بسمه تعالی

www.arianfile.ir

جزوه آشنایی با امنیت تجارت الکترونیک

ارائه شده توسط:

سایت آرین فایل

مرجع جدیدترین مقالات و جزوات

تجارت الکترونیک

فصل اول: نگاهی به مقوله امنیت در فناوری اطلاعات و شبکه

مقدمه

امروزه با توسعه و پیشرفت فناوری‌های نوین در جوامع و گسترش بی‌حد و مرز فناوری‌های اطلاعات در تمامی عرصه‌های زندگی بشر، همچنین استفاده از فناوری در جهت خلق رفاه و زندگی اجتماعی مناسب شاهد گسترش و توسعه دنیای مجازی در همه ابعاد زندگی خود هستیم. از یک سو گسترش شبکه‌های اطلاعاتی و دنیای مجازی به رفاه، آسایش و انجام کارها با سرعت و دقت بیشتر کمک می‌کند. از سوی دیگر چالش‌ها و موانعی نیز در به کارگیری فناوری اطلاعات و شبکه‌های اطلاعاتی رخ می‌دهد که یکی از مقوله‌ها امنیت فناوری اطلاعات یا امن بودن فضای تبادل اطلاعات است. هر روز شاهد اخباری در زمینه تهدیدات امنیتی در حوزه فناوری اطلاعات در گوشه و کنار جهان و سوء استفاده‌هایی که درعرصه تبادل اطلاعات می‌شود، هستیم؛ ازجمله هک شدن سایت‌ها توسط نفوذگران، انتشار ویروس‌های رایانه‌ای جدید و سرقت از حساب‌های مشتریان بانک‌ها، شکسته شدن قفل‌های نرم‌افزاری و ....

در دنیای امروز با واگذاری کارهای مالی، اداری و اطلاعاتی به شبکه‌های رایانه‌ای و همچنین وسعت زیاد تبادل اطلاعات بین نقاط مختلف در کشورهای جهان، باید نسبت به هشدارهای موجود در زمینه امنیت اطلاعات و امن بودن این حوزه بیش از پیش توجه شود.

در امور تجاری، تجارتی موفق محسوب می‌شود که در آن بسیاری از ملاحظات امنیتی مدنظر قرار گرفته باشد. برای یک سازمان تجاری موفق اطلاعات دارایی اصلی است. همانطور که در امر تجارت سنتی مجموعه‌ای از تمهیدات وجود دارد، در شکل پیچیده‌تر آن هم در محیط الکترونیکی وجود دارد. امنیت اطلاعات کمک می‌کند که آسیب‌ها کمینه، سرمایه اطلاعاتی بیشینه و فرصت‌های تجاری از دست‌اندازی رقبا محافظت گردد.

۱-۱) امنیت فناوری اطلاعات

موضوع امنیت فناوری اطلاعات از موضوعات مهم و دارای اولویت می‌باشد که در همه سازمان‌ها بخشی از تمرکز کاری نیروهای حوزه فناوری اطلاعات را بر خود معطوف کرده است. فناوری اطلاعات شامل فناوری‌هایی است که در خدمت ذخیره‌سازی، پردازش، انتقال و مدیریت اطلاعات است، اما امنیت فناوری اطلاعات به استفاده ایمن از این فناوری و اطمینان از وجود محیطی عاری از هرگونه تهدید بازمی‌گردد. دو بخش مهم امنیت در

فناوری اطلاعات شامل، امنیت رایانه (Computer Security) و امنیت ارتباطات (Communication Security) است که در زیر هر کدام را جداگانه توضیح می‌دهیم.

الف) امنیت رایانه

هدف از امنیت رایانه نگهداری از منابع اطلاعاتی در مقابل استفاده غیرمجاز (Anauthorized)، سوء استفاده (Abuse) و همچنین حفاظت در مقابل صدمات عمدی یا غیرعمدی، افشا (Disclosure) و تغییر و اصلاح (Modification) است.

ب) امنیت ارتباطات

حفاظت از اطلاعات در طی انتقال بین سیستم‌های رایانه‌ای و شبکه‌ها را امنیت ارتباطات گویند. باید دانست که به کارگیری فناوری اطلاعات در یک شبکه ارتباطی برای ارائه خدمات مورد نیاز می‌تواند همراه با خطرات امنیتی متعددی باشد. در استفاده از خدمات شبکه‌های رایانه‌ای و دنیای مجازی سه مولفه اصلی برای ارائه چنین خدماتی در نظر گرفته شده است که شامل کاربران انسانی (Human User)، ماشین (Host) و فرایندهای رایانه‌ای (Process) می‌باشد که به آنها عنصر (Principal) نیز گویند که به تعریف آنها می‌پردازیم.

کاربر: موجودیتی جوابگو و مسئول در قبال فعالیت‌های خود در تعامل با رایانه و شبکه است.

ماشین: موجودیتی دارای آدرس در یک شبکه ارتباطی که دارای نام و آدرس‌دهی خاص می‌باشد.

فرایند: عملیاتی که بر روی ماشین‌ها انجام می‌شود و معمولا با استفاده از مدل مشتری / سرویس‌دهنده (client/server) فرایند سمت مشتری و سرویس‌دهنده را از هم تشخیص می‌دهند. اما یکی از رایج‌ترین اصطلاحات در زمینه امنیت شبکه‌های رایانه‌ای نفوذ و نفوذگر می‌باشد که به تفصیل در این باره صحبت خواهیم کرد.

۱-۲) امنیت شبکه و اینترنت

قطعا تاکنون اخبار متعددی را در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده‌اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده‌اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آنان، یکی از روش‌های مناسب دفاعی است.

۱-۲-۱) اهمیت امنیت در شبکه و اینترنت

بدون شک کامپیوتر و اینترنت در مدت زمان کوتاهی توانسته‌اند حضور مشهود خود را در تمامی عرصه‌های حیات بشری به اثبات برسانند. وجود تحولات عظیم در ارتباطات (نظیر Email و تلفن‌های سلولی)، تحولات گسترده در زمینه تجهیزات الکترونیکی و سرگرمی (کابل دیجیتال، MP3)، تحولات گسترده در صنعت حمل و نقل (سیستم هدایت اتوماتیک اتومبیل، ناوبری هوائی)، تغییرات اساسی در روش خرید و فروش کالا (فروشگاه-های online، کارت‌های اعتباری)، پیشرفت‌های برجسته در عرصه پزشکی، صرفا نمونه‌هایی اندک در این زمینه می‌باشد.

اجازه دهید به منظور آشنایی با جایگاه کامپیوتر در زندگی انسان عصر حاضر و اهمیت امنیت اطلاعات، این پرسش را مطرح نمائیم که در طی یک روز چه میزان با کامپیوتر درگیر هستید و چه حجمی از اطلاعات شخصی شما بر روی کامپیوتر خود و یا سایر کامپیوترها، ذخیره شده است؟ پاسخ به سوال فوق، جایگاه کامپیوتر و اهمیت ایمن‌سازی اطلاعات در عصر اطلاعات را به خوبی مشخص خواهد کرد. امنیت در شبکه و اینترنت و حفاظت از اطلاعات با استناد به سه اصل اساسی زیر است:

- نحوه پیشگیری از بروز یک تهاجم
- نحوه تشخیص یک تهاجم
- نحوه برخورد با حملات

۱-۲-۲) برخی از انواع تهدیدات در اینترنت

اینترنت، علیرغم تمامی جنبه‌های مثبت دارای مجموعه‌ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنها بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردارند:

- عملکرد ویروس‌های کامپیوتری که می‌تواند منجر به حذف اطلاعات موجود بر روی یک کامپیوتر شود.
- نفوذ افراد غیر مجاز به کامپیوتر شما و تغییر فایل‌ها
- استفاده از کامپیوتر شما برای تهاجم علیه دیگران
- سرقت اطلاعات حساس نظیر شماره کارت اعتباری و خرید غیر مجاز با استفاده از آن

با رعایت برخی نکات می‌توان احتمال بروز و یا موفقیت این نوع از حملات را به حداقل مقدار خود رساند.

۱-۲-۳) مفاهیم اولیه امنیت اطلاعات در اینترنت

اولین مرحله به منظور حفاظت و ایمن‌سازی اطلاعات، شناخت تهدیدات و آگاهی لازم در خصوص برخی مفاهیم اولیه در خصوص ایمن‌سازی اطلاعات است که در ادامه بیان می‌گردد.

- Hacker، Attacker و یا Intruder: اسامی فوق به افرادی که همواره درصدد استفاده از نقاط ضعف و آسیب‌پذیر موجود در نرم‌افزارها می‌باشند اطلاق می‌گردد. با این که در برخی حالات ممکن است افراد فوق اهداف غیر مخربی را نداشته و انگیزه آنها صرفا کنجکاوی باشد، ماحصل عملیات آنان می‌تواند اثرات جانبی منفی را به دنبال داشته باشد.
- کد مخرب: این نوع کدها شامل ویروس‌ها، کرم‌ها و برنامه‌های تروجان (Trojan) بوده که هر یک از آنها دارای ویژگی‌های منحصر به فردی می‌باشند:

✓ ویروس‌ها: نوع خاصی از کدهای مخرب هستند که شما را ملزم می‌کنند به منظور آلودگی سیستم، عملیات خاصی را انجام دهید. این نوع از برنامه‌ها به منظور نیل به اهداف مخرب خود نیازمند یاری کاربران می‌باشند. باز نمودن یک فایل ضمیمه همراه Email و یا مشاهده یک صفحه وب خاص، نمونه‌هایی از همکاری کاربران در جهت گسترش این نوع کدهای مخرب است.

✓ کرم‌ها: این نوع از کدهای مخرب بدون نیاز به دخالت کاربر، توزیع و گسترش می‌یابند. کرم‌ها عموما با سوء استفاده از یک نقطه آسیب‌پذیر در نرم‌افزار فعالیت خود را آغاز نموده و سعی می‌کنند که کامپیوتر هدف را آلوده نمایند. پس از آلودگی یک کامپیوتر، تلاش برای یافتن و آلودگی سایر کامپیوترها انجام خواهد شد. همانند ویروس‌های کامپیوتری کرم‌ها نیز می‌توانند از طریق Email، وب‌سایت‌ها و یا نرم‌افزارهای مبتنی بر شبکه، توزیع و گسترش یابند. توزیع اتوماتیک کرم‌ها نسبت به ویروس‌ها یکی از تفاوت‌های محسوس بین این دو نوع کد مخرب محسوب می‌شود.

✓ برنامه‌های تروجان: این نوع از کدهای مخرب، نرم‌افزارهایی هستند که ادعای ارائه خدماتی را داشته ولی در عمل، اهداف خاص خود را دنبال می‌کنند (تفاوت در حرف و عمل). مثلا برنامه‌ای که ادعای افزایش سرعت کامپیوتر شما را برای یک مهاجم و یا سارق از راه دور ارسال نماید.

۱-۲-۴) سابقه امنیت در شبکه اینترنت

اینترنت در سال ۱۹۶۹ به صورت شبکه‌های به نام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخش‌های عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا فکر ایجاد شبکه برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود. در سال ۱۹۷۱ تعدادی از رایانه‌های دانشگاه‌ها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند.

با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مساله امنیت بیش از پیش اوج گرفت. در سال ۱۹۸۸ آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه مواجه شد که بعدا "کرم موریس" نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و به صورت هندسی تکثیر شود. آن زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتد.

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت که در هماهنگی فعالیت‌های مقابله با حملات ضدامنیتی، آموزش و تجهیز شبکه‌ها و روش‌های پیشگیرانه نقش موثری داشت. با رایج‌تر شدن و استفاده عام از اینترنت، مساله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/OILS WORM در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می‌شد. از آن زمان حملات امنیتی – اطلاعاتی به شبکه‌ها و شبکه جهانی روز به روز افزایش یافته است.

گرچه اینترنت در ابتدا با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمینان آن را بیش از پیش روشن نموده است.

۱-۳) فرایند توسعه امنیت سازمان

الف) تجزیه و تحلیل خطرات مطرح در سازمان یا سیستم

باید تجزیه و تحلیل حملات احتمالی و سطح آسیب‌پذیری سیستم مشخص شود یعنی با تحلیل خطر (ریسک) بین خطرآفرینی یک تهدید، امکان وقوع و تکرار آن، هزینه‌های ایجاد مکانیزم‌های حفاظتی بررسی شود.

ب) تدوین سیاست‌ها و خدمات امنیتی

به توجه به نتایج تجزیه و تحلیل خطرپذیری سیاست‌های امنیتی تعیین می‌شود. سیاست امنیتی مبادله‌ای منطقی بین خطرات و منابع موجود ارائه داده و در برگیرنده وظایفی است که آنها را خدمات امنیتی گویند. خدمات امنیتی به وسیله مکانیزم‌های امنیتی که مبتنی بر الگوریتم‌های رمزنگاری و پروتکل‌های امنیتی است، محقق می‌شود.

یک سیاست امنیتی، اعلامیه‌ای رسمی مشتمل بر مجموعه‌ای از قوانین است که می‌بایست توسط افرادی که به یک تکنولوژی سازمان و یا سرمایه‌های اطلاعاتی دستیابی دارند، رعایت و به آن پایبند باشند. به منظور تحقق اهداف امنیتی می‌بایست سیاست‌های تدوین شده در رابطه با تمام کاربران، مدیران شبکه و مدیران عملیاتی سازمان، اعمال گردد. مهم‌ترین هدف یک سیاست امنیتی، آگاهی دادن لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم، به منظور حفظ و صیانت از تکنولوژی و سرمایه‌های اطلاعاتی است. در ادامه ویژگی‌های یک سیاست امنیتی خوب و یک مثال از سیاست امنیتی، تعریف رمز عبور، بیان می‌گردد.

تعریف رمز عبور به عنوان یک مثال از سیاست امنیتی

- حداقل طول رمز عبور، دوازده و یا بیشتر باشد.
- در رمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و زیرخط استفاده شود.
- از کلمات موجود در دیکشنری استفاده نگردد.
- رمزهای عبور، در فواصل زمانی مشخص (سی و یا نود روز) به صورت ادواری تغییر داده شوند.

کاربرانی که رمزهای عبور ساده و قابل حدس را برای خود تعریف نموده‌اند، تشخیص و به آنها تذکر داده شود (عملیات فوق به صورت متناوب و در فواصل زمانی یک ماه انجام گردد).

ج) تعیین مکانیزم‌های امنیتی

پس از تدوین سیاست‌های امنیتی و شناسایی خدمات امنیتی مورد نیاز سازمان باید مکانیزم‌های امنیتی را به صورت خاص یا عمومی تعیین کرد. مانند رمزگذاری، امضای دیجیتال، کنترل دسترسی، صحت داده، احراز هویت، پوشش ترافیک، کنترل مسیریابی و تایید توسط عامل سوم.

به طور کلی نگاه به مقوله امنیت نمی‌تواند یک نگاه مطلق باشد یعنی امنیت به معنای مطلق در هیچ شبکه یا سیستم رایانه‌ای نمی‌تواند وجود داشته باشد، اما با ارزیابی‌های امنیتی و مدیریت بهتر مکانیزم‌های دفاعی در کنار استفاده از ابزار و فناوری‌های نوین و همچنین استفاده از مشاوران فنی خوب در کنار آموزش کارکنان و رعایت موارد امنیتی توسط کاربران می‌توان خطرات امنیتی را به حداقل رسانید (با توجه به این نکته که عدم استفاده صحیح از خدمات در دسترس کاربران و اشتباهات انسانی ضعف سیستم‌های دفاعی را افزایش می‌دهد). به بیان دیگر می‌توان با یک نگرش سیستماتیک و استفاده مداوم از یک چرخه ایمن‌سازی شامل طراحی، پیاده-سازی، ارزیابی و اصلاح، ضریب امنیتی سیستم‌های رایانه‌ای خود را بالا ببریم.

۱-۴) انواع ویژگی‌ها و سرویس‌های امنیتی در محیط‌های تجاری

احراز هویت – Authentication: فرستنده یا گیرنده هویت واقعی خود را برای طرف مقابل اثبات می‌کند.

کنترل اختیارات – Authorization: یعنی هر طرف فعالیت به چه سطح از اطلاعاتی دسترسی داشته و چه نوع از عمل (رویت، حذف، تغییر، اضافه) برایش مقدور باشد.

در دسترس بودن – Availability: خدمات باید همیشه در دسترس افراد مجاز باشد.

محرمانگی اطلاعات – Confidentiality: فقط فرستنده و گیرنده مورد نظر قابل به درک پیام باشند.

بازرسی – Auditing: امکان بررسی داده‌ها و اطلاعات موجود در سیستم ضبط رویدادها موجود باشد.

صحت داده‌ها (تمامیت و جامعیت) – Integrity: یعنی عدم امکان دستکاری داده‌ها توسط افراد یا نرم‌افزارهای غیر مجاز. به بیانی دیگر اطلاعاتی که درون پیغام و یا تبادلات وجود دارد در طول مسیر به طور اتفاقی یا عمدی مورد دستبرد قرار نمی‌گیرند.

انکارناپذیری – Non-Repudiation: یعنی هیچ کدام از طرفین (فرستنده و گیرنده پیام)، امکان انکار عملکرد خود (ارسال پیام) را نداشته باشد. به عبارت دیگر ارسال‌کننده نمی‌تواند منکر ارسال پیام یا تبادل مالی شود و دریافت‌کننده هم نمی‌تواند منکر دریافت آن شود.

فصل دوم: شناسایی برخی از انواع حملات در شبکه‌های کامپیوتری و اینترنت

مقدمه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس‌های فعال، پروتکل‌های استفاده شده و پورت‌های باز می‌باشد. یکی از مهم‌ترین وظایف کارشناسان فناوری اطلاعات اطمینان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین). در زمان ارائه، سرویس‌دهندگان مجموعه‌ای از سرویس‌ها و پروتکل‌ها را به صورت پیش‌فرض فعال و تعدادی دیگر را نیز غیرفعال کرده‌اند. این موضوع ارتباط مستقیمی با سیاست‌های یک سیستم عامل و نوع نگرش آن به مقوله امنیت دارد. در زمان نقد امنیتی سیستم‌های عامل، پرداختن به موضوع فوق یکی از محورهایی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنها را دنبال می‌نمایند.

اولین مرحله درخصوص ایمن‌سازی یک محیط شبکه، تدوین، پیاده‌سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه‌ریزی درخصوص ایمن‌سازی شبکه را شامل می‌شود. هر نوع برنامه‌ریزی در این رابطه مستلزم توجه به موارد زیر است:

- بررسی نقش هر سرویس‌دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- انطباق سرویس‌ها، پروتکل‌ها و برنامه‌های نصب شده با خواسته‌های یک سازمان
- بررسی تغییرات لازم درخصوص هر یک از سرویس‌دهندگان فعلی (افزودن و یا حذف سرویس‌ها و پروتکل‌های غیرضروری، تنظیم دقیق امنیتی سرویس‌ها و پروتکل‌های فعال)

تعلل و یا نادیده گرفتن فاز برنامه‌ریزی می‌تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد. متاسفانه در اکثر موارد توجه جدی به مقوله برنامه‌ریزی و تدوین یک سیاست امنیتی نمی‌گردد. فراموش نکنیم که فناوری‌ها به سرعت و به صورت مستمر در حال تغییر بوده و می‌بایست متناسب با فناوری‌های جدید، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس‌دهندگان و کاهش نقاط آسیب‌پذیر آنها با جدیت دنبال شود. نشستن پشت یک سرویس‌دهنده و پیکربندی آن بدون وجود یک برنامه مدون و مشخص، امری بسیار خطرناک بوده که بستر لازم برای بسیاری از حملاتی که در آینده اتفاق خواهند افتاد را فراهم می‌نماید. هر سیستم عامل دارای مجموعه‌ای از سرویس‌ها، پروتکل‌ها و ابزارهای خاص خود بوده و نمی‌توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنها توجه و از پتانسیل‌های آنها در جهت افزایش کارائی و ایمن‌سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس‌دهندگان، می‌بایست در فواصل

زمانی خاصی برنامه‌های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنها با توجه به شرایط موجود و فناوری‌های جدید ارائه شده، اعمال گردد. فراموش نکنیم که حتی راه حل‌های انتخاب شده فعلی که دارای عملکردی موفقیت‌آمیز می‌باشند، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح نباشند.

۲-۱) وظیفه یک سرویس‌دهنده

پس از شناسایی جایگاه و نقش هر سرویس‌دهنده در شبکه می‌توان در ارتباط با سرویس‌ها و پروتکل‌های مورد نیاز آن به منظور انجام وظایف مربوطه، تصمیم‌گیری نمود. برخی از سرویس‌دهندگان به همراه وظیفه آنها در یک شبکه کامپیوتری به شرح زیر است:

- Logon Server: این نوع سرویس‌دهندگان مسئولیت شناسایی و تایید کاربران در زمان ورود به شبکه را بر عهده دارند. سرویس‌دهندگان فوق می‌توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس‌دهندگان نیز انجام دهند.
- Services Network Server: این نوع از سرویس‌دهندگان مسئولیت میزبان نمودن سرویس‌های مورد نیاز شبکه را بر عهده دارند. این سرویس‌ها عبارتند از:

✓ DHCP (Dynamic Host Configuration Protocol)

✓ DNS (Domain Name System)

✓ WINS (Windows Internet Name Service)

✓ SNMP (Simple Network Management Protocol)

- Application Server: این نوع از سرویس‌دهندگان مسئولیت میزبان نمودن برنامه‌های کاربردی نظیر بسته نرم‌افزاری Accounting و سایر نرم‌افزارهای مورد نیاز در سازمان را بر عهده دارند.
- File Server: از این نوع سرویس‌دهندگان به منظور دستیابی به فایل‌ها و دایرکتوری‌های کاربران، استفاده می‌گردد.
- Print Server: از این نوع سرویس‌دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشته شده در شبکه، استفاده می‌شود.

- Web Server: این نوع سرویس‌دهندگان مسئولیت میزبانی برنامه‌های وب و وب‌سایت‌های داخلی و خارجی را بر عهده دارند.
- FTP Server: این نوع سرویس‌دهندگان مسئولیت ذخیره‌سازی فایل‌ها برای انجام عملیات Downloading و Uploading را بر عهده دارند. سرویس‌دهندگان فوق می‌توانند به صورت داخلی و خارجی استفاده گردند.
- Email Server: این نوع سرویس‌دهندگان مسئولیت ارائه سرویس پست الکترونیکی را بر عهده داشته و می‌توان از آنها به منظور میزبان نمودن فولدرهای عمومی و برنامه‌های Gropuware نیز استفاده نمود.
- News/Usenet (NNTP) Server: این نوع سرویس‌دهندگان به عنوان یک سرویس‌دهنده newsgroup بوده و کاربران می‌توانند اقدام به ارسال و دریافت پیام‌هایی بر روی آنها نمایند.

به منظور شناسایی سرویس‌ها و پروتکل‌های مورد نیاز بر روی هر یک از سرویس‌دهندگان، می‌بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنها به چه صورت است؟ شبکه داخلی، شبکه جهانی و یا هر دو مورد. پاسخ به سوال فوق زمینه نصب و پیکربندی سرویس‌ها و پروتکل‌های ضروری و حذف و غیرفعال نمودن سرویس‌ها و پروتکل‌های غیرضروری در ارتباط با هر یک از سرویس‌دهندگان موجود در یک شبکه کامپیوتری را فراهم می‌نماید.

۲-۲) حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه‌های کامپیوتری خصوصا اینترنت، امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس‌دهندگان می‌باشیم. علت بروز چنین حملاتی می‌تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد.

توجه به مکانیزم‌های جلوگیری از حملات امنیتی و سیاست‌های امنیتی محقق اهداف امنیت اطلاعات هستند. حملات امنیتی می‌تواند شامل قطع (Interruption)، دسترسی غیرمجاز (Interception)، دستکاری داده‌ها (Modification) و ساخت پیغام (Fabrication) باشد.

برای پیشگیری، شناسایی، برخورد سریع و توقف حملات باید در مرحله اول قادر به تشخیص و شناسایی زمان و موقعیت بروز یک تهاجم باشیم. به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه خود آگاه می-شویم؟ چگونه با آن برخورد نموده و در سریع‌ترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد؟ شناسایی نوع حملات و نحوه پیاده‌سازی یک سیستم حفاظتی مطمئن در مقابل آنها یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه‌های کامپیوتری است. شناخت دشمن و آگاهی از روش‌های تهاجم وی، احتمال موفقیت ما را در رویارویی با آنها افزایش خواهد داد. بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه‌های کامپیوتری شده است، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب نمود تا در آینده بتوانیم به نحو مطلوب از آنها استفاده نماییم. جدول زیر برخی از حملات متداول را نشان می‌دهد:

انواع حملات	
Distributed Denial of Service (DDoS) & (DoS) Denial of Service	
Spoofing	Back Door
Repaly	Middle Man in the
Brute Force	Hijacking TCP/IP
Password Guessing	Dictionary
Viruses	Exploitation Software
Worms	Horses Trojan
Engineering Social	Auditing
DNS Poisoning	Sniffing

۲-۲-۱) حملات DoS

شاید تاکنون شنیده باشید که یک وب‌سایت مورد تهاجمی از نوع DoS قرار گرفته است. این نوع از حملات صرفا متوجه وب‌سایت‌ها نبوده و ممکن است شما قربانی بعدی باشید. تشخیص حملات DoS از طریق عملیات متداول شبکه امری مشکل است ولی با مشاهده برخی علائم در یک شبکه و یا کامپیوتر می‌توان از میزان پیشرفت این نوع از حملات آگاهی یافت.

حملات از نوع (DoS: denial-of-servic)

در یک تهاجم از نوع DoS یک مهاجم باعث ممانعت دستیابی کاربران تایید شده به اطلاعات و یا سرویس‌های خاصی می‌نماید. یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه‌ای آن و یا کامپیوترها و شبکه‌ای از سایت‌هایی که شما قصد استفاده از آنها را دارید، باعث سلب دستیابی شما به سایت‌های Email، وب‌سایت‌ها، account های online و سایر سرویس‌های ارائه شده بر روی کامپیوترهای سرویس‌دهنده می‌گردد.

متداول‌ترین و مشهودترین نوع حملات DoS زمانی محقق می‌گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. زمانی که شما آدرس URL یک وب‌سایت خاص را از طریق مرورگر خود تایپ می‌کنید، درخواست شما برای سرویس‌دهنده ارسال می‌گردد. سرویس‌دهنده در هر لحظه قادر به پاسخگویی به حجم محدودی از درخواست‌ها می‌باشد، بنابراین اگر یک مهاجم با ارسال درخواست‌های متعدد و سیلاب‌گونه باعث افزایش حجم عملیات سرویس‌دهنده گردد، قطعا امکان پردازش درخواست شما برای سرویس‌دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می‌باشند، چرا که امکان دستیابی شما به سایت مورد نظر سلب شده است.

یک مهاجم می‌تواند با ارسال پیام‌های الکترونیکی ناخواسته که از انها با نام Spam یاد می‌شود، حملات مشابهی را متوجه سرویس‌دهنده پست الکترونیکی نماید. هر account پست الکترونیکی (صرف نظر از منبعی که آن را در اختیار شما قرار می‌دهد، نظیر سازمان مربوطه و یا سرویس‌های رایگانی نظیر یاهو و Hotmail) دارای ظرفیت محدودی می‌باشند. پس از تکمیل ظرفیت فوق، عملا امکان ارسال Email دیگری به account فوق وجود نخواهد داشت. مهاجمان با ارسال نامه‌های الکترونیکی ناخواسته سعی می‌نمایند که ظرفیت account مورد نظر را تکمیل و عملا امکان دریافت email های معتبر را از account فوق سلب نمایند.

حملات از نوع DDoS (distributed denial-of-service)

در یک تهاجم از نوع DDoS یک مهاجم ممکن است از کامپیوتر شما برای تهاجم برعلیه کامپیوتر دیگری استفاده نماید. مهاجمان با استفاده از نقاط آسیب‌پذیر و یا ضعف امنیتی موجود بر روی سیستم شما می‌توانند کنترل کامپیوتر شما را به دست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند. ارسال حجم بسیار بالای داده از طریق کامپیوتر شما برای یک وب‌سایت و یا ارسال نامه‌های الکترونیکی ناخواسته برای آدرس‌های Email خاصی، نمونه‌هایی از همکاری کامپیوتر شما در بروز یک تهاجم DDoS می‌باشد. حملات فوق توزیع شده می‌باشند، چرا که مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می‌کند.

نحوه پیشگیری از حملات

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoS و یا DDoS وجود ندارد. علیرغم موضوع فوق می‌توان با رعایت برخی نکات و انجام عملیات پیشگیری، احتمال بروز چنین حملاتی (استفاده از کامپیوتر شما برای تهاجم بر علیه سایر کامپیوترها) را کاهش داد.

