مجاز امکان پذیر نبوده و صرفا" افرادیکه دارای کلید رمز می باشند، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند.

رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمز نگاری است. استفاده از علم رمز نگاری دارای یک سابقه طولانی و تاریخی است. قبل از عصر اطلاعات، بیشترین کاربران رمزنگاری اطلاعات، دولت ها و مخصوصا" در موارد نظامی بوده است. سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می گردد. امروزه اغلب روش ها و مدل های رمزنگاری اطلاعات در رابطه با کامپیوتر بخدمت گرفته می شود. کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت.

اکثر سیستم های رمزنگاری اطلاعات در کامپیوتر به دو گروه عمده زیرتقسیم می گردند:

- رمزنگاری کلید – متقارن
- رمزنگاری کلید – عمومی

رمز نگاری کلید – متقارن

در روش فوق، هر کامپیوتر دارای یک کلید رمز (کد) بوده که از آن برای رمزنگاری یک بسته اطلاعاتی قبل از ارسال اطلاعات برروی شبکه و یا کامپیوتر دیگر،استفاده می نماید. دراین روش لازم است در ابتدا مشخص گردد که کدامیک از کامپیوترها قصد مبادله اطلاعاتی با یکدیگر را دارند، پس از مشخص شدن هر یک از کامپیوترها، در ادامه کلید رمز بر روی هر یک از سیستم ها می بایست نصب گردد. اطلاعات ارسالی توسط کامپیوترهای فرستنده با استفاده از کلید رمز، رمز نگاری شده وسپس اطلاعات رمز شده ارسال خواهند شد. پس از دریافت اطلاعات رمز شده توسط کامپیوترهای گیرنده،با استفاده از کلید رمز اقدام به بازگشائی رمز و برگرداندن اطلاعات بصورت اولیه و قابل استفاده خواهد شد. مثلا" فرض کنید پیامی را برای یکی از دوستان

خود رمز و سپس ارسال می نمائید. شما برای رمز نگاری اطلاعات از روشی استفاده نموده اید که بر اساس آن هر یک از حروف موجود در متن پیام را به دو حرف بعد از خود تبدیل کرده اید. مثلا" حروف A موجود در متن پیام به حروف C و حروف B به حروف D تبدیل می گردند.

پس از ارسال پیام رمز شده برای دوست خود، می بایست با استفاده از یک روش ایمن و مطمئن کلید رمز را نیز برای وی مشخص کرد. در صورتیکه گیرنده پیام دارای کلید رمز مناسب نباشد، قادر به رمز گشائی و استفاده از اطلاعات نخواهد بود. در چنین حالتی می بایست به دوست خود متذکر گردید که کلید رمز، " شیفت دادن هر حرف بسمت جلو و به اندازه دو واحد است". گیرنده پیام با انجام عملیات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود.

رمزنگاری کلید – عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" متعلق به کامپیوتر فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهائی که قصد برقراری ارتباط با یکدیگر را دارند، گذاشته می شود. برای رمزگشائی یک پیام رمز شده، کامپیوتر می بایست از کلید عمومی که توسط فرستنده ارائه شده، بهمراه کلید خصوصی خود استفاده نماید. یکی از متداولترین برنامه های رمزنگاری در این رابطه(**PGP**(Pretty Good Privacy است. با استفاده از PGP می توان هر چیز دلخواه را رمز نمود.

بمنظور پیاده سازی رمزنگاری کلید، عمومی در مقیاس بالا نظیر یک سرویس دهنده وب، لازم است از رویکردهای دیگری در این خصوص استفاده گردد." امضای دیجیتال" یکی از رویکردهای موجود در این زمینه است، یک امضای دیجیتالی صرفا" شامل اطلاعات محدودی بوده که اعلام می نماید، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام "امضای مجاز"، امین اطلاعات است. "امضای مجاز" بعنوان یک میانجی بین دو کامپیوتر ایفای وظیف می نماید. هویت و مجاز بودن هر یک از کامپیوترها

برای برقراری ارتباط توسط سرویس دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.

یکی از متداولترین نمونه های پیاده سازی شده از رمزنگاری کلید- عمومی، روش **SSL**(Secure Sokets Layer) است. روش فوق در ابتدا توسط "نت اسکیپ" پیاده سازی گردید. SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب بمنظور ارسال اطلاعات حساس، استفاده می گردد. SSL اخیرا" بعنوان بخشی از پروتکل **TLS**(Transport Layer Security) در نظر گرفته شده است.

در مرورگر می توان زمان استفاده از یک پروتکل ایمن نظیر TLS را با استفاده از روش های متعدد اعلام کرد. استفاده از پروتکل "https" درعوض پروتکل "http" یکی از روش های موجود است. در چنین مواردی در بخش وضعیت پنجره مرورگر یک "Padlock" نشان داده خواهد شد.

رمزنگاری کلید - عمومی، مدت زمان زیادی را صرف انجام محاسبات می نماید. بنابراین در اکثر سیستمها از ترکیب کلید عمومی و متقارن استفاده می گردد. زمانیکه دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می نمایند، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید – عمـومی، ارسال خواهد کرد. در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگاری کلید متقارن می باشند. پس از اتمام ارتباط، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد، می بایست مجددا" فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن ، ...)

مقدار Hash

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash، استوار است. مقدار فوق، بر اساس یک مقدار ورودی که دراختیار الگوریتم hashing گذاشته می گردد، ایجاد می گردد. در حقیقت مقدار hash ، فرم خلاصه شده ای از مقدار اولیه ای خود است. بدون آگاهی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید بنظر می رسد. مثال زیر نمونه ای در این زمینه را نشان می دهد:

عدد ورودی	الگوریتم	مقدار Hash
10,667	Input # x 143	1,525,381

تسخیص اینکه عدد ۱،۵۲۵،۳۸۱ (مقدار hash) از ضرب دو عدد ۱۰،٦٦۷ و ۱٤۳ بدست آمده است، کار بسیار مشکلی است. در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است، تشخیص عدد دوم کار بسیار ساده ای خواهد بود. (عدد ۱۰،٦٦۷). رمز نگاری مبتنی بر کلید عمومی بمراتب پیچیده تر از مثال فوق می باشند. مثال فوق صرفا" ایده اولیه در این خصوص را نشان می دهد. کلیدهای عمومی عموما" از الگوریتم های پیچیده و مقادیر Hash بسیار بزرگ برای رمزنگاری استفاده می نمایند. در چنین مواردی اغلب از اعداد ٤۰ و یا حتی ۱۲۸ بیتی استفاده می شود. یک عدد ۱۲۸ بیتی دارای $۲^{۱۲۸}$ حالت متفاوت است.

