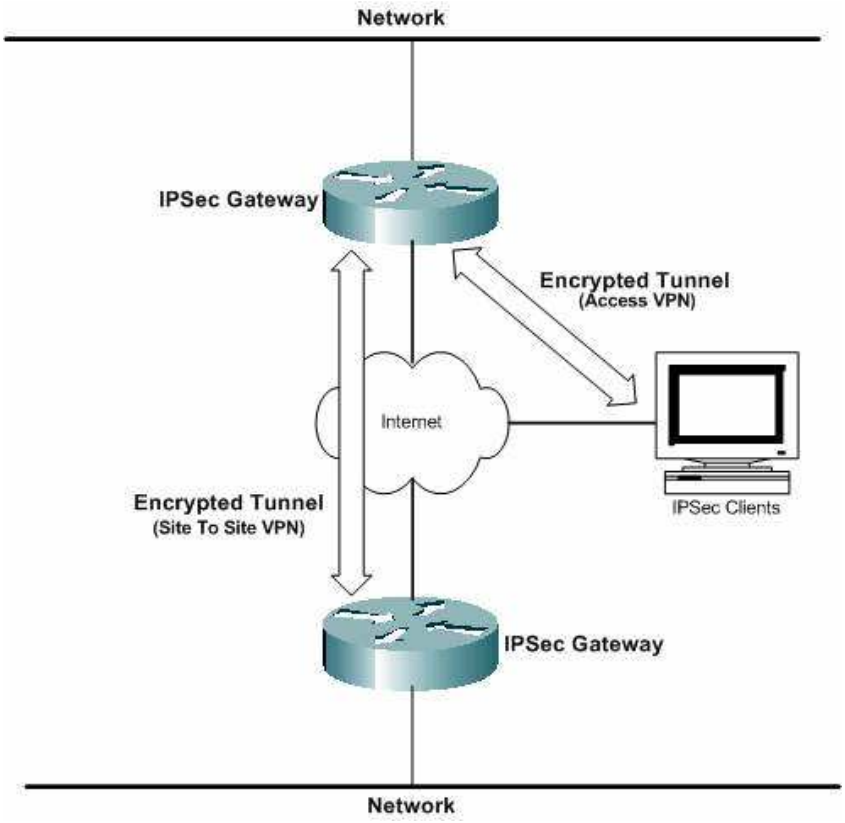
رمزنگاری در پروتکل‌های انتقال

تمرکز بیشتر روش‌های امنیت انتقال فایل بر اساس رمزنگاری دیتا در طول انتقال از طریق شبکه‌های عمومی مانند اینترنت است. دیتایی که در حال انتقال بین سازمانهاست بوضوح در معرض خطر ربوده شدن در هر کدام از محلها قرار دارد. – مثلا در شبکه‌های محلی برای هر یک از طرفین یا مرزهای Internet-LAN که سرویس‌دهندگان‌اینترنت از طریق آنها مسیر دیتا را تا مقصد نهایی مشخص می‌کنند. حساسیت دیتا ممکن است بسیار متغییر باشد، زیرا دیتای انتقالی ممکن است بهر شکلی از رکوردهای مالی بسته‌بندی شده تا تراکنش‌های مستقیم باشند. در بعضی موارد، ممکن است علاوه بر محافظت دیتا روی اینترنت، نیاز به محافظت دیتا روی LAN نیز باشد. مشخصاً، محافظت از دیتا در مقابل حملات LAN مستلزم رمزنگاری دیتای انتقالی روی خود LAN است. به این ترتیب، بهرحال، نیاز به بسط امنیت تا برنامه‌هایی است که خود دیتا را تولید و مدیریت می‌کنند، و تنها اطمینان به راه‌حلهای محیطی کفایت نمی‌کند و به این ترتیب بر پیچیدگی مسأله امنیت افزوده می‌شود.