نصب و نگهداری نرم‌افزار آنتی ویروس

نصب و پیکربندی یک فایروال

تبعیت از مجموعه سیاست‌های خاصی در خصوص توزیع و ارائه آدرس Email خود به دیگران

۲-۲-۲) حملات از نوع Back Door

Back Door برنامه‌ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم می‌کند. برنامه‌نویسان معمولا چنین پتانسیل‌هایی را در برنامه‌ها پیش‌بینی می‌کنند تا امکان اشکال‌زدایی و ویرایش کدهای نوشته شده در زمان تست به کارگیری نرم‌افزار، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق، مستند نمی‌گرند پس از اتمام مرحله تست به همان وضعیت باقی مانده و تهدیدات امنیتی متعددی را به دنبال خواهند داشت. به طور مثال برنامه Fire Wall Check Point که توسط اسرائیل تهیه شده دارای این مشکل است.

نحوه پیشگیری از حملات

بهترین روش برای پیشگیری از حملات Back Door آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم-افزارهای موجود است. به کاربران باید آموزش داد که صرفا از منابع و سایت‌های مطمئن اقدام به دریافت و نصب نرم‌افزار بر روی سیستم خود نمایند. نصب و استفاده از برنامه‌های آنتی ویروس می‌تواند کمک قابل توجهی در بلاک نمودن عملکرد اینچنین نرم‌افزارهایی (نظیر Back Orifice, NetBus, and Sub 7) را به دنبال داشته باشد. برنامه‌های آنتی ویروس باید به صورت مستمر به هنگام شده تا امکان شناسایی نرم‌افزارهای جدید فراهم گردد.

۲-۲-۳) حملات از نوع Spoofing- رهگیری

تکنیکی است برای دسترسی غیرمجاز به کامپیوترها. هکر ابتدا آدرس IP یک کامپیوتر مورد اعتماد را پیدا می-کند. پس از به دست آوردن این اطلاعات هکر شروع به ارسال اطلاعات به سیستم قربانی کرده و خود را مورد اعتماد وانمود می‌کند (خود را به جای یک کامپیوتر مورد اعتماد جا می‌زند)، پس از برقراری ارتباط شروع به دریافت اطلاعاتی می‌کند که در حالت معمول، مجاز به دسترسی به آنها نیست.

این حمله عمدتا متکی بر ضعف پروتکل IP و ضعف‌های ساختاری اینترنت برای دسترسی کاربران بر روی لایه Application است. در این حمله معمولا دو تکنیک معرفی می‌گردد:

- جعل هویت Impersonation
- تغییر قیافه Masquerading

در روش تغییر قیافه فرض می‌شود که فرد حمله‌کننده قبلا User Id و Pass Word فردی را دزدیده و حال با تغییر قیافه خود را به عنوان یک کاربر معتبر جا می‌زند.

اما در روش جعل هویت معمولا به طور مثال سناریوی زیر که نسبتا ساده ولی خطرناک است، انجام می‌گیرد:

در این روش مثلا وقتی یک کاربر معتبر می‌خواهد به سرور دانشگاه متصل گردد، قبلا دانشجوها به DNS دانشگاه حمله کرده‌اند و این سرور را به شکلی مختل کرده‌اند که بسته‌های اطلاعاتی به جای آنکه بین سرور دانشگاه و کلاینت جابجا شوند، بین کلاینت متقاضی و سرور جعلی مهاجم جابجا می‌شوند. یعنی اولین پیغام (Prompt) که بر روی صفحه کاربر ظاهر می‌شود دقیقا مشابه پیغامی است که سرور دانشگاه برای دریافت

User ID و Pass Word به کلاینت می‌دهد و از او خواسته می‌شود یوزرنیم و پسورد خود را وارد نماید و آنگاه این مشخصات به سرقت می‌رود و در ادامه بلافاصله پیغام "User Id or Pass Word Incorrect" بر روی صفحه ظاهر می‌شود و کاربر هم بدون اینکه احساس بدی پیدا کند، با تصور آنکه مشخصه یا کلمه خود را اشتباه وارد کرده مجددا آنها را وارد کرده و وارد سیستم دانشگاه می‌شود.

۲-۲-۴) حملات از نوع Man in the Middle

نفوذگر بین دو کامپیوتر کلاینت و سرور که در حال تبادل اطلاعات هستند قرار می‌گیرد. نفوذگر ترتیبی را اتخاذ می‌کند که دو کامپیوتر از وجود او بی‌اطلاع باشند. به این ترتیب دسترسی کاملی به اطلاعات بین دو نقطه پایانی دارد. در این حمله عمدتا هدف به دست آوردن کلمه عبور و رمز عبور است. سیستم‌های Wireless در معرض این حمله قرار دارند.

۲-۲-۵) حملات از نوع Replay

وقتی یک هکر به وسیله ابزار Sniffer (بو کشیدن) بسته‌های اطلاعاتی را از روی سیم برمی‌دارد، یک حمله Replay رخ می‌دهد. وقتی بسته‌ها دزدیده شدند، هکر اطلاعات مهم و نام‌های کاربری و کلمات عبور را از درون آن استخراج می‌کند. وقتی که اطلاعات از بسته‌ها استخراج شدند، دوباره بسته‌ها روی خط قرار می‌گیرند و یا به صورت دروغین به آنها پاسخ داده می‌شود. به عبارت دیگر وقتی بین یک سرویس‌دهنده و سرویس‌گیرنده مجاز براساس سطوح دسترسی مورد نظر یک تماس اتفاق می‌افتد، این جلسه ذخیره شده و مجددا توسط کاربر غیرمجاز تکرار می‌شود. لذا اگر به گونه‌ای ترتیب و توالی این جلسات مجددا مورد بررسی قرار نگیرد می‌تواند یک حمله انجام پذیرد.

۲-۲-۶) حملات از نوع TCP/IP Hijacking

معمولا به آن جعل نشست (Session Hijacking) نیز گفته می‌شود. هکر می‌تواند نشست TCP بین دو ماشین را به دست آورد. یک روش مشهور استفاده از Source-rout کردن IP ها می‌باشد. Source-rout کردن یعنی بسته‌های IP را طوری تغییر دهیم که از مسیری خاص بگذرند.

۲-۲-۷) حملات از نوع DNS Poisoning (مسمومیت DNS)

این حمله هنگامی است که فایل DNS شما با اطلاعات ناجوری پر شود. به صورت ساده تر هنگامی می‌باشد که نفوذگر رکوردهای DNS را که به Host های صحیحی اشاره دارند، به Host مورد نظر خود تغییر می‌دهد.

۲-۲-۸) حملات از نوع Social Engineering (مهندسی اجتماعی)

بیشتر زمانی رخ می دهد که هکر به سیستم های واقعی قصد نفوذ دارد. راه دیگر هنگامی می‌باشد که نفوذگر با استفاده از نقاط ضعف کاربر انتهایی (End User) راه نفوذ به شبکه را پیدا می‌کند. سوء استفاده از نقاط ضعف افراد با به دست آوردن عادت‌های شخصیتی افراد برای اغفال آنها و یا تحت فشار قرار دادن آنها تا اطلاعات مورد نیاز برای نفوذ به شبکه را در اختیار فرد هکر قرار دهد.

۲-۲-۹) حملات از نوع Brute Force

یک روش برای شکستن کلمات رمز و به دست آوردن آنهاست. حمله Brute Force حروف را به صورت ترکیبی استفاده می‌کند و با تست کردن آنها رمز عبور را پیدا می‌کند. برای مقابله با این روش باید از کلماتی استفاده کرد که در لغت‌نامه وجود ندارد. البته امروزه راه دیگر مقابله با تهدیدات از نوع Brute Force و Dictionary استفاده از یک فعالیت انسانی است. مثلا یک شکل گرافیکی با اشکالی که توسط سیستم‌های الکترونیکی قابل تشخیص نیستند، شما را مجبور به تایپ می‌کنند.

۲-۲-۱۰) حملات از نوع Software Exploitation

حمله علیه سوراخ‌ها و باگ‌های موجود در کدهای سیستم. برای اصلاح آنها باید از Hotfix ها و Service Pack ها استفاده کرد.

۲-۲-۱۱) حملات از نوع Sniffing

اطلاعاتی مانند عبور و رمز عبور توسط هکر بر روی خط شنود شده و یا اینکه با حمله به دیتابیس‌ها و به دست آوردن این اطلاعات، هکر می‌تواند خود را به جای کاربر مجاز معرفی کرده و سوء استفاده نماید.

فصل سوم: روش‌ها و سیستم‌های کنترل دسترسی

مقدمه

در این بحث تلاش می‌کنیم از دسترسی‌های غیرمجاز جلوگیری نماییم. این محافظت اطلاعات سه وجه دارد:

- محرمانگی (Confidentiality)
- تمامیت و صحت داده‌ها (Integrity)
- در دسترس بودن (Availability)

در بحث محرمانگی هدف اصلی آن است که دسترسی به اطلاعات و خواندن آنها بدون مجوز انجام نپذیرد.

در بحث صحت داده‌ها هدف آن است که اجازه ندهیم تغییرات هوشمندانه‌ای در مجموعه اطلاعات انجام گیرد. یعنی اجازه نوشتن اطلاعات را بدون مجوز ندهیم.

در بحث در دسترس بودن این انتظار را داریم در زمان‌های مشخص شده که به کاربر اجازه دسترسی داده می‌شود و با وجود پهنای باندی که باید در اختیارش باشد، همیشه این امکان یعنی دسترسی به منابع و اطلاعات برایش مقدور باشد.

برای مدل‌سازی بحث کنترل دسترسی دو مفهوم کلی باید مورد نظر قرار گیرد:

Subject: یک موجود فعال است مانند یک کاربر یا مثل یک برنامه، یک پروسس یا یک کامپیوتر و یا حتی یک دیتابیس که تلاش و فعالیت آنها در راستای دسترسی به یک منبع اطلاعاتی می‌باشد.

Object: منظور همان منبع اطلاعاتی می‌باشد که می‌تواند یک برنامه دیگر، یک فایل دیگر، یک کامپیوتر دیگر و یا اطلاعات مربوط به کاربری دیگر باشد. Object ها ماهیت غیرفعال دارند. در واقع عمل انتقال اطلاعات از Object به سمت Subject می‌باشد و ما در بحث کنترل دسترسی سعی می‌کنیم برای این انتقال اطلاعات رویه و روش خاصی را تعریف کنیم.

۳-۱) تکنیک‌های کنترل دسترسی

۳-۱-۱) قانون حداقل اجازه (Least Privilege)

یکی از مهم ترین تکنیک‌های کنترل دسترسی کنترل حداقل اجازه می‌باشد. دیدگاه اصلی حاکم بر این تکنیک این است که در یک شبکه متشکل از تجهیزات و منابع اعم از کامپیوترها، دیتابیس‌ها، فایل‌ها، چاپگرها و ... کاربر به هیچ عنوان نتواند اجازه دسترسی عمومی داشته باشد. یعنی به هیچ کس اجازه دسترسی عمومی داده نشود. به عبارت دیگر به هر Subject اجازه دسترسی به Object هایی را می‌دهیم که برای آن درخواست دارد برای انجام کار مشخصی که از قبل تعریف شده است. لازم به توجه است که این اصل با ماهیت اینترنت که به همه کس به صورت پیش‌فرض اجازه دسترسی عمومی به همه سرویس‌ها را داده است، در تضاد می‌باشد. لذا برای رسیدن به این هدف لازم است که زیرساخت‌های امنیتی را بر روی اینترنت به گونه‌ای شکل دهیم که ضمن استفاده اینترنت در دسترسی‌های عمومی قانون "حداقل اجازه" رعایت گردد.

برای انجام این منظور یک راه حل آن است که هنگامی که برای مجموعه کاربران یک شبکه سطوح دسترسی ایجاد می‌شود، ابتدا کلیه اجازه‌های دسترسی لغو گردد و آنگاه مورد به مورد با توجه به صلاحدید مدیر سیستم (Admin)، Object ها برای Subject ها فعال گردد.

۳-۱-۲) حسابرسی کاربران (Accountability)

از جمله محوری‌ترین پایه‌های مبحث کنترل دسترسی می‌باشد. درواقع این امکان با اضافه کردن لایه‌هایی به سازمان به وجود می‌آید. این لایه باعث می‌شود که اطلاعات هرگونه دسترسی یک Subject و اقدام بر روی یک Object بر روی سیستم ذخیره گردد. درنتیجه مدیر سیستم می‌تواند با مراجعه به این فایل ثبت وقایع (Log File) بررسی نماید که آیا Subject ها در مجموعه شرایط و قوانین امنیتی موردنظر مدیر سیستم عمل کرده-اند یا خیر.

این عمل به خودی خود در صورتی که کاربران از آن اطلاع داشته باشند، باعث کاهش تخلفات در سیستم می-گردد.

فرایند حسابرسی در اصل با یک عمل شناسایی هویت Subject آغاز می‌گردد. در این مرحله کاربر با ارائه کلمه عبور و رمز عبور و یا بهره‌گیری از کارت‌های هوشمند که در آن اطلاعات مربوط به هویت صاحب آن می‌باشد، خودش را به سیستم معرفی می‌کند.

۳-۱-۳) کنترل Object ها

در واقع جهت کنترل در محیط‌های فناوری اطلاعات سه لایه داریم:

- کنترل دسترسی فیزیکی (Physical Access Control)
- کنترل دسترسی اجرایی (Administrative Access Control)
- کنترل دسترسی منطقی (Logical Access Control)

به طور کلی هدف جلوگیری و امن‌سازی یک Object توسط تهدیدات است.

در کنترل دسترسی به روش فیزیکی هدف ایجاد حدود دسترسی‌ها به منابع (عمدتا سخت‌افزاری) است. این روش مشابه انواع روش‌های ممانعت فیزیکی ورود و خروج افراد به محیط و سازمان می‌باشد (استفاده از دیوار، قفل در و یا فنس‌کشی). مثلا در مراکز حیاتی IT که اطلاعات بانکی نگهداری می‌شود یا مراکز صدور گواهی دیجیتال آیین‌نامه‌های مشخص و پیچیده‌ای برای ورود از یک اطاق به اطاق دیگر وجود دارد. به طور مثال از سیستم‌های شناسایی به روش زیست‌سنجی (بیومتریک) مثلا اثر انگشت استفاده می‌گردد و یا کابل‌های انتقال اطلاعات از هرگونه برونداد یا شنود توسط مهاجمین محفوظ گردد.

اما در بحث کنترل دسترسی اجرایی، تکیه بر سیاست‌ها می‌باشد که برای امنیت سازمان تعریف گردیده و مدیر سیستم براساس این قوانین سطوح دسترسی هر فرد از سازمان را به اطلاعات، معین می‌نماید. یا اینکه در استخدام افراد برای اینگونه محیط‌ها بایستی ملاحظات امنیتی مورد توجه قرار گیرد. همچنین توجه به آموزش-های لازم امنیتی در این محیط‌ها در حوزه کنترل دسترسی اجرایی قرار می‌گیرد.

در بحث کنترل منطقی تکیه بر تکنیک‌های فنی و مهندسی است. یعنی با بهره‌گیری از روش‌های مهندسی بتوانیم اطلاعات سازمان خود را از دسترسی‌های بدون مجوز محفوظ نگه داریم.

در بخش دسترسی منطقی سه روش مهندسی مورد استفاده قرار می‌گیرد:

۱. محدودسازی دسترسی به Object ها (Object Access Restriction)
۲. رمزنگاری (Encryption)
۳. معماری دسترسی شبکه‌ای تفکیک شده (Network Architecture/Segregation)

در بخش اول (محدودسازی دسترسی به Objectها) هدف ایجاد محدودیت برای دسترسی به یک Object توسط Subject های مختلف است. یعنی تنها Subject هایی که در یک فرایند شناسایی احراز هویت گردیده‌اند و براساس رویه‌های امنیتی سیستم اجازه و حد دسترسی آنها به منابع تایید شده، قادر به دسترسی به Object خاصی هستند.

در بخش دوم یعنی رمزنگاری هدف محرمانه کردن اطلاعات با بهره‌گیری از تکنیک‌های رمزنگاری است. با بهره-گیری از این روش حتی اگر فرد غیر مجازی به اطلاعات سازمان ما دسترسی پیدا کند به دلیل اینکه همه اطلاعات به صورت رمز درآمده‌اند، این دستیابی برای او ثمری نخواهد داشت، چرا که قادر به فهم آن اطلاعات نخواهد بود.

در بخش سوم (معماری دسترسی شبکه‌ای تفکیک شده) جداسازی حداکثری در شبکه مد نظر است. مثلا در یک محیط نظامی که اطلاعات بسیار محرمانه‌ای بر روی یک کامپیوتر وجود دارد، اگر ضرورتی برای حضور این کامپیوتر در شبکه وجود ندارد، لازم نیست این کامپیوتر حتما به محیط شبکه متصل گردد یا اینکه مثلا بخش-های مختلف شبکه‌ای با توجه به اهداف آنها از یکدیگر جدا شوند.

۳-۲) انوع کنترل‌ها (Control Types)

حال در این مرحله سوالی مطرح می‌شود که این کنترل‌های دسترسی را چگونه به کار گیریم. به عبارت دیگر استراتژی کنترل ما چگونه می‌تواند باشد. اصولا در این مبحث پنج نوع استراتژی کنترلی معرفی می‌گردد:

۱. پیش‌گیرانه (Preventative)
۲. نمایان‌سازی و کشف (Detective)
۳. بازدارنده و تنبیه‌کننده (Deterrent)
۴. تصحیح‌کننده (Corrective)
۵. بازگشت و بازیابی (Recovery)

در تکنیک پیش‌گیرانه جلوگیری از رخداد یک حمله انجام می‌گیرد. درواقع از ابتدا اجازه نمی‌دهیم که یک Subject به یک Object غیرمجاز دسترسی داشته باشد.

در تکنیک نمایان‌سازی و کشف، استراتژی را به شکلی تعریف می‌کنیم که پس از وقوع یک حمله موفق اولا وقوعش اعلام شود و ثانیا اینکه توسط چه کسی حمله انجام شده مشخص گردد.

در روش بازدارنده و تنبیه‌کننده ما برای Subject مهاجم طبعاتی تعریف می‌کنیم. مثلا در سیاست‌های امنیتی تعریف می‌کنیم که چنانچه یک دسترسی به Object بدون اجازه انجام پذیرد، Subject مهاجم شناسایی می‌گردد و براساس تصمیمات سازمان که در بخش مدیریت سیستم تعریف گردیده با او برخورد می‌گردد.

در روش تصحیح در واقع هدف آن است که به محض بروز یک حمله بلافاصله سیستم را به وضعیت مناسب آن برگردانیم. به طور مثال فرض کنید به سرور پست الکترونیک یک سازمان یک حمله به منظور پر کردن حجم آن انجام گرفته است. در این روش (تصحیح‌سازی) برای برخورد با این حمله، مثلا تمام میل‌باکس‌ها را پاک می‌کنیم، خواه این میل‌باکس‌ها مربوط به افراد باشد و در آن نامه‌های درست باشد و خواه مربوط به فرد حمله‌کننده باشد.

۳-۳) بخش‌بندی تکنیک‌های کنترل دسترسی

همانطور که در صفحات گذشته مطرح گردید بعد از انجام مرحله احراز هویت و شروع مرحله ثبت وقایع و حسابداری (Accounting) مرحله بررسی کنترل حدود اختیارات دسترسی (Authorization) آغاز می‌گردد. این بدان معناست که بررسی شود هر Subject اختیار دسترسی به چه Object هایی را دارا می‌باشد.

این مرحله – یعنی Authorization- توسط تکنیک‌های کنترل دسترسی انجام می‌پذیرد. بدین معنا تکنیک‌های کنترل دسترسی را می‌توان به دو بخش تقسیم کرد:

۱) بصیرتی (Discretionary)

۲) غیر بصیرتی (Non Discretionary)

۳-۳-۱) کنترل دسترسی بصیرتی (Discretionary Access Control-DAC)

در این روش ایجادکننده یا اصطلاحا مالک (Owner) هر Object می‌تواند بر روی آن Object تغییری دهد، آن را حذف کند یا دوباره بنویسد و همینطور به دیگر Subject ها اجازه دسترسی و یا عدم دسترسی و همینطور نوع اختیارات (دیدن، تغییر، حذف و ...) را تفویض نماید. پس با توضیحات بالا می‌توان به این نتیجه هم

رسید که این روش متکی است بر شناسایی هر Subject. بدین دلیل این روش با عنوان Identity-Based Access Control نیز شناخته می‌شود.

این نوع از کنترل دسترسی بیشتر ماهیت غیرمتمرکز دارد، یعنی هر کس که یک Object را ایجاد می‌کند، خودش اقدام به صدور مجوز به Subject های دیگر برای دسترسی به آن Object می‌نماید.

این Subject ها می‌توانند یک کاربر داشته باشند یا در شکل عام‌تر آن نقش و وظیفه یک کاربر باشند. به طور مثال یک کاربر می‌تواند یک مدیر باشد که نقش مدیر سیستم را ایفا می‌نماید و در نقش دیگر ممکن است وظیفه بررسی و محاسبه حقوق کارمندان را انجام دهد.

برای انجام این نوع از کنترل دسترسی باید "لیست کنترل دسترسی" ایجاد گردد. این لیست مطابق جدول ۳-۱ دربردارنده جزئیاتی در خصوص اینکه چه کاربری می‌تواند به چه Object ی دسترسی پیدا کند می‌باشد. باید توجه داشت که در این روش Subject می‌تواند یک کاربر، یا یک نقش و وظیفه یا یک گروه باشد.

User	File A	File B	File C
User 1	Read/Write	Read/Write/Execute	Read
User 2	Read	No Access	No Access
User 3	Read	Read	Read/Write/Execute

جدول ۳-۱) لیست کنترل دسترسی (Access Control List)

باید توجه داشت این روش کنترل دسترسی بیشتر در محیط‌های تجاری استفاده می‌گردد.

۳-۳-۲) کنترل دسترسی الزامی (Mandatory Access Control – MAC)

در این روش سیستم به صورت غیرمتمرکز نمی‌باشد. بلکه براساس قوانین مشخص که توسط مدیریت سازمان مشخص گردیده است، تعریف می‌گردد. یعنی همه باید از تعدادی قوانین مشخص تبعیت کنند. این روش به نام Rule-Based Access Control نیز شناخته می‌شود. بدین منظور برای هر کاربر یک برچسب امنیتی تولید می‌شود. در محیط‌های تجاری این برچسب‌ها براساس طبقه‌بندی زیر انجام می‌گیرد:

- عمومی (Public)
- حساس در سطح دپارتمان (Sensitive)
- شخصی (Private)
- دارای مالکیت معنوی (Confidential)

همانطور که گفته شد برای هر کدام از Subject ها و Object ها یک برچسب امنیتی اختصاص می‌دهیم. یک مثال از این کاربرد در سیستم‌های فایروال می‌باشد. همانطور که می‌دانیم این سیستم‌ها یک سری قوانین مشخص دارند. مثلا آنهایی که در لایه IP قرار می‌گیرند، براساس اطلاعاتی مانند IP گیرنده، IP فرستنده و ... که به صورت قانون از قبل در آنها بارگذاری شده، تصمیم می‌گیرند که یک اتصال بین فضای بیرون فایروال و درون آن انجام شود یا نه. همانطور که ملاحظه می‌کنید در اینجا مهم نیست که اگر فردی می‌خواهد به Object ای دسترسی پیدا کند آیا مالک آن می‌باشد یا نه، بلکه اطلاعات مربوط به این درخواست با قوانین مشخص تعریف شده تطابق داده می‌شود.

۳-۳-۳) کنترل دسترسی غیر بصیرتی (Non Discretionary Access Control – NDAC)

این روش به دو شیوه زیر انجام می‌پذیرد:

- کنترل دسترسی براساس نقش و وظیفه (Role-Based Access Control)
- کنترل دسترسی براساس شبکه‌بندی (Lattice-Based Access Control)

در شیوه اول به هر مشخصه کاربر (User ID) مجموعه‌ای از اجازه‌های دسترسی را صادر نمی‌کنیم. بلکه براساس شرح خدمات هر کاربر این کار انجام می‌شود. در سازمان‌هایی که موقعیت شغلی افراد به سرعت تغییر می‌کند، افراد ممکن است دارای چندین مسئولیت گردند. به طور مثال در داخل یک پروژه، چندین زیر پروژه در بخش‌های مختلف زمانی تعریف می‌گردد و وظایف فرد تغییر می‌کند. پس در این روش اجازه دسترسی براساس شرح وظایف کاری یک کاربر انجام می‌پذیرد.

در شیوه دوم، از ترکیب دو روش بر مبنای نقش و وظیفه (Role-Based) و بر مبنای قوانین (Rule-Based) استفاده می‌شود. در این روش برای وظیفه افراد برچسب‌های امنیتی تعریف می‌گردد. مثلا کسی که مدیر سیستم است برچسب شخصی (Private) می‌گیرد. لذا این فرد اجازه دسترسی به اطلاعات سطح Private و

بالطبع اجازه دسترسی به سطوح پایین‌تر امنیتی یعنی Sensitive و Public را نیز دارا می‌باشد. اما در بعضی از مواقع لازم است براساس سیاست‌نامه امنیتی سازمان و قوانین پیش‌بینی شده در آن (Rules) فقط به بعضی از Object ها در سطوح پایین‌تر امکان دسترسی داشته باشد.

همانطور که در بالا اشاره شد این روش برای محیط‌های با تغییرات زیاد و دوره‌ای در پرسنل آن (مانند محیط-های پروژه‌ای) مناسب می‌باشد.

۳-۴) تعیین هویت (Identification) و احراز و تصدیق هویت (Authentication)

تاکنون در مورد نحوه Authorization مبتنی بر روش‌های کنترل دسترسی مطالعه کردیم. اما قبل از اینکه یک Subject مجاز یا غیرمجاز شناخته شود باید تعیین هویت یا اصطلاحا Identify شود. یعنی اسمش مورد شناسایی قرار گیرد و سپس این اسم احراز هویت یا اصطلاحا Authenticate گردد.

در مرحله Identification سیستمی که در واقع ایجادکننده یا مالک و یا محفظه قرارگیری یک Object است، براساس تکنیک‌های موجود از Subject تقاضای دادن اطلاعات منحصر به فردی می‌کند که می‌تواند شناسه یک نام کاربری باشد یا یک کارت هوشمند (Smart Card) باشد و یا مثلا یک نشانه (Token) باشد. پس از این مرحله سیستم شروع به مرحله احراز هویت می‌کند.

۳-۴-۱) تکنیک‌های احراز هویت (Authentication)

روش‌های احراز هویت به سه نوع تقسیم می‌گردد که هر کدام مبتنی بر یک خاصیت مربوط به Subject است.

نوع اول: What you Know

که یک اطلاع خاص منحصر به فردی است که تنها کاربر می‌داند و معمولا یک کلمه عبور (Pass Word) می-باشد. P/W ها یک رشته از کاراکترها می‌باشند که می‌تواند به صورت یک سری رقم یا اصطلاحا PIN باشد یا اینکه به صورت ترکیبی از اعداد و حروف باشند. معمولا یک P/W خوب دارای شرایطی است، مثل حداقل طول، تاریخ انقضاء، تصادفی، عدم انتخاب اسامی مشخص و آشکار، نگهداری محرمانه، غیر قابل حدس. از جمله نمونه‌های P/W های ضعیف انتخاب نام همسر، فرزند و حیواناتمان و یا انتخاب تاریخ تولد می‌باشد.

از آنجا که اطلاعات مربوط به P/W ها در داخل یک پایگاه داده نگهداری می‌شود و همیشه امکان حمله به این پایگاه وجود دارد، لذا این روش احراز هویت جزء روش‌های ضعیف محسوب می‌شود.

نوع دوم: What You Have

چیز منحصر به فردی که کاربر برای اثبات هویت خود به همراه می‌برد. مثل کارت هوشمند (Smart Card) و یا یک نشانه.

باید توجه داشت در سیستم‌ها عمدتا برای بالا بردن سطح امنیتی احراز هویت از روش چند فاکتوری (Multiple Factors) استفاده می‌شود. یعنی از میان نوع‌های ۱ و ۲ و ۳ حداقل از دو نوع به طور همزمان استفاده می‌گردد. به طور نمونه در سیستم‌های خودپرداز بانکی از دو نوع اول (Pass Word) و دوم (Smart Card) به صورت ترکیبی استفاده می‌شود.

همچنین باید به این نکته توجه کرد که اگر چه استفاده از روش Multiple Factors باعث بالا رفتن سطح امنیتی سیستم می‌شود، اما این بدان معنا نیست که استفاده از دو عنصر در یک نوع از انواع تکنیک‌های احراز هویت مثلا استفاده همزمان از دو P/W نیز عاملی برای افزایش امنیت احراز هویت می‌باشد.

مطلب دیگر حائز اهمیت، امکان بالا رفتن پیچیدگی کاری در روش‌های Multiple Factors می‌باشد. مثلا در صورتی که شما نشانه خود را که از نوع دوم است، گم کنید، حتی داشتن اطلاعات کامل احراز هویت نوع اول خود، مثلا P/W هیچ کمکی به شما نمی‌تواند بکند.

نوع سوم: What You Are

به معنای ویژگی‌های منحصر به فرد افراد می‌باشد (ویژگی‌های بیومتریک افراد). در این نوع تکنیک که بهترین اما گران‌ترین روش نیز می‌باشد، Subject که معمولا یک عامل انسانی است با توجه به مشخصات منحصر به فرد خودش شناسایی می‌شود. از جمله این مشخصات می‌توان به تصویر عنبیه، شبکیه، اثر انگشت دست، الگوی صدا، الگوی زدن کلید در صفحات کلید و امضای فیزیکی اشاره کرد.