آیا شما معتبر هستید ؟

همانگونه که در ابتدای بخش فوق اشاره گردید، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر، در ابتدا رمز و سپس ارسال خواهند شد. کامپیوتر دوم (گیرنده)، پس از دریافت اطلاعات می بایست، اقدام به رمزگشائی آنان نماید. یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات

توسط یک منبع ایمن و مطمئن، استفاده از روش معروف" اعتبارسنجی"است. در صورتیکه اطلاعات "معتبر" باشند، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده اند. با ترکیب فرآیندهای رمزنگاری و اعتبار سنجی می توان یک محیط ایمن را ایجاد کرد.

بمنظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر روی یک کامپیوتر از روش های متعددی استفاده می شود:

- **رمز عبور** . استفاده از نام و رمز عبور برای کاربران، متداولترین روش "اعتبار سنجی" است . کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق، بررسی می گردند. در صورتیکه نام و یا رمز عبور نادرست باشند، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد.

- **کارت های عبور** . این نوع کارت ها دارای مدل های متفاوتی می باشند. کارت های دارای لایه مغناطیسی (مشابه کارت های اعتباری) و کارت های هوشمند (دارای یک تراشه کامپیوتر است) نمونه هائی از کارت های عبور می باشند.

- **امضای دیجتالی** . امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی (نظیر: نامه الکترونیکی، فایل های متنی و...) است. استاندارد امضای دیجیتالی (DSS)، بر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای دیجیتالی (DSA) ایجاد می گردد. الگوریتم فوق شامل یک کلید عمومی (شناخته شده توسط صاحب اولیه سند الکترونیکی – امضاء کننده) و یک کلید عمومی است. کلید عمومی دارای چهار بخش است. در صورتیکه هر چیزی پس از درج امضای دیجیتالی به

یک سند الکترونیکی، تغییر یابد، مقادیر مورد نظری که بر اساس آنها امضای دیجیتالی با آن مقایسه خواهد شد، نیز تغییر خواهند کرد.

سیستم های متعددی برای "اعتبار سنجی" تاکنون طراحی و عرضه شده است. اکثر سیستم های فوق از زیست سنجی برای تعیین اعتبار استفاده می نمایند. در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می گردد. برخی از روش های اعتبار سنجی مبتنی بر زیست شناسی کاربران، بشرح زیر می باشند:

- پیمایش اثر انگشت (انگشت نگاری)
- پیمایش شبکیه چشم
- پیمایش صورت
- مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است. می بایست این اطمینان بوجود آید که اطلاعات دریافت شده، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده اند. در این راستا از روش های متعددی استفاده می گردد:

- **Checksum** . یکی از قدیمی ترین روش های استفاده شده برای اطمینان از صحت ارسال اطلاعات است. Checksum، به دو صورت متفاوت محاسبه می گردد. فرض کنید Checksum یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن (صفر و یا یک) را می تواند داشته باشد. در چنین حالتی ۲۵٦ وضعیت متفاوت می تواند وجود داشته باشد. با توجه به اینکه در اولین وضعیت، تمام هشت بیت مقدار صفر را دارا خواهند بود، می تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، ۲۵۵ و یا کمتر باشد، مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، بیش از ۲۵۵ باشد، Checksum معادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵٦ تقسیم نمائیم. مثال زیر، عملکرد CheckSum را نشان می دهد.

Checksum	Total	Byte 8	Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1
127	1,151	80	179	15	244	135	54	232	212

- 1,151 / 256 = 4.496 (round to 4)
- 4 x 256 = 1,024
- 1,151 - 1,024 = 127

● CRC(Cyclic Redundancy Check). روش CRC در مفهوم مشابه روش Checksum است. روش فوق از تقسیم چند جمله ای برای مشخص کردن مقدار CRC استفاده می کند. طول CRC معمولا" ١٦ و یا ٣٢ بیت است. صحت عملکرد روش فوق بسیار بالا است. در صورتیکه صرفا" یک بیت نادرست باشد، CRC با مقدار مورد نظر مطابقت نخواهد کرد. روش های Checksum وCRC امکانات مناسبی برای پیشگیری از بروز خطای تصادفی درارسال اطلاعات می باشند، روش های فوق در رابطه با حفاظت اطلاعات و ایمن سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات، امکانات محدودتری را ارائه می نمایند. رمزنگاری متقارن و کلید عمومی، امکانات بمراتب مناسب تری در این زمینه می باشند.

بمنظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه های اختصاصی، از روش های متعدد ایمنی استفاده می گردد. ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر: تلفن، پست ایمن تر می باشد. برای تحقق امرفوق می بایست از روش های متعدد رمزنگاری و پروتکل های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه های کامپیوتری خصوصا" اینترنت استفاده کرد.

شکستن کلیدهای رمزنگاری

چه طول کلیدی در رمزنگاری مناسب است؟

امنیت هر الگوریتم مستقیماً به پیچیده بودن اصولی مربوط است که الگوریتم بر اساس آن بنا شده است. امنیت رمزنگاری بر اساس پنهان ماندن کلید است نه الگوریتم مورد استفاده. در حقیقت، با فرض اینکه که الگوریتم از قدرت کافی برخوردار است (یعنی که ضعف شناخته‌شده‌ای که بتوان برای نفوذ به الگوریتم استفاده کرد، وجود نداشته باشد) تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است.

در بیشتر انواع حمله، حمله‌کننده تمام کلیدهای ممکن را تولید و روی متن رمزشده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتمهای رمزنگاری در برابر این نوع حمله آسیب‌پذیر هستند، اما با استفاده از کلیدهای طولانی‌تر، می‌توان کار را برای حمله‌کننده مشکل‌تر کرد. هزینه امتحان کردن تمام کلیدهای ممکن با تعداد بیتهای استفاده شده در کلید بصورت نمایی اضافه می‌شود، و این در حالیست که انجام عملیات رمزنگاری و رمزگشایی بسیار کمتر افزایش می‌یابد.

الگوریتمهای متقارن

DES که یک الگوریتم کلید متقارن است معمولا از کلیدهای ۶۴ بیتی برای رمزنگاری و رمزگشایی استفاده می‌کند. الگوریتم متن اولیه را به بلوکهای ۶۴ بیتی می‌شکند و آنها را یکی‌یکی رمز می‌کند.

DES۳ الگوریتم پیشرفته‌تر است و در آن الگوریتم DES سه بار اعمال می‌شود (در مقاله رمزنگاری به آن اشاره شده است). نسخه دیگری از این الگوریتم (پایدارتر از قبلیها) از کلیدهای ۵۶بیتی و با فضای کلید موثر ۱۶۸بیت استفاده می‌کند و سه بار عملیات رمزنگاری را انجام می‌دهد.

جدول زیر زمان لازم برای یافتن کلید در الگوریتم DES را نشان میدهد.

