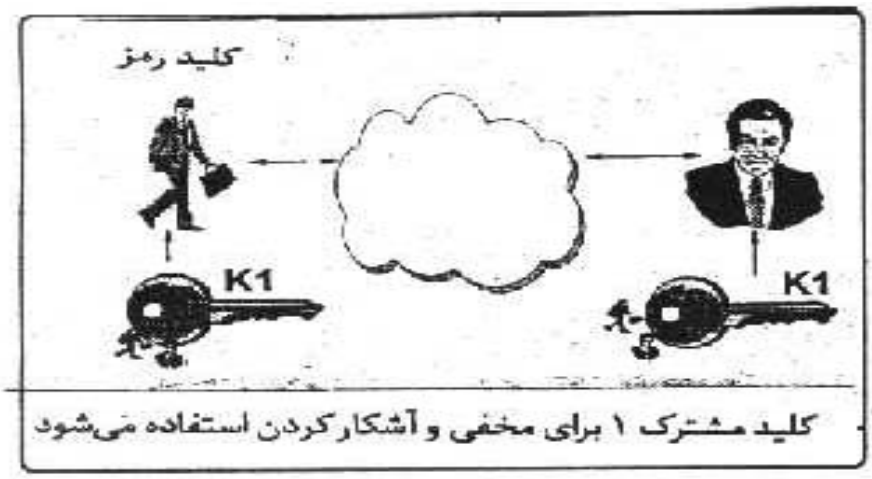
توانایی اطمینان از این که داده ها در طی انتقال تغییر نکرده، یعنی به طور منسجم نگهداری شده؛

توانایی امضای رقومی پیام ها، به صورتی که غیر قابل انکار و رد باشد.

اکنون شناسایی و تأیید طرفهای معامله، همچنین محرمانه بودن و صحت داده ها در طی انتقال ضروری است. راه حل ها سخت و مشکل خواهد شد، اما باید همیشه و تا حد ممکن برای استفاده کننده روشن باشد. دو فن آوری پذیرفته شده ای که برای این مراحل مفید و دارای توانایی های مختلفی هستند SSL(۷) و SHTTP(۸) می باشند.

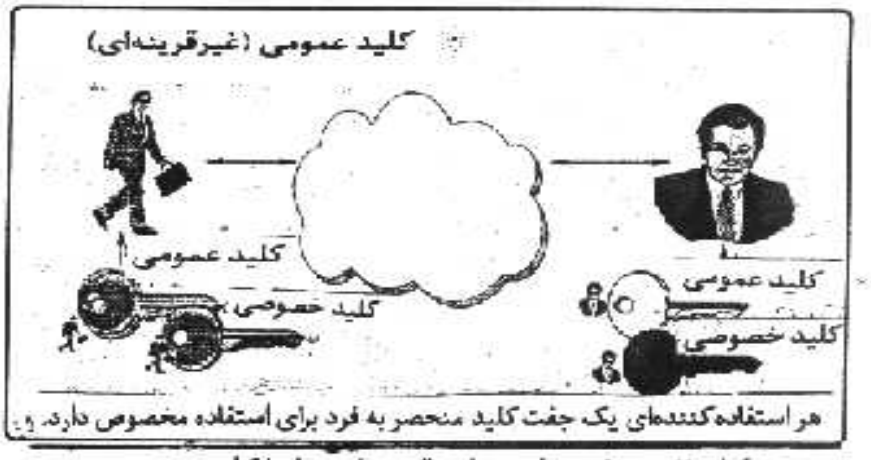
نشانه های رقومی(۹)

در رویکرد سنتی قرینه ای محرمانه سازی، دو طرف پیام نقش مهمی دارند و مخفی ماندن پیام های امنیتی را با رمزی کردن مندرجات پیام، با استفاده از الگوی مشترک و کلید مشترک تأمین می کنند.