روش بیومتریک هم در مرحله Identification و هم در نوع سوم Authentication می‌تواند مورد استفاده قرار گیرد. اگر روش بیومتریک در Identification استفاده شده باشد، یعنی بدون استفاده از ابزار نوع اول مستقیما از ابزار نوع سوم استفاده شده باشد، کار بسیار پیچیده می‌گردد. چرا که مشخصات دریافتی از دستگاه بیومتریک باید با دیتابیس بسیار بزرگی شامل همه Subject ها مقایسه شود. به این دلیل بهتر است برای

افزایش کارایی سیستم حتما از نوع اول و یا نوع دوم روش‌های احراز هویت در کنار نوع سوم احراز هویت – بیومتریک – بهره‌گیری شود.

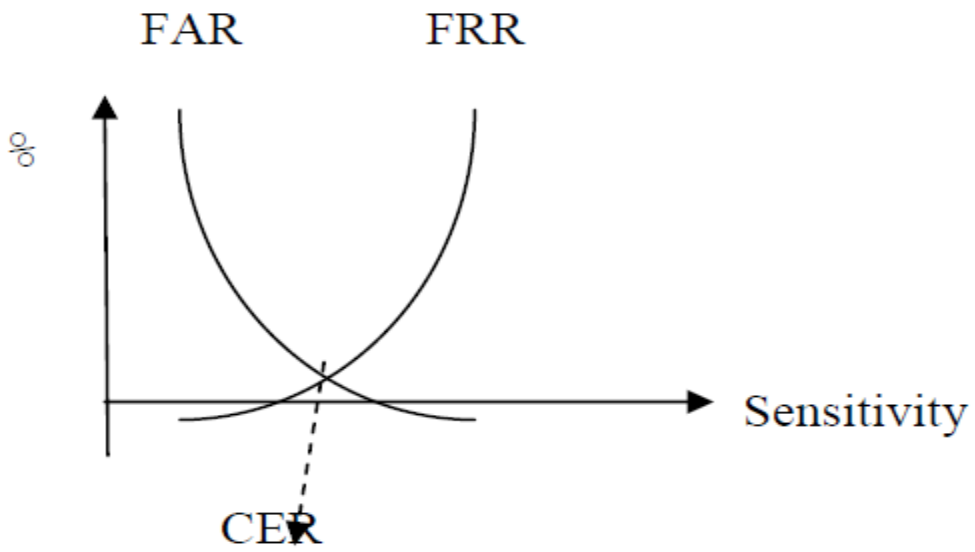
۳-۴-۲) خطاهای نوع سوم احراز هویت – بیومتریک

در دستگاه‌های مبتنی بر بیومتریک به دلیل میزان حساسیت دستگاه ما مواجه با دو نوع خطا می‌باشیم:

False Rejection Rate: یعنی میزان عدم تشخیص درست فرد دارای اعتبار برای سیستم. یعنی مثلا اثر انگشت فردی که در سیستم به عنوان فرد معتبر می‌باشد به دلیل آلودگی محیطی تشخیص داده نشود.

False Acceptance Rate: یعنی میزان پذیرفته شدن افراد غیر معتبر به عنوان فرد معتبر در سیستم می‌باشد که عمدتا به دلیل کافی نبودن حساسیت سیستم است.

حال اگر به منحنی میزان حساسیت دستگاه بیومتریک با دو میزان FAR و FRR توجه کنیم (شکل ۳-۱)، این نکته مشهود است که هر چه حساسیت دستگاه بالا رود FAR پایین می‌آید ولی در مقابل FRR بالا می‌رود. نقطه‌ای که این دو (FAR و FRR) برابر شوند، آن نقطه به عنوان Crossover Error Rate شناخته می‌شود، که ملاکی است برای اندازه‌گیری این نوع از دستگاه‌ها.



شکل ۳-۱) میزان حساسیت دستگاه‌های بیومتریک

۳-۵) روش‌های پیاده‌سازی احراز هویت

برای پیاده‌سازی احراز هویت معمولا از سه روش به شرح زیر استفاده می‌شود:

- متمرکز (Centralized)
- غیر متمرکز (Decentralized)
- ترکیبی (Hybrid)

در روش اول یعنی روش متمرکز، عملیات احراز هویت به طور متمرکز بر روی یک سرور انجام می‌پذیرد. حسن این روش آن است که چون کلیه احراز هویت برای دسترسی به Object ها در یک نقطه واحد انجام می‌گیرد، مدیریت آن به راحتی انجام می‌گیرد. ضعف این روش در زمانی است که امنیت آن سرور دچار اخلال شود، آنگاه امنیت کل سیستم مختل می‌شود. ضعف دیگر آن این است که در صورت بالا رفتن بار کاری کارایی این سرور پایین می‌آید، سرعت کل سیستم مختل می‌شود. مشکل دیگر مساله نقطه خرابی واحد یا به اصطلاح Single Point of Failure است، یعنی در صورت خرابی این سرور کل سیستم از کار می‌افتد.

در روش دوم یعنی روش غیر متمرکز، در واقع عمل احراز هویت از راه دور می‌باشد. مثلا وقتی از بیرون یک سازمان بخواهند عمل احراز هویت انجام دهند و به سرورهای مختلف آن سازمان دسترسی پیدا کنند، معمولا از این روش استفاده می‌کنند. در این شکل از کار معمولا مدیریت دسترسی در نزدیکی Object های مورد کنترل اعمال می‌شوند نه در مرکز اصلی IT سازمان. به طور مثال اگر دانشجویان نتایج کنکور را از سایت ببینند، عمل احراز هویت بر روی سرور نتایج کنکور انجام می‌گیرد نه بر روی سرور کل سازمان سنجش. در این روش چون در ذات خودش حالت توزیع‌شوندگی دارد، لذا نیاز به یک هارمونی یا هماهنگی بین سرورهایی که به صورت مشترک عملیات احراز هویت را انجام می‌دهند دارد، که این خود عاملی است برای افزایش پردازش‌های لازم (Overhead).

در روش سوم یعنی روش ترکیبی در واقع هدف استفاده از مزایای دو روش قبلی به طور همزمان می‌باشد. برای بعضی از منابع حیاتی سیستم مثل فایل‌های مهم و دیتابیس‌های فیزیکی بهتر است از روش متمرکز استفاده شود. برای سایر Object ها که از حساسیت کمتری برخوردار هستند می‌توان از روش غیر متمرکز استفاده کرد.

۳-۶) تکنیک‌های کاربردی برای مقابله با حملات علیه سیستم کنترل دسترسی

در این قسمت دو طرح اصلی را مورد بررسی قرار می‌دهیم:

- Monitoring
- Intrusion Detection System (IDS)

از جمله تکنیک‌های مورد استفاده در مقابل حملات در سیستم‌های Authentication روش مانیتورینگ می‌باشد. هدف اصلی که در این روش تعقیب می‌گردد این است که در قدم اول تمامی فعالیت Subject قابل حسابرسی باشد. در قدم دوم که استفاده امنیتی دارد هدف آن است که کلیه فعالیت‌های غیر مجاز و تلاش برای نفوذ در سیستم و یا خرابکاری آن مورد شناسایی قرار گیرد. مانیتورینگ بسیار وابسته به دو مبحث ثبت وقایع (Log) و حسابرسی (Auditing) می‌باشد. در بخش ثبت وقایع کلیه فعالیت‌های مهم قبل شروع یک نشست - مثل فعالیت درخواست شده توسط یک کاربر - در فایلی ثبت می‌گردد.

اما در مبحث IDS هدف جستجو و بازرسی در فایل‌های ثبت شده و همچنین اتفاقاتی که به صورت زنده در سیستم در حال انجام می‌باشد به منظور شناسایی تلاش‌های نفوذگران به سیستم است. در سیستم‌های کشف نفوذگر (IDS) معمولا دو شکل معرفی می‌گردد:

- بخشی از شبکه را به طور کامل تحت سرویس‌های امنیتی خود قرار دهد.
- تنها ماشین و یا Host خاصی را که عملیات با حساسیت بالایی انجام می‌دهد تحت پوشش سیستم کشف نفوذگر قرار دهد.

۳-۶-۱) سرویس‌های اصلی IDS

خدماتی که یک IDS در مقابل نفوذگران می‌دهد به سه دسته تقسیم می‌شود:

- فعال (Active)
- غیرفعال (Passive)
- مرکب (Hybrid)

در نوع فعال سیستم‌های کشف نفوذ، بلافاصله بعد از شناسایی یک نفوذ و تجاوز (Violation) با استفاده از سیاست‌های امنیتی یک اقدام و واکنش جدی صورت می‌گیرد. مثلا اگر IDS متوجه شود یک مجموعه از حملات Dos برای یک سرور در داخل شبکه تحت پوشش تدارک دیده شده، بلافاصله می‌تواند آن ارتباط را قطع کند.

اما در نوع دوم IDS که به عنوان روش غیر فعال شناخته می‌شود، در صورت انجام چنین اتفاقی واکنش سریعی انجام نمی‌گیرد و IDS فقط این رخداد را در فایل اتفاقات (Log File) ثبت می‌کند تا بعدا مدیر سیستم براساس اطلاعات ثبت و ضبط شده تصمیمات لازم را اتخاذ نماید.

اما در نوع سوم IDS یعنی روش ترکیبی هر دو کار به طور همزمان انجام می‌گیرد. یعنی هم اتفاقات ثبت و ضبط می‌شود و هم عکس‌العمل مناسب انجام می‌گیرد.

۳-۶-۲) نحوه شناسایی فعالیت‌های غیرمجاز (Intrusion Detection Methods)

شناسایی فعالیت‌های غیرمجاز در سیستم‌های IDS به دو طریق انجام می‌گیرد:

- مبتنی بر نشانه (Signature Based)
- مبتنی بر رفتار (Behavior Based)

در روش مبتنی بر نشانه ما از قبل برای وقوع حملات سناریوهایی را در نظر می‌گیریم. مثلا مدیر امنیت سیستم تجسم می‌کند که اگر فردی بخواهد به فایل حاوی رمزهای عبور (Pass Word) حمله کند چه کارهایی را انجام خواهد داد و از چه راه‌هایی خواهد گذشت و برای این سناریوی حمله یک سری نشانه را برای ورودی IDS قرار می‌دهد. آنگاه زمانی که IDS متوجه می‌شود که یک کاربر رفتار نامناسب انجام می‌دهد اطلاعات مربوط به رفتار کاربر را با اطلاعات درون دیتابیسی که حاوی ترتیب رفتاری نامناسب است و از قبل تدارک دیده شده ، مطابقت می‌دهد. در صورت بروز تطابق مشخص می‌شود که حمله‌ای تدارک دیده شده و یا در حال تدارک است، آنوقت IDS به صورت اتوماتیک پیغام هشداری برای یک عکس‌العمل مناسب (فعال، غیرفعال و یا ترکیبی) می‌فرستد.

اما در شکل دوم یعنی مبتنی بر رفتار، رفتارهای کاربران را در طی دوران‌های زمانی شناسایی و دسته‌بندی می-کنند. بدین شکل الگوهای رفتاری هر کاربر مجاز به دست آمده و در درون دیتابیس نگهداری می‌شود. در

صورتی که یک کاربر رفتار متفاوت با الگوهای شناسایی شده رفتاریش انجام دهد، معلوم می‌شود که این فرد که خود را به عنوان یک کاربر مجاز معرفی کرده، همان فرد مجاز نمی‌باشد بلکه یک نفوذگر است. روش مبتنی بر رفتار گاهی اوقات با نام Expert System هم معرفی می‌گردد.

فصل چهارم: مقدمه‌ای بر رمزنگاری (Cryptography)

مقدمه

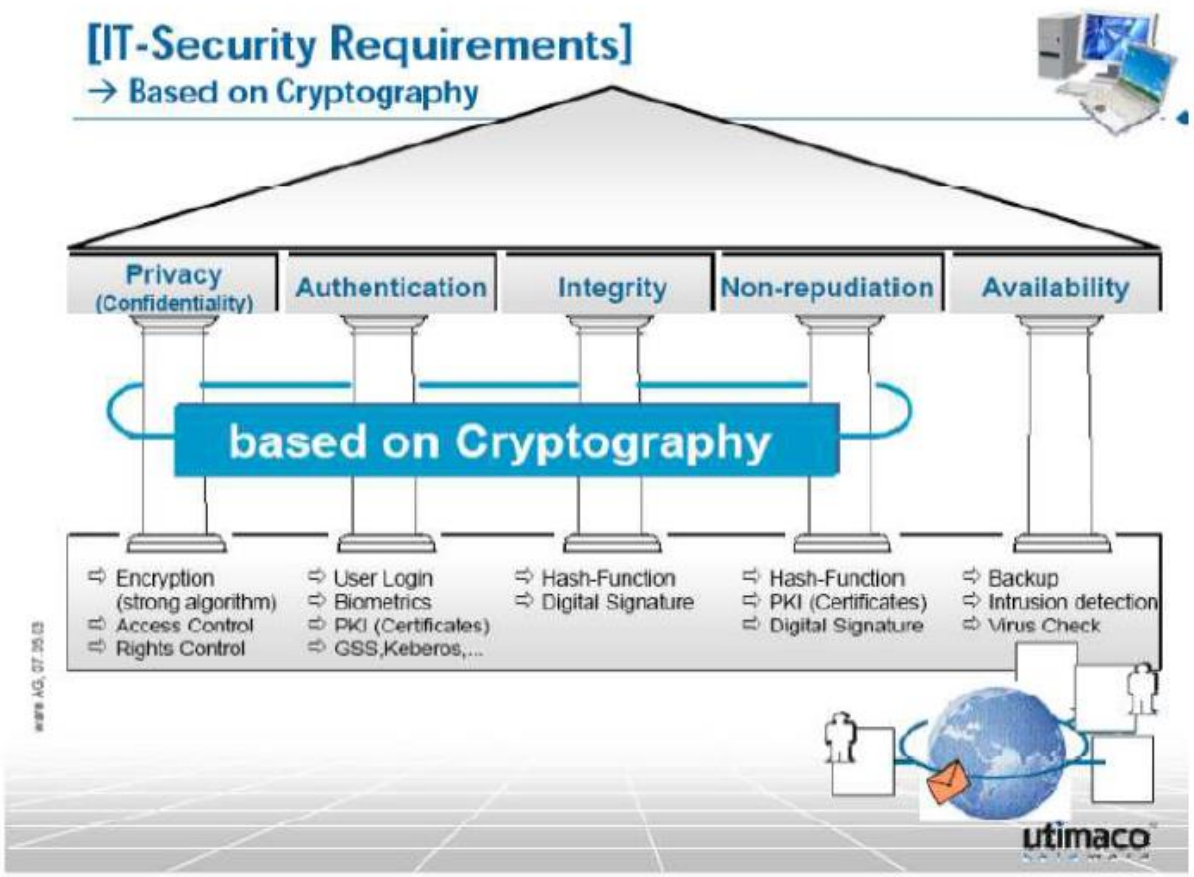
تاکنون امنیت را از مجموعه سرویس‌هایی مانند کنترل دسترسی، احراز هویت، در دسترس بودن معرفی کردیم و متوجه شدیم که چطور با تکنیک‌هایی مانند مانیتورینگ و سیستم‌های کشف نفوذ می‌توانیم امنیت سیستم را در مورد این سرویس‌های پایه بهبود بخشیم. در ادامه در این فصل به موضوع رمزنگاری می‌پردازیم.

به طور سنتی ورود به مبحث امنیت از طریق رمزنگاری بوده است، ولی این مورد به نوعی باعث خلط مبحث از منظر بسیاری از کارشناسان و مدیران شده است. این دو مقوله نزدیک به هم ولی متفاوت از هم می‌باشند. در واقع رمزنگاری یکی از سنگ‌های زیربنایی امنیت اطلاعات است. گسترش و رشد بی‌سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمان‌ها و موسسات شده است. امنیت اطلاعات یکی از مسائل مشترک شخصیت‌های حقوقی و حقیقی است. کاربران اینترنت در زمان استفاده از شبکه، اطلاعات حساس و مهمی را به دفعات ارسال و یا دریافت می‌کنند. اطمینان از عدم دستیابی افراد غیرمجاز به اطلاعات حساس از مهم‌ترین چالش‌های امنیتی در رابطه با توزیع اطلاعات در اینترنت است. اطلاعات حساس که ما تمایلی به مشاهده آنها توسط دیگران نداریم، موارد متعددی را شامل می‌شود. برخی از اینگونه اطلاعات به شرح زیر است:

- اطلاعات کارت اعتباری
- شماره‌های عضویت در انجمن‌ها
- اطلاعات خصوصی
- جزئیات اطلاعات شخصی
- اطلاعات حساس در یک سازمان
- اطلاعات مربوط به حساب‌های بانکی

تاکنون برای امنیت اطلاعات بر روی کامپیوتر و یا اینترنت از روش‌های متعددی استفاده شده است. ساده‌ترین روش حفاظت از اطلاعات، نگهداری اطلاعات حساس بر روی محیط‌های ذخیره‌سازی قابل انتقال نظیر فلاپی دیسک‌ها است. متداول‌ترین روش حفاظت اطلاعات رمز نمودن آنهاست. دستیابی به اطلاعات رمز شده برای افراد غیرمجاز امکان‌پذیر نبوده و صرفا افرادی که دارای کلید رمز می‌باشند، قادر به باز نمودن رمز و استفاده از اطلاعات هستند.

رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمزنگاری است. استفاده از علم رمزنگاری دارای یک سابقه طولانی و تاریخی است. قبل از عصر اطلاعات، بیشترین کاربران رمزنگاری اطلاعات، دولت‌ها و مخصوصا در موارد نظامی بوده است. سابقه رمز نمودن اطلاعات به دوران امپراطوری روم برمی‌گردد. امروزه اغلب روش‌ها و مدل‌های رمزنگاری اطلاعات در رابطه با کامپیوتر به خدمت گرفته می‌شود. کشف و تشخیص اطلاعاتی که به صورت معمولی در کامپیوتر ذخیره و فاقد هرگونه روش علمی رمزنگاری باشند، به راحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت.



شکل ۴-۱) شرایط لازم برای امنیت فناوری اطلاعات- براساس رمزنگاری

همانطور که در شکل ۴-۱ مشاهده می‌شود امنیت در محیط‌های فناوری اطلاعات به مثابه یک ساختمان می-باشد و سرویس‌های پایه‌ای لازم برای ایجاد امنیت در محیط‌های فناوری اطلاعات مانند احراز هویت، صحت اطلاعات، انکارناپذیری و محرمانگی می‌توانند براساس رمزنگاری اجرا گردند.

به طور ساده می‌توان گفت رمزنگاری عبارت است از انجام محاسبات بر روی متن داده‌ای ورودی به منظور تبدیل کردن آن به یک متن غیرواضح و غیر قابل آشکارسازی توسط افراد غیرمجاز.

در این فصل در ابتدا نکاتی در مورد تاریخچه رمزنگاری، مفاهیم اولیه رمزنگاری و حملات محتمل بر سیستم-های رمزنگاری مطرح کرده و در امتداد مروری کوتاه بر الگوریتم‌های رمزنگاری خواهیم داشت و در انتها فصل را با توضیح مختصری از زیرساخت‌های کلید عمومی به پایان خواهیم برد.

۴-۱) تاریخچه رمزنگاری

علم رمزنگاری دارای سابقه‌ای طولانی است. شاید بتوان گفت اولین سیستم رمزنگاری سیستمی باشد که توسط ژولیت سزار (پادشاه روم باستان) در جنگ‌های بیش از دو هزار سال قبل مورد استفاده قرار داده شده است. در این روش رمزنگاری الفبای رومی را ۳ حرف به سمت راست می‌چرخاندند (مانند شکل ۴-۲).

دانش رمزنگاری در طول زمان گسترش یافت به طوری که در طول جنگ جهانی دوم از آن به صورت گسترده‌ای استفاده گردید.

متن رمز شده	متن اصلی
DEF	ABC
Khoor	Hello
Dwwdfn	Attack

شکل ۴-۲) روش رمزنگاری سزار

مانند بقیه علوم، دانش رمزنگاری هم توسط نیروهای مسلح به ویژه در هنگام جنگ‌ها پیشرفت قابل ملاحظه‌ای داشته است. در زمان سزار به طور سنتی در طی سال‌ها از سیستم رمزی که به صورت جایگشتی عمل می‌کرده استفاده شده است.

۴-۲) مفاهیم رمزنگاری

در دانش رمزنگاری از مفاهیم پایه‌ای به کرات استفاده می‌گردد که برخی از آنها عبارتند از:

متن واضح (Plain Text)

آن پیغام یا داده اولیه است که به سهولت قابل خواندن است.

متن رمز شده (Cipher Text)

بعد از انجام یک عمل رمزنگارانه متن واضح اولیه را به یک متن رمز شده تبدیل می‌کنیم. این متن تنها زمانی قابل خواندن است که توسط الگوریتم رمزگشایی از حالت رمز خارج گردد. باید توجه داشت که الگوریتم رمزنگاری و الگوریتم رمزگشایی باید با هم رابطه داشته باشند، به گونه‌ای که بتوان با داشتن اطلاع خاصی (که معمولا از آن به عنوان کلید یاد می‌شود) بتوان متن رمز شده را به متن واضح برگرداند.

رمزنگاری (Cryptography)

به فرایندی که در آن متن واضح با اعمالی همچون آرایش مجدد و یا جایگزین کردن علامت، کاراکتر یا نشانه و یا علامت دیگری، از حالت قابل خواندن به متن غیر قابل خواندن تبدیل می‌شود، رمزنگاری اطلاق می‌گردد.

الگوریتم (Algorithm)

عبارت است از قدم‌های متوالی و از پیش تعیین شده‌ای که بر روی متن واضح انجام می‌شود و در خروجی آن متن رمز شده حاصل می‌گردد. باید توجه داشت که این تعریف شامل الگوریتم‌های رمزگشایی (Decryption) هم می‌شود، یعنی متن رمز شده را به الگوریتم رمزگشایی می‌دهیم و الگوریتم می‌تواند متن واضح را ایجاد کند.

کلید (Key)

یک تفاوت عمده بین الگوریتم‌های رمزنگاری و الگوریتم‌های متعارف کدینگ در بهره‌گیری الگوریتم‌های رمزنگاری از کلید است. در واقع بخش عمده‌ای از الگوریتم‌های متعارف رمزنگاری ارائه و منتشر شده‌اند. یعنی همه می‌دانند که ساختار و نحوه انجام عمل الگوریتم به چه ترتیبی است و این الگوریتم‌ها در طی چه مراحلی یک متن واضح را می‌گیرند و به یک متن رمزنگاری تبدیل می‌کنند و بالعکس. اما با این توصیفات چرا این متن

رمز شده توسط افراد غیر مجاز قابل خواندن نمی‌باشد، در حالیکه فرد غیر مجاز هم ممکن است الگوریتم را بداند؟ دلیل این موضوع مفهوم کلید است. در واقع هر الگوریتم به ازای کلید متفاوت، خروجی متفاوتی تولید می‌کند.

نکته بسیار مهم در بحث رمزنگاری مدیریت کلید است، به نحوی که اطلاعات به سادگی افشا نگردد. بالاخص در محیط‌های تجارت الکترونیک و دولت الکترونیک نمی‌توان به سمت الگوریتم‌های خاصی که در صنایع نظامی است و توسط افراد خاص استفاده می‌شود، رفت. در چنین محیط‌هایی باید سراغ الگوریتم‌های منتشر شده رفت. لذا آنچه به صورت محرمانه و مخفی بین طرف‌های مجاز جابجا می‌شود، کلید است.

۴-۳) انواع حملات به سیستم‌های رمزنگاری

حمله عبارت است از هر نوع تلاشی که توسط مهاجم انجام می‌گیرد که فضای جستجو را در بین متن‌های واضح برای یک متن رمز شده و یا در بین تمام فضای جستجو برای کلید، محدود می‌سازد. به طور مثال در مورد یک کلید n بیتی تمامی حالات ممکن این کلید می‌تواند فضای جستجو باشد. یعنی مثلا اگر یک کلید ۴ بیتی داشته باشیم، حمله‌کننده مواجه با یک فضای جستجوی $۲^۴=۱۶$ تایی است. لذا هر چه تعداد بیت‌های کلید اضافه شود فضای جستجوی مهاجم به روش نمایی اضافه می‌شود. اما در واقع این روش جستجو و حمله برای کلید ساده‌ترین شکل می‌باشد و به نام جستجوی فراگیر (Exhaustive Search) نامیده می‌شود. معمولا برای حمله به یک سیستم رمزنگاری از انواع تکنیک‌های زیر استفاده می‌شود.

۴-۳-۱) فقط متن رمز شده (Cipher Text Only)

در این خانواده از حملات فرد مهاجم فقط یک متن رمز شده دارد و از روی آن می‌خواهد کلید استفاده شده برای رمزنگاری را به دست آورد. در این حالت به طور طبیعی برای حمله‌کننده اطلاع خاصی وجود ندارد و باید سراغ روش‌های جستجوی فراگیر برود.

۴-۳-۳) متن واضح انتخاب شده (Chosen Plain Text)

در این روش مهاجم این امکان را دارد که برای تعدادی متن واضح که در اختیار دارد، متن رمز شده آن را تولید کند. در این روش نیز هدف مهاجم مشخص کردن کلید است. مثالی برای این روش آن است که مثلا فرد مهاجم منشی و یا کارمند یک دفتر است و یا دشمن در این دفتر جاسوس دارد و از طریق این جاسوس می‌تواند با دستگاه رمزنگاری این دفتر کار کند ولی نمی‌تواند کلید را تغییر دهد و یا تنظیم کند یا بخواند و فقط می‌تواند به دستگاه رمزنگاری متن واضح را وارد کند و متن رمز شده را به دست آورد. در این روش فرد مهاجم این امکان را دارد که دائما تحلیل کند و الگوهای واضح مورد نظر خودش را تولید کند و برای نزدیک شدن به کلید آنها را به دستگاه رمزنگار بدهد و دستگاه رمزنگار نیز با محاسبات درونی که انجام می‌دهد متن رمز شده را ارائه دهد. به این ترتیب در دفعات متوالی اطلاعات مهاجم نسبت به کلید اضافه می‌شود. به این ترتیب فضای جستجو و آنالیز برای به دست آوردن کلید مرتبا برای مهاجم کاهش پیدا می‌کند.

۴-۳-۴) متن رمز شده انتخاب شده (Chosen CipherText)

این روش چیز شبیه روش قبلی است با این تفاوت که در این روش فرد مهاجم می‌تواند متون رمز شده را به دستگاه رمزگشا بدهد و متون واضح را به دست آورد (عکس روش قبلی).

۴-۳-۵) متن انتخاب شده (Chosen Text)

این روش ترکیب دو روش قبلی است. یعنی فرد مهاجم می‌تواند به تعداد نامحدود متن واضح به دستگاه رمزنگار بدهد و متن رمز شده به دست آورد و هم عکس عمل را انجام دهد. یعنی تعدادی متن رمز شده را به دستگاه رمزگشا بدهد و متن واضح آن را به دست آورد. به این ترتیب فضای جستجو برای به دست آوردن کلید را مرتبا کاهش دهد.

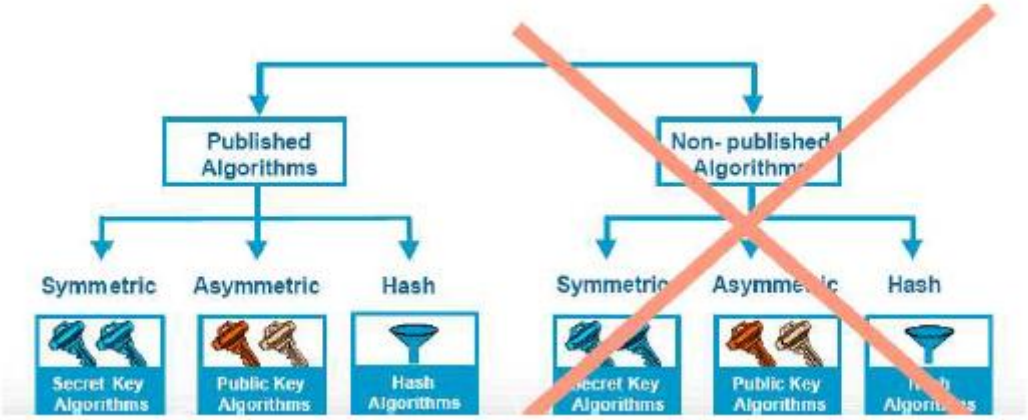
۴-۴) انواع الگوریتم‌های رمزنگاری

همانطور که قبلا مطرح شد الگوریتم‌های رمزنگاری به دو دسته کلی تقسیم می‌شوند:

- الگوریتم‌های منتشر شده (Published Algorithms)

- الگوریتم‌های منتشر نشده (Non- Published Algorithms)

گروه الگوریتم‌های منتشر شده الگوریتم‌هایی هستند که توسط گروه‌های تحقیقاتی طراحی گردیده و به بازار تجاری ارائه می‌شوند و توسط گروه‌های مختلف مورد آزمایش و بررسی قرار گرفته و معایب آن مرتفع می‌گردد. در این الگوریتم‌ها، اطلاعات مرتبط با ساختار الگوریتم و اقداماتی که به طور متوالی بر روی متن ورودی انجام می‌دهد به صورت عمومی منتشر می‌گردد.