طول کلید	تعداد کلیدهای ممکن	زمان مورد نیاز برای ۱ رمزگشایی در هر میلی‌ثانیه	زمان مورد نیاز برای ۱،۰۰۰،۰۰۰ رمزگشایی در هر میلی‌ثانیه
۳۲ بیت	$۲^{۳۲}$ = ۴/۳×$۱۰^{۹}$	۳۵/۸ دقیقه = $۲^{۳۱}$میلی‌ثانیه	۲/۱۵ میلی‌ثانیه
۵۶ بیت	$۲^{۵۶}$ = ۷/۲×$۱۰^{۱۶}$	۱۱۴۲ سال = $۲^{۵۵}$میلی‌ثانیه	۱۰ ساعت
۱۲۸ بیت	$۲^{۱۲۸}$ = ۳/۴×$۱۰^{۳۸}$	۵/۴×$۱۰^{۲۴}$ سال = $۲^{۱۲۷}$میلی‌ثانیه	۵/۴×$۱۰^{۱۸}$ سال
۱۶۸ بیت	$۲^{۱۶۸}$ = ۳/۷×$۱۰^{۵۰}$	۵/۹×$۱۰^{۳۶}$ سال = $۲^{۱۶۷}$میلی‌ثانیه	۵/۹×$۱۰^{۳۰}$ سال

ستون سوم مربوط به کامپیوترهایی است که می‌توانند در هر میلی‌ثانیه یک رمزگشایی را انجام دهند که برای کامپیوترهای امروزی توان محاسباتی معقولی محسوب می‌شود. ستون آخر برای سیستمهای بسیار بزرگ محاسباتی است بطوریکه قدرت پردازش یک میلیون برابر زیاد شده باشد. بدون در نظر گرفتن طول کلید، الگوریتمهای متقارن قوی نیز نمی‌توانند امنیت الگوریتمهای نامتقارن را داشته باشند، زیرا کلید باید بین دو طرف ارتباط مبادله شود.

الگوریتمهای نامتقارن

عموماً سیستمی امن محسوب می‌شود که هزینه شکستن آن بیشتر از ارزش دیتایی باشد که نگهداری می‌کند. اما در ذهن داشته باشید که با افزایش قدرت محاسباتی، سیستمهای رمزنگاری، آسانتر توسط روشهای سعی و خطا مورد حمله قرار خواهند گرفت.

برای مثال، طبق گزارشی از سایت RSA، تخمین زده می شود که یک کلید ۲۱۵ بیتی می تواند با هزینه ای کمتر از ۱ میلیون دلار و یک تلاش ۸ ماهه شکسته شود. RSA توصیه میکند که کلیدهای ۲۱۵ بیتی در حال حاضر امنیت کافی ایجاد نمی کنند و باید بنفع کلیدهای ۸۶۷ بیتی برای استفاده های شخصی کنار بروند! به همین ترتیب برای استفاده شرکتها کلیدهای ۱۰۲۴ بیتی و از ۲۰۴۸ بیت برای کلیدهای فوق العاده ارزشمند استفاده شود. البته پیش بینی شده است که این مقادیر تا حداقل سال ۲۰۰۴ معتبر خواهد بود. با پیشرفتهای موجود احتمالا در این زمان نیاز به افزودن بر طول کلید ها خواهد بود.

جدول زیر نشاندهنده افراد یا گروههایی است که توانایی شکستن کلیدها با طولهای متفاوت را دارند.

طول کلید	نفوذگران بالقوه
۲۵۶ بیتی	افراد عادی
۳۸۴ بیتی	گروههای تحقیق دانشگاهی و شرکتها
۵۱۲ بیتی	گروههای دولتی با تمام امکانات
۷۶۸ بیتی	امن برای کوتاه مدت
۱۰۲۴ بیتی	امن تا آینده نزدیک
۲۰۴۸	امن احتمالا تا چند ده سال!

پروتکل های انتقال فایل امن

در این قسمت برای شما بطور مختصر از پروتکل هایی خواهیم گفت که امکانFT یا (File Transfer) یا انتقال فایل را فراهم می آورند یا از بلوکهای سازنده پروتکل های ذکر شده در مقاله رمزنگاری در پروتکل های انتقال استفاده می کنند تا امکان FT امن را ایجاد کنند. درحالیکه پروتکلهای ذکر شده در مقاله مذکور سیستمهای امنیتی عمومی هستند که قابل کاربرد برای FT نیز هستند، آنچه در اینجا اشاره می شود، مشخصاً برای FT ایجاد شده اند:

AS2

AS۲ (Applicability Statement 2) گونه ای EDI (Electronic Date Exchange) یا تبادل دیتای الکترونیکی (اگرچه به قالبهای EDI محدود نشده) برای استفاده های تجاری با استفاده از HTTP است. AS2 در حقیقت بسط یافته نسخه قبلی یعنی AS1 است. AS2 چگونگی تبادل دیتای تجاری را بصورت امن و مطمئن با استفاده از HTTP بعنوان پروتکل انتقال توصیف می کند. دیتا با استفاده از انواع محتوایی MIME استاندارد که XML، EDI ، دیتای باینری و هر گونه دیتایی را که قابل توصیف در MIME باشد، پشتیبانی می کند، بسته بندی می شود. امنیت پیام (تایید هویت و محرمانگی) با استفاده از S/MIME پیاده سازی می شود. AS1 در عوض از SMTP استفاده می کند. با AS2 و استفاده از HTTPیا HTTP) HTTP/S با(SSL برای

انتقال، ارتباط بصورت زمان حقیقی ممکن می شود تا اینکه از طریق ایمیل انجام گیرد.

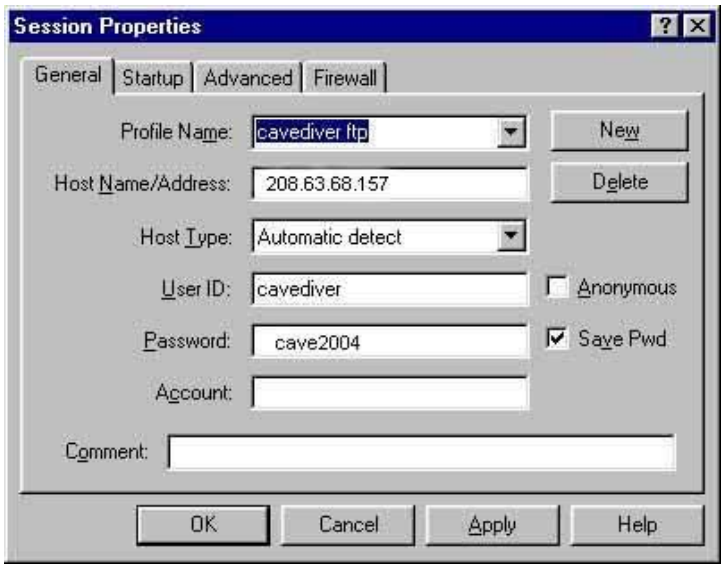
امنیت، تایید هویت، جامعیت پیام، و خصوصی بودن با استفاده از رمزنگاری و امضاهای دیجیتال تضمین می شود، که برپایه S/MIME هستند و نه SSL. استفاده از HTTP/S بجای HTTP استاندارد بدلیل امنیت ایجادشده توسط S/MIME کاملاً انتخابی است. استفاده از S/MIME اساس ویژگی دیگری یعنی انکارناپذیری را شکل می دهد، که امکان انکار پیام های ایجادشده یا فرستاده شده توسط کاربران را مشکل می سازد، یعنی یک شخص نمی تواند منکر پیامی شود که خود فرستاده است.