پروتکل‌ها

اگرچه ثابت‌شده است که رمزنگاری راه‌حل بدیهی مسائل محرمانگی است، اما سردرگمی در مورد دو نوع رمزنگاری (برنامه در مقابل شبکه) همچنان وجود دارد و بدلیل وجود پروتکلهای ارتباطی گوناگون است که نیازهای تعامل بیشتر آشکار می‌شود. (مانند IPSec ، S/MIME، SSL و TLS) اگرچه این پروتکلها قول تعامل را می‌دهند، اما تعامل کامل بدلیل مستقل بودن محصولات پروتکلها در حال حاضر وجود ندارد. آزمایشهایی در حال حاضر در حال انجام هستند که به حل شدن این مسائل کمک می‌کنند، اما کاربران باید مطمئن شوند که تعامل بین محصول انتخابیشان و محصولات سایر شرکای تجاری امری تثبیت شده است. پروتکل‌های ساده‌تر (SSL/TLS، IPSec و تا حدی پایین‌تر S/MIME) عموماً مسائل کمتری از نظر تعامل دارند.



پروتکل‌های رمزنگاری انتقال

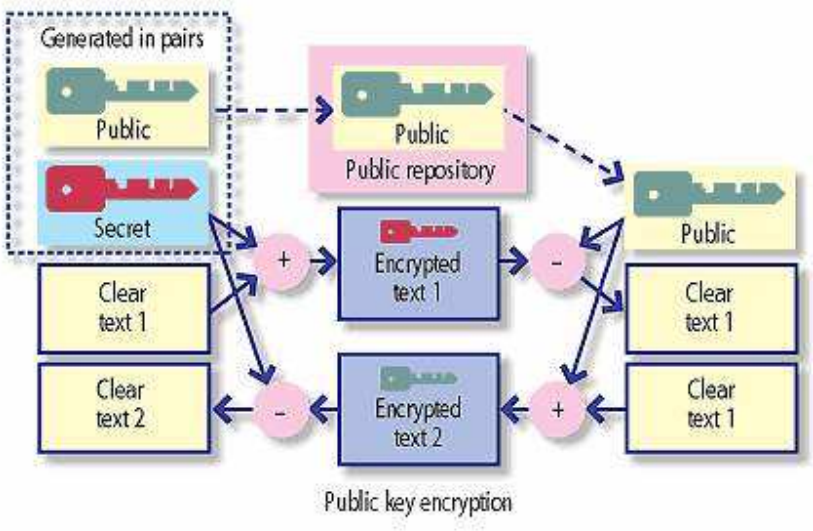
با ترکیب توانایی‌ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه‌های امنیت را فراهم می‌کنند. تقریباً تمام پروتکلها نیازهای جامعیت را پشتیبانی می‌کنند به طوری که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آنها از Non-Repudiation پشتیبانی نمی‌کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند می‌دهند، ندارند.

به این چند پروتکل به طور مختصر اشاره می‌شود:

SSL

تکنولوژی SSL (Secure Socket Layer) اساس World Wide Web امن را تشکیل می‌دهد. SSL که در مرورگرهای وب کاملاً جاافتاده است، توسط بسیاری از سازمانها برای رمزنگاری تراکنش‌های وبی خود و انتقال فایل استفاده می‌شود. بعلاوه SSLبصورت روزافزون بعنوان یک مکانیسم امنیت در تلاقی با پروتکلهای پرشمار دیگر استفاده می‌شود و بهمین ترتیب ابزاری برای ارتباط سروربه‌سرور امن است. SSL ارتباطات رمزشده و بشکل آغازین خود تایید هویت سرور از طریق استفاده از گواهی را (در حالت کلاینت‌به‌سرور) پشتیبانی می‌کند. کاربران اغلب برای استفاده از برنامه‌ها از طریق کلمه عبور تایید هویت می‌شوند، و با پیشرفت SSL استاندارد (مثلا SSL V.3.0) تایید هویت کلاینت از طریق گواهی به این پروتکل اضافه شده است.

***برای FT (انتقال فایل):** ابزار FT اغلب از SSL برای انتقال فایل در یکی از دو حالت استفاده می‌کنند. اولی، مد کلاینت‌به‌سرور است که کاربر را قادر می‌سازد، در حالیکه در حال استفاده از یک مرورگر وب استاندارد است مستندات را از یک سرور دریافت یا آنها را به سرور منتقل کند. که این قابلیت نیاز به نرم‌افزار مختص انتقال در کلاینت را برطرف می‌سازد و بسیار راحت است، اما اغلب فاقد بعضی ویژگیهای پیشرفته مانند نقاط آغاز مجدد و انتقالهای زمانبندی‌شده است که سازمانها نیاز دارند. SSL همچنین می‌تواند برای اتصالات سروربه‌سرور امن – برای مثال، در اتصال با FTP و سایر پروتکلها – مورد استفاده قرار گیرد.



TLS

TLS (Transport Layer Security)، جانشین SSL، برپایه SSL3.0 بنا شده است، اما به کاربران یک انتخاب کلید عمومی و الگوریتمهای Hashing می‌دهد. (الگوریتمهای Hashing فانکشن‌های یک‌طرفه‌ای برای حفظ جامعیت پیامها هستند و توسط بیشتر پروتکلها استفاده می‌شوند.) اگرچه TLS و SSL تعامل ندارند، اما چنانچه یکی از طرفین ارتباط TLSرا پشتیبانی نکند، ارتباط با پروتکل SSL3.0 برقرار خواهد شد. بیشتر مزایا و معایب SSL به TLS هم منتقل می‌شود، و معمولا وجه تمایز خاصی وجود ندارد، و از همه نسخه‌ها به عنوان SSL یاد می‌شود.

S/MIME

S/MIME (Secure Multipurpose Internet Mail Extention) که اختصاصاً برای پیام‌رسانی ذخیره-و-ارسال طراحی شده است، بعنوان استاندارد امنیت ایمیل برتر شناخته شده است. مانند بیشتر پروتکل‌های رمزنگاری

(مثلا SSL ، TLS و IPSec)،S/MIME با رمزنگاری تنها سروکار ندارد. بهرحال، علاوه بر تصدیق هویت کاربران و ایمن‌سازی جامعیت پیامها (برای مثال مانند آنچه SSL انجام می‌دهد)، S/MIME توسط امضای دیجیتال، رکوردهای پایداری از صحت پیامها ایجاد می‌کند (ضمانت هویت فرستنده چنانچه به محتوای پیام مشخصی مرتبط شده). این عمل باعث می‌شود فرستنده پیام نتواند ارسال آن‌را انکار کند.

***برای FT :**

سیستم‌های ایمیل رمزشده (با استفاده از S/MIME) می‌توانند برای ارسال فایل‌های کوچک استفاده شوند (محدودیت حجم فایل بخاطر داشتن محدودیت حجم فایل در بیشتر سرورهای ایمیل است)، ولی S/MIME کلاً می‌تواند برای انتقال فایل‌های بزرگتر توسط پروتکلهای انتقال فایل استفاده شود.

SSH

SSH (Secure Shell) هم یک برنامه و یک پروتکل شبکه بمنظور وارد شدن و اجرای فرمانهایی در یک کامپیوتر دیگر است. به این منظور ایجاد شد تا یک جایگزین رمزشده امن برای دسترسی‌های ناامن به کامپیوترهای دیگر مثلا rlogin یا telnetباشد. نسخه بعدی این پروتکل تحت نام SSH2 با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک‌های SSH منتشر شد.

***برای FT :**

SSH می تواند برای پشتیبانی انتقال فایل رمزشده (به شکل SFTP) استفاده شود اما طبیعت خط فرمان بودن آن به این معنی است که بیشتر توسط مدیران سیستمها برای ارسال درون سازمان استفاده می‌شود تا برای انتقال فایل تجاری. بعلاوه استفاده از SSH نیاز به نرم‌افزار یا سیستم عاملهای سازگار با SSH در دو طرف اتصال دارد، که به این ترتیب SSH برای سروربه‌سرور انجام می‌گیرد.