شکل ۴-۳) انواع الگوریتم‌های رمزنگاری

اما در مقابل الگوریتم‌های منتشر نشده وجود دارند که معمولا در صنایع مخابراتی و نظامی مورد استفاده قرار می‌گیرند. باید توجه داشت از آنجا که این الگوریتم‌ها برای مراکز خاصی طراحی می‌شوند و کاربرد عمومی ندارند، ساختار این الگوریتم‌ها هیچ‌گاه مورد انتشار عمومی قرار نمی‌گیرند و لذا مدیریت آنها در مقابل تهاجمات آسان‌تر است. همانطور که در شکل ۴-۳ مشاهده می‌گردد هدف ما در این درس الگوریتم‌های منتشر شده است.

۴-۵) انواع الگوریتم‌های منتشر شده

الگوریتم‌های منتشر شده به سه دسته کلی تقسیم می‌شوند:

- متقارن (Symmetric)
- نا متقارن (Asymmetric)
- توابع درهم‌ریزی (Hash)

۴-۵-۱) الگوریتم‌های متقارن (Symmetric Algorithms)

الگوریتم متقارن یا الگوریتم کلید خصوصی (Secret Key Algorithm) الگوریتمی است که در آن کلید رمزنگاری و کلید رمزگشایی در هر دو طرف گیرنده و فرستنده یا با هم برابرند یا به سهولت توسط توابع ساده ریاضی می‌توان از روی کلید رمزنگاری کلید رمزگشایی را استحصال کرد.

۴-۵-۱-۱) الگوریتم جایگشتی

یکی از الگوریتم‌های متقارن الگوریتم جایگشتی است که در ادامه به توضیح آن می‌پردازیم. برای توضیح این موضوع می‌توان به شکل ۴-۴ توجه کرد.

I	S	A	A	C
4	5	1	2	3
I	L	I	K	E
L	E	A	R	N
K	E	Y		

شکل ۴-۴) مثالی از الگوریتم جایگشتی

فرض کنید متن واضحی بدین شکل داریم: "I LIKE LEARN KEY" و می‌خواهیم توسط کلید خصوصی "ISAAC" این متن واضح را به متن رمز شده تبدیل کنیم. با توجه به اینکه کلید خصوصی ما پنج حرفی است، جدولی با ۵ ستون تشکیل می‌دهیم و آنگاه در سطر دوم جدول شماره هر کدام از حروف مربوط به کلید را با توجه به جایگاه آن در حروف الفبا قرار می‌دهیم. در ادامه کلیه حروف مربوط به متن واضح را در خانه‌های مختلف جدول می‌چینیم. حال برای به دست آوردن متن رمز شده ابتدا نگاه می‌کنیم به ستون با کمترین شماره. این ستون در این جدول ستون شماره ۳ است، آنگاه حروف مربوط به آن ستون را پشت سر هم قرار می-دهیم (LAY). ستون بعدی ستون شماره ۴ است (KR)، دقت کنید که با توجه به آگاهی از طول متن واضح از اینکه آخرین خانه این ستون خالی است مطلع می‌باشیم. در ادامه نوبت به حروف ستون ۵ می‌رسد (EN) و بعد

ستون شماره ۱ (ILK) و در نهایت ستون ۲ (LEE). در نهایت متن رمز شده روبرو به دست می‌آید: IAYKR ENILK LEE.

حال به طور معکوس در طرف گیرنده برای تبدیل متن رمز شده به متن واضح، مجددا این جدول را داریم. در این جدول ۲ سطر اول باز برای طرف گیرنده مشخص است. یعنی طرف گیرنده به کلید (ISAAC) آگاهی دارد و بر این اساس می‌تواند شماره ستون‌ها را بچیند (توجه کنید که کلید ISAAC که یک کلید متقارن است بین دو طرف گیرنده و فرستنده محرمانه می‌باشد و فرد دیگری نسبت به آن اطلاع ندارد). حال بعد از چیدن حروف کلید در جدول، گیرنده شروع می‌کند به چیدن حروف در ستون شماره ۳، که سه حرف می‌باشد. دقت کنید با توجه به اینکه طول متن رمز مشخص می‌باشد، گیرنده می‌تواند تشخیص دهد تعداد سطرهای جدول چه میزان است، پس به سادگی می‌تواند تعداد سلول‌های خالی را تشخیص دهد. در ادامه مابقی حروف را نیز در جدول قرار می‌دهد. در نهایت برای به دست آوردن متن واضح به جای آنکه آن را ستونی بخواند به صورت سطری می‌خواند.

۴-۵-۱-۲) الگوریتم جانشینی

نوع دیگر الگوریتم‌های متقارن الگوریتم مبتنی بر جانشینی (Substitution) است، که در ادامه به توضیح این روش خواهیم پرداخت. در الگوریتم جانشینی به طور کلی هر حرف مربوط به متن واضح را با یک مقدار حرف جدید جایگزین می‌کنیم. در واقع ما به جدولی نیاز داریم که در آن جدول مشخص می‌شود که به ازای هر کاراکتر چه کاراکتری باید جایگزین شود. مثال ساده آن الگوریتم رمز سزار یا روتیشن ۳ بود که در گذشته از آن سخن به میان آوردیم. در این نوع رمزنگاری هم فرستنده و هم گیرنده از یک جدول جانشینی استفاده می‌کنند که این جدول است که باید به صورت محرمانه بین این دو باقی بماند. باید توجه داشت که این دست از الگوریتم‌ها در ذات خود به صورت تئوریک قابل شکستن می‌باشند. اما یک الگوریتم جانشینی که در ذات خود به صورت تئوریک غیر قابل شکستن است الگوریتم One-Time-Pad (OTP) است. این الگوریتم مبتنی بر اعداد واقعا تصادفی می‌باشد. در این الگوریتم ما یک جدول خواهیم داشت و در این جدول تعدادی حرف را به صورت تصادفی تولید می‌کنیم و این حروف به مجموعه‌ای از حروف جدید نشانه‌گذاری می‌شوند. در این روش پیغام را رمز کرده و ارسال می‌کنیم و طرف گیرنده عمل عکس را انجام می‌دهد. دقت کنید چون در هر بار عمل رمزنگاری یک OTP جدید تولید می‌کنیم، پی بردن به این OTP ها که به صورت کاملا تصادفی ایجاد می-

گردد برای حمله‌کننده غیرممکن است. پس در این روش کانال ارسال این OTP ها بین گیرنده و فرستنده باید کاملا امن باشد ولی متن رمز شده می‌تواند از کانال ناامن نیز ارسال گردد.

یکی دیگر از الگوریتم‌های جانشینی، رمز جانشینی ویگنر (Substitution Cipher-Vigenere) است که به شکل رمز چند الفبایی است. بدین معنی که به ازای هر کاراکتر در متن واضح چندین کاراکتر به عنوان کاراکتر رمز شده قرار می‌دهیم و به این دلیل حمله‌کننده دیگر با حملاتی مثل حملات تکرار و تعداد کاراکترهای رمز شده در متن رمز شده به اطلاعات متن واضح دسترسی پیدا نمی‌کند.

همانطور که در شکل ۴-۵ مشهود است جدول ویگنر جدولی است که در اولین سطر آن حروف انگلیسی به ترتیب الفبا و در هر سطر یک حرف الفبای انگلیسی به سمت راست شیفت پیدا کرده است. روش کار برای به رمز درآوردن متون واضح بین فرستنده و گیرنده متن با بهره‌گیری از این جدول بدین شکل است که این جدول به صورت ثابت بین گیرنده و فرستنده تبادل شده است. ارسال‌کننده اطلاعات یک متن را به عنوان کلید در نظر گرفته و تلاش می‌کند این متن را به تعدادی که کل حروف متن واضح را پوشش دهد در زیر متن واضح تکرار کند. به طور مثال فرض کنید متن واضح جمله: "ATTACK AT DOWN" باشد و متن کلید کلمه "SECRET" باشد. پس متن جمله واضح و جمله کلید به شکل زیر می‌باشد:

متن واضح: ATTACKATDOWN

متن کلید: SECRETSECRET

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

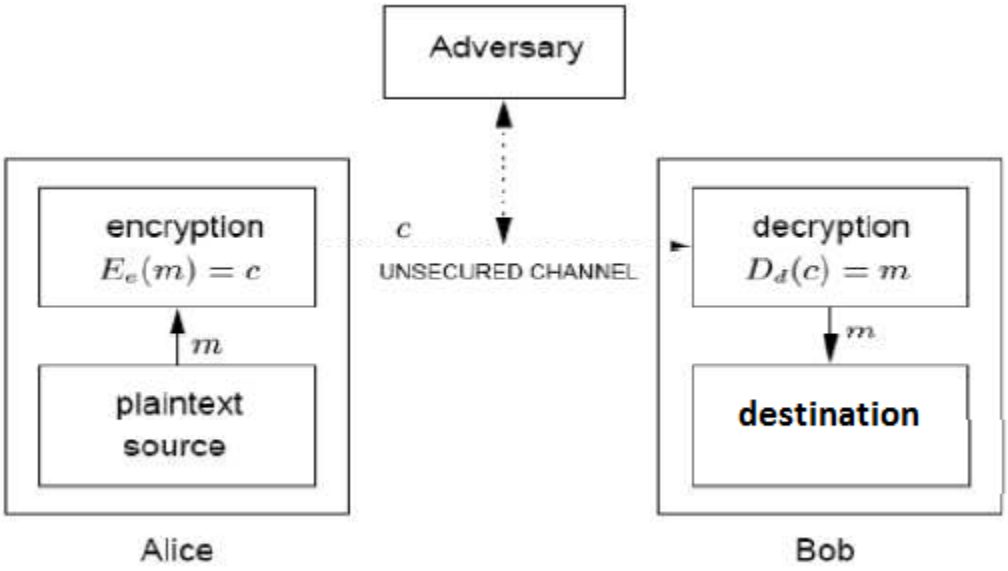
شکل ۴-۵) جدول جانشینی ویگنر

حال می‌خواهیم طبق جدول حروف متن واضح را به حروف رمز درآوریم. همانطور که می‌بینیم اولین حرف ما در متن واضح حرف "A" است و اولین حرف مطابق با آن در متن کلید حرف "S" می‌باشد. طبق جدول مکان تلاقی ستونی که با حرف "A" شروع شده و سطری که با حرف "S" شروع شده پیدا می‌کنیم. می‌بینیم که محل تلاقی این سطر و ستون حرف "S" است، پس اولین حرف جمله رمز ما حرف "S" می‌شود. به همین ترتیب حرف دوم متن واضح ما حرف "T" و دومین حرف جمله کلید حرف "E" می‌باشد که محل تلاقی ستون و سطر مربوطه در جدول حرف "X" می‌باشد که دومین حرف جمله رمز شده ما می‌شود. به همین ترتیب مراحل را برای دیگر حروف متن واضح به انجام می‌رسانیم. متن رمز شده نهایی به شکل زیر است:

متن رمز شده: sxvrgdsxfrag

همانطور که در ورش‌های رمزنگاری که تاکنون بیان گردید مشاهده کردید یکی از محدودیت‌هایی که باعث می-شود سطح اعتماد روش رمزنگاری پایین بیاید طول کلید است. به صورت کلی هرچه طول کلید کمتر باشد افراد

مهاجم با عملیات ساده‌تری برای شناسایی کلید رمزنگاری و شکستن رمز مواجه هستند. این نکته حائز اهمیت است که روش‌های رمزنگاری که تاکنون مطرح گردیده مبتنی بر رمزنگاری رشته‌ای بودند. در واقع در این روش رمزنگاری هر بیت اطلاعات به طور جداگانه مورد پردازش قرار می‌گیرند. اما نوع دیگر روش‌های رمزنگاری مبتنی بر بلوکی از بیت‌ها می‌باشند. در این روش یک بلوک از بیت‌های متن واضح با یک بلوک از بیت‌های متن کلید در طی پردازش‌هایی متن رمز شده را تولید می‌کنند. لذا تغییر در یک بیت متن واضح تغییرات گسترده‌ای را در متن رمز شده ایجاد می‌کند. به طور کلی عمل رمزنگاری را می‌توان مطابق شکل ۴-۶ توصیف کرد.

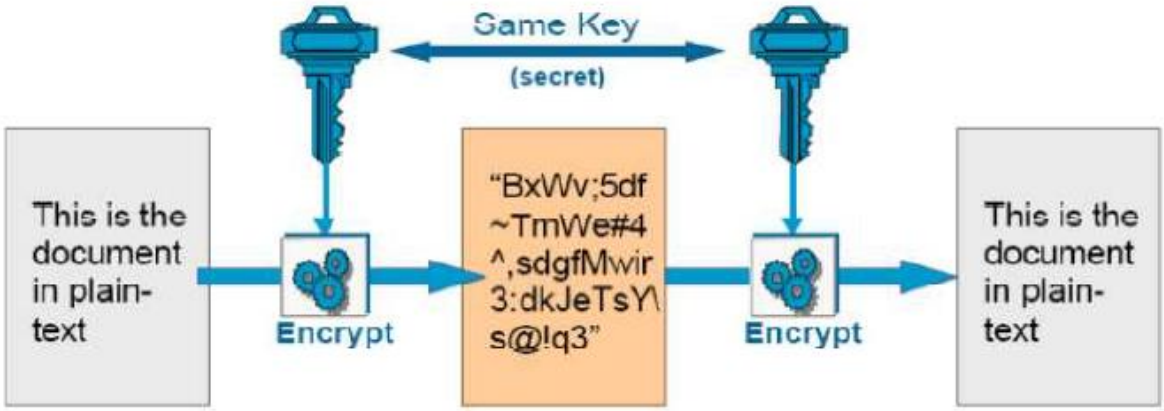


شکل ۴-۶) مدل رمزنگاری

همانطور که در شکل بالا مشهود است فرستنده‌ای به نام Alice درصدد ارسال پیام به سمت گیرنده‌ای به نام Bob می‌باشد. فرستنده متن واضحی را از منبع متون واضح خودش مثل m انتخاب می‌کند. آنگاه یک تبدیل رمزنگارانه مبتنی بر کلید e را بر روی آن انجام می‌دهد. نتیجه متن رمز شده c می‌باشد که فرستنده می‌تواند از طریق کانال ناامنی برای گیرنده ارسال نماید. گیرنده نیز با دریافت متن رمز شده c و اعمال الگوریتم رمزگشایی مبتنی بر کلید d به متن واضح m دست پیدا می‌کند. همانطور که در شکل مشهود است دشمنان و رقبا بع کانال ارسال متن رمز شده دسترسی دارند ولی به دلیل آنکه متن رمز شده می‌باشد، امکان استفاده از آن برایشان مقدور نیست. توجه نمایید که این نوع از رمزنگاری مبتنی بر زوج کلید می‌باشد. حال در ادامه نحوه عملکرد الگوریتم‌های رمزگذاری متقارن را بیشتر توضیح می‌دهیم.

۴-۵-۱-۳) توضیحات تکمیلی در مورد الگوریتم‌های رمزگذاری متقارن

این الگوریتم‌ها، الگوریتم‌های کلید مخفی نیز نامیده می‌شوند. در این الگوریتم، کلید رمزنگاری و کلید رمزگشایی مشابه هستند و یا اینکه به سهولت و از طریق محاسبات نسبتا ساده از روی یکدیگر قابل محاسبه می‌باشند. مثلا یک کلید عکس کلید دیگر است. این الگوریتم دارای نقاط ضعفی است از جمله اینکه توزیع کلید بین طرفین مبادله کلید به خودی خود کاری مشکل و پرمخاطره می‌باشد. این بدان معنی است که کلید رمزنگاری و یا رمزگشایی باید از کانال امنی انتقال یابد. مشکل دیگر این الگوریتم‌ها این است که سرویس انکارناپذیری را پوشش نمی‌دهند. همچنین این نوع از رمزنگاری مقیاس‌پذیر نمی‌باشد، یعنی نمی‌توان این نوع از رمزنگاری را به صورت بلوکی و به ازای طول بلوک‌های مختلف انجام داد. البته در مقابل این نقاط ضعف، این الگوریتم‌ها در مقایسه با الگوریتم‌های نامتقارن بسیار سریع هستند.

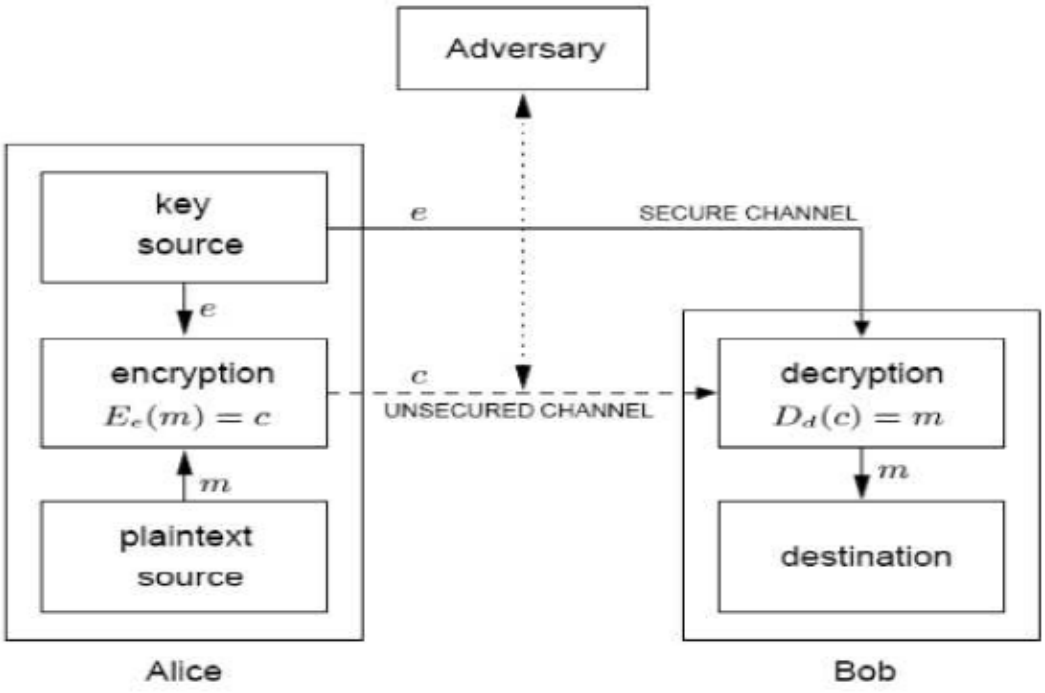


شکل ۴-۷) شمایی از الگوریتم رمزنگاری متقارن

همانطور که در شکل ۴-۷ مشاهده می‌شود در الگوریتم رمزنگاری متقارن گیرنده و فرستنده برای اعمال رمزنگاری و رمزگشایی از یک کلید مشابه استفاده می‌کنند.

در شکل ۴-۸ روش توزیع کلید در الگوریتم متقارن به تصویر کشیده شده است. آلیس به عنوان فرستنده متن با استفاده از کلید رمزنگاری e که توسط یک تولیدکننده کلید دریافت کرده، متن واضح m را به متن رمز شده c با بهره‌گیری از الگوریتم E، رمزنگاری می‌کند. باید توجه داشت در این راستا کلید رمزنگاری باید از طریق یک

کانال امن به گیرنده پیام یعنی باب فرستاده شود، ولی برای ارسال پیام رمز شده c، نیازی به کانال ارسال امن نمی‌باشد.



شکل ۴-۸) روش توزیع کلید در الگوریتم متقارن

توجه کنید در این روش رمزنگاری به دلیل امکان لو رفتن کلید رمزنگاری، طرفین رمزنگاری باید به صورت دوره‌ای کلید رمزنگاری را تغییر دهند.

مشکل دیگر در این روش رمزنگاری این است که با بالا رفتن طرفین تبادل اطلاعات، تعداد کلید رمزنگاری به صورت نمایی افزایش می‌یابد یعنی اگر به جای آنکه فقط دو نفر آلیس و باب تبادل اطلاعات کنند، سه نفر به تبادل اطلاعات بین یکدیگر بپردازند، برای رمزنگاری نیاز به ۳ کلید رمزنگاری می‌باشد. به این ترتیب با بالا رفتن نفرات، تعداد کلید افزایش می‌یابد (تعداد کلید از فرمول n(n-1)/2 تبعیت می‌کند که در این فرمول n تعداد نفرات است). بدین ترتیب حفظ امنیت کلید و مدیریت این کلیدها در یک شبکه به یک کار بسیار پیچیده تبدیل می‌شود.

از جمله الگوریتم‌های رمزنگاری می‌توان به الگوریتم‌های DES، Blowfish، IDEA، AES، Triple DES اشاره کرد. بعضی از مشخصات این الگوریتم‌ها عبارتند از:

DES: دارای کلید با طول ۶۵ بیت، تا سال ۱۹۹۸ استاندارد دولتی آمریکا بود. ولی امروزه به اندازه کافی قدرتمند نمی‌باشد، که به عنوان استاندارد دولتی محسوب گردد.

Triple DES: سه بار عملیات الگوریتم DES را انجام می‌دهد. دارای کلیدی با طول ۱۶۸ بیت است و کاربرد وسیعی دارد. نسبت به DES امن‌تر است ولی کند می‌باشد.

AES: طول کلید متغیر دارد. آخرین استاندارد دولتی آمریکا می‌باشد و جای الگوریتم DES را گرفته است.

IDEA: دارای کلید ۱۲۸ بیتی بوده و برای استفاده نیاز به مجوز دارد.

Blowfish: طول کلید متغیر دارد. الگوریتم آن مجانی و در اختیار عموم بوده و بسیار سریع است.

۴-۵-۲) الگوریتم‌های نامتقارن (Asymmetric Algorithms)

با توجه به مشکلاتی که در مساله توزیع کلید در الگوریتم‌های رمزنگاری متقارن یا مبتنی بر کلید خصوصی داریم، به تدریج در دنیای رمزنگاری مبحثی به نام الگوریتم‌های کلید عمومی یا به اصطلاح الگوریتم‌های نامتقارن شکل گرفت.

در این روش، در واقع فرستنده اطلاعات یک زوج کلید را تولید می‌کند. یکی از کلیدها مخفی و خصوصی و دیگری کلید عمومی است که آن را در اختیار عموم افراد قرار می‌دهد. برای انجام رمزنگاری، فرستنده اطلاعات متن مورد نظر خود را با کلید عمومی گیرنده متن به رمز درآورده و این متن رمز شده را از طریق کانال ناامنی برای گیرنده ارسال می‌کند. گیرنده هم با استفاده از کلید خصوصی خود این متن را رمزگشایی کرده و به متن اصلی و واضح دست پیدا می‌کند. نکته حائز اهمیت آن است که با انتشار کلید عمومی، هکرها و کاربران غیر مجاز هم قادر به آن هستند که اطلاعاتی را رمزگذاری کرده و به سمت گیرنده ارسال کنند و با اینکه هکر هم به کلید عمومی و هم به الگوریتم رمزگذاری دسترسی دارد، اما نمی‌تواند کلید خصوصی دریافت‌کننده پیام را کشف و شناسایی کند.

این نوع الگوریتم‌ها در انجام سرویس‌های امنیتی کاربرد وسیعی دارند. این الگوریتم‌ها برای انجام سرویس‌های امنیتی محرمانگی، احراز هویت و انکارناپذیری استفاده می‌شوند. این الگوریتم‌ها در دنیای امنیت به عنوان الگوریتم‌های کلید عمومی نیز نامیده می‌شوند.

۴-۵-۲-۱) انجام سرویس محرمانگی با بهره‌گیری از الگوریتم‌های نامتقارن

برای تحقق سرویس محرمانگی که هدف محرمانه نگه داشتن اطلاعات انتقالی بین طرفین مبادله پیغام می‌باشد، روش انجام کار بدین شکل می‌باشد که فرد دریافت‌کننده پیام از قبل زوج کلید رمزنگاری را برای خود تدارک دیده است (یک کلید به عنوان کلید خصوصی و یک کلید به عنوان کلید عمومی). این گیرنده پیام کلید عمومی خود را برای اطلاع دیگران منتشر کرده است، مثلا آن را برای اطلاع دیگران بر روی وب‌سایت خود قرار داده و یا آن را از طریق نشریات تبلیغاتی به اطلاع دیگران رسانیده است. البته لازم به توجه است که کلید دوم یعنی کلید خصوصی را تنها پیش خود به صورت محرمانه نگه داشته است. حال فرستنده پیام با آگاهی از کلید عمومی فرستنده، متن مورد نظر را با کلید عمومی گیرنده رمز کرده و از طریق کانال ناامنی برای گیرنده ارسال می‌کند. گیرنده هم با دریافت متن رمز شده با بهره‌گیری از کلید خصوصی خود، این متن رمز شده را از رمز خارج کرده و به یک متن واضح تبدیل می‌کند. روشن است که فرد مهاجم و دشمن علی‌رغم اطلاع از کلید رمزنگاری عمومی و دستیابی به متن رمز شده، چون از کلید خصوصی آگاهی ندارد، قادر به اطلاع از متن واضح نمی‌باشد.

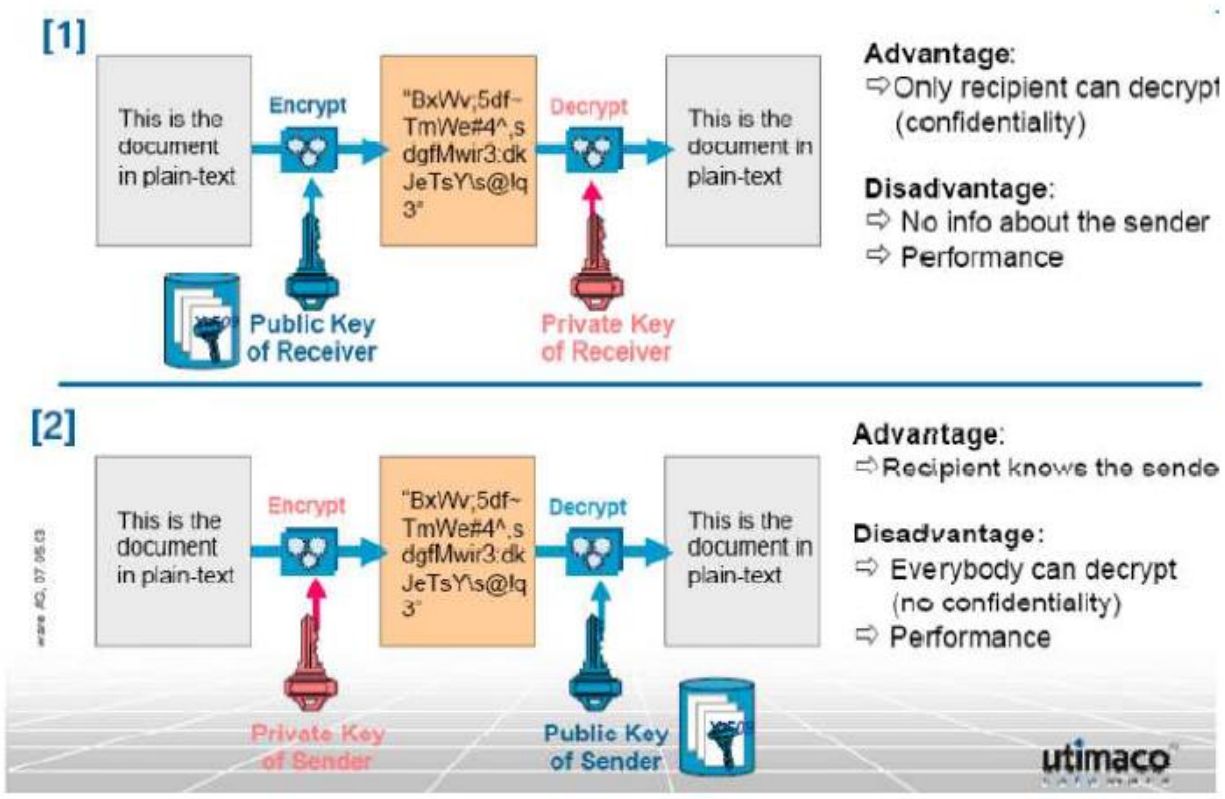
از جمله نقاط قوت این روش این است که سرویس انکارناپذیری را پشتیبانی می‌کند، مدیریت کلیدها راحت است، چرا که تعداد کلیدها به تعداد کاربران می‌باشدو همچنین توزیع کلید راحت است. اما نقطه ضعف آن هم پایین بودن سرعت آن است، چرا که میزان محاسبات در الگوریتم‌های نامتقارن بیشتر از الگوریتم‌های متقارن است.