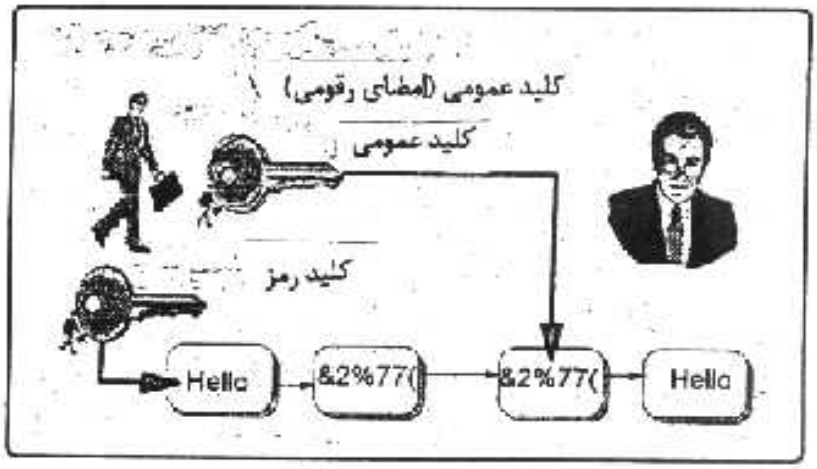


شکل ۱. مخفی‌سازی به صورت قرینه‌ای

در روش قرینه ای یا عمومی، هر یک از طرفین یک جفت کلید مرتبط منحصر به فرد دارد، یکی از این کلیدها، کلید عمومی او و دیگری کلید خصوصی است. کلید عمومی کاربرد گسترده دارد و استفادهٔ آن برای همگان است. کلید خصوصی فقط مال کسی است که به عنوان مالک شناخته شده است. هر چیزی که با کلید عمومی به صورت مخفی در می آید، فقط به وسیله کلید خصوصی مربوطه قابل بازیابی است. تصویر ۲ گویای این مطلب است. کلیدهای عمومی / خصوصی به وسیله مقام مدیدریت گواهینامه صادر می شود. زیرا دانستن این مسئله که کلید عمومی یا خصوصی در واقع متعلق به شخص خاصی است، مهم است.



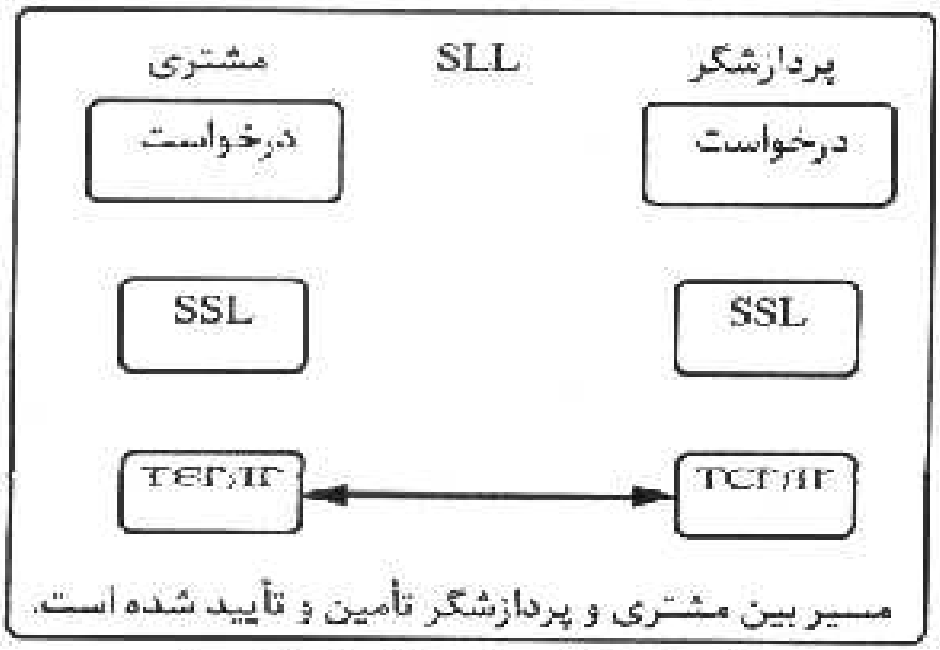
شکل ۲. مخفی‌سازی غیر قرینه‌ای یا با کلید عمومی



شکل ۳. امضای رقومی

SSL

SSL مسیر انتقال بین مشتری و پردازشگر را جهت معامله مسیر می کند. تأمین، مرحلهٔ دوم سطح تقاضا می باشد، و تقاضا کنترلی بر بخش خدمات، در درخواست گزارش(۱۰) خاص ندارد. امنیت تمام گزارش ها عموماً بدین شیوه تأمین می شوند. SSL مجرای ارتباطی بین دو مشارکت کنندهٔ تأیید شده می باشد. پروتکل SSL پروتکل امنیتی است که محرمانه بودن استفاده از اینترنت را فراهم می کند. این پروتکل به مشتری/ پردازشگر امکان می دهد درخواست هایش را به روشی مرتب نماید که استراق سمع نشود. هر پردازشگر دارای یک جفت کلید عمومی/ خصوصی است و با این کلیدهای عمومی/ مخفی شده همیشه تأیید می شوند. مشتریان نیز می توانند (به طور اختیاری) اگر بخواهند یک جفت کلید عمومی/ خصوصی تأیید شده داشته باشند. SSL برای انتقال نامه و پذیرش آن به پروتکل حمل و نقل مطمئنی مانند TCP/IP (۱۱)، نیاز دارد. پروتکل SSL، پروتکل درخواستی غیر مستقل، و یک پروتکل سطح بالا است مانندHTTP(۱۲)، FTP(۱۳)، TELNET، که آشکارا در سطح بالایی از دیگر پروتکال ها قرار می گیرد. شکل ۴ گویای این مطلب است.