- برای FT :

(File Transfer

AS۲ مشخصاً برای درکنارهم قراردادن ویژگیهای امنیتی با انتقال فایل یعنی تایید هویت، رمزنگاری، انکارناپذیری توسط S/MIME و SSL انتخابی، طراحی شده است. از آنجا که AS2 یک پروتکل در حال ظهور است، سازمانها باید تولید کنندگان را به پشتیبانی سریع از آن تشویق کنند. قابلیت وجود انکارناپذیری در تراکنش های برپایه AS2 از اهمیت خاصی برای سازمانهایی برخوردار است که می خواهند پروسه های تجاری بسیار مهم را به سمت اینترنت سوق دهند. وجود قابلیت برای ثبت تراکنش پایدار و قابل اجراء برای پشتبانی از عملکردهای بسیار مهم مورد نیاز است. AS۲ از MDN (Message Disposition Notification) بر پایه RFC 2298 استفاده می کند. MDN (که می تواند در اتصال به سایر پروتکل ها نیز استفاده شود) بر اساس محتوای MIME است که قابل خواندن توسط ماشین است و قابلیت آگاه سازی و اعلام وصول

پیام را بوجود می آورد، که به این ترتیب اساس یک ردگیری نظارتی پایدار را فراهم می سازد.



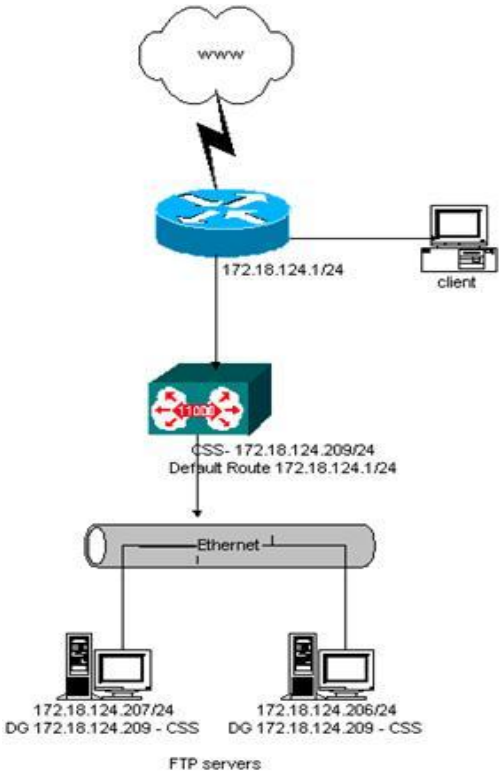
(File Transfer Protocol) **FTP**

FTP یا پروتکل انتقال فایل به منظور انتقال فایل از طریق شبکه ایجاد گشته است، اما هیچ نوع رمزنگاری را پشتیبانی نمی کند. FTP حتی کلمات عبور را نیز بصورت رمزنشده انتقال می دهد، و به این ترتیب اجازه سوءاستفاده آسان از سیستم را می دهد. بسیاری سرویس ها FTP بی نام را اجراء می کنند که حتی نیاز به کلمه عبور را نیز مرتفع می سازد (اگرچه در این صورت کلمات عبور نمی توانند شنیده یا دزدیده شوند)

- برای **FT**:

FTP بعنوان یک روش امن مورد توجه نیست، مگر اینکه درون یک کانال امن مانند SSL یا IPSec قرار گیرد.

گرایش زیادی به FTP امن یا FTP بر اساس SSL وجود دارد.
(می‌توانید به SFTP و SSL مراجعه کنید)



FTPS و SFTP

SFTP به استفاده از FT بر روی یک کانال که با SSH امن شده، اشاره دارد، در حالیکه منظور از FTPS استفاده از FT بر روی SSL است. اگرچه SFTP دارای استفاده محدودی است، FTPS (که هر دو شکل FTP روی SSL و FTP روی TLS را بخود می گیرد) نوید کارایی بیشتری را می دهد. RFC 2228 (FTPS) رمزنگاری کانالهای دیتا را که برای ارسال تمام دیتا و کلمات عبور استفاده شده اند، ممکن می سازد اما کانالهای فرمان را بدون رمزنگاری باقی می گذارد (بعنوان کانال فرمان شفاف شناخته

می شود). مزیتی که دارد این است که به فایروالهای شبکه های مداخله کننده اجازه آگاهی یافتن از برقراری نشست ها و مذاکره پورتها را می دهد. این امر به فایروال امکان تخصیص پورت پویا را می دهد، بنابراین امکان ارتباطات رمزشده فراهم می شود بدون اینکه نیاز به این باشد که تعداد زیادی از شکاف های دائمی در فایروال پیکربندی شوند.

اگرچه معمول ترین کاربردهای FTP (مخصوصاً بسته های نرم افزاری کلاینت) هنوز کاملاً FTPS (FTP روی (SSL را پشتیبانی نمی کنند و پشتیبانی مرورگر برای SSL، برای استفاده کامل از مجموعه کامل فانکشن های RFC 2228 FTPS کافی نیست، اما این امر در حال پیشرفت است. بسیاری از تولیدکنندگان برنامه های کاربردی در حال استفاده از SSL استاندارد در کنار FTP استاندارد هستند. بنابراین، گرچه در بعضی موارد مسائل تعامل همچنان وجود دارند، اما امیدواری برای پشتیبانی گسترده از FT امن در ترکیب با SSL وجود دارد. (و حتی امیدواری برای پذیرش گسترده مجموعه کامل فانکشن های RFC 2228 FTPS)