۴-۵-۲-۲) انجام سرویس احراز هویت با بهره‌گیری از الگوریتم‌های نامتقارن

اما در ابتدای این پاراگراف اشاره داشتیم به اینکه یکی از سرویس‌های امنیتی دیگر که توسط الگوریتم‌های نامتقارن پشتیبانی می‌شوند، سرویس احراز هویت است. برای انجام این سرویس فرستنده با کلید خصوصی خود یک متن معنی‌دار را به یک متن رمز شده تبدیل کرده و آن را منتشر می‌نماید. در اینجا تمام کسانی که به کلید عمومی او دسترسی دارند، می‌توانند روی متن رمز شده عمل رمزگشایی را انجام داده و متن واضح را شناسایی کنند. باید توجه داشت که در این سرویس هدف، محرمانگی این اطلاعات نمی‌باشد، بلکه احراز هویت فرستنده پیام است. بدین ترتیب گیرنده پیام با به دست آوردن متن واضح و دارای معنا با استفاده از کلید عمومی فرستنده که بر روی متن رمز شده اعمال کرده است، می‌تواند از صحت ارسال‌کننده آن مطمئن شود.

در امتداد این نکته قابل توجه است که ما می‌توانیم با بهره‌برداری از الگوریتم کلید عمومی، دو سرویس محرمانگی و احراز هویت را در کنار هم داشته باشیم. یعنی با استفاده از کلید منتشر شده یک گیرنده می‌توانیم برایش متن رمز شده و محرمانه ارسال کنیم. همچنین فرد فرستنده می‌تواند با رمز کردن این متن رمز شده با کلید خصوصی خودش و ارسال آن به گیرنده، گیرنده در ابتدا با کلید عمومی فرستنده مرحله اول رمزگشایی را انجام دهد و در نتیجه می‌تواند به صحت فرستنده پی ببرد و آنگاه با رمزگشایی مجدد با کلید خصوصی خود به متن واضح اصلی دست یابد.

در شکل ۴-۹ شمایی از دو سرویس امنیتی محرمانگی و احراز هویت با استفاده از الگوریتم کلید عمومی، در دو بخش ۱ و ۲ آورده شده است.

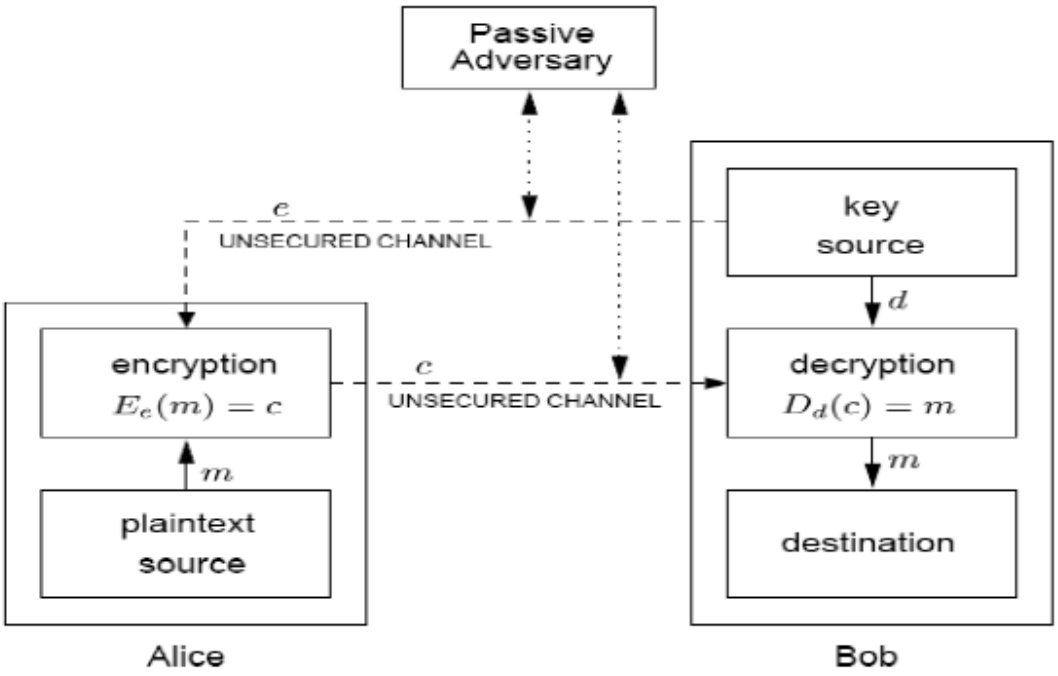


شکل ۴-۹) شمایی از دو سرویس محرمانگی و احراز هویت با استفاده از الگوریتم کلید عمومی

همچنین با توجه به شکل ۴-۱۰ می‌توان از نحوه توزیع کلید در الگوریتم متقارن مطلع گردید. همانطور که در شکل ملاحظه می‌کنید گیرنده یعنی باب، از یک منبع محاسباتی ایجاد و توزیع کلید، زوج کلید خود را دریافت می‌کند. باب کلید خصوصی خود (یعنی d) را به صورت محرمانه نزد خود نگه داشته ولی کلید عمومی خود (یعنی e) را برای دیگران از طریق کانال ناامن منتشر می‌کند. توجه کنید که در طرح نسبت به الگوریتم

سیمتریک، این آزادی عمل را داریم که از یک کانال ناامن برای توزیع کلید عمومی هم استفاده کنیم. بدین معنی که دشمن اجازه دارد هم کلید عمومی را ببیند و هم متن رمز شده ارسالی را.

آلیس به عنوان ارسال‌کننده، متن واضح (یعنی m) را با کلید رمزگذاری عمومی باب (e) – که توسط باب منتشر شده و در اختیار دارد- از طریق الگوریتم رمزنگاری E، به متن رمز شده تبدیل می‌کند و این متن رمز شده را باز از طریق کانال ناامن برای باب می‌فرستد. باب هم پس از دریافت متن رمز شده (c) با اعمال کلید رمزگشای شخصی خود (d) و استفاده از الگوریتم رمزگشایی (D) از حالت رمز شده خارج کرده و به یک متن واضح تبدیل می‌کند.



شکل ۴-۱۰) روش توزیع کلید در الگوریتم نامتقارن

برای درک بهتر تفاوت‌های دو نوع الگوریتم متقارن و نامتقارن جدول ۴-۱ در زیر آورده شده است. همانطور که در جدول ملاحظه می‌کنید:

در روش سیمتریک کلید منحصر به فرد بین دو طرف به اشتراک گذاشته می‌شود. ولی در الگوریتم آسیمتریک از دو کلید عمومی و خصوصی استفاده می‌شود. عمل جابجایی کلید در سیمتریک باید در کانال جدا از کانال ارسال پیام‌ها انجام گیرد و این در حالی است که در آسیمتریک عمل انتقال کلید در همان کانال در نظر گرفته

شده برای انتقال متن، منتقل می‌گردد. الگوریتم‌های رمزگذاری سیمتریک مقیاس‌پذیر نیستند، یعنی قابلیت اعمال بر روی بلوک‌های مختلف داده‌ای با اندازه‌های مختلف را ندارند، ولی در آسیمتریک این کار امکان‌پذیر است.

سیمتریک‌ها دارای سرعت بالاتر اجرایی نسبت به آسیمتریک‌ها هستند.

سیمتریک‌ها برای اجراء بر روی حجم بالای داده مناسب هستند، در حالیکه آسیمتریک‌ها بیشتر برای اعمال بر روی حجم کوچک‌تر داده به کار می‌روند و برای تولید امضای الکترونیکی، گواهی دیجیتالی و پاکت دیجیتالی استفاده می‌شوند.

سیمتریک صرفا برای سرویس محرمانگی به کار می‌رود، در حالیکه آسیمتریک علاوه بر سرویس محرمانگی، سرویس‌های احراز هویت و انکارناپذیری را نیز پشتیبانی می‌کند.

Symmetric	Asymmetric
Single shared key	Key pair sets
Out-of-band exchange	In-band exchange
Not scalable	Scalable
Fast	Slow
Bulk encryption	Small blocks of data, digital signatures, digital envelopes, digital certificates
Confidentiality	Integrity, authenticity, nonrepudiation

جدول ۴-۱) مقایسه الگوریتم‌های رمزنگاری سیمتریک و آسیمتریک

۴-۵-۳) توابع درهم‌ریزی (Hash Algorithms)

الگوریتم درهم‌ریزی با هدف تامین سرویس امنیتی صحت و جامعیت داده به کار گرفته می‌شود. درهم‌ریزی یک تابع یک طرفه است که سایزی ثابت از مقادیر مبتنی بر اندازه‌های مختلف از حجم داده ورودی را تولید می‌کند. یک تابع درهم‌ریزی در هر بار اجراء بر روی دیتای مشخصی، خروجی ثابت دارد و این بدان معنی است که با

اجرای مختلف بر روی داده مشخصی خروجی متفاوتی نمی‌دهد. بعضی از الگوریتم‌های درهم‌ریزی معروف عبارتند از: MD-4, MD-5, SHA-1.

تابه درهم‌ریزی را می‌توان با اثر انگشت مقایسه کرد. همانطور که اثر انگشت انحصاری است و دارای اندازه ثابتی می‌باشد، نتیجه تابع درهم‌ریزی هم انحصاری بوده و نمی‌توان مقادیر یکسان از داده‌های متفاوت به دست آورد. بعضی از مشخصات توابع درهم‌ریزی MD-4, MD-5, SHA-1 عبارتند از:

MD-4: خروجی آن یک مقدار ۱۲۸ بیتی است. خیلی سریع است و برای اهداف امنیتی سطح متوسط مناسب می‌باشد.

MD-5: خروجی آن یک مقدار ۱۲۸ بیتی است. سریع می‌باشد (اما نه به اندازه MD-4). از MD-4 امن‌تر است و در بسیاری از مکان‌ها استفاده می‌شود.

SHA-1: خروجی آن یک مقدار ۱۶۰ بیتی است. استاندارد دولتی آمریکا می‌باشد، اما از MD-5 کندتر است.

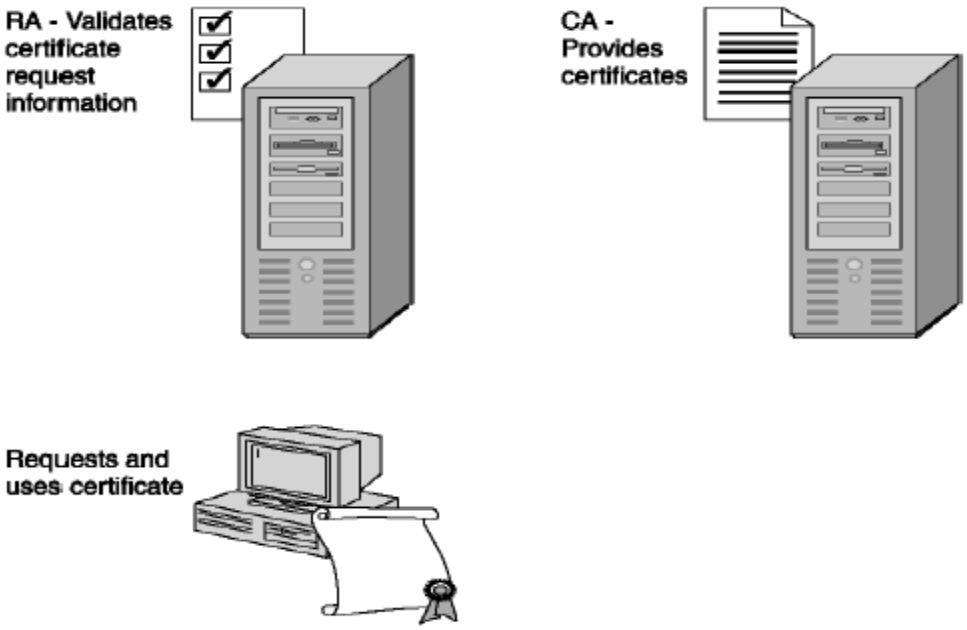
۴-۶) معرفی اجزاء زیرساخت کلید عمومی

استفاده از زوج کلید در الگوریتم آسیمتریک برای پیاده‌سازی در محیط‌های کوچک و افراد کم، کاری ساده است. اما در محیط‌های بزرگ با کاربردهای وسیع، توزیع کلید عمومی و مدیریت کلید خصوصی کاری بس دشوار می‌گردد. زمانی که یک کلید خصوصی مورد هجوم قرار می‌گیرد، پاک کردن آن و جایگذاری آن سخت است. بدین منظور زیرساخت‌های امنیتی با نام زیرساخت‌های کلید عمومی (Public Key Infrastructure) یا به اختصار PKI، به وجود آمده‌اند. PKI از زوج کلید آسیمتریک، نرم‌افزارهای ترکیبی و تکنولوژی‌های رمزنگاری برای ایجاد امنیت ارتباطات و تراکنش‌های تجاری استفاده می‌کنند. استاندارد PKI که در محیط‌های اینترنتی مورد استفاده قرار می‌گیرد، استاندارد X509 می‌باشد. این استاندارد شامل: تاییدیه، تاییدکننده تاییدیه، ابزار مدیریتی تاییدیه‌ها و برنامه‌های کاربردی که تاییدیه‌ها را به کار می‌گیرند، می‌باشد.

۴-۶-۱) اجزاء PKI

همانطور که در شکل ۴-۱۱ مشاهده می‌کنید اجزاء اصلی این زیرساخت عبارتند از:

- تاییدیه دیجیتالی (Digital Certificate): که یک اعتبارنامه الکترونیکی برای احراز هویت کاربر است.
- مرکز قانونی صدور تاییدیه (Certification Authority- CA): یک کامپیوتر که تاییدیه دیجیتالی را صادر می‌کند، یک لیست تاییدیه‌های معتبر را نگهداری می‌کند و همچنین یک لیست از تاییدیه‌هایی که به دلایلی اعتبار آن باطل شده را هم نگهداری می‌کند.
- مرکز قانونی ثبت نام (Registration Authority- RA): مرکزی که برای رسیدگی به شرایط ثبت-نامی و ثبت‌نام از متقاضیان درخواست تاییدیه‌های دیجیتالی و ارسال درخواست‌ها به CA، فعالیت می-کنند.
- ابزار مدیریت تاییدیه‌ها و کلیدها (Key and Certification Management Tools): ابزار برای حسابرسی و مدیریت تاییدیه‌های دیجیتالی.
- نقطه انتشار تاییدیه‌ها (Certificate Publication Point): مکانی که تاییدیه‌ها ذخیره و منتشر می‌شوند.
- سرویس و برنامه‌های فعال‌ساز کلید عمومی (Public Key-Enabled Applications and Services): برنامه‌های کاربردی و سرویس‌هایی که استفاده از تاییدیه را پشتیبانی می‌کنند.



شکل ۴-۱۱) اجزاء اصلی PKI

۴-۶-۲) تاییدیه چیست؟

تاییدیه یک معرف دیجیتالی است که شما را معرفی کرده و توسط CA صادر می‌شود. این CA معمولا به عنوان سوم شخص قابل اعتماد یا Trusted Third Party (TTP) هم شناخته می‌شود. در هر تاییدیه مشخصات سوم شخص معتمد صادرکننده آن، تاریخ اعتبار تاییدیه و امضاء تاییدیه سوم شخص معتمد برای تایید صدور آن، وجود دارد. تاییدیه می‌تواند توسط برنامه‌های کاربردی و سرویس‌های امنیتی مختلف برای انجام مواردی همچون احراز هویت، صحت و یکپارچگی داده‌ها و امنیت به کار رود. کاربردهای تاییدیه شامل موارد زیر است:

- امن‌سازی ایمیل: از پروتکل S/MIME برای اطمینان از صحت و جامعیت، مبدا و محرمانگی ایمیل استفاده می‌شود.
- امن‌سازی ارتباطات وب: استفاده از تاییدیه در پروتکل SSL/TLS برای احراز هویت و رمزنگاری ارتباطات میان سرور و کلاینت.
- امن‌سازی سرور وب: استفاده از تاییدیه برای احراز هویت دسترسی به وب‌سایت‌های امن.
- راه حل‌های امنیت مشتریان: استفاده از تاییدیه برای اجرای محرمانگی، صحت، احراز هویت و انکارناپذیری در برنامه‌های کاربردی مشتریان.

فصل پنجم: امن‌سازی زیرساخت‌های شبکه

مقدمه

در این فصل به بحث امنیت در زیرساخت‌های شبکه از سه بعد کانال‌های ارتباطی و تجهیزات ارتباطی و شبکه-ای خواهیم پرداخت. سازمان‌ها و اشخاص علاقه‌مند به محافظت از داده‌ها، تجهیزات، اسرار تجاری و حفظ حریم شرکای خود می‌باشند. یک حمله موفق به شبکه ممکن است عاملی برای به خطر انداختن هر یک از ابعاد فوق باشد. برای محافظت از زیرساخت‌های شبکه خود در مقابل حملات در ابتدا باید نسبت به انواع حملات ممکن فراروی این زیرساخت آگاه باشید. بعضی از این تهدیدات عبارتند از:

- تخریب فیزیکی تجهیزات
- شنود بسته‌های اطلاعاتی
- اسکن پورت‌های شبکه و نقشه شبکه برای شناسایی اهداف جهت تدارک حمله
- چیدمان مجدد و یا غیر فعال کردن ارتباطات تجهیزات امنیتی
- استفاده از تجهیزات شبکه برای تدارک حمله به شبکه‌ای دیگر
- استفاده از شبکه شما برای میزبانی سرویس‌های غیرقانونی، مخرب و ناشناخته.
- پاک کردن و تخریب داده‌ها

در راستای نیل به اهداف امنیتی بعضی از راه‌ها برای امن کردن فیزیکی تجهیزات به قرار زیر است:

- استخدام گارد حفاظتی
- نصب سنسور و تلویزیون‌های مدار بسته برای نظارت بر تجهیزات
- استفاده از کارت‌های امن برای دسترسی فیزیکی
- نصب سیستم برق اضطراری
- پوشش کابل‌های شبکه و یا قرار دادن آنها درون دیوارها
- قفل کردن دری اطاق سرور
- قرار دادن تجهیزات در پوشش‌های مناسب و مهر و موم کردن آنها
- نصب فنس و گیت‌های ورود و خروج
- نصب سیستم ضد حریق
- اطمینان از استانداردهای نصب و پیاده‌سازی تجهیزات.

۵-۱) امنیت در کانال‌های ارتباطی شبکه

بسیاری از شبکه‌های کامپیوتری از انواع مختلف کابل برای ارتباط استفاده می‌کنند. در این درس شما با بعضی از این کابل‌ها و نحوه حمله به آنها آگاه می‌شوید. کابل‌های اساسی در شبکه عبارتند از: کابل‌های کواکسیال، کابل‌های زوج سیم مسی، کابل فیبر نوری. البته لازم به ذکر است که خطوط بی‌سیم نیز از انواع خطوط ارتباطی هستند.

۵-۱-۱) کابل‌های کواکسیال

کابل‌های کواکسیال دارای انواع مختلف ولی دارای ساختار نسبتا یکسان هستند. هر کابل کواکسیال شامل: رشته سیم رسانای مرکزی، یک رشته سیم رسانای بیرونی و یک پوشش بیرونی است. انتقال الکترونیکی (داده‌های در حال انتقال) از میان رشته سیم رسانای مرکزی صورت می‌گیرد.

۵-۱-۱-۱) حملات علیه کابل‌های کواکسیال

کابل‌های کواکسیال معمولا از دو جنبه تخریب و یا استراق سمع اطلاعات مورد تهاجم قرار می‌گیرند. این کابل‌ها معمولا برای نصب شبکه با توپولوژی باس (Bus) مورد استفاده قرار می‌گیرند. به این دلیل قطع شدن بخشی از آن باعث قطعی کل شبکه می‌شود.

یکی از تخریب‌هایی که علیه این کابل‌ها انجام می‌گیرد برش آنها به وسیله قیچی‌های فلزبر (علی‌رغم محکم بودن این کابل‌ها) می‌باشد. همچنین منبع گرمایی شدید در مجاورت این کابل‌ها عامل دیگری برای تخریب آنها می‌باشد.

اما از بعد فرکانسی هم این کابل‌ها آسیب‌پذیر هستند. این کابل‌ها در مقابل امواج رادیویی و امواج مغناطیسی دچار آشفتگی اطلاعاتی می‌شوند. همچنین جداسازی قطعه تمام‌کننده در قسمت انتهایی خطوط در این کابل‌ها باعث قطعی شبکه می‌شود.

اما بعد از استراق سمع، چون این کابل‌ها معمولا در توپولوژی باس مورد استفاده قرار می‌گیرند و در این توپولوژی سیگنال‌های اطلاعاتی در کل شبکه به انتقال درمی‌آیند، پس هر نود اتصال به این شبکه در صورت لحاظ نشدن موارد امنیتی در شبکه، امکان استراق سمع اطلاعات را دارا می‌باشد. همچنین هر بخش از کابل

شبکه مکان مناسبی برای یک اتصال جدید به شبکه توسط مهاجمین است. البته لازم به ذکر است که برای ایجاد اتصال به شبکه در این کابل‌ها توسط مهاجمین باید قسمتی از کابل قطع شود و به دلیل نوع توپولوژی شبکه‌هایی که از کابل‌های کواکسیال استفاده می‌کنند (توپولوژی باس)، آنگاه کل شبکه در آن زمان از کار می-افتد.

۵-۱-۱-۲) امن‌سازی کابل‌های کواکسیال

از روش‌های زیر برای امن‌سازی کابل‌های کواکسیال در برابر تخریب و شنود استفاده می‌شود:

- قرار دادن این کابل‌ها در زیر سطح زمین، قرار دادن آنها در دیوارها، پوشش‌گذاری حداکثری آنها برای جلوگیری از استراق سمع
- مستندسازی کابل‌کشی‌ها
- وارسی کردن تمامی راه‌های خروجی شبکه کابل کواکسیال
- بازرسی فیزیکی به صورت دوره‌ای از تمامی زیرساخت‌های کابل
- وارسی کردن تمامی تجهیزات میزبان و اتصالات مستند نشده

۵-۱-۲) زوج سیم مسی

هر کابل زوج سیم مسی دارای یک یا بیشتر زوج سیم تابیده شده به هم قرار گرفته در یک غلاف پلاستیکی می‌باشند. هر سیم از جنس مسی است که توسط لایه پلاستیکی به عنوان پوشش در دور آن جهت عدم اتصال الکتریکی سیم‌ها به یکدیگر محافظت می‌شود. هر زوج تک سیم به دور یکدیگر جهت جلوگیری از هرز رفتن سیگنال‌های الکتریکی درونشان، به هم تابیده شده‌اند.

۵-۱-۲-۱) حملات علیه زوج سیم مسی

این سیم‌ها به دلیل جنس نازکشان به راحتی قابل تخریب و بریده شده هستند. همچنین حرارت گرمایی نیز بر روی آنها تاثیر مخربی دارد. اما به دلیل آنکه اینگونه کابل‌ها عمدتا در شبکه‌های مبتنی بر توپولوژی ستاره

استفاده می‌شوند، لذا قطع شدن یکی از این سیم‌ها باعث قطعی کل شبکه نمی‌شود. اما از بعد استراق سمع، این کابل‌ها به ۳ شکل مورد تهاجم قرار می‌گیرند:

اتصال فیزیکی یک پروتکل آنالیزر به یک نقطه اتصال از این زوج سیم‌های مسی. پروتکل آنالیزر یک دستگاه و یا یک برنامه نرم‌افزاری کامپیوتری می‌باشد که به مهاجم اجازه تصرف و رمزگشایی ترافیک موجود بر روی شبکه را می‌دهد یا به اصطلاح دیگر امکان بو کشیدن اطلاعات را می‌دهد.

به هم تابیدن به داخل کابل زوج سیم مسی.

استفاده از سیگنال‌های الکترومغناطیسی برای استراق سیگنال‌های عبوری از میان زوج سیم مسی.

۵-۱-۲-۲) امن‌سازی زوج سیم مسی

- محافظت فیزیکی کابل بالاخص در مراکز حساس آن مثل محل اتصالات به هاب و سوئیچ و ...
- استفاده از سوئیچ به جای هاب، چرا که سوئیچ ترافیک مورد نظر را مستقیما به میزبان مورد نظر اصلی می‌فرستد، در حالیکه هاب ترافیک را به سمت تمامی میزبان‌های موجود در شبکه گسیل می‌دارد.
- مدیریت سوئیچ‌ها، هاب‌ها و روترها به شکلی که در صورت صدمه دیده بخشی از شبکه و یا ورورد یک اتصال جدید به شبکه، به مدیر شبکه پیغام دهد.

۵-۱-۳) فیبر نوری

کابل فیبر نوری از یک رشته و تار شیشه‌ای یا پلاستیکی برای انتقال پالس‌های نوری تشکیل شده است. کابل-های فیبر نوری بسیار امن‌تر از انواع دیگر کابل‌ها می‌باشند، چرا که توسط امواج رادیویی و مغناطیس تحت تاثیر قرار نمی‌گیرند. این کابل‌ها گران‌تر و نصب آنها نیز سخت‌تر است.

۵-۱-۳-۱) حملات علیه فیبر نوری

خرابی بر روی این کابل‌ها بسیار راحت‌تر می‌باشد. این کابل‌ها به راحتی می‌توانند آسیب دیده، مچاله شده و یا شکسته شوند. اما شنود بر روی کابل فیبر نوری غیرممکن است، مگر آنکه فرد مهاجم بخشی از فیبر نوری را بریده و یک کارت قرائت‌گر فیبر نوری وارد مسیر شبکه نماید.

۵-۱-۳-۲) امن‌سازی فیبر نوری

مهم‌ترین عاملی که جهت امن‌سازی این کابل‌ها ذکر می‌شود محافظت فیزیکی از آنها و همینطور پیکربندی شبکه به شکلی که در صورت قطعی در شبکه، به دلیل تلاش مهاجم برای وارد کردن یک کارت قرائت‌گر فیبر نوری در بخشی از شبکه، فورا هشدارهای لازم به مدیران شبکه داده شود.

۵-۲) امنیت در تجهیزات ارتباطی شبکه

بسیاری از تجهیزات ارتباطی در شبکه دارای بخش‌های سخت‌افزاری و پیکربندی منطقی هستند که فرد مهاجم می‌تواند از ضعف در هر یک از این دو بخش برای تدارک حمله بهره‌برداری نماید. این تجهیزات به شرح زیر می-باشند:

- Hub
- Switch and Bridge
- Router
- Firewall
- Modem
- Wireless

۵-۲-۱) Hubs

همانطور که می‌دانید هاب یک وسیله ارتباط و اتصال در شبکه‌های از نوع اترنت است که دارای دو نوع فعال و غیرفعال می‌باشد. در نوع فعال آن سیگنال‌های شبکه تکرار و تقویت می‌گردد و چون هاب محل ارتباط اصلی در شبکه است لذا مورد توجه مهاجمین برای تدارک حمله است.

۴-۲-۱-۱) تخریب هاب

هاب به راحتی قابل تخریب است، اگر مهاجم به آن دسترسی فیزیکی داشته باشد. هاب به راحتی می‌تواند از اتصال خارج و یا خراب شود، یا اگر از نوع فعال باشد به راحتی خاموش شود. در این صورت تجهیزات متصل به شبکه امکان ارتباطی خودشان با یکدیگر را از دست می‌دهند. شنود بر روی هاب نیز امکان‌پذیر است. اگر یک پورت بر روی هاب آزاد باشد و یا اگر امکان جداسازی یک دستگاه تایید شده متصل به هاب برای حمله‌کننده وجود داشته باشد، فرد حمله‌کننده می‌تواند از آن پورت برای دستیابی به اطلاعات و یا تخریب بر روی دیگر تجهیزات متصل در شبکه سود ببرد.

۵-۲-۱-۲) امن‌سازی هاب

به دلیل خاصیت فیزیکی هاب، امکان حفاظت فیزیکی آن هم وجود دارد. هاب باید درون محفظه‌ای امن قرار داده شود. اگر هاب درون اطاق یا محفظه‌ای قفل شده نیست، تلاش شود توسط دیگر بسته‌بندی‌های محافظتی امن گردد. حداقل به صورت دوره‌ای هاب مورد بازدید قرار گیرد تا از امن بودن اتصالات آن و عدم اتصال یک فرد غیرمجاز به آن مطمئن شویم. هاب‌های قابل مدیریت می‌توانند برای آشکارسازی تغییرات فیزیکی در به هم بستن آنها به کار رود. هاب‌های قابل مدیریت اطلاعات آماری و اطلاعات اتصالی خود را برای مدیریت نرم‌افزار ارسال می‌کنند. لذا شما می‌توانید هاب را برای اعلام خطر به هنگام تغییر در به هم‌بندیش مجهز کنید. اما از آنجا که این روش مدیریت موقعیت و به هم‌بندی به شکل نرم‌افزاری انجام می‌گیرد، فرد مهاجم می‌تواند چیدمان نرم‌افزاری را تخریب و یا تدارک حمله‌ای دیگر از این ناحیه را ببیند.

۵-۲-۲) Switches and Bridges

سوئیچ و بریج در لایه دوم شبکه (در مدل استاندارد OSI) متصل می‌گردد. آنها عمل سوئیچینگ و پل‌بندی را بر مبنای آدرس کنترل دسترسی کانال‌های ارتباطی (MAC) هر یک از اتصالات شبکه، انجام می‌دهند. سوئیچ و بریج جدولی را برای کمک به ارسال بسته‌های اطلاعاتی به بخش‌های مناسب شبکه، ایجاد می‌کنند. پل یا به اصطلاح بریج نوعا یک شبکه را به دو بخش تقسیم می‌کند ولی سوئیچ‌ها نوعا هر بخش از شبکه را به چندین قسمت کوچک‌تر تقسیم می‌کنند و هر قسمت برای هر پورت سوئیچ می‌باشد. این تجهیزات عمدتا تنها برای

انتقال اطلاعات تک مقصده (Unicast) مورد استفاده قرار می‌گیرند و اطلاعاتی که برای چند مقصد به طور همزمان ارسال می‌شوند از این تجهیزات گذر می‌کنند.