شکل ۴. SSL در ارتباط با دیگر سطوح

در یک ارتباط WWW پردازشگر/ مشتری، پروتکل SSL،به صورت پروتکل دستی(۱۴)، به مشتری اجازه می دهد تا پردازشگر را تأیید نماید. این کار بر روی یک الگوی مخفی انجام می شود تا مشتری و پردازشگر با ایجاد کلید کنفرانس برای کنفرانش خصوصی، داده های خویش را ارسال یا دریافت نمایند. مشتریان همیشه ارتباط خودرا با پردازشگر، از طریق انتخاب مکان یاب منابع یکدست(۱۵) که مکان صفحهٔ Web را مشخص میکند، آغاز می کنند. مشتری باید بداند که پردازشگر SSL را حمایت می کند یا نه. این از طریق مکان یاب به مشتری نشان داده می شود. در این حالت اگر با http:// آغاز کرده باشد، مشتری می داند که پردازشگر نیازی به SSL ندارد، و ارتباط معمولی به وجود می آید. ارتباط SSL نوعی ارتباط معمولی بین دو طرف است، و زمانی که به طور کامل انجام گردد، پروتکل دستی که در زیر توصیف شده اجرا می شود. هنگامی که پروتکل دستی انجام می گیرد، اولین درخواست اطلاعات آغاز و ادامه می یابد. بعد از آن، پردازشگر مشتری را تأیید می کند. اگر فرآیند دستی موفقیت آمیز باشد، کلید کنفرانس برای مخفی کردن اطلاعات در طی کنفرانس، بین دو طرف ایجاد می شود و اطلاعات درخواستی، توسط کلید کنفرانس تأمین و به جریان می افتد. پروتکال دستی در بخش بعدی مورد بررسی قرار می گیرد و مسیر مطمئنی بین مشتری و پردازشگر ایجاد می کند. در این فرایند، صحت پردازشگر تأیید می شود. بخشی از این فرایند مربوط به ایجاد یک کلید کنفرانس(۱۶) بین مشتری و پردازشگر است که برای مخفی کردن هر نوع اطلاعات تبادل شده بین این دو است.. در اینجا به سه وضعیت اشاره شده است :

هنوز کنفرانسی نداریم که بین مشتری و پردازشگر ایجاد کنیم.

کنفرانسی ایجاد شده،اما خاتمه یافته است و درباره راه اندازی می شود . این کار برای حذف موارد غیر ضروری صورت می گیرد.

پردازشگر می خواهد مشتری را در طی کنفرانس ایجاد شده تأیید نماید.

پروتکل دستیSSL

۱/۱ ایجاد کنفرانس بین مشتری و پردازشگر

۱/۱/۱ مشتری پیغامی را برای پردازشگرمی فرستد. مخفی ماندن پیغام باید از طرف مشتری صورت پذیر.

۱/۱/۲ پردازشگر با پیغامی پاسخ می دهد. این پیام شامل یک سری ارتباط است که هر کدام به پردازشگر متصل، و همچنین گواهی کلید عمومی و مرزهای پردازشگر می باشد.

۱/۱/۳ مشتری حالا یک کلید اصلی را به وجود می آورد، و از یک رمز انتخاب شده از رمزهای کددار پردازشگر استفاده می کند. کلید اصلی دردو قسمت ایجاد شده است.

از کلید اصلی، درخواست به پردازشگر در مرحلهٔ ۱/۱/۱ فرستاده می شود؛ همچنین ارتباط متقابل از پردازشگر در مرحلهٔ ۱/۱/۲ در یافت گردد. مشتری دو کلید خصوصی برای مخفی کردن ایجاد می کند و در طی این مدت، اجلاس کنفرانس توسط پردازشگر(کلیدهای کنفرانس) به وجود می آید. یکی از این کلید ها کلید "نوشتن – مشتری" نامیده می شود و برای مخفی کردن داده هایی که به پردازشگر فرستاده می شود، استفاده خواهد شد. کلید دیگر کلید "خواندن – مشتری" نامیده می شود و برای آشکار کردن داده های دریافتی از پردازشگر استفاده خواهد شد. کلید اصلی و نیز کلید کنفرانس در بخش ذخیره سازی مشتری ذخیره می شوند.

۱/۱/۴ پردازشگر دو قسمت کلید اصلی را دریافت می کند، از قسمت مخفی و آشکار شده توسط کلید مخفی و کلید اصلی استفاده می شود. با استفاده از روش مشابه چون مشتری، پردازشگر نیز دو کلید ایجاد میکند که شبیه کلید مشتری است. یکی از این کلیدها، کلید "نوشتن پردازشگر" نامیده می شود و شبیه کلید "خواندن – مشتری" است. این دو کلید همچنین کلیدهای اصلی ذخیره شده هستند. حالا پردازشگر در انتظار اتمام پیام از طرف مشتری است.

۱/۱/۵ مشتری از طریق کلید "نوشتن مشتری" ارتباطی را که با پردازشگر برقرار نموده آشکار می سازد و پیام پایان صحبت مشتری را به پردازشگر می فرستد.

۱/۱/۶ پردازشگر در این حالت خواست های مشتری را که در مرحلهٔ ۱/۱/۱ فرستاده شده از طریق کلید "نوشتن پردازشگر" مخفی نگاه می دارد و آن را از طریق پیام تأیید پردازشگر برای مشتی می فرستد.

۱/۱/۷ مشتری داده های دریافت شده از طریق کلید "خواندن- مشتری" را آشکار می کند و مندرجات را با پیام اصلی فرستاده شده، مقایسه می کند.