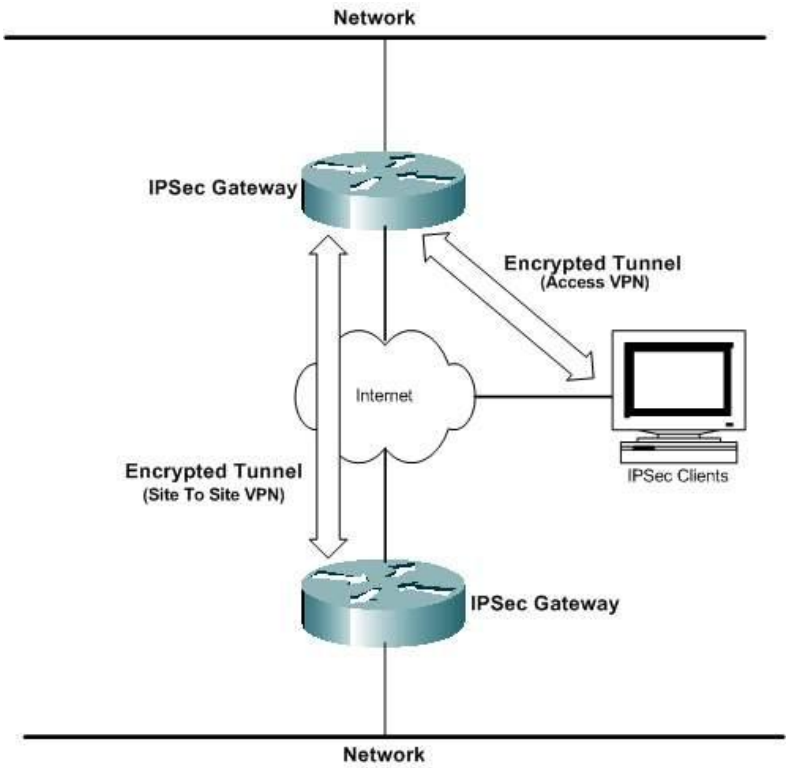
رمزنگاری در پروتکل‌های انتقال

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

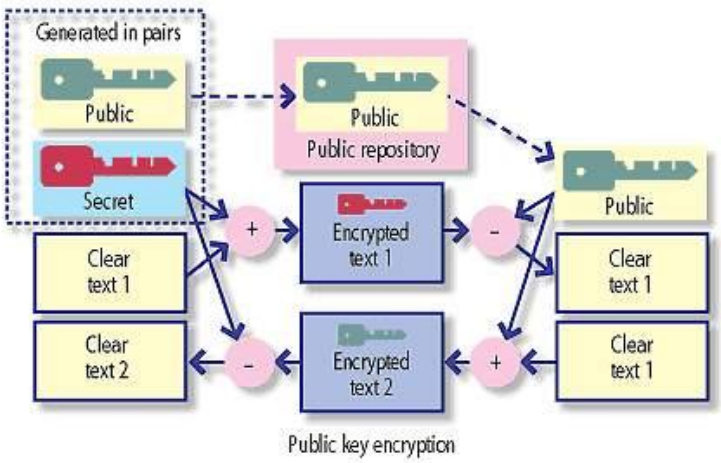
با ترکیب توانایی‌ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه‌های امنیت را فراهم می‌کنند. تقریباً تمام پروتکلها نیازهای جامعیت را پشتیبانی می‌کنند به طوری که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آنها از Non-Repudiation 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 SSL بصورت 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 telnet باشد. نسخه بعدی این پروتکل تحت نام SSH2 با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک‌های SSH منتشر شد.

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 سروربه سرور انجام می‌گیرد.

بخش هفتم

Internet Security

حفاظت کامپیوتر قبل از اتصال به اینترنت (۱)

تعداد بسیار زیادی از کاربران اینترنت را افرادی تشکیل می دهند که فاقد مهارت های خاصی در زمینه فن آوری اطلاعات بوده و از امکانات حمایتی مناسبی نیز برخوردار نمی باشند. سیستم های اینگونه کاربران دارای استعداد لازم به منظور انواع تهاجمات بوده و بطور غیر مستقیم شرایط مناسبی را برای مهاجمان به منظور نیل به اهداف مخرب آنان، فراهم می نمایند. بر اساس گزارشات متعددی که در چندین ماه اخیر منتشر شده است، تعداد حملات و آسیب پذیری اینگونه سیستم ها، بطرز کاملا" محسوسی افزایش یافته است. علت این امر را می توان در موارد زیر جستجو نمود:

- تعداد بسیاری از تنظیمات پیش فرض کامپیوترها ، غیر ایمن می باشد.
- کشف نقاط آسیب پذیر جدید در فاصله بین زمانی که کامپیوتر تولید و پیکربندی می گردد و تنظیماتی که اولین مرتبه توسط کاربر انجام می شود.
- در مواردی که ارتقاء یک نرم افزار از طریق رسانه های ذخیره سازی نظیر CD و یا DVD انجام می شود، همواره این احتمال وجود خواهد داشت که ممکن است نقاط آسیب پذیر جدیدی نسبت به زمانی که نرم افزار بر روی رسانه مورد نظر مستقر شده است، کشف شده باشد.
- مهاجمان دارای آگاهی لازم در خصوص دامنه های آدرس های IP از نوع Dial-up و یا Broadband بوده و آنان را بطور مرتب پویش می نمایند.
- کرم های بسیار زیادی بطور مرتب و پیوسته بر روی اینترنت در حال فعالیت بوده تا کامپیوترهای آسیب پذیر را شناسائی نمایند.

با توجه به موارد فوق، متوسط زمان لازم به منظور یافتن کامپیوترهای آسیب پذیر در برخی شبکه های کامپیوتر به مرز دقیقه رسیده است.

توصیه های استاندارد به کاربران خانگی، Download و نصب Patch های نرم افزاری در اسرع وقت و پس از اتصال یک کامپیوتر جدید بر روی اینترنت است. فرآیند فوق ، با توجه به این که مهاجمان به صورت دائم اقدام به پویش و یافتن قربانیان خود می نمایند، ممکن است در موارد متعددی توام با موفقیت کامل نگردد.
به منظور حفاظت کامپیوترها قبل از اتصال به اینترنت و نصب هر یک از Patch های مورد نیاز، موارد زیر پیشنهاد می گردد:

- **در صورت امکان، کامپیوتر جدید را از طریق یک فایروال شبکه ای (مبتنیظبر سخت افزار) و یا روتر فایروال به شبکه متصل نمائید.**
یک فایروال شبکه ای و یا روتر فایروال، سخت افزاری است که کاربران می توانند آن را بین کامپیوترهای موجود در یک شبکه و دستگاههای Broadband نظیر مودم کابلی و یا DSL نصب نمایند . با بلاک نمودن امکان دستیابی به کامپیوترهای موجود بر روی یک شبکه محلی از طریق اینترنت، یک فایروال سخت افزاری قادر به ارائه یک سطح حفاظتی مناسب برای کاربران در خصوص دریافت و نصب patch های نرم افزاری ضروری خواهد بود. در صورتی که قصد اتصال کامپیوتر خود به اینترنت را از طریق یک فایروال و یا روتری با پتانسیل NAT:Networirk Address Translation، داشته باشید و یکی از موارد زیر درست باشد: الف) ماشین جدید تنها کامپیوتر متصل شده به شبکه محلی از طریق فایروال است. ب) سایر ماشین های متصل شده به شبکه محلی پشت فایروال نسبت به نصب patch های مورد نیاز بهنگام بوده و بر روی آنان کرم ها و یا ویروس هائی وجود ندشته باشد، ممکن است به وجود یک فایروال نرم افزاری نیاز نباشد.