توجه: ممکن است در کاتالوگ‌های بازاریابی کارکرد این تجهیزات در لایه‌های ۳ و ۴ شبکه را هم ملاحظه کرده باشید که در این صورت دیگر نام این تجهیزات "روتر با کارایی بالا" می‌باشد.

۵-۲-۲-۱) تخریب سوئیچ و پل

همانطور که دیدید سوئیچ‌ها و پل‌ها جدولی به نام MAC برای نشان دادن اتصالات به هر نقطه اتصالی ایجاد می‌کنند. این جدول امکان ارتباط با بخش صحیح شبکه یا پورتی را برای سوئیچ و یا پل در لایه دوم شبکه امکان‌پذیر می‌سازد که این موضوع پتانسیل خوبی را برای حمله‌کنندگان برای تدارک حمله‌ای به ارمغان می-آورد. همچنین یک سوئیچ مرکزی مکان مناسبی برای هدف‌گذاری یک حمله می‌باشد. خراب کردن یک سوئیچ مرکزی یا قطع برق آن یا قطع کابل‌های متصل به آن باعث از کار افتادن تمام ارتباطات عبوری از آن می‌شود. به موازات این تخریب‌های فیزیکی غرق‌سازی جدوا MAC با آدرس‌های بی‌مقصد در سوئیچ و بریج (البته آن دسته از سوئیچ‌ها و پل‌هایی که قابلیت آموزش دارند) باعث کند شدن کار شبکه می‌گردد. دیگر تخریب‌های ممکن به اشکال زیر اتفاق می‌افتد:

الف) تملیک دسترسی مدیریت شبکه

اگر فرد مهاجم بتواند امکان دسترسی مدیریتی شبکه را به دست آورد، او می‌تواند ارتباطات شبکه را مسیردهی مجدد کند. این ارتباطات می‌تواند به سمت ماشینی که تحت کنترل حمله‌کننده است مسیردهی شود. آنگاه تا زمانی که مهاجم امکان اتصال مدیریتی به شبکه را دارا باشد، می‌تواند شبکه را تخریب نماید. این کار با دسترسی به شناسه و کلمه عبور مدیر سیستم انجام می‌گیرد. سوئیچ‌ها خصوصا فانکشنی به نام "معکوس‌سازی پورت" (Mirroring Port) دارند، که مدیر سیستم را قادر به نگاشت ورودی و خروجی از یک یا چند پورت سوئیچ به یک پورت خاص می‌سازند. این به منزله روشی برای عیب‌زدایی مشکلات ارتباطی در شبکه است. حال اگر مهاجمی امکان دسترسی به این فانکشن را داشته باشد، می‌تواند تمام ترافیک عبوری از شبکه را مشاهده نماید. به این شکل او می‌تواند تمام اطلاعات رمز نشده در شبکه مثل اطلاعات شناسه و کلمه عبور دیگر سیستم‌های متصل به شبکه را به دست آورد.

ب) مسموم‌سازی حافظه ARP (ARP Cache Poisoning)

اگر چه سوئیچ و پل شبکه را بخش‌بندی می‌کنند، این امکان وجود دارد که فرد مهاجم حافظه پروتکل تجزیه و تحلیل (ARP) را مسموم نماید. بدین شکل ترافیک شبکه را در شبکه پخش نماید. کش ARP برای نگهداری اطلاعات نگاشت پروتکل اینترنت (IP) به آدرس MAC به کار می‌رود.

برای اینکه حمله‌کننده این مسمومیت را انجام دهد، ابتدا باید به صورت فیزیکی به یک بخش داخلی از شبکه دسترسی پیدا کند. آنگاه تخریب‌گر باید کش ARP مربوط به ماشین‌های آن قسمت شبکه را تخریب نماید. به این ترتیب می‌تواند تمام ترافیک ماشین‌های آن بخش شبکه را به سمت کامپیوتر خودش روان سازد.

۵-۲-۲-۲) امن‌سازی سوئیچ‌ها و پل‌ها

مانند دیگر تجهیزات شبکه حفاظت فیزیکی از آنها شرط اولیه است. اما دیگر راه‌ها به نحو زیر می‌باشد:

- امن کردن کلیه اتصالات فیزیکی در شبکه. اطمینان از امکان‌پذیر نبودن ارتباط افراد تعریف نشده جهت اتصال به این تجهیزات. همچنین محدودسازی دسترسی به مکان این تجهیزات و نظارت بر تجهیزات از جهت اطمینان از امن بودن اتصالات.
- استفاده از کلمات عبور مرکب و پیچیده برای کنسول‌های مدیریتی. در اختیار داشتن این کلمات عبور تنها افراد خاصی و تغییرات آنها به صورت دوره‌ای و تغییر آن در صورت تعویض افراد، از جمله دیگر مواردی است که باید مورد توجه قرار گیرد.
- ورود دستی نگاشت‌های ARP در تجهیزات بحرانی، همچون سرورها، سوئیچ‌ها و پل‌های مرکزی. اگر کلیه آدرس‌های MAC به صورت دستی در جداول وارد شوند، این عمل از یادگیری آدرس‌های جدید به صورت اتوماتیک توسط سوئیچ‌ها و پل‌ها جلوگیری می‌کند.
- سوئیچ‌ها و پل‌ها را توسط آخرین نسخه‌های وصله‌های امنیتی طراحی شده توسط سازندگان آنها مجهز نمائیم.
- مستندسازی نحوه به هم‌بندی دستگاه برای یادآوری ارتباطات نرمال و مجاز در آینده.
- مانیتور کردن شبکه با ابزارهای مدیریتی برای آگاهی از اتصالات غیرمجاز. ابزاری به نام ARPWATCH می‌تواند فعالیت‌ها بر روش شبکه را مانیتور کرده و یک دیتابیس از اطلاعات نگاشت MAC و IP را در خود نگه دارد. همچنین این ابزار می‌تواند شما را از تغییرات ایجاد شده در این بخش مطلع سازد.

۵-۲-۳) Routers

همانطور که می‌دانید مسیریاب (Router) ارتباطات را در لایه سوم مدل مرجع شبکه (OSI) یعنی لایه شبکه، به عهده دارد. روتر همچنین از ARP Cache و جدول مسیردهی (Routing table) برای انجام وظیفه مسیردهی در شبکه بهره می‌گیرد.

۵-۲-۳-۱) تخریب مسیریاب‌ها

همانطور که گفتیم روترها هر دوی ARP Cache و جدول مسیردهی را برای انتقال و مسیردهی مناسب ارتباطات استفاده می‌کند. این خود نقطه‌ای برای تدارک حمله می‌تواند باشد. روتر مرکزی همچنین می‌تواند مکان مناسبی برای تخریب باشد. خراب کردن روتر مرکزی، قطع کردن برق، یا قطع کردن اتصالات کابل-های روتر می‌تواند عاملی برای جلوگیری از گذر اطلاعات در بین دستگاه در شبکه باشد. از آنجا که روترها از ARP Cache استفاده می‌کند، نمی‌توانند مستعد حمله مسمومسازی ARP Cache باشند. به علاوه روترها از Routing table که می‌تواند از طریق اتصال از راه دور و یا اتصال کنسول مدیریت از طریق کابل تغییر یابد، استفاده می‌کنند. اگر مهاجمی بتواند این جدول را تغییر دهد، ترافیک شبکه می‌تواند به صورت ناصحیح به سمت یک کامپیوتر که تحت کنترل مهاجم است مسیردهی شود. همانطور که در گذشته هم دیدید شما می‌توانید با نظارت نقاط اتصال فیزیکی در شبکه خود از این حمله پیشگیری کنید.

اگر یک حمله‌کننده بتواند دسترسی مدیریتی به روتر پیدا کند، می‌تواند مسیردهی مجدد در شبکه را انجام دهد. این ارتباطات می‌تواند به سمت یک میزبان تحت کنترل مهاجم در شبکه مسیردهی مجدد شود.

همچنین مهاجم می‌تواند پروتکل اطلاعات مسیردهی (RIP) را برای به روزرسانی اطلاعات جدول مسیریابی با اطلاعات نادرست مورد استفاده قرار دهد. این عمل RIP Spoofing نامیده می‌شود و مربوط به تجهیزاتی است که از روایه یکم آن ($RIPv_1$) استفاده می‌کنند. به هر حال روایه دوم آن ($RIPv_2$) روتر را برای تنظیم کلمه عبور مجاز می‌سازد. بنابراین در این نسخه فرد مهاجم باید برای قرار دادن اطلاعات نادرست حتما کلمه عبور را داشته باشد.

همانطور که در بخش‌های قبل گفته شد دستگاه‌های ارتباطی ممکن است مشکلات به هم‌بندی نرم‌افزاری و یا نقاط آسیب‌پذیر امنیتی داشته باشند. به طور مثال ممکن است شخصی دریابد که یک روتر می‌تواند به روز و یا غیرفعال شود بدون مجوز مدیریت (به این معنی که در صورت دسترسی به شبکه می‌تواند آن روتر

را تخریب نماید). فروشندگان این تجهیزات در صورت اطلاع از این ضعف‌ها غالبا قادر به حل آن می‌باشند، لذا برای محافظت از تجهیزات ارتباطی حتما پیگیری از فروشندگان آنها را برای دریافت وصله‌های مرتفع-کننده مشکل، فراموش نکنید.

۵-۲-۳-۲) امن‌سازی مسیریاب‌ها

یک روتر مرکزی هدف مناسبی برای مهاجمین است. تخریب یک روتر مرکزی، قطع برق آن و یا قطع نمودن کلیه کابل‌های ارتباطی آن ممکن است کلیه ارتباطات متصل به این دستگاه را مختل سازد. برای امن‌سازی آن باید مراقبت‌های زیر را انجام داد:

- اطمینان از نگهداری روتر در اطاق قفل‌دار یا در پوشش مناسب
- امتحان امنیت تمامی اتصالات ورودی و خروجی
- محدودسازی دسترسی فیزیکی به تجهیزات زیربنایی شبکه کابل و اطاق‌های سرور
- مانیتورینگ تجهیزات برای حفاظت از نقاط اتصال و تجهیزات
- به کارگیری کلمات عبور ترکیبی برای کنسول‌های مدیریتی. در اختیار داشتن این کلمات عبور تنها توسط افراد خاصی و تغییرات آنها به صورت دوره‌ای و تغییر آن در صورت تعویض افراد، از جمله دیگر مواردی است که باید مورد توجه قرار گیرد.
- به هنگام نگه داشتن روترها با آخرین نسخه وصله‌های امنیتی ارائه شده توسط فروشندگان
- اطمینان از مستندسازی و نظارت مجدد بر چیدمان و به هم‌بندی شبکه
- غیرفعال‌سازی $RIPv_1$ و به کارگیری $RIPv_2$ و یا دیگر پروتکل‌های مسیردهی که امکان تغییرات دو روتر را تنها با ارائه کلمات عبور میسر می‌سازند.

۵-۲-۴) Firewalls

کلمه دیواره آتش به صورت عمومی برای توضیح تجهیزاتی به کار می‌رود که برای محافظت از یک شبکه داخلی (یا یک میزبان) در مقابل مهاجمین با کدهای مخرب از شبکه خارجی (یا شبکه‌ای که آن میزبان به آن متصل است) به کار می‌رود. دیواره‌های آتش معمولا از اعمال متفاوتی برای فیلتر کردن ترافیک‌های ورودی و یا خروجی مضر و مخرب، استفاده می‌کنند. آنها اغلب برای پیاده‌سازی بین ارتباط شبکه داخلی

سازمان و اینترنت به کار می‌روند. البته گاها بعضی از دیواره‌های آتش برای جداسازی شبکه داخلی و یا حتی محافظت از یک کامپیوتر تنها نیز به کار می‌رود.

دیواره‌های آتش یک زیر سیستم از نرم‌افزار و سخت‌افزار کامپیوتری هستند که از ورود و خروج داده‌ها به شبکه داخلی (LAN) جلوگیری می‌کنند. این دیواره‌ها هستند که براساس مقررات امنیتی موجود تصمیم می‌گیرند کدام داده‌ها وارد شبکه شوند یا از شبکه خارج گردند.

تحول و پیشرفت سیستم‌های اطلاعات در سال‌های اخیر به مرحله‌ای رسیده که دیگر اتصال به اینترنت، یک گزینه اختیاری نیست، بلکه نیازی ضروری به نظر می‌رسد. اتصال به اینترنت، چه از طریق یک شبکه محلی و چه به وسیله خط تلفن، به دنیای بیرون امکان دسترسی به شبکه داخلی را می‌دهد. این مساله حفاظت از داده‌ها را در برابر دسترسی‌های غیرمجاز، الزامی کرده است. اولین راه حلی که به نظر می‌رسد، تجهیز کلیه دستگاه‌ها به ابزارهای امنیتی از قبیل سیستم مهاجم‌یاب[1] و ... است که بدون شک راه حل کارآ و مفیدی نیست.

راه حل مورد قبول امروزی، استفاده از دیواره آتش است. امروزه دیواره آتش از اجزای اصلی و ضروری شبکه‌های کامپیوتری است. نحوه عمل یک دیواره آتش بر ایده اعمال یک مکانیزم کنترل مرکزی استوار است. به این معنا که دیواره آتش بین شبکه داخلی و دنیای خارج قرار گرفته و در واقع در تنها نقطه تماس این دو شبکه، سیاست‌های کنترلی را بر تمام ترافیک ورودی و خروجی اعمال می‌کند.

دیواره آتش در ساده‌ترین حالت، نرم‌افزاری است که روی یک کامپیوتر شخصی نصب می‌شود، اما می‌تواند یک سیستم سخت‌افزار- نرم‌افزار ویژه هم باشد.

۵-۲-۴-۱) وظایف کلی دیواره آتش

۱. فیلترینگ: اصلی‌ترین وظیفه دیواره آتش، محافظت از شبکه داخلی در برابر نفوذهای بیرونی است. این کار براساس مجموعه قواعدی معروف به rule set که توسط مدیر دیواره آتش تنظیم می‌شود، انجام می‌گیرد. در ساده‌ترین حالت، براساس مقادیر فیلدهای مختلف header یک بسته، فیلترینگ انجام می‌شود. به این نوع دیواره اتش، packet filter گفته می‌شود. در اغلب دیواره‌های آتش فعلی، فیلترینگ در لایه ۲ (براساس آدرس‌های فیزیکی یا MAC) هم قابل انجام است. نوع پیشرفته‌تر

[1] Intrusion Detection System

فیلترینگ، علاوه بر header هر بسته، به ارتباط بسته‌ها با یکدیگر هم توجه و براساس آن تصمیم‌گیری می‌کند. به این نوع فیلترینگ، stateful inspection گفته می‌شود، که در آن state هر connection نگهداری و برای انجام فیلترینگ استفاده می‌شود. در برخی دیگر از آنها، امکان فیلتر کردن محتوای بسته‌ها هم وجود دارد.

۲. Network Address Translation: دیواره آتش معمولا در نقش دروازه برای شبکه داخلی عمل می‌کند. لذا کل ترافیک ورودی و خروجی از آن می‌گذرد. به دلایل مختلف امنیتی و اقتصادی، معمولا ماشین‌های شبکه داخلی را از دید بیرون پنهان می‌کنند. این کار در اغلب موارد با استفاده از تخصیص IP های Invalid (غیر قابل route در اینترنت) به ماشین‌های شبکه داخلی و ترجمه این IP ها به IP قابل route انجام می‌گیرد. این عمل ترجمه، معمولا درون دیواره اتش که همان دروازه شبکه به بیرون است، انجام می‌گیرد.

۳. کلیه امکانات یک دیواره آتش می‌تواند در حالت شفاف ارائه شود. در این حالت هنگام قرار دادن دیواره اتش در شبکه، اولا هیچ گونه نیازی به تغییر نرم‌افزاری توپولوژی شبکه نیست، ثانیا هیچ کدام از برنامه-های کاربردی نیازی به پیکربندی خاص (معرفی دیواره آتش به عنوان default gateway، proxy و ...) ندارند.

۵-۲-۴-۲) فوائد و ضعف‌های دیواره آتش

برخی از فوائد استفاده از دیواره آتش عبارت است از:

- توانایی کنترل ترافیک در هر دو جهت ورودی و خروجی
- قابلیت اعمال کنترل متمرکز و یکپارچه به جای کنترل توزیع شده
- قابلیت محدود کردن دسترسی به سرویس‌های غیر امن
- توانایی انجام فیلترینگ در لایه‌های مختلف (Data Link تا Application)
- هزینه کمتر جهت امن کردن شبکه، در مقایسه با امن کردن مستقل هر یک از host ها
- پیچیدگی کمتر در مقایسه با امن کردن host ها، به خاطر نداشتن سیستم عامل و برنامه‌های کاربردی پیچیده

در مقابل، تکنولوژی دیواره آتش دارای نقاط ضعفی هم هست که به اختصار به بعضی از آنها اشاره می‌کنیم:

- دیواره آتش کانون نفوذهای امنیتی است، در صورتی که مهاجم به آن راه پیدا کند، به احتمال قریب به یقین دسترسی نامحدود به کل منابع شبکه پیدا می‌کند.
- دیواره آتش، خواه ناخواه برای کاربران قانونی هم محدودیت‌های دسترسی ایجاد می‌کند.
- دیواره اتش حملات Back Door را نمی‌تواند تشخیص دهد
- دیواره آتش در برابر بسیاری از نقاط ضعف امنیتی در سطح application راه حلی ندارد
- به خاطر اینکه تمام ترافیک از دیواره آتش می‌گذرد، این مساله می‌تواند به یک معضل برای thoughput سیستم تبدیل شود.
- نفوذهایی که از درون شبکه داخلی و به مقصد ماشینی در همان شبکه انجام می‌شود، از دید دیواره آتش پنهان می‌ماند، چرا که اصولا بسته‌های مربوطه از دیواره آتش عبور نمی‌کنند. یکی از دلایل لزوم استفاده از سیستم‌های مهاجم‌یاب نیز همین است.

۵-۲-۴-۳) تخریب دیواره‌های آتش

پیاده‌سازی و نصب ضعیف دیواره‌های آتش یک دلیل اساسی برای تخریب دیواره‌های آتش است. دیواره‌های آتش می‌توانند به دو شکل "قوانین اجازه به صورت پیش‌فرض" و "قوانین عدم اجازه به صورت پیش‌فرض" پیکربندی شوند. در شکل قوانین اجازه پیش‌فرض، دیواره آتش به تمام بسته‌های اطلاعاتی ورودی به شبکه به جز آنهایی که ممنوع شده‌اند اجازه ورود می‌دهند، در حالیکه در روش دوم یعنی قوانین عدم اجازه پیش‌فرض، به هیچ بسته اطلاعاتی ورودی به شبکه به جز آنهایی که اجازه داده شده، اجازه ورود نمی‌دهد. معمولا مدیران امنیتی شبکه روش اول را به عنوان یک روش سهل‌انگارانه می‌دانند و معمولا این روش را قابل اعتماد نمی‌دانند.

نقص و عیب در بخش نرم‌افزاری دیواره آتش دیگر دلیل برای رخداد تخریب در آنها می‌باشد. معمولا فروشندگان دیواره‌های آتش پس از پی بردن به این نقائص برای رفع آنها، بالاخص برای خریداران قبلی، وصله‌هایی را برای نصب بر روی آنها و رفع عیب طراحی می‌کنند.

دلیل دیگر برای تخریب دیواره‌های آتش دسترسی مهاجم به رمز عبور کنسول مدیریت دیواره آتش می‌باشد. معمولا این کنسول‌ها در یکی از دو شکل ارتباط نزدیک و از طریق کابل و یا ارتباط از راه دور به وسیله ارتباطات بی‌سیم به وسیله مدیران شبکه قابلیت دسترسی به سیستم فایروال را ایجاد می‌کنند.

راه دیگر برای تخریب دیواره‌های آتش، راه دسترسی مستقل دیگر برای شبکه است. به طور مثال امکان تماس از طریق شماره‌گیری برای سرور به خارج از شبکه که این امکان تحت نظارت فایروال نباشد، می‌تواند به عنوان نقطه‌ای برای حمله به فایروال توسط مهاجمین باشد.

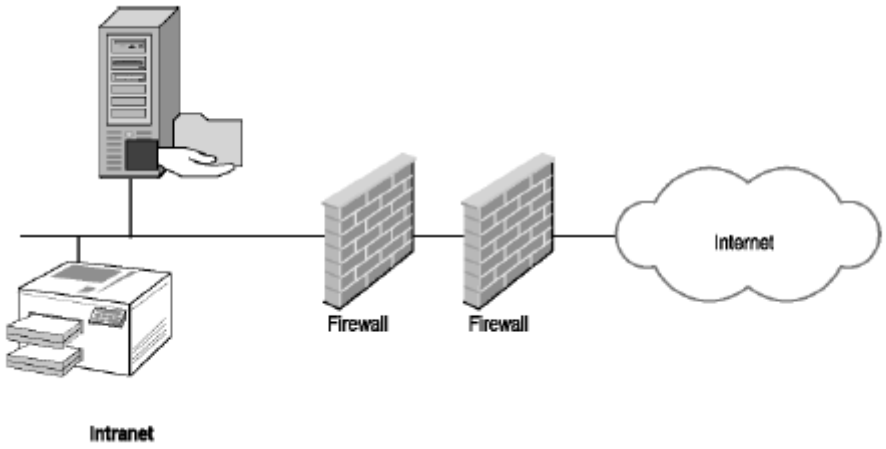
در انتها امکان دسترسی فیزیکی به فایروال توسط مهاجمین می‌تواند شرایط را برای خراب کردن و یا قطع کردن ارتباطات سیستم فایروال را برای مهاجمین به ارمغان آورد.

۵-۲-۴-۴) امن‌سازی دیواره‌های آتش

همانطور که توضیح داده شد روش‌های متفاوتی برای تخریب دیواره‌های آتش به وسیله مهاجمین وجود دارد که برای جلوگیری از این روش‌ها باید از راه‌های زیر بهره برد:

زیر نظر داشتن و پیگیری از فروشندگان فایروال برای دریافت وصله‌های رفع خطای به روز از آنها

- به روزسازی فایل‌های شناسایی ویروس‌ها
- حفاظت فیزیکی از فایروال‌ها
- مستندسازی نحوه به هم‌بندی سیستم‌های فایروال و بررسی مجدد آن به صورت دوره‌ای
- محدودسازی روش‌های مدیریت فایروال‌ها تا حد ممکن. به طور مثال اگر نیاز زیادی به دسترسی مدیریتی به فایروال از راه دور نمی‌باشد، این امکان را غیرفعال سازیم. در غیر اینصورت در صورت لزوم به این امکان ارتباطی – ارتباط از راه دور به سیستم فایروال توسط مدیران شبکه- حتما از روش‌های احراز هویت مطمئن استفاده شود.
- استفاده از رمزهای عبور ترکیبی برای دسترسی به فایروال‌ها و تغییر این رمز عبور به صورت دوره‌ای توسط مدیران شبکه
- اطمینان از عدم وجود راه‌های دسترسی به شبکه که تحت مدیریت فایروال نباشد
- استفاده از چند فایروال به صورت پشت سر هم، بالاخص استفاده پشت سر هم فایروال‌های شرکت‌های سازنده مختلف، کمک زیادی به امن‌سازی شبکه ما می‌کند (همانطور که در شکل ۵-۱ مشاهده می‌شود).



شکل ۵-۱) استفاده از فایروال چندگانه

Modems (۵-۲-۵

مودم‌ها امکان اتصال کامپیوترها به اینترنت و یا شبکه داخلی را فراهم می‌سازند. اما انها ممکن است توسط مهاجمین تخریب گردند. مودم‌ها می‌توانند امکان دسترسی به یک سیستم در شبکه و همچنین به صورت بالقوه امکان دسترسی به دیگر تجهیزات در شبکه را فراهم می‌سازد. لذا از همین امکان فرد مهاجم می‌تواند برای نفوذ به شبکه سوء استفاده کند.

برای محافظت از مودم‌ها در مقابل حملات تخریب‌گرایانه باید اعمال زیر را انجام داد:

- جداسازی همه مودم‌های غیرضروری از کامپیوترهای داخل شبکه
- بررسی به روز بودن همه نرم‌افزارهای موجود بر روی کامپیوترهای شبکه که نیاز به مودم دارند. مثلا به روزسازی آنتی‌ویروس‌ها و یا به روزسازی وصله‌های رفع عیب همه نرم‌افزارهای موجود بر روی این کامپیوترها
- پیگیری از فروشندگان مودم‌ها برای دریافت وصله‌های برطرف‌کننده نقائص مودم‌ها و به روزسازی آنها
- نظارت دوره‌ای بر کامپیوترهای دارای مودم برای انکه مورد تخریب قرار نگرفته باشند.

Wireless (۶-۲-۵

بسیاری از تولیدکنندگان نقاط دسترسی بی‌سیم (Aps) را که به وسیله کارت‌های شبکه‌ای بی‌سیم قابل دسترسی است، بر روی تجهیزات خود تدارک دیده‌اند. ارتباطات ما بین نقاط دسترسی و کارت‌های شبکه از

طریق سیگنال‌های رادیویی و سیگنال‌های مادون قرمز در فضا انجام می‌گیرد. مهاجمین که ممکن است از این تجهیزات حتی مایل‌ها دور باشند، می‌توانند به صورت بالقوه این سیگنال‌ها را استراق سمع کنند. لذا برای فرد مهاجم نیازی به اتصال فیزیکی و یا برش بر روی سیم‌ها جهت اتصال به شبکه وجود ندارد. این نقاط دسترسی همچنین می‌توانند مانند هاب‌ها، سوئیچ‌ها و یا روترها عمل نمایند. بنابراین تمام حملاتی که در گذشته بر روی این تجهیزات مطرح گردیده بر روی نقاط دسترسی هم متصور است.

امروزه در بسیاری از سازمان‌ها در کنار شبکه داخلی، امکان اتصال به شبکه اینترنت در اطراف فضای اداری برای اتصال عموم مردم به شبکه اینترنت هم پیش‌بینی می‌شود، که این خود نقطه بسیار خطرناکی برای نفوذ مهاجمین به شبکه داخلی می‌باشد. لذا استفاده از روش‌های احراز هویت و همچنین رمزگذاری اطلاعات مهم، راه مناسبی برای جلوگیری بسیاری از تخریب‌ها در این شبکه است. اما باید توجه داشت که در کنار استفاده از این روش‌های پیشرفته احراز هویت و رمزگذاری، امکانات، روش‌ها و ابزارهای پیشرفته‌ای نیز برای کمک به مهاجمین به صورت روزانه وارد بازار می‌گردد. لذا به روز نگه داشتن تجهیزات امنیتی و استفاده از آخرین وصله‌های برطرف‌کننده عیوب این تجهیزات که توسط تولیدکنندگان انها به بازار عرضه می‌شود، می‌تواند کمک شایانی برای مقابله با مهاجمین در اختیار ما قرار دهد.

راه حل دیگر برای جلوگیری از پراکندگی سیگنال‌های سیستم‌های بی‌سیم، پیاده‌سازی این تجهیزات در بخش-های زیرین زمین و استفاده از دیوارهای ضخیم می‌باشد.

همچنین امواج تجهیزات بی‌سیم ممکن است در مقابل امواج رادیویی و مغناطیس دیگر آسیب‌پذیر باشند، لذا بالا بردن توان سیگنالینگ این تجهیزات راه حل مناسبی برای این مشکل می‌باشد. همچنین در حین نصب تجهیزات بی‌سیم مطمئن گردید که نقاط دسترسی آنها در کنار منابع امواج رادیویی و مغناطیسی دیگر مانند آسانسور، ماشین‌های کپی، فرستنده‌های رادیویی و دیگر تجهیزات صنعتی نمی‌باشد.

۵-۳) امنیت در منابع شبکه‌ای

در این بخش اطلاعاتی در خصوص محافظت زیربنایی شبکه شما با توجه ویژه به منابع شبکه‌ای و مانیتورینگ آنها ارائه خواهد شد.