۱/۱/۸ حالا پردازشگر، کنفرانس دیگری علاوه بر کنفرانس قبلی ایجاد می کند. مکان کنفرانس ایجاد شده در بایگانی است و کنفرانس جدید در قسمت کلید "خواندن – پردازشگر" نگه داشته می شود.

۱/۱/۹ با دریافت بازیابی کنفرانس از سوی مشتری، وی آن را در قسمت بایگانی ذخیره می کند. وقتی مشتری و پردازشگر پیام پایان را می فرستند، پروتکل دستی SSL اجرا می شود و می توان پروتکل کاربردی را اجرا و شروع کرد.

۱/۲- استفاده از یک کنفرانس ایجاد شده بین مشتری و پردازشگر
در این حالت، پردازشگر توسط مشتری تأیید شده؛ پردازشگر نیز می خواهد مشتری را دوباره تأیید کند. ممکن است یک کنفرانس، با یک کنفرانس مشابه(۱۷) باشد، کنفرانسی که در ابتدا ایجاد شده وبرای کارهای مختلفی استفاده می شود، تمام شده، و گاه مجدداً توسط مشتری استفاده خواهد شد.
۱/۲/۱ مشتری پیام خود را به پردازشگر می فرستد، که شامل یک دعوت و توافق قبلی برای کنفرانس مشابه می باشد [و از آن طرف پردازشگر جواب مشتری را می دهد.]
۱/۲/۲ پردازشگر پیام "سلام- پردازشگر" را بازگشت می دهد، و شامل "ارتباط مشابه"(۱۸) است که در ۱/۱/۲ نیز توصیف شده. اگر کنفرانس مشابهی توسط مشتری ارائه شده باشد، همچنین نحوهٔ "ایجاد کنفرانس مشابه" برای پردازشگر شناخته شده است. محتویات با استفاده از طریق کلید "نوشتن- پردازشگر" مخفی شده است. اگر کنفرانس مشابه برای پردازشگر شناخته نشده باشد، به مرحله ۱/۱/۲ برمی گردیم.
۱/۲/۳ مشتری ارتباط برقرار شده با پردازشگر را در مرحلهٔ ۱/۲/۱ مخفی می سازد و از طریق کلید "نوشتن- مشتری" استفاده می کند و پیام "پایان – مشتری" به پردازشگر فرستاده می شود.
۱/۲/۴ پردازشگر پیام مشتری را مخفی می سازد، و از کلید "نوشتن پردازشگر" استفاده می کند و آن را با استفاده از پیام "تأیید پردازشگر" برای مشتری می فرستد.
۱/۲/۵ مشتری داده های دریافت شده را از طریق کلید "خواندن- مشتری" آشکار می کند و آن را با محتویات پیام اصلی فرستاده شده مقایسه می کند.
۱/۲/۶ پردازشگر دوباره کنفرانس ایجاد شده را از طریق کلید "نوشتن- مشتری" آشکار می کند، و آن را از طریق کلید پیام "پایان- پردازشگر" برای مشتری می فرستد.
مشتری و پردازشگر هر دو پیام پایان را می فرستند، پروتکل دستی انجام می شود، و پروتکل کاربردی دوباره می تواند اجرا و استفاده شود. کلید کنفرانس برای توده ای از پیام های مخفی شدخ ایجاد شده است.

استفاده از کنفرانس ایجاد شده بین مشتری و پردازشگر و ملزم کردن مشتری به رعایت علائم، چنانچه کلید عمومی/ خصوصی در اختیار دارد.
در زمان ایجاد مجدد یک کنفرانس که در بالا توصیف شده، پردازشگر می تواند از مشتری بخواهد که با استفاده از کلید رمز مشتری، اگر چنین کلیدی را در اختیار داشته باشد، خود را تأیید کند.

۱/۲ بعد از مرحلهٔ ۱/۲/۳، پردازشگر می تواند پیام "تأیید درخواست" را اعلام کند. پیام شامل بعضی داده های درخواستی است و درخواست های مشتری به طور مناسب به پردازشگر ارائه می شود.
۲/۲ مشتری دهده های دریافت شده از پردازشگر را با کلید خصوصی مشخص می کند و آن را به شکل های مشخص شده همراه با یک نسخه از موارد تأیید شده خودش می فرستد، و از پیام "تأیید مشتری" استفاده می کند.
۲/۳ پردازشگر مشتری را با آشکار کردن داده های تعیین شده از طریق کلید عمومی مشتری، بازیابی و تأیید می کند.

پروتکل ثبت شده SSL(۱۹)

داده های SSL همچنین در طی فرآیند دستی نیز در قالب موارد ثبت شدهٔ(۲۰) SSL فرستاده می شود. ملید داده های ثبت شده به طور مکانیزه با شماره ترتیب خاصی، همزمان بین مشتری و پردازشگر ارائه می شود. حفاظت صحیح از داده ها، کلاً داده های ثبت شده به طور خودکار با نشانهٔ تأیید پیام(۲۱) ارائه می شوند. بیش تراستفاده کنندگان WWW از SSL با خبرند، بدین معنی که ترافیک WWW می تواند به طور همزمان توسط SSL تأمین شود.