- **در صورت امکان، از فایروال نرم افزاری همراه کامپیوتر نیز استفاده نمائید.**

در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده می باشد، پیشنهاد می گردد آن را فعال نموده تا امکان اتصال سایرین به شما وجود نداشته باشد. همانگونه که اشاره گردید، در صورتی که کامپیوتر شما از طریق یک فایروال به شبکه متصل است و تمامی کامپیوترهای موجود در شبکه محلی نسبت به نصب هر یک از Patch های مورد نیاز بهنگام شده می باشند، این مرحله می تواند اختیاری باشد .علیرغم موضوع فوق، در بخشی از استراتژی "دفاع در عمق" به این موضوع اشاره شده است که بهتر است فایروال نرم افزاری ارائه شده همراه سیستم عامل،همواره فعال گردد. در صورتی که سیستم عامل موجود برروی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده نمی باشد، می توان یک نرم افزار فایروال مناسب را تهیه نمود. پیشنهاد می گردد که اینگونه نرم افزارها از طریق رسانه های ذخیره سازی نظیر CD و یا DVD نصب گردند (در مقابل اتصال به یک شبکه و دریافت نرم افزار مورد نیاز از یک کامپیوتر حفاظت نشده). در غیر اینصورت همواره این احتمال وجود خواهد داشت که کامـــپیوتر شما قبل از اینکه قادر به دریافت و نصب اینچنین نرم افزارهائی گردد، مورد تهاجم واقع شود.

- **غیر فعال نمودن سرویس های غیرضروری نظیر "اشتراک فایل و چاپگر"**

اکثر سیستم های عامل به صورت پیش فرض پتانسیل "اشتراک فایل و چاپ " را فعال نمی نمایند. در صورتی که شما سیستم خود را به یک سیستم عامل جدید ارتقاء داده اید و کامپیوتر دارای گزینه فعال "اشتراک فایل و چاپ" می باشد، بدیهی است که سیستم عامل جدید نیز این گزینه را فعال نماید. سیستم عامل جدید ممکن است دارای نقاط آسیب پذیری باشد که شما آنان را در نسخه قبلی سیستم عامل مربوطه از طریق نصب تمامی patchهای مورد نیاز، برطرف کرده

-
- باشید و در سیستم عامل جدید این وضعیت وجود ندارد. برای حل مشکل فوق پیشنهاد می گردد قبل از ارتقاء سیستم عامل، پتانسیل "اشتراک فایل و چاپ " را غیر فعال نموده و در ادامه فرآیند ارتقاء را انجام دهید. پس از ارتقاء سیستم و نصب Patch های مورد نیاز، می توان در صورت ضرورت اقدام به فعال نمودن پتانسیل "اشتراک فایل و چاپ" نمود.
- **دریافت و نصب patch های مورد نیاز**

پس از ایمن سازی کامپیوتر در مقابل حملات با استفاده از فایروال های سخت افزاری و یا نرم افزاری و غیر فعال نمودن پتانسیل "اشتراک فایل و چاپ "، می توان با اطمینان بیشتری سیستم خود را به منظور دریافت و نصب patch های مورد نیاز به شبکه متصل نمود. به منظور دریافت patch های نرم افزاری، توصیه می گردد که حتما" از سایت های ایمن و مطمئن (وب سایت تولید کنندگان) استفاده گردد . بدین ترتیب احتمال این که یک مهاجم قادر به دستیابی سیستم شما از طریق برنامه هائی موسوم به Trojan گردد، کاهش می یابد.

حفاظت کامپیوتر قبل از اتصال به اینترنت (۲)

در این مطلب چندین راهنمایی برای اتصال یک کامپیوتر جدید (یا ارتقاء یافته) برای اولین بار به اینترنت آورده شده است و مخاطبان آن کاربران خانگی، دانشجویان، شرکت های تجاری کوچک، یا هر مکانی با اتصال پرسرعت (مودم کابلی، DSL) یا از طریق خط تلفن است.

انگیزه

این مطلب بدلیل ریسک فزاینده برای کاربران اینترنتِ بدون حمایت مختص IT است. در ماه های اخیر، جهان شاهد گرایش به سمت سوءاستفاده از کامپیوترهای جدید یا محافظت نشده بوده است. این جریان بدلیل بعضی دلایل تشدید می شود:

بسیاری از پیکربندی های پیش فرض کامپیوترها نا امن هستند.

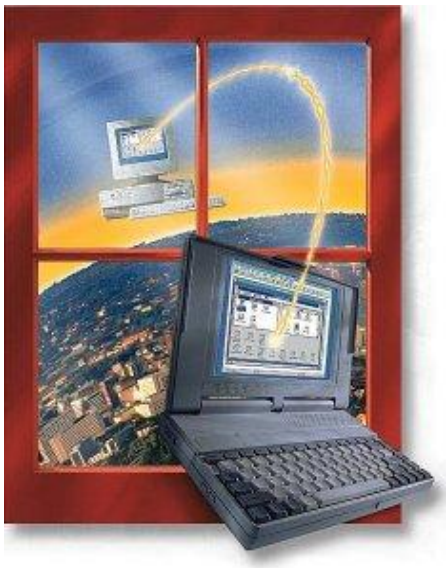
شکاف های امنیتی تازه ای ممکن است در مدت زمان ساخت و پیکربندی کامپیوتر توسط سازنده و تنظیم کامپیوتر برای اولین بار توسط کاربر، کشف شده باشد.

هنگام ارتقا نرم افزار از طریق ابزار مرسوم (مانند CD-ROM و DVD-ROM) شکافهای امنیتی جدید ممکن است از زمان ساخت دیسک تا کنون کشف شده باشد.

حمله کنندگان دامنه آدرس های IP خطوط پرسرعت و dial-up را می دانند و بطورمنظم پیمایش می کنند.

تعداد زیادی از کرمها از قبل در حال چرخیدن در اینترنت هستند و بطور پیوسته کامپیوترهای جدید را بمنظور سوءاستفاده پیمایش می کنند.

جالب است که زمان میانگین برای حمله به کامپیوترها در بعضی شبکه ها برای کامپیوترهای محافظت نشده بر حسب دقیقه اندازه گیری می شود، مخصوصاً این موضوع برای محدوده آدرس های استفاده شده توسط مودم های کابلی، DSL و dial-up صحت دارد.



توصیه ها

ادامه این مطلب به دوقسمت اختصاص دارد، اول راهنمایی عمومی و بعد گام های مختص به سیستم های عامل مشخص.

راهنمایی عمومی

هدف این مطلب فراهم آوردن حفاظت کافی برای یک کامپیوتر جدید است تا یک کاربر بتواند هر وصله نرم افزاری را که از زمان ساخت کامپیوتر یا نصب نرم افزار اولیه از

طریق CD، منتشر شده است، دانلود و نصب کند. توجه کنید که این مراحل راهنمایی کاملی برای نگه داری امن یک کامپیوتر از زمان دانلود اولیه و نصب وصله ها نیستند، بلکه قدم های اولیه و اساسی هستند.

تذکر:

- توصیه می شود که این مراحل را هنگام ارتقاء به سیستم عامل جدید و همچنین اولین اتصال یک کامپیوتر جدید به اینترنت انجام دهید.
- این مراحل را قبل از اولین اتصال به اینترنت انجام دهید.

اینها مراحلی هستند که توصیه می شوند:

۱- اگر ممکن است، کامپیوتر جدید را از طریق یک فایروال شبکه یا روتر- فایروال به اینترنت متصل کنید.