۵-۳-۱) امن‌سازی و مانیتورینگ ایستگاه‌های کاری (Work Station Security)

ایستگاه‌های کاری در شبکه شما جهت مقاصد کاربردی می‌باشد، اما این ایستگاه‌ها می‌توانند آسیب‌پذیر در مقابل مهاجمین باشند. تخریب ایستگاه‌های کاری در شبکه باعث اتلاف وقت کاربران انها و همچنین از دست رفتن اطلاعات ذی‌قیمت می‌شوند. اگر یک مهاجم بتواند به یک ایستگاه کاری در شبکه شما وارد شود و اخلالی را ایجاد نماید، احتمالا می‌تواند به دیگر تجهیزات در شبکه نیز دست‌اندازی کند. در زیر بعضی از روش‌ها برای محافظت این ایستگاه‌ها ذکر شده است:

- نصب آنتی‌ویروس‌ها و به روز نگه داشتن آنها
- مانیتورینگ فایل‌های ثبت وقایع (Log File) برای ایرادات به وجود آمده
- نصب سیستم ثبت اطلاعات و حسابرسی برای سیستم‌ها و منابع داده‌ای حساس در شبکه
- محدودسازی دسترسی به هر ایستگاه کاری توسط یک کاربر یا گروه مشخصی از کاربران
- کنترل دسترسی به منابع داخلی و یا منابع به اشتراک گذاشته شده در شبکه
- برداشتن برنامه‌ها و سرویس‌های غیرضروری بر روی آنها
- نصب سیستم‌های اتوماتیک یا مرکزی تهیه نسخه پشتیبان
- اطمینان از نصب به روزترین تعمیرکنندگان امنیتی (وصله) بر روی سیستم‌های عامل و برنامه‌های کاربردی

همچنین سیستم‌های مانیتورینگ و سیستم‌های کشف نفوذ که بعدا توضیح داده خواهد شد، می‌تواند به حفظ امنیت ایستگاه‌های کاری در شبکه شما کمک کند.

از جمله مواردی که در مانیتورینگ ایستگاه‌های کاری می‌تواند مورد توجه قرار گیرد، عبارتند از:

سیستم ثبت وقایع: نظارت بر پیغام‌های خطا درباره تغییرات در سیستم فایل‌ها، تغییر اجازه‌های دسترسی، سرویس‌هایی که دیگر امکان شروع و انجام آنها وجود ندارد و یا دیگر تغییرات در سیستم

فضای هارد دیسک: ایستگاه‌های کاری ممکن است از انجام ثبت وقایع، ثبت خطاها، کشف حملات و دیگر موارد به شکل صحیح به دلیل پر شدن فضای هارد دیسک باز بمانند. پس مانیتورینگ میزان فضای خالی هارد دیسک ضروری است.

۵-۳-۲) محافظت تجهیزات سیار (Mobile Dvice)

لپ‌تاپ، نوت‌بوک، دستیار دیجیتالی شخصی (PDA) و دیگر تجهیزات سیار امروزه به شکل فزاینده‌ای در بسیاری از شبکه‌های کامپیوتری به کار گرفته می‌شود. حفاظت از این تجهیزات نیز در شبکه امری ضروری است. البته مانیتورینگ این تجهیزات سخت‌تر از مانیتورینگ ایستگاه‌های کاری است. تمامی مواردی که برای امن‌سازی ایستگاه‌های کاری مطرح گردید برای امنیت تجهیزات سیار نیز در صورت امکان ضروری است. اما دیگر موارد برای برقراری امنیت درخصوص این تجهیزات عبارتند از:

تجهیزات ضد سرقت: کاربرد تجهیزات هشداردهی و آلارم‌های تغییر جا برای این تجهیزات، کابل‌های قفل شده

استفاده از علائم و رنگ‌های شناسایی اضافی: اگر این تجهیزات دارای رنگ‌های خاصی باشند و یا بر روی آنها علائم شناسایی و حتی نام سازمان حک شده باشد، پیگیری آنها را در بیرون سازمان هم مقدورتر می‌سازد. از طرفی به کارگیری این روش سارقان را در سرقت آنها بی‌میل‌تر می‌سازد.

رمزگذاری داده‌ها: اگر تجهیزات موبایل شما برای نگهداری و یا انتقال داده‌های سری و مهم به کار گرفته می‌شود، حتما اینگونه داده‌ها توسط الگوریتم‌های پیشرفته رمزنگاری به صورت رمز شده دراورده شود، تا در صورت دستیابی توسط مهاجمین به این تجهیزات اطلاعات درون آنها قابلیت استفاده برای مهاجم را نداشته باشد.

۵-۳-۳) امن‌سازی و مانیتورینگ سرورها (Servers Security)

شما باید همان عملکردها که برای امن‌سازی ایستگاه‌های کاری انجام داده‌اید برای سرورها هم انجام دهید. البته سرورها نیاز به مراقبت بیشتری نسبت به یک ایستگاه کاری دارند، چرا که تخریب یک سرور افراد بیشتری را تحت شعاع خود قرار می‌دهد. از بعضی جهات حفاظت از سرورها راحت‌تر از حفاظت ایستگاه‌های کاری می‌باشد، چرا که آنها نیازی به دستیابی فیزیکی یا ورود به وسیله کاربران عادی ندارند. بعضی دیگر از راه‌های امنیتی برای محافظت از سرورها به شرح زیر می‌باشد:

- امن‌سازی فیزیکی سرورها از طریق قرار دادن آنها در اطاق‌های قفل‌دار
- جلوگیری از ورود کاربران به وسیله کنسول‌ها به آنها
- کنترل دقیق و مانیتورینگ دسترسی به کلیه سرویس‌ها. سرویس‌های اضافی همچون دیتابیس کاربران، سرویس وب و دیگر سرویس‌های ارائه شده توسط سرور. همچنین شما باید خطاهای ایجاد شده در دسترسی به سرویس‌ها، خطا در اجرای سرویس‌ها و هر تغییری در اجرای سرویس‌ها را رهگیری کنید.

- ایجاد نسخه‌های پشتیبان به صورت دوره‌ای از به هم‌بندی سرورها، داده‌های به اشتراک گذاشته شده و دیگر داده‌ها که نیاز به حفاظت از آنها وجود دارد. همچنین باید از حفاظت فیزیکی از این نسخه‌های پشتیبان مطمئن گردید. قرار دادن رمز عبور بر روی آنها و رمزگذاری آنها و قرار دادن آنها در گاوصندوق‌های ضدحریق از دیگر موارد مهم امنیتی می‌باشد.
- همچنین باید از مانیتورینگ دسترسی‌ها و در دسترس بودن منابع بر روی سرورها مطمئن گردید. به طور مثال شما باید از امکان‌پذیر بودن سرویس HTTP برای دسترسی به وب‌سایت‌ها بر روی سرور خود اطمینان حاصل کنید.

۵-۳-۴) مانیتورینگ تجهیزات اتصال

امروزه سیستم‌های مدیریت شبکه ارائه شده توسط بسیاری از فروشندگان که اطلاعات از تجهیزات اتصال را جمع‌آوری می‌کنند، در دسترس می‌باشند. به طور مثال اگر یک روتر یا سوئیچ بعضی از فریم‌های اطلاعاتی را به دلیل حجم بالای دیتاهای ورودی از دست بدهد، یک هشدار می‌تواند به سمت کنسول مدیریت شبکه و یا دیگر مکان‌های بالقوه مثل پیجر مدیر شبکه ارسال گردد. بسیاری از سیستم‌های مدیریت شبکه از پروتکل (SNMP- Simple Network Management Protocol) برای جمع‌آوری اطلاعات از سیستم‌های مختلف شامل میزبان‌های انفرادی موجود در شبکه، استفاده می‌کنند. بعضی از شرکت‌هایی مانند: IBM، Cisco و Hewlett-Packard سیستم‌های مدیریت شبکه‌ای را پیشنهاد می‌دهند که می‌توانند تجهیزات شبکه را مانیتور کنند.

فصل ششم: امن‌سازی برنامه‌های کاربردی

مقدمه

همانطور که در فصول پیشین دیدید راه‌های متفاوتی برای تخریب یک شبکه توسط مهاجمین وجود دارد. در این فصل تلاش می‌شود بر روی راه‌های تخریب از طریق برنامه‌های کاربردی موجود در شبکه و همچنین روش-های جلوگیری از این حملات مطالبی ارائه گردد. البته توجه شود که تمرکز اصلی این فصل بر روی بررسی برنامه‌های کاربردی در سمت کاربر (Client) می‌باشد. البته در برنامه‌های کاربردی سمت سرویس‌دهنده (Server) نیز امکانات تخریبی وجود دارد که در صورت داشتن زمان در این ترم تحصیلی در فصل جداگانه‌ای مطالب مربوط به این بخش نیز توضیح داده خواهد شد. در این فصل بر روی ۲ برنامه اصلی شامل پست الکترونیک (Email) و تارنمای وب (Web) توضیحات لازم ارائه خواهد شد.

۶-۱) امنیت بر روی پست الکترونیکی

اتصال بین یک کاربر و سرویس‌دهنده در شبکه جهانی اینترنت از میان تعدادی سیستم غیر مرتبط به طرفین این ارتباط گذر می‌کند. لذا در هر نقطه اتصالی از این ارتباط، ترافیک در حال گذر قابل مانیتور می‌باشد. انتقال اطلاعات رمزگذاری نشده در اینترنت عاملی است برای نادیده گرفتن محرمانگی.

امروزه پست الکترونیک یکی از روش‌های ارتباطی متداول می‌باشد. در این قسمت بعضی از موضوعات وابسته به امنیت در پست الکترونیک مورد توجه قرار می‌گیرد. بعضی از مهم‌ترین سرفصل‌های این قسمت عبارتند از: رمزگذاری ایمیل، ابعاد آسیب‌پذیر ایمیل، ایمیل‌های ناخواسته، ایمیل‌های گول‌زننده (Hoaxes) و ایمیل‌های اسکم (Scam).

۶-۱-۱) امن‌سازی پیغام‌های الکترونیکی

شبیه ارسال کارت پستال از طریق پست معمولی، ایمیل‌های استاندارد اولیه نیز دارای نقاط آسیب‌پذیر از آن جهت که توسط افراد غیر هم خوانده شود، وجود دارد. ایمیل‌ها می‌توانند توسط تجهیزاتی مانند پروتکل آنالایزر در طول مسیر انتقالشان مورد شنود قرار گیرند. طبق آمار تیم امنیتی CERT، در سال ۱۹۹۴ بیش از یک درصد ماشین‌های موجود بر روی اینترنت مورد تعرض شنود ایمیل‌ها برای دستیابی به موضوعات مهم درون آنها

مانند کلمه و رمز عبور توسط پروتکل آنالایزرها قرار گرفته‌اند. از طرفی به دلیل فقدان محرمانگی، ایمیل‌ها به راحتی قابل جعل می‌باشند. یک فرد حمله‌کننده می‌تواند با تغییر فیلد ارسال‌کننده در ایمیل‌ها، آنها را به شکلی که از طرف فرد مطمئن و معتبری ارسال شده‌اند، جلوه دهد.

لذا امن‌سازی انتقال اطلاعات می‌تواند این ابعاد ایمنی را لحاظ کند. رمزگذاری ایمیل‌ها این امکان را می‌دهد که تنها توسط افراد مورد نظر شما قابل فهم باشد. همچنین امن‌سازی پیغام‌های الکترونیکی می‌تواند شامل امضاء الکترونیکی ایمیل‌ها هم شود. با این کار گیرنده نامه هم مطمئن می‌گردد که این ایمیل از جانب شخص شما می‌باشد.

PGP (۲-۱-۶

Pretty Good Privacy مجموعه‌ای از ابزارهای نرم‌افزاری است که به شما امکان رمزگذاری، رمزگشایی و امضاء الکترونیکی بر روی اطلاعات داخل کامپیوترتان و همچنین ایمیل‌ها را می‌دهد. روش رمزگذاری و رمزگشایی در PGP به صورت نامتقارن می‌باشد. PGP برای رمزگذاری و امضاء الکترونیکی اعمال زیر را انجام می‌دهد:

- تولید کلیدها: PGP زوج کلید عمومی و خصوصی را برای شما ایجاد می‌کند.
- مدیریت کلیدها: PGP امکان نگهداری کلید عمومی دیگران را به صورت محلی برای شما امکان‌پذیر می‌سازد.
- رمزگذاری و رمزگشایی ایمیل‌ها: دوستان شما می‌توانند با کلید عمومی شما پیغام‌ها را رمزگذاری کنند و شما هم می‌توانید با کلید خصوصی خودتان این پیغام‌ها را از رمز درآورید.
- امضاء ایمیل‌ها: شما می‌توانید با استفاده از کلید خصوصی خودتان پیغام‌های ارسالی به دوستانتان را امضاء کنید و دوستانتان هم با داشتن کلید عمومی شما می‌توانند این امضاء را رمزگشایی کنند و از اینکه شما ارسال‌کننده واقعی ایمیل هستید مطمئن گردند.
- شما باید کلید عمومی خود را برای افرادی که علاقه‌مندید برای شما نامه به صورت رمزگذاری شده بفرستند یا بتوانند نامه‌های شما را که امضاء دیجیتالی کرده‌اید، دریافت کنند، بفرستید. کلید خصوصی شما هم در کامپیوتر شما مورد استفاده شخصی شما می‌باشد. شما همچنین می‌توانید کلید خصوصی خود را در تجهیزات قابل حمل مانند فلاپی دیسک نیز قرار دهید. کلید خصوصی با قرار دادن رمز عبور

که شما هنگام نصب PGP قرار می‌دهید، محافظت می‌گردد. این رمز عبور هر زمان که از کلید خصوصی برای رمزنگاری یا امضاء استفاده می‌کنید از شما خواسته می‌شود.

توجه: PGP می‌تواند با برنامه‌های کاربردی ایمیل زیر مجتمع گردد:

Qualcomm Eudora, Microsoft Exchange, Microsoft Outlook, Microsoft Outlook Express, Lotus Notes

۶-۱-۳) S/MIME

این نرم‌افزار هم شبیه PGP می‌باشد، با این تفاوت که کاربران به تاییدیه‌های ایجاد شده توسط PKI اعتماد می‌کنند. شما برای استفاده از S/MIME باید از برنامه‌های کاربردی که S/MIME را قادر به استفاده می‌کنند و همچنین دسترسی به یک تاییدیه PKI، استفاده کنید. این تاییدیه می‌تواند توسط یک PKI داخلی سازمان در اختیار شما قرار گیرد و یا توسط یک زیرساخت تولید کلید خارجی (PKI عمومی) در اختیار شما قرار گیرد. دو نوع از این PKI های عمومی، شرکت Verisign با آدرس *(http:/www.virisign.com)* و شرکت Thwate با آدرس *(http://www. Thwate.com)* می‌باشد. البته در کشور ما ایران نیز به تازگی یکی از شرکت‌های وابسته به وزارت بازرگانی در حال ارائه امضاء الکترونیکی و کلید عمومی و خصوصی می‌باشد. معروف‌ترین برنامه‌های کاربردی که S/MIME را قادر به استفاده می‌کنند عبارتند از:

Netscape, Microsoft Outlook, Microsoft Outlook Express

۶-۱-۴) نقاط آسیب‌پذیری پست الکترونیک

نقاط آسیب‌پذیری اغلب بر روی نرم‌افزارها دیده می‌شود و ایمیل هم یک مستثناء نمی‌باشد. علاوه بر اینکه ایمیل دارای نقاط آسیب‌پذیری برای تخریب خودی می‌باشد، بلکه بسیاری از مهاجمین از این نقاط آسیب برای تخریب دیگر امکانات سیستم مثل پاک کردن اطلاعات بر روی کامپیوتر شما سوء استفاده می‌کنند.

برای محافظت از شبکه و سازمان خود در مقابل نقاط آسیب‌پذیری پست الکترونیکی، شما باید در مقابل هشدارهای امنیتی سیستم هوشیار بوده و همچنین از ویروس‌یاب‌های به روز شده استفاده نمایید. سرور درگاه ایمیل می‌تواند با اسکن ایمیل‌های ورودی این درگاه را ایزوله کرده و یا ویروس‌های متصل به ایمیل‌ها را اجازه ورود به شبکه ندهد. این یک راه عمومی برای بسیاری از سازمان‌ها برای دفاع می‌باشد. اما تک تک کامپیوترهای موجود در شبکه شما هم می‌توانند از ویروس‌یاب‌ها برای دفاع محکم‌تر استفاده کنند. این کار علاوه بر جلوگیری

از ورود ویروس‌های بیرون از شبکه به کامپیوتر شما، از ویروس‌های ایجاد شده توسط کاربران داخل شبکه شما نیز برای ورود به کامپیوتر جلوگیری می‌نماید.

شما همچنین باید کاربران شبکه خود را در خصوص نقاط احتمالی حمله به وسیله ایمیل‌ها آموزش دهید. به طور مثال بسیاری از کدهای مخرب به صورت فایل‌های متصل به ایمیل‌ها برای شما می‌آید، لذا کاربران باید آموزش‌های لازم برای باز نکردن این ایمیل‌های مزاحم را دیده باشند.

هر زمانی که تخریبی بر روی یک نرم‌افزار ایمیل اتفاق می‌افتد، فروشندگان این نرم‌افزارها نسبت به رفع نقاط آسیب آنها از طریق وصله‌های امنیتی مبادرت می‌کنند. لذا ارتباط با فروشندگان و رهگیری این وصله‌ها و نصب آنها بر روی کامپیوترهای شبکه کمک شایانی به حفاظت از آنها در مقابل تهدیدات ناشی از ایمیل‌های می‌کند.

۶-۱-۵) انواع ایمیل‌های مخرب

در این بخش ما انواع ایمیل‌های مخرب را به سه دسته کلی تقسیم می‌کنیم:

- Spams
- Scams
- Hoaxes

۶-۱-۵-۱) Spams

این عنوان برای آن دسته از ایمیل‌های ناخواسته (مانند تبلیغات تجاری) که به آدرس‌های زیادی ارسال می‌گردند اطلاق می‌شود. در سال ۲۰۰۲ سایت آنلاین Business Week اعلام کرد نزدیک به نیمی از ایمیل‌های بعضی از سرویس‌دهندگان اینترنتی و ایمیل مربوط به این نوع از ایمیل‌ها می‌باشد.

برای محافظت از سازمان در مقابل این نوع ایمیل‌های مزاحم، شما باید از نرم‌افزارهای فیلترکننده در درگاه سرور ایمیل‌تان و همچنین تک تک کامپیوترهای شبکه خود استفاده نمایید. بعضی از این فیلترها عبارتند از:

SpamAssassin, BrightMail, Cloudmark, DigiPortal's ChoiceMail, Mailshell

شما همچنین باید کاربران خود را برای برخورد با این ایمیل‌ها آموزش دهید. بعضی از این آموزش‌ها عبارتند از:

- عدم پاسخگویی به اسپم‌ها: پاسخگویی به ایجادکنندگان اسپم‌ها باعث می‌شود که آنها از فعال بودن آدرس ایمیل شما مطمئن شده و حتی آدرس ایمیل شما را به دیگر تولیدکنندگان اسپم بفروشند.

- آدرس ایمیل خود را در داخل صفحات وب‌سایت‌ها پست نکنید: آدرس ایمیل قرار داده شده در داخل صفحات اختصاصی وب‌سایت شما و یا دیگران می‌تواند کمک شایانی برای شناسایی آدرس ایمیل شما توسط نرم‌افزارهای اسکنری که توسط تولیدکنندگان اسپم به طور دائم بر روی اینترنت و صفحات وب برای پیدا کردن آدرس‌های ایمیل جستجو می‌کنند، نماید.
- برای استفاده از گروه‌های خبری از آدرس ایمیل دومی استفاده کنید. گروه‌های خبری مکان مناسبی برای جمع‌آوری آدرس‌های ایمیل توسط تولیدکنندگان اسپم می‌باشد. لذا برای اینکه آدرس ایمیل شما لو نرود حتما برای ورود به گروه‌های خبری از آدرس ایمیل دوم استفاده نمایید.
- هرگز آدرس ایمیل خود را بدون دانستن دلیل اصلی برای خواستن آن در جایی عرضه نکنید. بسیاری از سایت‌ها برای اینکه بتوانید وارد آنها شوید از شما آدرس ایمیلتان و یک کلمه عبور درخواست می‌کنند. حتما قبل از ورود آدرس ایمیلتان از عبارات رعایت حریم ایمیل درخواستی توسط آن سایت مطمئن گردید.
- از فیلترهای اسپم استفاده کنید. بعضی از این فیلترها به شما اجازه می‌دهند براساس قوانینی که توسط شما تعریف می‌گردد عمل فیلترینگ انجام گیرد. مثل قوانینی بر مبنای عنوان ایمیل، فرستنده یا بدنه متن ایمیل.
- هیچ‌گاه چیزی را که در یک اسپم تبلیغ شده خریداری نکنید.

Scams (۲-۵-۱-۶

شبیه مورد قبلی این ایمیل‌ها هم ناخواسته می‌باشند. تفاوت این دو در آن است که Scam ها محصولات و کالایی را برای فروش ارائه نمی‌دهند، بلکه به طور خاص هدفشان سرقت پول، کالاها و سرویس‌ها می‌باشد. اغلب آنها از قربانی تقاضای ارسال پول، یا ارائه مشخصات حساب بانکی و یا اطلاعات کارت اعتباری می‌کنند. یکی از معروف‌ترین این ایمیل‌ها با نام ایمیل پول‌شویی نیجریه‌ای معروف است. اگر چه محل ارسال حتمی این ایمیل‌ها کشور نیجریه نمی‌باشد، ولی این ایمیل‌ها به این نام شهرت گرفته‌اند. در این ایمیل‌ها مثلا از فرد مورد تهاجم درخواست می‌گردد برای اینکه پولی که از طرف فردی که از دنیا رفته و آن پول به شما به ارث رسیده به حساب شما واریز گردد، مشخصات حساب بانکی خود را بدهید و یا اینکه حسابی مثلا در فلان بانک افتتاح کنید. بدین طریق فرد طمعکار قربانی اهداف پول‌شویی باندهای تبهکاری قرار گرفته و از طریق حساب بانکی این فرد اعمال خلاف قانون پول‌شویی انجام می‌گیرد.

برای محافظت کامپیوتر خود یا شبکه خود از سوء استفاده این ایمیل‌ها، تنظیم سیاست‌نامه امنیتی و قرار دادن مطالبی در خصوص رعایت محرمانگی اطلاعات ویژه مانند شماره حساب بانکی و یا شماره بیمه‌نامه و ... در آن امری لازم است. شما باید در این سیاست‌نامه مشخص سازید چه اطلاعاتی حساس می‌باشند. همچنین باید در این سیاست‌نامه کانال‌های امن ارسال داده و کانال‌های ناامن مشخص شوند. همچنین آموزش این نکات امنیتی به کاربران شبکه لازم می‌باشد. همچنین آموزش اینکه چه ایمیل‌هایی می‌توانند یک ایمیل Scam باشند به کاربران ضروری است. بعضی از مشخصه‌های موجود در یک ایمیل که می‌تواند بیانگر یک Scam باشد به شرح زیر است:

- فرصت‌های تجاری (Business Opportunity Scams)
- پول‌سازی از طریق ارسال ایمیل‌های عمده (Make Money by Sending Bulk E-Mail)
- نامه‌های زنجیره‌ای (Chain Email)
- برنامه کار در خانه (Work-at-Home Scheme)
- سلامتی و رژیم (Health and Diet Scams)
- درآمد بدون تلاش (Effortless Income)
- کالای مجانی (Free Goods)
- فرصت‌های سرمایه‌گذاری (Investment Opportunities)
- وام‌ها و یا اعتبارهای تضمین شده (Guaranteed Loans or Credit)
- اصلاح اعتبار (Credit Repair)

۶-۱-۵-۳) Hoaxes

یک ایمیل از نوع Hoaxes مانند یک نامه زنجیره‌ای در شبکه پخش می‌گردد. این ایمیل‌ها حاوی اطلاعات غلط ولی قابل باوری هستند و معمولا از سوی یک شخص به تعداد زیادی از افراد برای اینکه ایده یا دیدگاهی را در افراد به باور برسانند ارسال می‌گردند. معمولا در این ایمیل‌ها از گیرنده درخواست می‌شود که آن را برای دوستان خود هم ارسال کند. یکی از معروف‌ترین این ایمیل‌ها ایمیلی با عنوان Good Time است که به سرعت در شبکه پخش گردید و با داشتن کد مخرب درون خود باعث تخریب اطلاعات درون هاردیسک‌ها بسیاری از کامپیوترها گردید.

بعضی از این ایمیل‌ها به شما اعلام می‌کنند که مثلا کامپیوتر شما توسط یک نامه که از طرف دوست شما ارسال گردیده ویروسی شده و نام فایل ویروس را هم اعلام می‌کنند. در حالیکه این فایل یکی از فایل‌های اصلی سیستم شما مثلا Sulfnbk.exe , jdbgmgr.exe می‌باشد و شما به تصور اینکه این فایل‌ها ویروس می-باشند نادانسته آن را از روی سیستم خود پاک کرده و ادامه کار کامپیوتر خود را دچار اخلال می‌نمایید.

برای محافظت از شبکه خود در مقابل این نوع از ایمیل‌ها باید سیاست‌نامه امنیتی مبنی بر شناسایی این نامه‌ها و نحوه برخورد با آنها را در سازمان خود تنظیم کرده و آن را به کاربران شبکه خود هم آموزش دهید. بعضی از عناوین در این نوع ایمیل‌ها که کمک به شناسایی آنها می‌کند عبارتند از:

- فوری (Urgent): کلماتی مانند فوری، مهم، خطر، هشدار ویروس معمولا در عنوان این ایمیل‌ها وجود دارند.
- به دوستان خود بگویید (Tell all your Friends): معمولا این درخواست در داخل ایمیل می‌تواند وجود داشته باشد.
- این یک Hoax نیست (This isn’t a Hoax): این پیغام‌ها معمولا شامل معرفی افرادی به عنوان تاییدکننده آن هست که افراد قابل اعتمادی می‌باشند. به طور مثال فرستنده اصلی آن می‌تواند عبارتی مانند "این هشدار توسط فلان مقام قانونی و یا فلان ایستگاه خبری تایید شده" را برای فریب افراد در آن قرار دهد.
- پیامد ناگوار (Dire Consequence): این ایمیل‌ها می‌تواند حاوی اخطارهای بسیار فوری مبنی بر اینکه مثلا اطلاعات در کامپیوتر شما در حال تخریب می‌باشد، باشند.
- تاریخچه (History): اگر یک پیغام حاوی FW در قسمت موضوع خود باشد و یا تعداد زیادی پرانتز زاویه‌دار در عنوان خود باشد، این پیغام احتمالا چندین بار فوروارد شده و می‌توان احتمال داد این یک ایمیل Hoax می‌باشد.

۶-۲) امنیت بر روی وب

همانطور که در گذشته گفته شد سرقت بسته‌های اطلاعاتی عاملی است برای اینکه فرد مهاجم بتواند شبکه و کامپیوترهای یک سازمان را تخریب کند. معمولا این حمله متکی بر ضعف‌های برنامه‌های کاربردی است که ناشی از ضعف در مرحله طراحی و برنامه‌نویسی آنها می‌باشد. حتی مهاجمین می‌توانند کاربران را برای دریافت

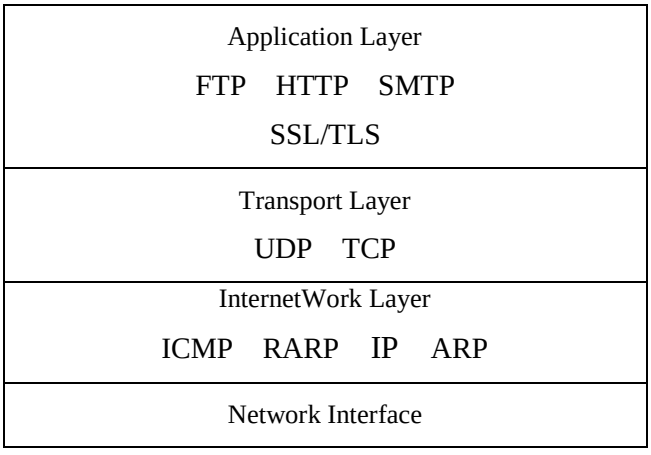
برنامه‌هایی که حاوی ویروس می‌باشند فریب دهند. در این بخش هدف بیان مخاطرات و نحوه مقابله با این مخاطرات در محیط وب می‌باشد.

SSL/TLS (۱-۲-۶

پروتکل‌های لایه سوکت امن (Secure Sockets Layer) و امنیت لایه انتقال (Transport Layer Security) برای پیاده‌سازی امنیت در تبادلات کلاینت/ سرور در اینترنت به کار برده می‌شود.

در سال ۱۹۹۴ شرکت نتاسکیپ پروتکلی به نام SSL را ارائه کرد. اساس این پروتکل مبتنی بر رمزگذاری به وسیله کلیدهای غیر متقارن که توسط شرکت RSA ارائه می‌گردد، بود. در سال ۱۹۹۹ سازمان IETF پروتکل جدیدی را ارائه کرد که مبتنی بر SSL بود که آن را TLS نامید. امروزه بسیاری از تولیدکنندگان نرم‌افزار در دنیا محصولاتی ارائه می‌دهند که این پروتکل‌های امنیتی را پشتیبانی می‌کنند. علاوه بر این از این دو پروتکل در اکثر مواقع به صورت متشابه در غالب عنوان مشترک SSL/TLS یاد می‌شود.

SSL/TLS ارتباطات اینترنتی را در مقابل استراق سمع، مداخله و جعل محافظت می‌کنند. کلاینت و سرور می‌توانند با استفاده از آن یکدیگر را احراز هویت کرده و پیغام‌ها را به شکل رمزگذاری شده در اینترنت انتقال دهند. SSL/TLS پروتکل غیر وابسته به لایه‌ای در شبکه است که طبق شکل ۶-۱ مابین دو لایه کاربردی و انتقال قرار می‌گیرد. هر برنامه کاربردی در شبکه مبتنی بر IP که به طور خاص پروتکل SSL/TLS را در خود پیش‌بینی کرده باشد، می‌تواند از این پروتکل به نحو احسن برای امن‌سازی انتقال اطلاعات بین کلاینت و سرور بهره‌برداری کند.



شکل ۶-۱) SSL/TLS در پشته پروتکل TCP/IP

احراز هویت سرور برای کلاینت: زمانی که یک مشتری قصد خرید کالایی از یک فروشنده بر روی وب‌سایت را دارد، مشتری می‌خواهد از اینکه این وب‌سایت توسط یک فروشنده واقعی جهت فروش محصولاتش ایجاد شده مطمئن گردد. SSL/TLS این امکان را برای کامپیوترهای مشتریان فراهم می‌کند که از مطمئن بودن سرویس فروش و تعلق آن به فروشنده واقعی آن محصول مطمئن گردد (و اینکه این سایت فروش از جانب یک سارق برای به سرقت بردن اطلاعات کارت فروش مشتری تدارک دیده نشده است). برای این منظور این سرور باید یک گواهینامه از یک CA قابل اعتماد برای کاربر، دریافت کرده باشد.

مبادله الگوریتم رمزگذاری مشترک: کلاینت و سرور می‌توانند الگوریتم رمزگذاری مورد استفاده خود را مبادله کنند. این کار طرفین کلاینت و سرور را برای پشتیبانی از تکنیک رمزگذاری قادر می‌سازد.

احراز هویت کلاینت برای سرور (اختیاری): وقتی که محدودسازی دسترسی به سرور توسط کلاینت‌ها مورد نظر باشد، کامپیوترهای کلاینت باید گواهینامه معتبری از یک CA را بر روی خود نصب کرده باشند. البته در بسیاری از خریدهای اینترنتی این کار انجام نمی‌گیرد چرا که بسیاری از خریداران گواهینامه معتبری در دست ندارند. لذا برای شناسایی کلاینت‌ها در تجارت الکترونیکی معمولا از مشخصاتی مثل شماره کارت اعتباری، تاریخ اعتبار آن و آدرس صدور صورت‌حساب برای شناسایی کلاینت‌ها توسط سرورها استفاده می‌شود.

استفاده از رمزگذاری غیرمتقارن برای ارسال رمزهای اشتراکی: رمزگذاری غیرمتقارن (یا کلید عمومی) برای شکسته شدن سخت می‌باشد و رمزگذاری متقارن برای انتقال داده‌های حجیم بسیار کارآ می‌باشد. SSL/TLS از رمزگذاری غیرمتقارن برای ارسال رمزهای اشتراکی (کلید متقارن) استفاده می‌کند. بنابراین رمزگذاری داده واقعی بسیار سریع‌تر می‌شود و در عین حال روش برقراری ارتباطات رمزگذاری شده نیز بسیار امن می‌باشد.

برقراری یک اتصال رمزگذاری شده: در انتها و البته بسیار مهم تمام ارتباطات میان کلاینت و سرور رمزگذاری شده می‌باشد.

HTTPS (۶-۲-۲

ارتباطات وب با به کارگیری HTTP اجرا می‌گردد. ارتباطات وبی که به وسیله SSL/TLS امن شده است با عنوان HTTPS نامیده می‌شود. مرورگرهای وب که ارتباطات HTTPS را نشان می‌دهند از علامت https://

به جای http:// در بخش آدرس استفاده می‌کنند. اگرچه HTTPS ارتباط بین کلاینت و سرور را رمزگذاری می‌کنند، اما قابل اعتماد بودن فروشنده یا امن بودن سرور فروشنده را تضمین نمی‌کند.

SSL/TLS جهت شناسایی سرور فروشنده و رمزگذاری ارتباطات بین کلاینت و سرور طراحی شده است. SSL/TLS قادر به جلوگیری از اعمال غیر اخلاقی بر روی اطلاعات جمع‌آوری شده از کارت‌های اعتباری توسط فروشنده، نمی‌باشد. همچنین SSL/TLS قادر به محافظت از اطلاعات ذخیره شده بر روی کامپیوتر سرور فروشنده نمی‌باشد. متاسفانه بسیاری از کامپیوترهای سرور سمت فروشنده مورد تعرض قرار می‌گیرند (و مشخصات کارت اعتباری خریداران سرقت می‌شود). به این دلیل بسیاری از فروشندگان اطلاعات کارت اعتباری خریداران را بر روی سرور خود ذخیره نمی‌کنند.

Buffer Overflows (۳-۲-۶

بافر به فضای داده‌ای اطلاق می‌شود که به وسیله هر دو عنصر تجهیزات سخت‌افزاری و پروسس‌های نرم‌افزاری به اشتراک گذاشته می‌شود. در این بخش تمرکز ما بر روی بافرهای برنامه‌ای، که اجازه اجرای برنامه‌های مختلف با اولویت‌های مختلف را می‌دهند، می‌باشد. هر بافر دارای سطح مشخص و یک مرز می‌باشد.

سرریزی بافر زمانی اتفاق می‌افتد که یک برنامه تلاش می‌کند داده‌های بیشتر از ظرفیت بافر را وارد آن کند. این کار گاها باعث آن می‌شود که حجم داده اضافی بر روی بافرهای کناری ریزش کرده و باعث خرابی داده‌های موجود در انها شود. سرریزی بافر ممکن است به دلیل ضعف در ساختار برنامه و یا ناشی از یک حمله تخریب-آمیز باشد. یک مهاجم از این روش برای در اختیار گرفتن کامپیوتر قربانی استفاده می‌کند. در یک حمله سرریز بافر ممکن است باعث خراب شدن فایل‌ها، تغییرات داده‌ها، استحصال اطلاعات محرمانه و یا اجرای کد بر روی ماشین هدف گردد.

بهترین راه در برخورد با این مشکل این است که پیاده‌کنندگان نرم‌افزار از روش‌های برنامه‌نویسی امن طبعیت کنند. اجرای عملیات امن آن در ذهن برنامه‌نویس می‌باشد. توجه به اینکه چگونه این برنامه می‌تواند تخریب و یا جهت تخریب دیگر برنامه‌ها استفاده شود، از راهکارهای اجرایی می‌باشد. بسیاری از پیشنهادات مربوط به طراحی امن یک برنامه را در کیت پیاده‌سازی برنامه (SDKs) می‌توان یافت. این کیت یک راهنمای برنامه-نویسی است که در آن موضوعاتی از قبیل ساختار یک برنامه، فانکشن‌ها و روش‌های پیاده‌سازی یک برنامه بر روی پلت‌فرمی خاص بیان گردیده است.

یکی دیگر از راه‌های برخورد صحیح با این پدیده، رهگیری از فروشندگان برنامه‌ها برای بهره‌برداری از وصله‌هایی است که در مرور زمان برای حل مشکلات این نرم‌افزارها توسط فروشندگان آن به بازار عرضه می‌گردد.

Active Content (۴-۲-۶

در راستای تلاش برای اینکه مرور صفحات وب مهیج، کاربردی و مفید گردند، تولیدکنندگان و فروشندگان نرم-افزارها محتواهای فعال را ایجاد می‌کنند. مواد محتواهای فعال برنامه اجرایی کوچک و یا کدهای اسکریپت هستند که به داخل مرورگرهای وب ارئه می‌شوند. به طور مثال بعضی از بانک‌ها حسابگرهایی برای محاسبه میزان پرداخت رهن را در داخل وب‌سایت‌هایشان پیشنهاد می‌دهند. این ماشین‌حساب‌های محاسب رهن به عنوان محتوای فعال شناخته می‌شوند. به عنوان مثال‌های دیگر می‌توان از بعضی از محتواهای ویدئویی و انیمیشن بر روی صفحات وب نام برد. دو نوع مرسوم محتواهای فعال جاوا اسکریپت‌ها (JavaScript) و اکتیوکس (ActiveX) می‌باشند. محتواهای فعال برای اجرای یک اسکریپت در داخل سیستم کلاینت طراحی شده‌اند. متاسفانه این امکان باعث ایجاد ریسک‌های امنیتی در سیستم‌ها هم می‌شود: بعضی از این اسکریپت‌ها باعث ایجاد عملکردهای مخرب در ماشین کلاینت هم می‌شوند. در این فصل تمرکز اصلی ما بر روی این محتواهای فعال در سمت کلاینت و امکانات تخریب‌آمیز ممکنه آنها می‌باشد.

Java Applets (۱-۴-۲-۶

جاوا زبان برنامه‌نویسی ارائه شده توسط شرکت سان (Sun Microsystems) می‌باشد که دارای امکاناتی است که استفاده از آن را برای محیط وب مناسب می‌سازد. برنامه‌های کوچک کامل در این زبان Java Applets نامیده می‌شود، که بر روی بیشتر مرورگرهای سمت کلاینت اجرا می‌گردد. به طور مثال نت اسکیپ و اینترنت اکسپلورر این برنامه‌های کوچک را پشتیبانی می‌کنند.

این برنامه‌های کوچک از داخل یک صفحه وب توسط برچسب‌های اپلت (APPLET tag) آدرس‌دهی می-شوند. این برچسب‌ها برای بارگذاری فایل‌های مربوط به متن کد جاوا استفاده می‌شوند. کد متن جاوا توسط موتوری بر روی کلاینت به نام ماشین مجازی جاوا (Java Virtual Machine) اجراء می‌شوند. این VM ها بر روی بسیاری از سیستم‌های عامل مانند یونیکس، مکینتاش و ویندوز اجراء می‌شوند.

توجه: سیستم عامل Windows XP به همراه خود این VM را ندارد و این بدان معناست که به خودی خود امکان اجرای Java Applet ها را ندارد. لذا در صورت نیاز به اجرای این اپلت‌ها بر روی این سیستم عامل حتما نرم‌افزار ماشین مجازی جاوا را بر روی کامپیوتر خود دریافت کنید.

متاسفانه مهاجمین می‌توانند از این امکان برای حمله به سیستم‌های سمت کلاینت استفاده کنند. شما برای اینکه خود و سازمان خود را در مقابل حملات از طریق Java Applets محافظت کنید، می‌توانید امکان پشتیبانی جاوا را بر روی ماشین خود غیرفعال کنید. بسیاری از مرورگرها (مثل نت اسکیپ و اینترنت اکسپلورر) امکان غیرفعال کردن جاوا را به شما می‌دهند.

Java Script (۲-۴-۲-۶

شرکت نت اسکیپ جاوا اسکریپت را به وجود آورد، یک زبان اسکریپت که تعداد زیادی از استراکچرها و ویژگی-های جاوا را به مشارکت می‌گذارد. به هر حال، جاوا و جاوا اسکریپت به صورت مستقل از هم پیاده‌سازی شده‌اند و دو زبان مستقل از هم تلقی می‌شوند.

بسیاری از مرورگرهای وب، شامل نت اسکیپ و اینترنت اکسپلورر، جاوا اسکریپت را پشتیبانی می‌کنند. جاوا اسکریپت نوعا در داخل صفحات HTML قرار داده می‌شود و توسط مرورگر وب در سمت کلاینت خوانده می-شود. یک برچسب اسکریپت در داخل کدهای HTML برای نشانه‌گذاری جاوا اسکریپت قرار داده می‌شود. جاوا اسکریپت معمولا برای ارتباط با دیگر اجزاء (مانند برنامه‌های CGI که بعدا توضیح داده خواهد شد) و یا دریافت اطلاعات ورودی از کاربران مورد استفاده قرار می‌گیرد.

توجه: جاوا اسکریپت می‌تواند برای باز کردن جاوا اپلت‌ها هم مورد استفاده قرار گیرد. به طور مثال جاوا اسکریپت و جاوا اپلت ممکن است به همراه هم برای ایجاد یک محاسب میزان رهن، نقشه‌های تعاملی و بسیاری از موارد دیگر استفاده شوند.

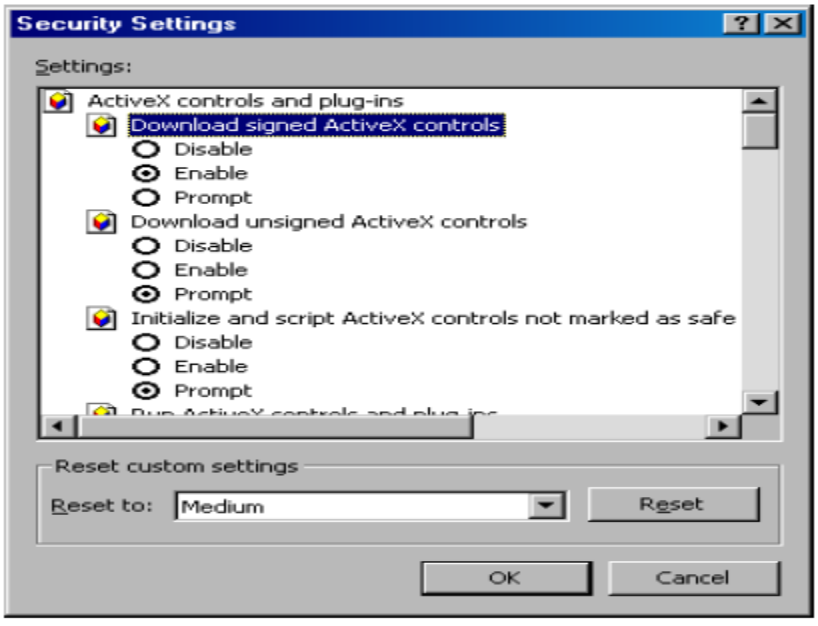
مهاجمین می‌توانند از جاوا اسکریپت‌ها برای حمله به سیستم کلاینت‌ها سوء استفاده کنند. برای محافظت از خودتان و سازمان در مقابل جاوا اسکریپت‌ها مخرب، می‌توانید جاوا اسکریپت را بر روی کامپیوتر خود غیرفعال کنید. هرچند غیرفعال کردن جاوا اسکریپت بر روی کامپیوتر شما را در مقابل این نوع حملات بیمه می‌کند، اما شما را از بهره‌گیری استفاده‌های مفید از محتواهای فعال نیز محروم می‌سازد. به هر حال، شما می‌توانید به صورت انتخابی در مورد سایت‌هایی که به آنها وارد می‌شوید و دارای اپلت‌های جالب و قابل اعتمادی هستند،

جاوا اسکریپت خود را فعال کنید. در صورتی که علاقه‌مند باشید جاوا اسکریپت خود را فعال نگه دارید حتما باید مرورگر وب خود را با آخرین نسخه‌های وصله‌های نرم‌افزاری به روز نگه دارید. در صورت غیرفعال کردن جاوا اسکریپت بر روی مرورگر خود، در صورتی که وب‌سایتی بخواهد بر روی کامپیوتر شما محتوای فعالی بفرستد، شما بر روی صفحه کامپیوتر خود جملات زیر را مشاهده خواهید کرد که در صورت کلیک بر روی آنها راه فعال-سازی مرورگر وب شما برای دریافت محتوای فعال را به شما نشان می‌دهد.

"To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options..."

۶-۲-۴-۳) ActiveX

این تکنولوژی هم برای فراهم‌سازی محتوای فعال به وجود آمده است. لازم به توجه است که این تکنولوژی توسط شرکت مایکروسافت تنها برای استفاده در مرورگرهای اینترنت اکسپلورر طراحی گردیده و در حال حاضر در هیچ مرورگر دیگری پشتیبانی نمی‌شود. شبیه جاوا اسکریپت، اکتیوکس هم می‌تواند با دیگر برنامه‌های کاربردی ارتباط برقرار کرده، داده‌های ورودی توسط کاربران را دریافت کند و سرویس‌های کاربردی را برای کاربران تدارک ببیند. همچنین مانند جاوا اسکریپت در معرض سوء استفاده توسط مخربین برای حملات می-باشد.



شکل ۶-۲) تنظیمات ActiveX در اینترنت اکسپلورر

برای کمک به حفاظت سیستم‌ها از تخریب‌های ناشی از سوء استفاده از اکتیوکس، اینترنت اکسپلورر به شما امکان انتخاب دریافت و اجرای کنترل‌های اکتیوکس مطابق شکل ۶-۲ را می‌دهد. شما می‌توانید اینترنت اکسپلورر را به شکلی تنظیم کنید که به صورت اتوماتیک کنترل اکتیوکس را دریافت نماید، یا قبل از دریافت به شما پیغامی مبنی بر دریافت یا عدم دریافت دهد و یا به طور کلی دریافت هرگونه کنترل اکتیوکس را غیرفعال نماید.

اگر شما لازم است از کنترل اکتیوکس استفاده کنید، باید به طور دائمی سایت فروشنده نرم‌افزار را برای هشدارهای امنیتی و اطلاعاتی در مورد احتمالات تخریب مورد مطالعه قرار دهید. اگر شما متوجه شدید که یک کنترل‌کننده خاص اکتیوکس دچار مخاطراتی برای امکان حمله می‌باشد، باید آن را غیرفعال کرده تا وصله امنیتی آن ارائه گردد.

Signing Active Content (۶-۲-۴-۴)

در تلاش برای افزایش امنیت محتواهای فعال، بعضی از فروشندگان فرایندی را برای انجام امضای دیجیتالی قبل از نصب محتواهای فعال، پیاده‌سازی کرده‌اند. تولیدکنندگان محتواهای فعال قبل از ارسال این محتواهای فعال آنها را امضای دیجیتالی می‌نمایند. این ارائه‌دهندگان تاییدیه امضاء برای امضاء کردن محصولاتشان را از یک CA قابل اعتماد (مانند Verisign) دریافت می‌کنند. امضاء الکترونیکی کمک به ایجاد اعتماد از آن جهت که محتوای فعال ارائه شده از یک فروشنده معتبر می‌باشد، می‌کند.

مایکروسافت از یک تکنولوژی در اینترنت اکسپلورر به نام Authenticode برای بررسی صحت امضاء قبل از دریافت محتوای فعال از یک فروشنده، استفاده می‌کند.

باید توجه داشت اگر چه این کار امنیت زیادی را برای دریافت محتواهای الکترونیکی به ارمغان می‌آورد، اما در مقابل مشکلاتی که ممکن است از طرف یک فروشنده مورد اعتماد به وجود آید، یا در مورد حفره‌های امنیتی که ممکن است در نرم‌افزاری در آینده مشخص شود، قادر به عملکرد پیشگیرانه نمی‌باشد. لذا همیشه توجه داشته باشید که آخرین وصله‌های امنیتی را هم از فروشندگان برای رفع عیوب دریافت کنید.

Cookies (۵-۲-۶

کوکی عبارت است از مقدار کوچکی از اطلاعات که یک وب سرور در مورد یک کاربر بر روی کامپیوتر خود کاربر ذخیره می‌کند. به طور مثال، کوکی ممکن است تبلیغات مختلفی که یک مرورگر کلاینت دریافت کرده را ضبط نماید. این امر به وب سرور کمک می‌کند تبلیغات متفاوتی غیر از تبلیغاتی که برای کاربر در گذشته نشان داده است را به نمایش گذارد.

مرورگر سمت کلاینت معمولا به سرورها اجازه ذخیره‌سازی کوکی‌ها را می‌دهند. بسیاری از مرورگرها به این دلیل این اجازه را صادر می‌کنند که امروزه کوکی‌ها در حجم بالایی مورد استفاده هستند و بسیاری از وب سرورها قادر به انجام فعالیت صحیح خود بدون آنها نمی‌باشند. کوکی‌ها بسته به مرورگر وب مورد استفاده در مکان‌های مختلفی ذخیره می‌شوند. به طور مثال نت اسکیپ کوکی‌ها در فایلی به نام Cookies.txt و اینترنت اکسپلورر هر کوکی را در فایل‌های جداگانه‌ای در پوشه‌ای به نام Internet Files/Temporery %windir% ثبت می‌نماید.

کوکی‌ها به دلایل مختلف استفاده می‌شوند. به طور مثال بعضی از کوکی‌ها برای ثبت علائق کاربران وقتی به وب‌سایتی متصل می‌شوند، به کار می‌روند. دیگر کوکی‌ها برای پشتیبانی از وضعیت اطلاعات به کار می‌روند (وضعیت اتصال بین کلاینت و سرور). بعضی از سرورها هم از کوکی‌ها برای مقاصد احراز هویت کلاینت‌ها استفاده می‌کنند. متاسفانه کوکی‌ها هم می‌توانند توسط مهاجمین به طرق زیر برای مقاصد سوء مورد استفاده قرار گیرند:

- کوکی‌ها می‌توانند اداره شوند و یا دزدیده شوند. حمله‌کننده می‌تواند کوکی‌ها را برای به دست آوردن اطلاعات مهم در مورد کاربران شبکه، سازمان و مسائل امنیتی در شبکه داخلی شما به سرقت ببرد.
- مهاجم می‌تواند با قرار دادن یک اسکریپت به داخل کامپیوتر کلاینت، کوکی‌های داخل سیستم کلاینت را به طرف سیستم خود انتقال دهد. حتی احتمال استراق سمع کوکی توسط مهاجمین در حین انتقال وجود دارد.

برای محافظت سازمان و کلاینت‌های سازمان خود در برابر تخریب‌های ناشی از سوء استفاده از کوکی‌ها، باید از روش‌های زیر بهره ببرید:

- وب سرور خود را با اتکا و اعتماد بر اطلاعات ذخیره شده در کوکی‌های سمت کلاینت جهت دسترسی به منابع یا ارائه هر سرویس اضافه، پیکربندی نکنید. چرا که ممکن است از این طریق توسط مهاجمی که بر روی کوکی‌ها دسترسی داشته، تخریبی بر روی وب سرور شما انجام گیرد.
- از کوکی‌ها برای نگهداری اطلاعات محرمانه و مهم مانند کد شماره حساب بانکی و گواهینامه‌های احراز هویت (مانند کلمه عبور) استفاده نکنید.
- اگر لازم است که اطلاعات مهمی در کوکی‌ها نگهداری شود، حتما از SSL/TLS برای محافظت از اطلاعات داخل کوکی‌ها استفاده شود.

CGI (۶-۲-۶

برنامه‌های CGI معمولا برای تولید محتواهای فعال در وب سرورها مورد استفاده قرار می‌گیرد. CGI ها معمولا برای ارسال اطلاعات میان برنامه کاربردی و وب سرورها می‌باشند. به طور مثال آنها معمولا برای انجام کارهایی مانند وارد کردن داده، جستجو، فانکشن‌های بازیابی در دیتابیس‌ها مورد استفاده قرار می‌گیرند.

با زبان‌های مختلف برنامه‌نویسی می‌توان CGI ها را ایجاد کرد، زبان‌هایی همچون C, C++, Visual Basic Fortran, PERL.

این برنامه‌ها می‌توانند هدف حمله برای تخریب وب سرورها قرار گیرند. برخلاف Java Script و ActiveX که بر روی کامپیوتر کلاینت اجرا می‌شوند، بر روی کامپیوتر وب سرور اجرا می‌گردد. البته شبیه دیگر برنامه‌ها این برنامه هم می‌تواند دارای حفره‌ها امنیتی باشد که توسط مخربین سوء استفاده شود. در زیر برخی از تخریب-های ممکنه براساس این برنامه‌ها آورده شده است:

- اجرای چندین‌باره یک برنامه CGI از طریق مرورگرهای چندگانه وب. هرگاه یک برنامه CGI توسط مرورگری اجرا گردد، بخشی از ظرفیت منابع سیستمی بر روی وب سرور را برای اجراء در اختیار می-گیرد، حال اگر مهاجمی به کرات دستور اجرای این برنامه را بر روی مرورگر خود بدهد، ظرفیت منابع وب سرور مورد استفاده قرار می‌گیرد و این عاملی است برای پایین آمدن سرعت سرویس‌دهی وب سرور.

- تهدید از طریق برنامه‌های CGI که بعضا در کنار خود وب سرور به صورت پیش‌فرض ارائه می‌گردد. این برنامه‌ها ممکن است دارای حفره‌های امنیتی باشند و بدین شکل مخربین از آن سوء استفاده نمایند.
- تهدید از طریق برنامه‌های مجانی CGI، این برنامه‌ها هم ممکن است دارای حفره‌های امنیتی باشند.
- ارسال داده‌های جعلی به سمت برنامه‌های CGI که می‌تواند باعث تخریب برنامه گردد.

برای اینکه یک سرور قادر به اجرای یک برنامه CGI باشد، شما باید به وب سرور اجازه خواندن و اجراء را در دایرکتوری برنامه‌های CGI بدهید. اما باید مطمئن گردید که امکان نوشتن در این دایرکتوری را غیرفعال کنید. بدین روش امکان وارد کردن اطلاعات مخرب به این دایرکتوری از طرف فرد مخرب را هم سلب می‌کنید.

برای محافظت از وب سرور در مقابل مخاطرات ناشی از برنامه‌ها CGI، باید روش‌های زیر را به کار بندید:

- ایجاد محدودی در کاربرد برنامه‌های CGI. به این طریق از ایجاد بار زیاد بر روی وب سرور و نتیجتا کاهش سرعت آن، می‌کاهید.
- نصب برنامه‌های CGI به شکلی که در شرایط قانون حداقل اجازه (Least Privileged User) اجراء گردد.
- پاک کردن تمام برنامه‌های CGI به صورت پیش‌فرض موجود در درون وب سرور.
- بررسی برنامه‌های CGI در جهت پیدا کردن حفره‌های امنیتی آنها. استفاده از برنامه‌هایی که از مراحل تست لازم عبور کرده باشند.

۶-۲-۷) Instant Messaging

پیغام‌گذاری لحظه‌ای یا IM روشی است که امروزه برای انتقال صحبت، فایل، صدا بین کاربران مختلف به صورت مستقیم بر روی وب مورد استفاده قرار می‌گیرد. این برنامه‌ها برای اجرا و بهره‌برداری بسیار راحت می‌باشند، اما متاسفانه دارای شرایطی هستند که توسط مهاجمین برای تدارک حمله مورد استفاده قرار می‌گیرند. از جمله مشکلات می‌توان به موارد زیر اشاره کرد:

- انتقال داده‌های رمز نشده. مردم اغلب داده‌های مهم مثل کلمه عبور و رمز عبور را از این طریق برای افراد مورد اعتماد خود ارسال می‌کنند. غافل از اینکه این ارتباط می‌تواند توسط هکر با استفاده از پروتکل آنالایزر مورد استراق سمع قرار گیرد.

- فایل‌های ارسالی ممکن است ویروس‌یاب‌ها را دور بزنند. IM به کاربران اجازه انتقال فایل، جدا از سیستم ایمیل که دارای ویروس‌یاب می‌باشد را می‌دهد و چون فایل ارسالی از طریق ایمیل ارسال نمی-شود، لذا مورد بررسی ویروس‌یاب ایمیل قرار نمی‌گیرد. پس انتقال ویروس از این طریق امکان‌پذیر می-باشد.
- هکر می‌تواند نقاط ضعف این سیستم را شناسایی کند، مواردی همچون سرریز بافر. شبیه دیگر برنامه-های کاربردی، IM ها هم می‌توانند دارای حفره‌های امنیتی باشند، اما این حفره‌های امنیتی به طور بالقوه خطرناک‌تر می‌باشد، چرا که اتصال به صورت مستقیم بین کاربران می‌باشد. همچنین اشکال برنامه‌ای در یک طرف ارتباط می‌تواند عاملی گردد که طرف مقابل ارتباطی کنترل کامپیوتر دیگری را در اختیار گیرد.
- هکر می‌تواند طرف مقابل ارتباطی خود را با استفاده از اطلاعات دروغ فریب داده و او را مجاب به افشای اطلاعات محرمانه کند (حملاتی از نوع مهندسی اجتماعی).

بعضی از سازمان‌ها خود را در مقابل تهدیدات ناشی از IM با جلوگیری از استفاده از IM در سازمان خود، بیمه کرده‌اند. بعضی از سازمان‌ها اجازه استفاده از IM هایی را که امن باشند، می‌دهند. اگر امکان حذف کامل سیستم IM در سازمان شما نمی‌باشد، حتما موارد امنیتی زیر را مد نظر داشته باشید:

- انحصار در استفاده از IM هایی که برای استفاده شما مجاز می‌باشند. این عمل شما را از پشتیبانی، امن‌سازی، مشکلات ممکنه چندگانه ناشی از IM های مختلف خلاص می‌کند.
- اگر اطلاعات انتقالی بین کلاینت‌ها باید امن باشد، از برنامه IM ی استفاده کنید که قابلیت رمزگذاری داشته باشد.
- تنظیم نظام‌نامه امنیتی برای استفاده از IM. مثلا اینکه از طریق IM انتقال فایل انجام نگیرد.
- آموزش کاربران برای آگاهی آنها از خطرات ممکن IM. به آنها توضیح دهید که انتقال فایل از این طریق چقدر خطرناک است و اینکه یک هکر ممکن است برای فاش شدن اطلاعات محرمانه او تلاش کند.
- اطمینان از اینکه تمامی استفاده‌کنندگان از IM، از ویروس‌یاب‌های به روز شده استفاده می‌کنند.
- پیگیری فروشندگان نرم‌افزارهای IM برای دریافت آخرین وصله‌های امنیتی.