پروتکل انتقال مطمئن فرامتنی

اگر WWW به عنوان ابزار بازاریابی معرفی شود، که بیش تر بر تحویل انتخابی اطلاعات مورد نیاز کنترل دارد، SHTTP نیز به عنوان ابزار دستیابی در نظر گرفته می شود. پروتکل مطمئن فرامتمی می تواند امنیت انتقال اسناد شخصی را به روش های گوناگون تأمین کند، زیرا سطوح امنیتی مختلفی در آن به کار بده شده است. بنابراین، کاربرد آن به صورت کنترل کامل بر روی خدماتی است که برای اسناد خاص کاربرد دارد. پس SHTTP اسناد شخصی را مانند علائم خصوصی و غیره مشخص می کند . SHTTP توسعه یافته از HTTP، و پروتکلی است که برای ارتباط از طریق WWW از آن استفاده می شود. توسعه HTTP باعث می شود تا امنیت بیش تری برای پیام ها از طریق WWW تأمین شود. SHTTP دامنهٔ وسیعی از روند امنیت موجود برای پردازشگر های HTTP و مشتریان فراهم می کند و حتی به مشتریان و پردازشگر اجازه می دهد تا روندی را که برای امنیت ارتباطاتشان می خواهند دقیقاً انجام دهند. سرویس های امنیتی ارائه شده توسط SHTTP عبارت اند از:

محرمانه(۲۲)

درستی(۲۳)

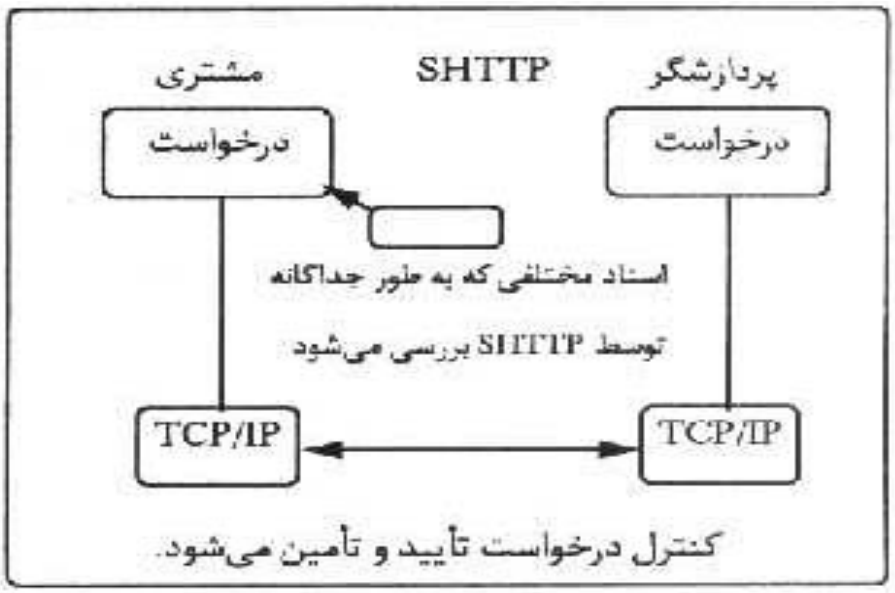
انسجام(۲۴)

غیر قابل انتشار(۲۵)

امنیت مجدد(۲۶)

این سرویس ها به نام "تقویت های خصوصی"(۲۷) در SHTTP نامیده می شوند. ما در مورد روندهای آن نمی خواهیم به طور جزئی بحث کنیم، اما می توان بر عملکرد و توصیف سطح بالایی

از وضعیت SHTTP پرداخت . SHTTP در سطوح کاربردی اجرا می شود. بدین معنی که کنترل کاربردی برروی مسائل امنیتی که باید استفاده شود، وجود دارد. استفاده از SHTTP برای هر رکود، و بازیابی آن با آگاهی پردازشگر می تواند از طریق مختلف انجام شود. بنابراین طراح باید عملکردهای امنیتی، همچنین قسمتی از طرح و کاربرد آن را به روش های مختلف و به طور خاص به کار گیرد. شکل ۵ این مسئله را به تصویر کشیده است.



شکل ۵. پروتکل انتقال مطمئن فرامتنی

SHTTP استفاده ازکلید عمومی را به صورت مخفی فراهم میکند. هر پردازشگر حداقل یک جفت کلید عمومی و خصوصی دارد. مالکیت های متفاوتی برای پردازشگر وجود دارند؛ پردازشگر ممکن است یک جفت کلید عمومی و خصوصی برای هر شخص داشته باشد. گرچه امکان دارد مشتریان یک جفت کلید خصوصی/ عمومی داشته باشند و SHTTP می تواند یک جفت کلید در اختیار داشته باشد، کلیدهای مشتری ضروری نیستند. SHTTP شکل مرکب و کامل را ترجیح می دهد؛ به خاطر این که بیش ترین اختیارهای قابل دسترس در پروتکل در نظر گرفته شده است. سعی داریم به طرق مختلف این اختیارها را هدایت کنیم تا دیدگاه تقریبا" کاملی به دست آوریم. سعی شده با مثالی، ساده ترین راه عملکرد SHTTP و استفاده از آن توضیح داده شود. اجازه دهید با ارجاع HTML شروع کنیم، که وضعیت های مطمئن SHTTP را به صفحهٔ رجوع شده افزایش می دهد.