فایروال شبکه یا روتر- فایروال سخت افزاری است که کاربران می توانند بین کامپیوترها روی LAN و وسیله پرسرعت اتصال به اینترنت (مودم کابلی یا DSL) نصب کنند. با مسدود کردن دسترسی به کامپیوترهای شبکه داخلی از طریق اینترنت (البته هنوز اجازه دسترسی برای این کامپیوترها به اینترنت وجود دارد)، یک فایروال سخت افزاری اغلب می تواند حفاظت کافی را برای یک کاربر برای دانلود و نصب وصله های نرم افزاری لازم فراهم آورد. فایروال سخت افزاری درجه بالایی از حفاظت را برای کامپیوترهای تازه ای که به اینترنت متصل می شوند، ایجاد می کند.

چنانچه کامپیوتری را از طریق فایروالی که عمل NAT را انجام می دهد، به اینترنت متصل می کنید و یکی از شرایط ذیل برقرار است (الف) ماشین جدید تنها کامپیوتری است که از طریق فایروال به اینترنت متصل می شود یا (ب) تمام ماشینهای دیگر متصل به اینترنت از طریق فایروال، بروز شده باشند و آلوده به ویروسها، کرمها، یا کدهای آسیب رسان دیگر نباشند، در اینصورت شما ممکن است نیاز به فعال کردن فایروال نرم افزاری نباشید.

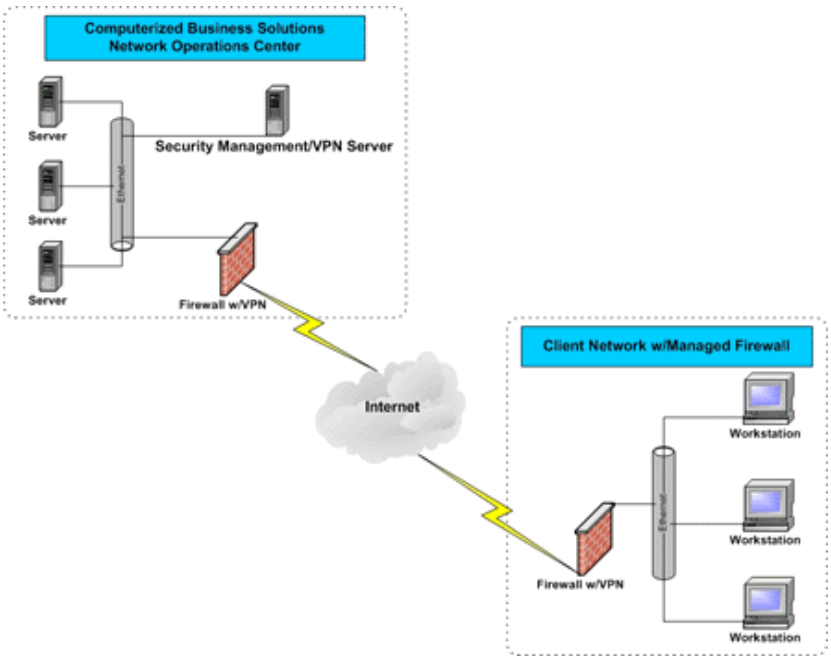
۲- اگر دسترسی دارید، فایروال نرم افزاری موجود در کامپیوتر را فعال کنید.

اگر سیستم عامل شما شامل یک فایروال نرم افزاری است، توصیه می شود که بمنظور مسدود کردن اتصالات از سایر کامپیوترهای موجود در اینترنت آن را فعال کنید.

چنانچه در بالا گفته شد، اگه کامپیوتر شما در حال متصل شدن به یک LAN است که یک فایروال سخت افزاری دارد و بقیه کامپیوترها روی این شبکه کاملاً محافظت شده و بدون کدهای زیان رسان باشند، این مرحله اختیاری است. بهرحال، به عنوان بخشی از استراتژی «دفاع در عمق»، توصیه می شود که فایروال نرم افزاری موجود در سیستم عامل فعال شود.

اگه سیستم عامل شما فاقد فایروال نرم افزاری است، ممکن است که بخواهید برنامه فایروال شخص ثالثی را نصب کنید. بسیاری از چنین برنامه هایی بطور تقریباً رایگان وجود دارند.

بهرحال، با توجه به این مسأله که مورد نظر ما در این مقاله، همان زمان کوتاه اتصال کامپیوتر محافظت نشده به اینترنت است، توصیه می شود که هر برنامه فایروال ثالثی از ابزاری مانند CD، DVD یا **Floppy** قبل از اتصال به اینترنت نصب گردد تا اینکه مستقیماً برروی کامپیوتر محافظت نشده دانلود گردد. در غیر اینصورت، ممکن است که این کامپیوتر قبل از کامل شدن دانلود و نصب نرم افزار مطلوب مورد سوءاستفاده قرار گیرد.



۳- سرویس های غیرضروری را مانند اشتراک فایل و پرینتر غیرفعال کنید.

بیشتر سیستم عامل ها بصورت پیش فرض اشتراک فایل و پرینتر را فعال نمی کنند، بنابراین نباید مسأله ای برای کاربران باشد. بهرحال، اگر کامپیوتر خود را به سیستم عامل جدید ارتقاء می دهید و اشتراک فایل آن فعال است، امکان دارد که در سیستم عامل جدید

نیز این گزینه فعال باشد. از آنجا که سیستم عامل جدید ممکن است شکاف های امنیتی داشته باشد که در نسخه قدیمی تر نبودند، اشتراک فایل را در نسخه قبلی قبل از ارتقاء سیستم عامل غیرفعال کنید. بعد از کامل شدن عمل ارتقاء و نصب تمام وصله های مربوطه، اشتراک فایل در صورت نیاز می تواند مجدداً فعال شود.

۴- وصله های نرم افزاری را در صورت نیاز دانلود و نصب کنید.

زمانی که کامپیوتر از حمله قریب الوقوع از طریق استفاده از فایروال سخت افزاری ویا نرم افزاری و غیرفعال کردن اشتراک فایل و پرینتر محافظت شده است، باید تقریباً اتصال به اینترنت بمنظور دانلود و نصب وصله های نرم افزاری لازم امن باشد. مهم است که این گام حتماً انجام گیرد چون درغیراینصورت کامپیوتر می تواند در معرض سوءاستفاده قرار گیرد اگر بعداً در زمان دیگری فایروال غیرفعال شود یا اشتراک فایل فعال شود.

وصله های نرم افزاری را از سایت های قابل اعتماد و شناخته شده (مانند سایتهای خود فروشندگان نرم افزار)، دانلود کنید تا امکان اینکه یک مزاحم از طریق استفاده از یک اسب تروا کنترل را در اختیار گیرد، به حداقل برسد.

حفاظت کامپیوتر قبل از اتصال به اینترنت (۳)

در. قسمت قبل راهنمای کلی از نظر امنیت برای نصب کامپیوترهای جدید ارائه گردید. بهرحال، عمل به بعضی از آن توصیه ها بستگی به سیستم عامل مورد استفاده دارد. این قسمت مشخصاً به سیستم های عامل ویندوز XP و Apple Macintosh OSX و چند اشاره به سایر سیستم عاملها دارد.