نمونه ای از معاملهٔ SHTTP

۱/۱ درخواست

مشتری با صفحهٔ HTML مواجه می شود. در صفحهٔ HTML چندین ابر پیوند(۲۸) ممکن است ظاهر شود که احتمالاً به اسنادی که به افراد مختلف تعلق دارد، ارجاع می هد. ابر پیوند ها از SHTTP برای نشان دادن //:shttp به جای //:http استفاده می کنند، و به مشتری نشان می دهند که پردازشگر از ارجاعات خاص او آگاه است. با هر ابر پیوند //:Shttp؛ دو پشتیبان مناسب دیگر ارتباطی به وجود می آید:

گروه cryptopts، اطلاعاتی در مورد الگوریتم های استفاده شده، همچنین افزایش اطلاعات خصوصی را شامل می شود. افزایش اطلاعات خصوصی و خاص، در عمل با پردازشگری که بتواند ابر پیوند خاصی را ارجاع دهد در ارتباط می باشد. و همچنین به وسیلهٔ ابر پیوند به صفحهٔ مورد نظر ارجاع می دهد.

نام تفکیک شدهٔ (DN)(۲۹) از مواردی است که پردازشگر برای افزایش موارد خصوصی بدان نیاز دارد. ممکن است تفاوتی بین اسناد شخصی بر روی پردازشگر وجود داشته باشد، و هر شخصی با نام مجزا، اسنادی خواهد داشت.

صفحهٔ HTML همچنین کلید عمومی است که تمام DNهای با //:shttp مشخص شده در آن صفحه را تأیید می کند. اکنون مشتری درخواست HTTP را ایجاد کرده تا صفحهٔ مورد نظر بازیابی شود و نیازهای خصوصی به طور خاص در بالا مخفی می شود؛ مشتری کلید DES را اجرا می کند و درخواستش به وسیلهٔ کلید DES مخفی می شود و کلید DES با کلید عمومی بازیابی شده DN ها در صفحهٔ HTML ظاهر می گردد. سرایندهای(۳۰) SHTTP با یکدیگر جمع می شوند تا درخواست و اطلاعات مشخص شده در مورد فلورچارت های استفاده شده به وسیلهٔ مشتری و شکلی از درخواست مخفی نگه داشته شود. پیام SHTTP برمی گردد و برای مشتری ارسال می شود. تاکنون عملکردهای مشتری برای تقویت امنیت و اطمینان بوده است. بنابراین توسط تقویت های امنیتی مطوئن از ابر پیوند //:shttp انتخاب و اداره می شود.

۱/۲ عملکردهای پردازشگر

پردازشگر از اطلاعات سرآینده های SHTTP برای یافتن کلید خصوصی که قبلاً توسط مشتری نگهداری می شده و از این کلید برای باریابی درخواست های مشتری استفاده می کند. حالا پردازشگر اسناد خاص مورد درخواست را باریابی می کند. عملکردهای امنیتی پردازشگر بستگی به این دارد که بر حسب انتخاب ابر پیوند چگونه اطلاعات را به مشتری تحویل دهد. و فایل ثابت، یک فایل پیکربندی امنیتی محلی داردکه در هر کدام، عملکردهای پردازشگر بر حسب تحویل نتایج به مشتری، معین و معلوم شده اند. هر برنامهٔ CGL(۳۱) یک سرآیند خصوصی را شامل می شود که عملکردهای آن به وسیله پردازشگر برای تحویل نتایج به مشتری تعریف و معین شده اند. فرض کنید مشتری یک صفحه ثابت را انتخاب می کند. پردازشگر فایل پیکربندی محلی را وارسی می نماید و اگر مخفی کردن آن مورد نیاز باشد از طریق کلید کنفرانس توسط مشتری انجام می شود. این کار توسط سرآیندهای SHTTP صورت می گیرد.

۱/۳ عملکردهای مشتری

با استفاده از اطلاعات سرآیندهای SHTTP،و کلید DES مشتری می تواند اسناد موردنیاز HTML را مخفی می کند. فرض کنید برای بازیابی یک صفحه، یک ابر پیوند بر روی پردازشگر وجود دارد. برای این کار باید درخواست مشتری به صورت امضای رقومی، قبل از فرستادن بر روی پردازشگر صورت گیرد. در این حالت مشتری درخواست را همراه با کلید خصوصی امضا می کند؛ در غیر این صورت کار انجام نمی شود. فرض کنید مشتری آن را امضا کرده؛ با استفاده از سرآیندهای مختلف SHTTP اطلاعات به صورت نمودار به کار برده می شود و کلید عمومی مشترک با پیام همراه و به پردازشگر فرستاده می شود. در این روش هر صفحه یا درخواست را می توان به روش های گوناگون بررسی کرد. تأکید بیش تر بر امنیت مورد نیاز برای صفحهٔ خاص است.

مرحلهٔ سه

در این مرحله مؤسسه شروع به استفاده از اینترنت و WWW برای خرید الکترونیکی در یک محیط بسته می نماید؛ در اینجا مشتری باید یادداشت کند، و معامله ها فقط با پذیرش انجام خواهد شد. چون پرداخت در این مرحله صورت می گیرد، مؤسسات مالی و کارت های اعتباری مؤسسات از قسمت های ضروری این محیط است. پرداخت در این مرحله معمولاً دستی و به وسیلهٔ تولیدکنندگان موجود انجام می شود. مشتریان بالقوه باید توسط مؤسسه پذیرش شوند، و تهیه الکترونیکی فقط برای مشتریان از قبل پذیرش شده امکان پذیر است. شناسایی و صحت مشتری از طریق کلمه عبور مشترک بین مشتری و مؤسسه صورت می گیرد.

مرحلهٔ چهار

در این مرحله خرید الکترونیکی به صورت باز صورت می گیرد و معامله ها را می توان به وسیله مشتریان حاضر و شمارهٔ کارت اعتباری آنها صورت داد. در این محیط اطلاعات لازم درباره مشتری در مؤسسه موجود است و مؤسسه به مشتری اجازه می دهد که به صورت ناشناخته خرید الکترونیکی را انجام دهد. همچنین مؤسسه می خواهد از صحت مشتری خود و شمارهٔ کارت اعتباری وی اطمینان حاصل کند تا از کارت اعتباری به صورت صحیح و مستند در معامله استفاده شود. خطرات امنیتی این محیط، نیز بیش از دیگر محیط ها است و بیش تر، پروتکل های پیشرفته مورد نیاز است. همچنین دو پروتکل عمده و مهم در این حوزه وجود دارند: یکی STT(۳۲) که برای همکاری بین مایکروسافت و وزیرا(۳۳) به کار گرفته شده، دیگری SEPP(۳۴) که توسط IBMو Mastercard و تعدادی دیگر به وجود آورده است. در این بخش SEPP بررسی خواهد شد، پروتکلی که به طور ساده گسترش پذیر است و بیش تر جنبه های مهم آن مورد بحث و بررسی قرار می گیرند. عوامل زیر در این مسئله نقش فعالی دارند:

صاحب کارت (مشتری بالقوه)(۳۵)

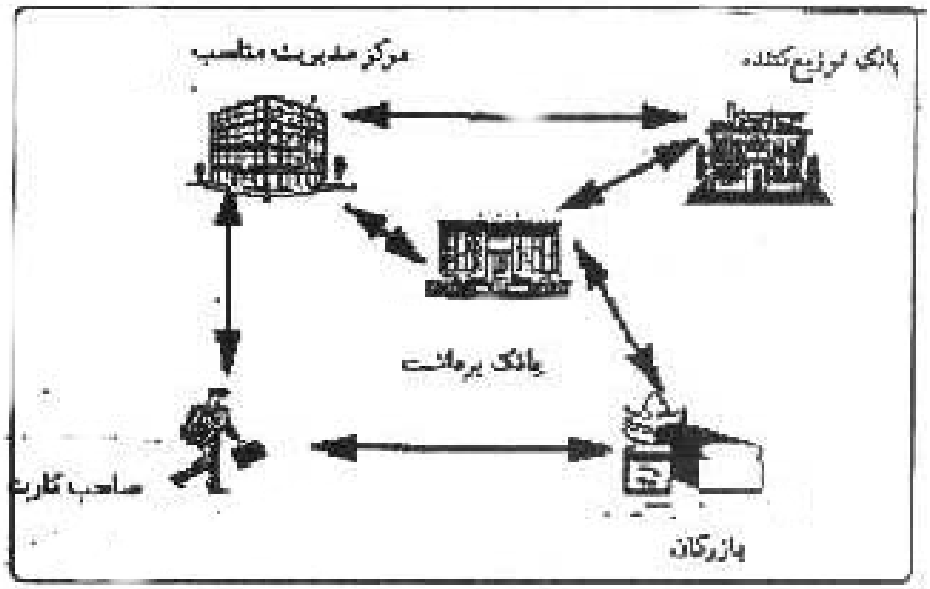
بازرگان(۳۶)

بانک برداشت(۳۷)

بانک توزیع کننده(۳۸)

سیستم مدیریت مناسب(۳۹)

تصویر شمارهٔ ۶ رابطه این قسمت ها را به تصویر کشیده است.



فرض کنید که صاحب کارت مرحلهٔ مذاکره را به طور کامل انجام داده و مرحلهٔ تورق را نیز انجام می دهد و احتمالاً بعد از مذاکره با بازرگان تصمیم دارد مرحلهٔ خرید و پرداخت را انجام دهد. SEPP مرحلهٔ خرید و پرداخت را مشخص می کند.

پیام یک

اولین پیام، پیام آغازین است که از طرف صاحب کارت بخ بازرگان فرستاده می شود. این پیام خریدار و مارک مشابهی از کارت اعتباری ارائه شده را شامل می شود.

پیام دو

اکنون بازرگان پیامی را که شامل اطلاعات در بارهٔ قیمت کالاها و امضای رقومی است با کلید خصوصی خودش ایجاد می کند. این مسئله بازرگان را نسبت به کالاهای توافق شده و قیمت آن ها متعهد می نماید که او در مراحل بعدی نمی تواند هیچ کدام را انکار کند. این پیام به صورتحساب صاحب کارت ارسال می شود.

پیام سه

اکنون صاحب کارت محتویاتی از پیام صورتحساب را از طریق پیدا کردن محتویات استفاده شدهٔ کلید عمومی بازرگان وارسی می کند.

اگر این کار موفقیت آمیز و درست باشد، بازرگان و تعهدات آن را نسبت به کالاها و قیمت خاص آن تأیید می شود. صاحب کارت اکنون پیام "درخواست- سفارش- خرید" را ایجاد می کند که شامل موارد زیر است:

اطلاعاتی دربارۀ قیمت کالاهای توافق شده و شمارۀ کارت اعتباری و تاریخ انقضا، که توسط کلید عمومی برداشت کننده مخفی نگه داشته می شود/ این مرحله را M1 می نامیم. این بدین معنی است که بازرگان نمی تواند شمارۀ کارت اعتباری و تاریخ انقضا را پیدا کند، همچنین اطلاعات کالاها و قیمت آن ها را نمی تواند تغییر دهد.

کالاها و قیمت تمام شدۀ آن برای صاحب کارت از طریق کلید خصوصی به صورت رقومی مشخص شده است. این بدان معنی است که صاحب کارت نمی تواند سفارش قبلی خودش را برای کالاها و قیمت توافق شده انکار کند. در این مرحله پیام "در خواست- سفارش- خرید" به بازرگان فرستاه می شود.

پیام چهار

اکنون بازرگان پیام "درخواست تأیید" را ایجاد می کند و هر کدام برای برداشت کنندۀ فرستاده می شود تامعامله را تأیید کند. این پیام موارد زیر را شامل می شود:

M1 که در بالا توصیف شد.

اطلاعاتی در بارۀ کالاها و قیمت توافق شده و امضای رقومی توسط بازرگان. این مرخله را M2 می نامیم. اکنون برداشت کننده محتویاتی از M1 را بازیابی می کند و قیمت خرید که از طرف صاحب کارت ادعا شده برایش مشخص می شود. برداشت کننده همچنین محتویاتی از M2 را بازیابی می کند و قیمت فروش که بازرگان ادعا کرده برایش مشخص می شود. اگر چیزی مورد نیاز باشد، اکنون برداشت کننده درخواست تأیید از توزیع کننده دارد. برداشت کننده نشانۀ برگشتی تأیید شده را دریافت می کند.

پیام پنج

برداشت کننده اکنون پیام "پاسخ تأیید" را که شامل نشانۀ تأیید و امضای رقومی توسط برداشت کننده می باشد، ایجاد می کند. این پیام برای بازرگان فرستاده می شود.

پیام شش

اکنون بازرگان پیام "پاسخ- سفارش- خرید" را برای صاحب کارت می فرستد. این پیام شامل نشانۀ تأیید با امضای رقومی برداشت کننده می باشد. در این مرحله معامله به طور کامل و اصولی انجام می شود. پیام های دیگر به صورت تأییدهای مورد نیاز و وارسی شده و غیره مشخص شده اند، اما پیام های بالا موقعیتی را که به طور کامل تأیید شده باشد، توصیف می کند.

پی نوشت ها

1. **World wide web**
2. **Client**
3. **Server Registered**
4. **Registered**
5. **Unauthorised outsiders**
6. **Authenticate**
7. **Secure sockets layer (SSL)**
8. **Secure Hypertext transport protocol (SHTTP)**
9. **Digital wignatures**
10. **Document**
11. **Transmission control protocol/ Inernet protocol**
12. **Hypertext transport protocol (HTTP)**
13. **File transfer protocol (FTP)**
14. **Handshake protocol**
15. **Uniform resource locator (URL)**
16. **Session**
17. **Session- id**
18. **Connectioned**
19. **SSL Record protocol**
20. **Records**
21. **Message authentication code (MAC)**
22. **Confidentiality**
23. **Authenticity**
24. **Integrity**
25. **Non- repudiability**
26. **Replay- securing**
27. **privacy enhancements**
28. **Hyperlink**
29. **Distinguished Name**
30. **Headers**
31. **Common gateway onterface**
32. **Secure transaction technology protocol**
33. **Visa**
34. **Secure electronic payment protocol**
35. **Card holder (potential customer)**
36. **Merchant**
37. **Acquirer Bank**
38. **Issuer Bank**
39. **Certificate Management system**

منابع

1.Phleeger (1989) secyrity in computing, prentice hall
2.Refernce 1 http://www.Netscape.con/info/SSL.Html
3.Reference 2 http://www.Commerce.Net/information/standards/drafts/shttp.txt
4.Reference 3 http://www.Visa.com/visa-stt/stt-home.html
5.Reference 4 http://mastercark.com/sepptoc.htm