۱- ویندوز XP

بمنظور انجام این مراحل، شما نیاز دارید که به یک اکانت با اختیارات مدیر محلی وارد شوید.

الف. قسمت قبل را مرور کنید.

ب. در صورت امکان، از طریق یک فایروال سخت افزاری متصل شوید.

(به این مرحله در شماره قبل اشاره شده است.)

پ. Internet Connection Firewall موجود در XP را فعال کنید.

(مایکروسافت دستورهای فعال کردن این فایروال را ارائه کرده است.)

http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx

ت. اشتراکها را اگر فعال هستند، غیرفعال کنید.

۱- به Control Panel بروید.

۲- "Network and Internet Connections" را باز کنید.

۳- "Network Connections" را باز کنید.

۴- روی Connection که می خواهید تغییر ایجاد کنید کلیک راست کنید.

۵- "Properties" را انتخاب کنید.

۶- مطمئن شوید که "File and Printer Sharing for Microsoft Networking" انتخاب نشده است.

ث. به شبکه متصل شوید.

ج. به آدرس http://windowsupdate.microsoft.com بروید.

چ. دستورهای موجود در آنجا را برای نصب تمام بروز رسانیهای مهم دنبال کنید.

ح. «امن ماندن» را در زیر مرور کنید.

۲- Apple Macintosh OSX

الف. قسمت قبل را مرور کنید.

ب. در صورت امکان، از طریق یک فایروال سخت افزاری متصل شوید.

پ. فایروال نرم افزاری را فعال کنید.

۱- "System Preferences" را باز کنید.

۲- "Sharing" را انتخاب کنید.

۳- نوار "Firewall" را انتخاب کنید.

۴- روی "Start" کلیک کنید.

۵- نوار "Services" را انتخاب کنید.

۶- بررسی کنید که هیچکدام از سرویس ها انتخاب نشده باشند.

ت. به اینترنت متصل شوید.

ث. نرم افزار نصب شده را به روز کنید.

۱- "System Preferences" را باز کنید.

۲- "Software Updates" را انتخاب کنید.

۳- با انتخاب " Automatically check for updates when you have a network connection " به روزرسانی خودکار را فعال کنید.

۴- زمان بروزرسانی مناسبی انتخاب کنید (بصورت روزانه توصیه می شود)

۵- روی "Check Now" کلیک کنید.

۶- تمام به روزرسانیهای توصیه شده را نصب کنید.

ج. «امن ماندن» را در زیر مرور کنید.

۳- سایر نرم افزارها

در حالیکه یک بسته نرم افزاری آنتی ویروس به روز شده، نمی تواند در برابر تمام کدهای آسیب رسان از یک سیستم محافظت کند، برای بیشتر کاربران بهترین وسیله دفاعی در خط مقدم علیه حملات کدهای آسیب رسان است. بسیاری بسته های آنتی ویروس از بروزرسانیها پشتیبانی می کنند.

پ. اگر امکان دارد بروز رسانیهای خودکار نرم افزار را فعال کنید.

فروشندگان معمولاً هنگامی که یک شکاف امنیتی کشف می گردد، بسته های آن را ارائه می دهند. بیشتر مستندات محصولات روشی برای دریافت به روزها و وصله ها ارائه می دهند. باید بتوانید به روز رسانیها را از سایت فروشنده دریافت کنید.

بعضی برنامه ها بصورت خودکار وجود بروزرسانیها را بررسی می کنند، و بسیاری فروشندگان از طریق لیست ایمیل بصورت خودکار وجود بروزرسانی ها را اطلاع می دهند. وب سایت مورد نظر خود را برای اطلاعات در مورد این نحوه آگاهی نگاه کنید. اگر هیچ لیست ایمیل یا مکانیسم دیگر آگاه سازی بصورت خودکار ارائه نمی شود، نیاز است که وب سایت فروشنده در فواصل زمانی معین برای وجود بروزرسانی ها سرزده شود.

ت. از رفتار ناامن خودداری کنید.

- هنگام بازکردن پیوست های ایمیل یا هنگام استفاده از اشتراک نقطه به نقطه، پیام رسانی فوری یا اتاق های گفتگو، احتیاط کنید.
- اشتراک فایل را روی واسط های شبکه که به طور مستقیم در معرض اینترنت هستند، فعال نکنید.

ث. اصول کمترین حقوق دسترسی را دنبال کنید.

به استفاده از یک اکانت با تنها حقوق «کاربر» بجای حقوق «مدیر» یا سطح «ریشه» برای کارهای روزانه توجه کنید. بسته به سیستم عامل، شما تنها نیاز به استفاده از سطح دسترسی مدیر برای نصب نرم افزار جدید، تغییر پیکربندی سیستم و مانند اینها دارید. حتی بسیاری از سوءاستفاده ها از شکافهای امنیتی (مانند ویروس ها و اسب های تروا) در سطح دسترسی کاربر اجرا می شود، بنابراین بسیار خطرناکتر می شود که همواره بعنوان مدیر وارد سیستم شد.

امنیت تجهیزات شبکه

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

الف – عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می‌دهد که با دستیابی به تجهیزات امکان پیکربندی آنها را به گونه‌ای که تمایل دارند آن سخت‌افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان‌پذیر خواهد شد.

ب – برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهزات بر روی شبکه الزامی است. توسط این حمله‌ها نفوذگران می‌توانند سرویس‌هایی را در شبکه از کار بیاندازند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای AAA فراهم می‌شود.

در این بخش اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می‌گیرد. عناوین برخی از این موضوعات به شرح زیر هستند:

- امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
- امنیت تجهیزات شبکه در سطوح منطقی

- بالابردن امنیت تجهیزات توسط افزونگی در سرویس‌ها و سخت‌افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند:

- امنیت فیزیکی
- امنیت منطقی

۱ – امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله‌اند. با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات (که توسط عملکرد مشابه سخت‌افزار و یا سرویس‌دهنده مشابه جایگزین می‌شود) بدست می‌آید.

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق تجهزات شبکه را تهدید می‌کنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه‌حل‌ها و ترفندهای دفاعی در برار این‌گونه حملات پرداخت.

۱-۱ – افزونگی در محل استقرار شبکه

یکی از راه‌کارها در قالب ایجاد افزونگی در شبکه‌های کامپیوتری، ایجاد سیستمی کامل، مشابه شبکه‌ی اولیه‌ی در حال کار است. در این راستا، شبکه‌ی ثانویه‌ی، کاملاً مشابه شبکه‌ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که می‌تواند از نظر

جغرافیایی با شبکه‌ی اول فاصله‌ای نه چندان کوتاه نیز داشته باشد برقرار می‌شود. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم جندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

۲-۱ – توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند.

در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

الف – طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی ستاره‌ای : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از خادم اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال