

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

### مقدمه

امروزه با توسعه و پیشرفت فناوریهای نوین در جوامع و گسترش بی حد و مرز فناوری اطلاعات در تمامی عرصه های زندگی بشر، همچنین گری از فناوری در جهت خلق رفاه و زندگی اجتماعی مناسب شاهد گسترش و توسعه دنیای مجازی در همه ابعاد زندگی خود هستیم از يك سو گسترش شبکه های اطلاعاتی و دنیای مجازی به رفاه، آسایش و انجام کارها با سرعت و دقت بیشتر کمک می کند، از سوی دیگر چالشها و موانعی نیز در به کارگیری فناوری اطلاعات و شبکه های اطلاعاتی رخ می دهد که یکی از مقوله ها امنیت فناوری اطلاعات یا امن بودن فضای تبادل اطلاعات است. هرروزه شاهد اخباری در زمینه تهدیدات امنیتی در حوزه فناوری اطلاعات در گوشه و کنار جهان و سوء استفاده هایی که از عرضه تبادل اطلاعات می شود، هستیم از جمله هک شدن سایتها توسط نفوذگران، انتشار ویروسهای رایانه ای جدید و سرقت از حسابهای مشتریان بانکها، شکسته شدن قفلهای نرم افزاری و... در دنیای امروز با واگذاری کارهای مالی، اداری و اطلاعاتی به شبکه های رایانه ای 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 می گردد که در آن بسیاری از ملاحظات امنیتی مد نظر قرار گرفته باشد برای يك سازمان تجاری موفق اطلاعات دارایی اصلی است همانطور که در امر تجارت سنتی مجموعه ای از تمهیدات وجود دارد، در شکل پیچیده تر آن هم در محیط الکترونیکی وجود دارد امنیت اطلاعات کمک می کند که آسیبها کمینه، سرمایه اطلاعاتی بیشینه، و فرصتهای تجاری از دست اندازی رقبا محافظت گردد

### 1-1) امنیت فناوری اطلاعات

موضوع امنیت فناوری اطلاعات از موضوعات مهم و دارای اولویت می باشد که در همه سازمانها بخشی از تمرکز کاری نیروهای حوزه فناوری اطلاعات را بر خود معطوف کرده است. فناوری اطلاعات شامل فناوریهای است که در خدمت ذخیره سازی، پردازش، انتقال و مدیریت اطلاعات است، اما امنیت فناوری اطلاعات به استفاده

این از این فناوری و اطمینان از وجود محیطی عاری از هرگونه تهدید باز می گردد. 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 می دهیم.

### الف) امنیت رایانه:

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

### ب) امنیت ارتباطات:

حفاظت از اطلاعات در طی انتقال بین سیستم های رایانه ای و شبکه ها را امنیت ارتباطات گویند. باید دانست که به کارگیری فناوری اطلاعات در یک شبکه ارتباطی برای ارائه خدمات مورد نیاز می تواند همراه با خطرات امنیتی متعددی باشد. در استفاده از خدمات شبکه های رایانه ای 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 رایانه ای (Process) می باشد که به آنها عنصر (Principal) نیز گویند که به تعریف آنها می پردازیم. 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 آدرس دهی خاص می باشد. فرآیند: عملیاتی که بر روی ماشین ها انجام می شود و معمولا با استفاده از مدل مشتری / سرویس دهنده (client / server) فرآیند سمت مشتری و سرویس دهنده را از هم تشخیص می دهند. اما یکی از رایج ترین اصطلاحات در زمینه امنیت شبکه های رایانه ای نفوذ و نفوذگر می باشد که به تفصیل در این باره صحبت خواهیم کرد.

## 2-1) امنیت شبکه و اینترنت

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

### 1-2-1) اهمیت امنیت در شبکه و اینترنت

بدون شک کامپیوتر و اینترنت در مدت زمان کوتاهی توانسته اند حضور مشهود خود را در تمامی عرصه های حیات بشری به اثبات برسانند . وجود تحولات عظیم در ارتباطات ( نظیر Email و تلفن های سلولی ) ، تحولات گسترده در زمینه تجهیزات الکترونیکی و سرگرمی ( کابل دیجیتال ، mp3 ) ، تحولات گسترده در صنعت حمل و نقل ( سیستم هدایت اتوماتیک اتومبیل ، ناوبری هوایی ) ، تغییرات اساسی در روش خرید و فروش کالا ( فروشگاههای online ، کارت های اعتباری ) ، پیشرفت های برجسته در عرصه پزشکی ، صرفاً " نمونه هایی اندک در این زمینه می باشد .

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 کامپیوترهای دیگر ، ذخیره شده است ؟ پاسخ به سوال فوق، جایگاه کامپیوتر و اهمیت ایمن سازی 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

### 1-2-2) برخی از انواع تهدیدات در اینترنت

اینترنت، علیرغم تمامی جنبه های مثبت دارای مجموعه ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنان بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردار می باشند :

- عملکرد ویروس های کامپیوتری که می تواند منجر به حذف اطلاعات موجود بر روی یک کامپیوتر شود .
- نفوذ افراد غیر مجاز به کامپیوتر شما و تغییر فایل ها
- 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 می توان احتمال بروز و یا موفقیت این نوع از حملات را به حداقل مقدار خود رساند .

### 1-2-3) مفاهیم اولیه امنیت اطلاعات در اینترنت

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

- **Attacker , Hacker و یا Intruder** . اسامی فوق به افرادی که همواره در صدد استفاده از نقاط ضعف و آسیب پذیر موجود در نرم افزارها می باشند ، اطلاق می گردد . با این که در برخی حالات ممکن است افراد فوق اهداف غیر مخربی را نداشته و انگیزه آنان صرفاً " کنجکاوی باشد، حاصل عملیات آنان می تواند اثرات جانبی منفی را به دنبال داشته باشد .
- **کد خرب** : این نوع کدها شامل ویروس ها ، کرم ها و برنامه های تروجان ( Trojan ) بوده که هر یک از آنان دارای ویژگی های منحصر بفردی می باشند :

□ **ویروس‌ها** ، نوع خاصی از کدهای مخرب می باشند که شما را ملزم می نمایند به منظور آلودگی سیستم ، عملیات خاصی را انجام دهید . این نوع از برنامه ها به منظور نیل به اهداف مخرب خود نیازمند یاری کاربران می باشند . باز نمودن یک فایل ضمیمه همراه Email و یا مشاهده یک صفحه وب خاص ، نمونه هایی از همکاری کاربران در جهت گسترش این نوع از کدهای مخرب است.

□ **کرم‌ها** : این نوع از کدهای مخرب بدون نیاز به دخالت کاربر ، توزیع و گسترش می یابند . کرم ها ، عموماً " با سوء استفاده از یک نقطه آسیب پذیر در نرم افزار فعالیت خود را آغاز نموده و سعی می نمایند که کامپیوتر هدف را آلوده نمایند . پس از آلودگی یک کامپیوتر ، تلاش برای یافتن و آلودگی سایر کامپیوتر انجام خواهد شد . همانند ویروس های کامپیوتری ، کرم ها نیز می توانند از طریق Email ، وب سایت ها و یا نرم افزارهای مبتنی بر شبکه ، توزیع و گسترش یابند . توزیع اتوماتیک کرم ها نسبت به ویروس ها یکی از تفاوت های محسوس بین این دو نوع کد مخرب ، محسوب می گردد .

□ **برنامه های تروجان** : این نوع از کدهای مخرب ، نرم افزارهایی می باشند که ادعای ارائه خدماتی را داشته ولی در عمل، اهداف خاص خود را دنبال می نمایند . ( تفاوت در حرف و عمل ) . مثلاً " برنامه ای که ادعای افزایش سرعت کامپیوتر شما را می نماید ، ممکن است در عمل اطلاعات حساس موجود بر روی کامپیوتر شما را برای یک مهاجم و یا سارق از راه دور ، ارسال نماید .

## 1-2-4) سابقه امنیت در شبکه اینترنت

اینترنت در سال 1969 بصورت شبکه‌های بنام 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 1971 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 مسأله امنیت بیش از پیش اوج گرفت. در سال 1988، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که بعداً، «کرم موریس» نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به یک رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و بصورت هندسی تکثیر شود. آن زمان 88000 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 ضد امنیتی، آموزش و تجهیز شبکه‌ها و روش‌های پیشگیرانه نقش مؤثری داشت. با رایج‌تر شدن و استفاده عام از اینترنت، مسأله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/OILS WORM در سال 1989، Sniff packet در سال 1994 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 روزبه‌روز 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.

## 1-3) فرایند توسعه امنیت سازمان:

## الف) تجزیه و تحلیل خطرات مطرح در سازمان یا سیستم

باید تجزیه و تحلیل حملات احتمالی و سطح آسیب پذیری سیستم مشخص شود یعنی با تحلیل خطر (ریسک) بین خطر آفرینی یک تهدید، امکان وقوع و تکرار آن، هزینه های ایجاد مکانیزم های حفاظتی بررسی شود.

## ب) تدوین سیاستها و خدمات امنیتی:

با توجه به نتایج تجزیه و تحلیل خطر پذیری سیاستهای امنیتی تعیین می شود. سیاست امنیتی مبادله ای منطقی بین خطرات و منابع موجود ارائه داده و در برگزیده وظایفی است که آنها را خدمات امنیتی گویند. خدمات امنیتی به وسیله مکانیزمهای امنیتی که مبتنی بر الگوریتم های رمز نگاری و پروتکل های امنیتی است محقق می شود.

یک سیاست امنیتی، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که میبایست توسط افرادی که به یک تکنولوژی سازمان و یا سرمایه های 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 سرمایه های اطلاعاتی است. در ادامه ویژگیهای یک سیاست امنیتی خوب و یک مثال از سیاست امنیتی، تعریف رمز عبور، بیان می گردد.

### • 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<sup>1</sup> استفاده شود.
- از کلمات موجود در دیکشنری استفاده نگردد.
- رمزهای عبور، در فواصل زمانی مشخصی (سی و یا نود روز) به صورت ادواری تغییر داده شوند.

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

<sup>1</sup>- Underline

### 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 مسیر یابی و تأیید توسط عامل سوم.

به طور کلی نگاه به مقوله امنیت نمی تواند یک نگاه مطلق باشد یعنی امنیت به معنای مطلق در هیچ شبکه یا سیستم رایانه ای نمی تواند وجود داشته باشد اما با ارزیابی های امنیتی و مدیریت بهتر مکانیزم های 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 می توان خطرات امنیتی را به حداقل رسانید (با توجه با این نکته که عدم استفاده صحیح از خدمات در دسترس کاربران و اشتباهات انسانی ضعف سیستم های دفاعی را افزایش می دهد). به بیان دیگر می توان با یک نگرش سیستماتیک و استفاده مداوم از یک چرخه این سازی شامل طراحی، پیاده سازی، ارزیابی و اصلاح، ضریب امنیتی سیستم های رایانه ای خود را بالا ببریم.

### 1-4) انواع ویژگیها و سرویسهای امنیتی در محیطهای تجاری

- احراز هویت - Authentication:
- فرستنده یا گیرنده هویت واقعی خود را برای طرف مقابل اثبات می کند.
- 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 داده ها و اطلاعات موجود در سیستم ضبط رویدادها (Log File) موجود باشد.
- صحت داده ها (تمامیت و جامعیت) - Integrity:
- یعنی عدم امکان دستکاری داده ها توسط افراد یا نرم افزارهای 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
- انکار ناپذیری - Non-Repudiation :
- یعنی هیچ‌کدام از طرفین (فرستنده و گیرنده پیام)، امکان انکار عملکرد خود (ارسال پیام) را نداشته باشد. یا 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 شبکه های کامپیوتری و اینترنت

### مقدمه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس های فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطمینان از این بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطر و سنگین ) . در زمان ارائه ، سرویس دهندگان مجموعه ای از سرویس ها و پروتکل ها را به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال کرده اند. این موضوع ارتباط مستقیمی با سیاست های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهای است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند.

اولین مرحله در خصوص این سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص این سازی شبکه را شامل می شود . هر نوع برنامه ریزی در این رابطه مستلزم توجه به موارد زیر است :

- ✓ بررسی نقش هر سرویس دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- ✓ انطباق سرویس ها ، پروتکل ها و برنامه های نصب شده با خواسته های یک سازمان
- ✓ بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس ها و پروتکل های غیرضروری ، تنظیم دقیق امنیتی سرویس ها و پروتکل های فعال )

تعلل و یا نادیده گرفتن فاز برنامه ریزی می تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد . متأسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری ها به سرعت و به صورت مستمر در حال تغییر

بوده و می بایست متناسب با فن آوری های جدید ، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس دهندگان و کاهش نقاط آسیب پذیر آنان با جدیت دنبال شود . نشستن پشت یک سرویس دهنده 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 می نماید . هر سیستم عامل دارای مجموعه ای از سرویس ها ، پروتکل ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل های آنان در جهت افزایش کارایی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنان با توجه به شرایط موجود و فن آوری های جدید ارائه شده ، اعمال گردد . فراموش نکنیم که حتی راه حل های انتخاب شده فعلی که دارای عملکردی موفقیت آمیز می باشند ، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح نباشند .

## (1-2) وظیفه یک سرویس دهنده

پس از شناسایی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس ها و پروتکل های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم گیری نمود . برخی از سرویس دهندگان به همراه وظیفه آنان در یک شبکه کامپیوتری به شرح زیر می باشد :

- Logon Server : این نوع سرویس دهندگان مسئولیت شناسایی و تائید کاربران در زمان ورود به شبکه را برعهده دارند . سرویس دهندگان فوق می توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس دهندگان نیز انجام دهند .
- Services Network Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن سرویس های مورد نیاز شبکه را برعهده دارند . این سرویس ها 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 سرویس دهندگان مسئولیت میزبان نمودن برنامه های کاربردی نظیر بسته نرم افزاری Accounting و سایر نرم افزارهای مورد نیاز در سازمان را برعهده دارند .
- File Server : از این نوع سرویس دهندگان به منظور دستیابی به فایلها و دایرکتوریهای کاربران ، استفاده می گردد .
- Print Server : از این نوع سرویس دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشته شده در شبکه ، استفاده می شود .
- Web Server : این نوع سرویس دهندگان مسئولیت میزبان نمودن برنامه های وب و وب سایت های داخلی و یا خارجی را برعهده دارند .
- FTP Server : این نوع سرویس دهندگان مسئولیت ذخیره سازی فایلها برای انجام عملیات Downloading و Uploading را برعهده دارند. سرویس دهندگان فوق می توانند به صورت داخلی و یا خارجی استفاده گردند .
- Email Server : این نوع سرویس دهندگان مسئولیت ارائه سرویس پست الکترونیکی را برعهده داشته و می توان از آنان به منظور میزبان نمودن فولدرهای عمومی و برنامه های Gropuware ، نیز استفاده نمود.
- (News/Usenet (NNTP Server : این نوع سرویس دهندگان به عنوان یک سرویس دهنده newsgroup بوده و کاربران می توانند اقدام به ارسال و دریافت پیام هائی بر روی آنان نمایند .

به منظور شناسائی سرویسها و پروتکل های مورد نیاز بر روی هر یک از سرویس دهندگان ، می بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنان به چه صورت است ؟ : شبکه داخلی ، شبکه جهانی و یا هر دو مورد . پاسخ به سوال فوق زمینه نصب و پیکربندی سرویسها و پروتکل های ضروری و حذف و غیر فعال نمودن سرویسها و پروتکل های غیرضروری در ارتباط با هر یک از سرویس دهندگان موجود در یک شبکه کامپیوتری را فراهم می نماید .

## (2-2) حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصا " اینترنت ، امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد .

توجه به مکانیزم های جلوگیری از حملات امنیتی و سیاست های امنیتی محقق اهداف امنیت اطلاعات هستند . حملات امنیتی می تواند شامل ؛ قطع (Interruption) ، دسترسی غیرمجاز (Interception) ، دستکاری داده ها (Modification) و ساخت پیغام (Fabrication) باشد .

برای پیشگیری ، شناسایی ، برخورد سریع و توقف حملات ، می بایست 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 پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است . شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویارویی با آنان افزایش خواهد داد . بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم . جدول زیر برخی از حملات متداول را نشان می دهد :

### انواع حملات

(Distributed Denial of Service (DDoS) & (DoS) Denial of Service

Spoofing

Back Door

Replay

Middle Man in the

Brute Force

Hijacking TCP/IP

Password Guessing

Dictionary

|                    |                       |
|--------------------|-----------------------|
| Viruses            | Exploitation Software |
| Worms              | Horses Trojan         |
| Engineering Social | Auditing              |
| DNS Poisoning      | Sniffing              |

## 2-2-1 حملات DoS

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoS قرار گرفته است. این نوع از حملات صرفاً "متوجه وب سایت ها 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 می توان از میزان پیشرفت این نوع از حملات آگاهی یافت.

### حملات از نوع (DoS: denial-of-service)

در یک تهاجم از نوع DoS، یک مهاجم باعث همانعت دستیابی کاربران تائید شده به اطلاعات و یا سرویس های خاصی می نماید. یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه ای آن و یا کامپیوترها و شبکه ای از سایت هائی که شما قصد استفاده از آنان را دارید، باعث سلب دستیابی شما به سایت های Email، وب سایتها، account های online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد.

متداولترین و مشهودترین نوع حملات DoS، زمانی محقق می گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. زمانی که شما آدرس URL یک وب سایت خاص را از طریق مرورگر خود تایپ می نمائید، درخواست شما برای سرویس دهنده ارسال می گردد. سرویس دهنده در هر لحظه قادر به پاسخگویی به حجم محدودی از درخواست ها می باشد، بنابراین اگر یک مهاجم با ارسال درخواست های متعدد و سیلابگونه باعث افزایش حجم عملیات سرویس دهند گردد، قطعاً امکان پردازش درخواست شما برای سرویس دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می باشند، چراکه امکان دستیابی شما به سایت مورد نظر سلب شده است.

یک مهاجم می تواند با ارسال پیام های الکترونیکی ناخواسته که از آنان با نام Spam یاد می شود، حملات مشابهی را متوجه سرویس دهنده پست الکترونیکی نماید. هر account پست الکترونیکی (صرفنظر از منبعی که آن را در اختیار شما قرار می دهد،

نظیر سازمان مربوطه و یا سرویس های رایگانی نظیر یاهو و hotmail ( دارای ظرفیت محدودی می باشند. پس از تکمیل ظرفیت فوق ، عملاً امکان ارسال Email دیگری به account فوق وجود نخواهد داشت . مهاجمان با ارسال نامه های الکترونیکی ناخواسته سعی می نمایند که ظرفیت account مورد نظر را تکمیل و عملاً 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 بر علیه کامپیوتر دیگری استفاده نماید . مهاجمان با استفاده از نقاط آسیب پذیر و یا ضعف امنیتی موجود بر روی سیستم شما می توانند کنترل کامپیوتر شما را بدست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند. ارسال حجم بسیار بالایی داده از طریق کامپیوتر شما برای یک وب سایت و یا ارسال نامه های الکترونیکی ناخواسته برای آدرس های Email خاصی ، نمونه هایی از همکاری کامپیوتر شما در بروز یک تهاجم DDOS می باشد . حملات فوق ، "توزیع شده " می باشند ، چراکه مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می نماید .

### نحوه پیشگیری از حملات

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

- نصب و نگهداری نرم افزار آنتی ویروس
- نصب و پیکربندی یک فایروال
- تبعیت از مجموعه سیاست های خاصی در خصوص توزیع و ارائه آدرس Email خود به دیگران

### 2-2-2 حملات از نوع Back Door

Back door ، برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی ، فراهم می نماید . برنامه نویسان معمولاً چنین پتانسیل هایی را در برنامه ها پیش بینی تا امکان اشکال زدائی و ویرایش کدهای نوشته شده در زمان تست بکارگیری نرم افزار ، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق ، مستند نمی گردند ، پس از اتمام مرحله

تست به همان وضعیت باقی مانده و تهدیدات امنیتی متعددی را به دنبال خواهند داشت. به طور مثال برنامه FireWall Check Point که توسط اسراییل تهیه شده دارای این مشکل می باشد.

### نحوه پیشگیری از حملات

بهترین روش به منظور پیشگیری از حملات Back doors، آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود می باشد. به کاربران می بایست آموزش داده شود که صرفاً از منابع و سایت های مطمئن اقدام به دریافت و نصب نرم افزار بر روی سیستم خود نمایند. نصب و استفاده از برنامه های آنتی ویروس می تواند کمک قابل توجهی در بلاک نمودن عملکرد اینچنین نرم افزارهایی ( نظیر: Back Orifice, NetBus, and Sub7 ) را به دنبال داشته باشد. برنامه های آنتی ویروس می بایست به صورت مستمر بهنگام شده تا امکان شناسایی نرم افزارهای جدید، فراهم گردد.

### 2-2-3) حملات از نوع Spoofing - ره گیری

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

این حمله عمدتاً متکی است بر ضعف پروتکل IP و ضعفهای ساختاری اینترنت برای دسترسی کاربران بر روی لایه Application. در این حمله معمولاً دو تکنیک معرفی می گردد:

- جعل هویت Impersonation

- تغییر قیافه Masquerading

در روش تغییر قیافه فرض می شود که فرد حمله کننده قبلاً User Id و Pass Word فردی را دزدیده و حال با تغییر قیافه خود را به عنوان یک کاربر معتبر جا می زند.

اما در روش جعل هویت معمولاً به طور مثال سناریوی زیر که نسبتاً ساده ولی خطرناک می باشد انجام می گیرد:

در این روش مثلاً وقتی یک کاربر معتبر می‌خواهد به سرور دانشگاه متصل گردد، قبلاً دانشجویها 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 دقیقاً مشابه پیغامی است که سرور دانشگاه برای دریافت User Id. و Pass Word به کلاینت می‌دهد و از او خواسته می‌شود Id. و P/W 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 مجدداً آنها را وارد کرده و وارد سیستم دانشگاه می‌شود.

## 2-2-4) حملات از نوع Man in the Middle

نفوذگر بین دو کامپیوتر Client و Server 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 عمدتاً هدف بدست آوردن کلمه عبور و رمز عبور می‌باشد.

سیستم های Wireless در معرض این حمله قرار دارند.

## 2-2-5) حملات از نوع Replay

وقتی یک هکر به وسیله ابزار Sniffer (بو کشیدن) بسته های اطلاعاتی را از روی سیم بر می‌دارد، یک حمله Replay رخ داده است. 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 بدانها به صورت دروغین پاسخ داده می‌شود.

یا به عبارت دیگر وقتی بین یک سرویس‌دهنده و سرویس‌گیرنده مجاز بر اساس سطوح دسترسی موردنظر یک تماش (Session) اتفاق می‌افتد، این جلسه ذخیره گردیده و مجدداً توسط کاربر غیر مجاز این جلسه تکرار می‌گردد. لذا اگر به‌گونه‌ای ترتیب و توالی این جلسات (sessions) مجدداً مورد بررسی قرار نگیرد می‌تواند یک حمله انجام پذیرد.

## 2-2-6 حملات از نوع TCP/IP Hijacking

معمولا به آن جعل نشست (Session Hijacking) نیز گفته می شود. هکر می تواند نشست TCP بین دو ماشین را به دست آورد. یک روش مشهور استفاده از Source-rout کردن IP ها می باشد. Source-rout کردن یعنی بسته های IP را طوری تغییر دهیم که از مسیری خاص بگذرند.

## 2-2-7 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 می باشد که نفوذگر رکوردهای DNS را که به Host های صحیحی اشاره دارند، به Host مورد نظر خود تغییر می دهد.

## 2-2-8 حملات از نوع Social Engineering (مهندسی اجتماعی)

بیشتری زمانی رخ می دهد که هکر به سیستم های واقعی قصد نفوذ دارد. راه دیگر هنگامی می باشد که نفوذگر با استفاده از نقاط ضعف کاربر انتهایی (End User) راه نفوذ به شبکه را پیدا می کند. سوءاستفاده از نقاط ضعف افراد با به دست آوردن عادت های 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.

## 2-2-9 حملات از نوع Brute Force

یک روش برای به شکستن کلمات رمز و به دست آوردن آنهاست. حمله Brute-force حروف را به صورت ترکیبی استفاده می کند و با تست کردن آنها رمز عبور را پیدا می کند.

برای مقابله با این روش باید کلمات رمز با طول زیاد انتخاب کرد و یا کلمات رمز را هر دفعه تغییر داد.

## 2-2-10 حملات از نوع Dictionary

یک روش برای به دست آوردن کلمات رمز عبور است. کلمه Dictionary در اصل لغتنامه ای از کلمات معروف می باشد که در یک فایل ذخیره شده اند و به وسیله یک ابزار برای شکستن کلمات رمز، مورد استفاده قرار می گیرند.

برای مقابله با این حمله 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. مثلاً یک شکل گرافیکی با اشکالی که توسط سیستمهای الکترونیکی قابل تشخیص نیستند، شما را مجبور به تایپ میکنند.

## 2-2-11 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.

## 2-2-12 حملات از نوع Sniffing

اطلاعاتی مانند نام عبور (U/Id) و رمز عبور (P/W) 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 غیر مجاز (Unauthorized Access) جلوگیری نماییم. این محافظت اطلاعات 3 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. Objectها ماهیت غیر فعال (Passive) 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.

### 3-1) تکنیک‌های کنترل دسترسی

### (1-1-3) قانون حداقل اجازه (Least Privilege)

یکی از مهمترین تکنیکهای کنترل دسترسی کنترل حداقل اجازه می باشد. 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 (Global Access) داده نشود. به عبارت دیگر به هر Subject اجازه دسترسی به Objectهایی 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 بصورت پیشفرض اجازه دسترسی عمومی به همه سرویسها را داده است، در تضاد میباشد. لذا برای رسیدن به این هدف لازم است که زیر ساختهای امنیتی را بر روی اینترنت به گونه ای شکل دهیم که ضمن استفاده اینترنت در دسترسیهای عمومی قانون "حداقل اجازه" رعایت گردد.

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

### (2-1-3) حسابرسی کاربران (Accountability)

از جمله محوریترین پایه های مبحث کنترل دسترسی میباشد. در واقع این امکان با اضافه کردن لایه هایی به سازمان IT مان بوجود می آید، این لایه باعث میگردد که اطلاعات هر گونه دسترسی یک Subject و اقدام بر روی یک Object بر روی سیستم ذخیره (log) گردد. در نتیجه مدیر سیستم میتواند با مراجعه به این فایل ثبت وقایع (Log File) بررسی نماید که آیا Subjectها در مجموعه شرایط و قوانین امنیتی مورد نظر 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 میگردد.

فرآیند حسابرسی در اصل با یک عمل شناسایی (Identification) هویت Subject آغاز میگردد. در این مرحله کاربر با ارائه کلمه عبور و رمز عبور و یا بهره گیری از کارتهای هوشمند (Smart Card) که در آن اطلاعات مربوط به هویت صاحب آن میباشد، خودش را به سیستم معرفی میکند.

### 3-1-3) کنترل Object ها

در واقع جهت کنترل در محیط‌های فن‌آوری اطلاعات 3 لایه داریم:

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

و بطور کلی هدف جلوگیری و امن سازی یک Object توسط تهدیدات می‌باشد.

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

اما در بحث کنترل دسترسی اجرایی، تکیه بر سیاستها (Policy) می‌باشد که برای امنیت سازمان تعریف گردیده و مدیر سیستم (Admin) بر اساس این قوانین سطوح دسترسی هر فرد از سازمان را به اطلاعات، معین می‌نماید. و یا اینکه در استخدام افراد برای اینگونه محیط‌ها بایستی ملاحظات امنیتی مورد توجه قرار گیرد. همچنین توجه به آموزش‌های 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 را از دسترسی‌های بدون مجوز محفوظ نگه داریم.

در بخش کنترل دسترسی منطقی 3 روش مهندسی مورد استفاده قرار می‌گیرد:

- 1- محدود سازی دسترسی به Object ها (Object Access Restriction)
- 2- رمزنگاری (Encryption)
- 3- معماری دسترسی شبکه‌ای تفکیک شده (Network Architecture/Segregation)

در بخش اول (محدود سازی دسترسی به Object ها) هدف ایجاد محدودیت برای دسترسی به يك Object توسط Subject هاي مختلف می‌باشد. یعنی تنها Subject هایی که در يك فرآیند شناسایی (Authentication) احراز هویت گردیده‌اند و بر اساس رویه‌های امنیتی سیستم اجازه و حد دسترسی‌شان به منابع تایید گردیده، قادر به دسترسی به Object خاصی را داشته باشند.

در بخش دوم یعنی رمزنگاری هدف محرمانه کردن اطلاعات با بهره‌گیری از تکنیک‌های رمزنگاری می‌باشد. با بهره‌گیری از این روش حتی اگر فرد غیر مجازی به اطلاعات سازمان ما دسترسی پیدا نماید به دلیل اینکه همه اطلاعات به صورت رمز درآمده اند، این دستیابی برایش 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 می‌باشد. مثلاً در يك محیط نظامی که اطلاعات بسیار محرمانه‌ای بر روی يك کامپیوتر وجود دارد، اگر ضرورتی برای حضور این کامپیوتر در شبکه وجود ندارد، لازم نیست این کامپیوتر حتماً به محیط شبکه متصل گردد. و یا اینکه مثلاً بخش‌های مختلف شبکه‌ای با توجه به اهداف آنها از همدیگر جدا شوند.

## 2-3) انواع کنترل‌ها (Control Types)

حال در این مرحله سوالی مطرح می‌شود که چطور این کنترل‌های دسترسی را بکار گیریم. و یا به عبارت دیگر استراتژی کنترلی ما چگونه می‌تواند باشد.

اصولاً در این مبحث 5 نوع استراتژی کنترلی معرفی می‌گردد:

- 1- پیشگیرانه (Preventative)
- 2- نمایان سازی و کشف (Detective)
- 3- بازدارنده و تنبیه کننده (Deterrent)
- 4- تصحیح کننده (Corrective)
- 5- بازگشت و بازیابی (Recovery)

در تکنیک پیشگیرانه جلوگیری از رخداد يك حمله انجام می‌گیرد. در واقع از ابتدا اجازه نمی‌دهیم که يك Subject به يك Object غیر مجاز دسترسی داشته باشد.

در تکنیک نمایان سازی و کشف، استراتژی را به شکلی تعریف می‌کنیم که پس از وقوع يك حمله موفق، اولاً وقوعش اعلام شود و ثانیاً اینکه توسط چه کسی حمله انجام پذیرفته مشخص شود.

در روش بازدارنده و تنبیه کننده ما برای Subject مهاجم طبقاتی تعریف می‌کنیم. مثلاً در سیاست‌های امنیتی تعریف می‌کنیم که چنانچه يك دسترسی به Object بدون اجازه انجام پذیرد، Subject مهاجم شناسایی می‌گردد و بر اساس تصمیمات سازمان که در بخش مدیریت سیستم تعریف گردیده با او (Subject متخاصم) برخورد می‌گردد.

در روش تصحیح در واقع هدف آن است به محض بروز يك حمله بلافاصله سیستم را به وضعیت مناسب آن برگردانیم. بطور مثال فرض کنید به سرور پست الکترونیک يك سازمان يك حمله به منظور پر کردن حجم آن انجام گرفته است. در این روش (تصحیح سازی) برای برخورد با این حمله، مثلاً تمام میل باکس‌ها را پاک (Delete) می‌کنیم، خواه این Mail Box مربوط به افراد باشد و در آن نامه‌های درست باشد، و یا خواه مربوط به فرد حمله کننده باشد.

### 3-3) بخش‌بندی تکنیک‌های کنترل دسترسی

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

این مرحله \_ یعنی Authorization - توسط تکنیک‌های کنترل دسترسی انجام می‌پذیرد.

بدین معنا تکنیک‌های کنترل دسترسی را می‌توان را می‌توان به دو بخش تقسیم‌بندی نمود:

(1) بصیرتی (Discretionary)

(2) غیر بصیرتی (Non Discretionary)

### 3-3-1 کنترل دسترسی بصیرتی (Discretionary Access Control - DAC)

در این روش ایجاد کننده یا اصطلاحاً 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، ...) را تفویض نماید. پس با توضیحات بالا میتوان به این نتیجه هم رسید که این روش متکی است بر شناسایی (Identify) هر Subject.

بدین دلیل این روش با عنوان: Identity- Based Access Control نیز شناخته میشود.

این نوع از کنترل دسترسی بیشتر ماهیت غیر متمرکز دارد، یعنی هر کسی که Object ای را ایجاد میکند، خودش اقدام به صدور مجوز به Subject های دیگر برای دسترسی به آن Object نماید.

این Subject ها میتوانند یک کاربر باشند یا در شکل عام تر آن نقش و وظیفه (Role) یک کاربر باشند. بطور مثال یک کاربر میتواند یک مدیر باشد که در یک نقش وظیفه مدیر سیستم (Admin) را ایفا نماید 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 شکل 3-1 در بردارنده جزئیاتی در خصوص اینکه چه کاربری میتواند به چه Object ای 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 |

شکل 3-1 لیست کنترل دسترسی (Access Control List)

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

### 3-3-2) کنترل دسترسی الزامی (Mandatory Access Control - MAC)

در این روش سیستم به صورت غیر متمرکز نمی‌باشد. بلکه بر اساس قوانین مشخصی (Rules) 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. و برای این منظور برای هر کاربر یک برچسب (Label) امنیتی تولید می‌شود. در محیط‌های تجاری این برچسب‌ها بر اساس طبقه‌بندی زیر انجام می‌گیرد:

- عمومی (Public)
- حساس در سطح دیپارتمان (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 (Fire Wall) می‌باشد. همانطور که می‌دانیم این سیستم‌ها یک سری قوانین مشخصی دارند. مثلاً آنهایی که در لایه IP قرار می‌گیرند، بر اساس اطلاعاتی مانند IP گیرنده، IP فرستنده، و ... که به صورت قانون از قبل در آنها بارگزاری 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.

### 3-3-3) کنترل دسترسی غیر بصیرتی (Non Discretionary Access Control - NDAC)

این روش به دو شیوه زیر انجام می‌پذیرد

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

در شیوه اول به هر مشخصه کاربر (User ID) مجموعه‌ای از اجازه‌های دسترسی را صادر نمی‌کنیم بلکه بر اساس 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. بطور 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 بر اساس 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. مثلاً کسی که مدیر سیستم است برچسب شخصی (Private) می‌گیرد. لذا این فرد اجازه دسترسی به اطلاعات سطح Private و بالطبع آن اجازه دسترسی با سطوح پایینتر امنیتی یعنی Sensitive و Public را نیز دارا می‌باشد. اما در بعضی از مواقع لازم است بر اساس سیاستنامه امنیتی سازمان و قوانین پیش‌بینی شده در آن (Rules)، فقط به بعضی از Objectها 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 محیط‌های پروژه‌ای) مناسب می‌باشد.

### 3-4) 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 غیر مجاز شناخته شود باید تعیین هویت یا اصطلاحاً Identify شود. یعنی اسمش مورد شناسایی قرار گیرد. و سپس این اسم احراز هویت یا اصطلاحاً Authenticate گردد.

در مرحله Identification، سیستمی که در واقع ایجاد کننده یا مالک و یا محفظه قرارگیری یک Object می‌باشد، بر اساس تکنیک‌های موجود از Subject تقاضای دادن اطلاعات منحصر بفردی می‌کند که می‌تواند این شناسه یک نام کاربری (User ID) باشد یا یک کارت

هوشمند (Smart Card) باشد و یا مثلاً یک نشانه (Token) باشد. پس از این مرحله سیستم شروع به مرحله احراز هویت می‌کند.

### 3-4-1) تکنیک‌های احراز هویت (Authentication)

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

#### - نوع اول: What You Know

که یک اطلاع خاص منحصر بفردی است که تنها کاربر می‌داند. که معمولاً یک کلمه عبور (Pass Word) می‌باشد. P/W ها یک رشته ای از کاراکترها می‌باشند که می‌تواند بصورت یک سری رقم یا اصطلاحاً PIN باشد یا اینکه بصورت ترکیبی از اعداد و حروف باشند. معمولاً 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 حیواناتان 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 بفردی که کاربر برای اثبات هویت خودش به همراه می‌برد. مثل کارت هوشمند (Smart Card) و یا یک نشانه (Token).

باید توجه داشت در سیستم‌ها عمدتاً برای بالا بردن سطح امنیتی احراز هویت از روش چند فاکتوری (Multiple Factors) استفاده می‌شود. یعنی از میان نوع‌های 1 یا 2 و یا 3 حداقل از دو نوع بطور همزمان استفاده می‌گردد. بطور 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 نمی‌باشد که استفاده از دو

عنصر در يك نوع از انواع تكنيك‌هاي احراز هويت - مثلا استفاده همزمان از دو P/W- نیز عاملي براي افزايش امنيت احراز هويت مي‌باشد.

مطلب ديگر حائز اهميت، امكان بالا رفتن پيچيدگي كاري در روشهاي Multiple Factors مي‌باشد. مثلا در صورتي كه شما نشانه (Token) خود را كه از نوع دوم مي‌باشد گم كنيد، حتي داشتن اطلاعات كامل احراز هويت نوع اول خود - مثلا P/W - هيچ كمكي به شما نمي‌تواند بکند.

- نوع سوم: What You Are

به معنای ویژگی‌های منحصر بفرد افراد می‌باشد (ویژگی‌های بیومتریک افراد). در این نوع تکنیک که بهترین اما گرانترین روش نیز می‌باشد، Subject که معمولاً يك عامل انساني است با توجه به مشخصات منحصر بفرد خودش شناسایی می‌شود. از جمله این مشخصات می‌توان به تصویر عنبیه، شبکیه، اثر انگشت دست، الگوی صدا، الگوی زدن کلید در صفحات کلید، و یا امضاء 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 مستقیماً 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 حتماً از نوع اول و یا نوع دوم روش‌های احراز هويت در کنار نوع سوم احراز هويت - بیومتریک - بهره‌گیری شود.

### 3-4-2) خطاهای نوع سوم احراز هويت \_ بیومتریک

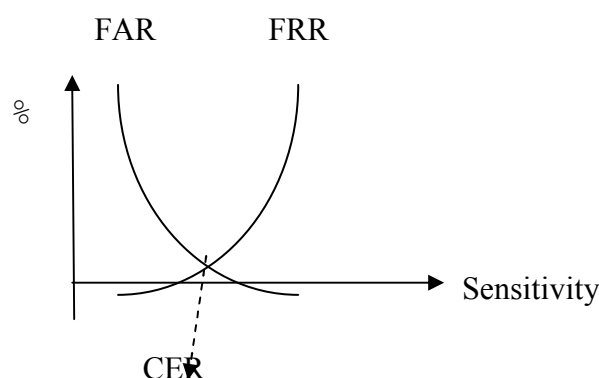
در دستگاه‌های مبتنی بر بیومتریک به دلیل میزان حساسیت دستگاه ما مواجه با دو نوع خطا می‌باشیم:

- False Rejection Rate: یعنی میزان عدم تشخیص درست فرد دارای اعتبار برای سیستم. یعنی مثلاً 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 عمدتاً بدلیل کافی نبودن حساسیت سیستم می‌باشد.

حال اگر به منحنی میزان حساسیت دستگاه بیومتریک با دو میزان FAR و FRR توجه کنیم (شکل 2-3)، این نکته مشهود می‌باشد هرچه 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 2-3) میزان حساسیت حساسیت دستگاه‌های بیومتریک

### 3-5) روش‌های پیاده‌سازی احراز هویت

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

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

در روش اول یعنی روش متمرکز، عملیات احراز هویت بطور متمرکز بر روی یک سرور انجام می‌پذیرد. حسن این روش آنست که چون کلیه احراز هویت برای دسترسی به Objectها در یک نقطه واحد انجام می‌گیرد، مدیریت آن براحتی انجام می‌گیرد. و ضعف این روش در زمانی است که امنیت آن سرور دچار اختلال شود، آنگاه امنیت کل

سیستم مختل می‌شود. ضعف دیگر آن این است که در صورت بالا رفتن بار کاری کارایی این سرور پایین آید، سرعت کل سیستم مختل می‌شود. و مشکل دیگر مساله نقطه خرابی واحد یا باصطلاح 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. مثلاً وقتی از بیرون یک سازمان بخواهند عمل احراز هویت انجام دهند و به سرورهای مختلف آن سازمان دسترسی پیدا کنند، معمولاً از این روش استفاده می‌کنند. در این شکل از کار معمولاً مدیریت دسترسی در نزدیکی Object های مورد کنترل اعمال می‌شوند نه در مرکز اصلی IT سازمان. بطور 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 توزیع شونده دارد، لذا نیاز به یک هارمونی یا هماهنگی بین سرورهایی که بصورت 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 بطور همزمان می‌باشد. برای بعضی از منابع حیاتی سیستم مثل فایل‌های مهم و دیتابیس‌های فیزیکی بهتر است از روش متمرکز استفاده شود. و برای سایر Object ها که از حساسیت کمتری برخوردار هستند می‌توان از روش غیر متمرکز استفاده کرد.

### 3-6) 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. و 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. معمولاً در فایل‌های ثبت وقایع، رخداد‌های مربوط به سه بخش: سیستم، برنامه کاربردی، و کاربر ثبت و ضبط می‌گردد.

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

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

### 3-6-1) سرویس‌های اصلی IDS

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

- فعال (Active)
- غیر فعال (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. مثلاً 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 بعداً مدیر سیستم بر اساس اطلاعات ثبت و ضبط شده تصمیمات لازم را اتخاذ نماید.

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

### (2-6-3) نحوه شناسایی فعالیت‌های غیر مجاز (Intrusion Detection Methods)

شناسایی فعالیت‌های غیر مجاز 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 سناریوهای را در نظر می‌گیریم. مثلاً 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 دیتابیس که حاوی ترتیب رفتاری نامناسب می‌باشد و از قبل تدارک دیده شده است، مطابقت می‌دهد. و در صورت بروز تطابق مشخص می‌شود که حمله‌ای تدارک دیده شده و یا در حال تدارک است، آنوقت IDS به صورت اتوماتیک پیغام هشدار برای یک عکس‌العمل مناسب (فعال، غیر فعال، و یا ترکیبی) می‌فرستد.

اما در شکل دوم یعنی مبتنی بر رفتار، رفتارهای کاربران را در طی دوره‌های زمانی شناسایی و دسته‌بندی می‌کنند. بدین شکل الگوهای رفتاری هر کاربر مجاز به دست آمده و در درون دیتابیس نگه داری می‌شود. و در صورتی که یک کاربر رفتار متفاوت با الگوهای شناسایی شده رفتاریش انجام دهد، معلوم می‌گردد که این فرد که خود را به عنوان یک کاربر مجاز معرفی کرده، همان فرد مجاز نمی‌باشد، بلکه یک نفوذگر می‌باشد.

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، اهراز 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، ولیکن این مورد به نوعی باعث خلط مبحث از منظر بسیار از کارشناسان و مدیران شده است. این دو مقوله نزدیک به هم ولی متفاوت از هم می‌باشند. در واقع رمزنگاری یکی از سنگ‌های زیر بنایی امنیت اطلاعات می‌باشد.

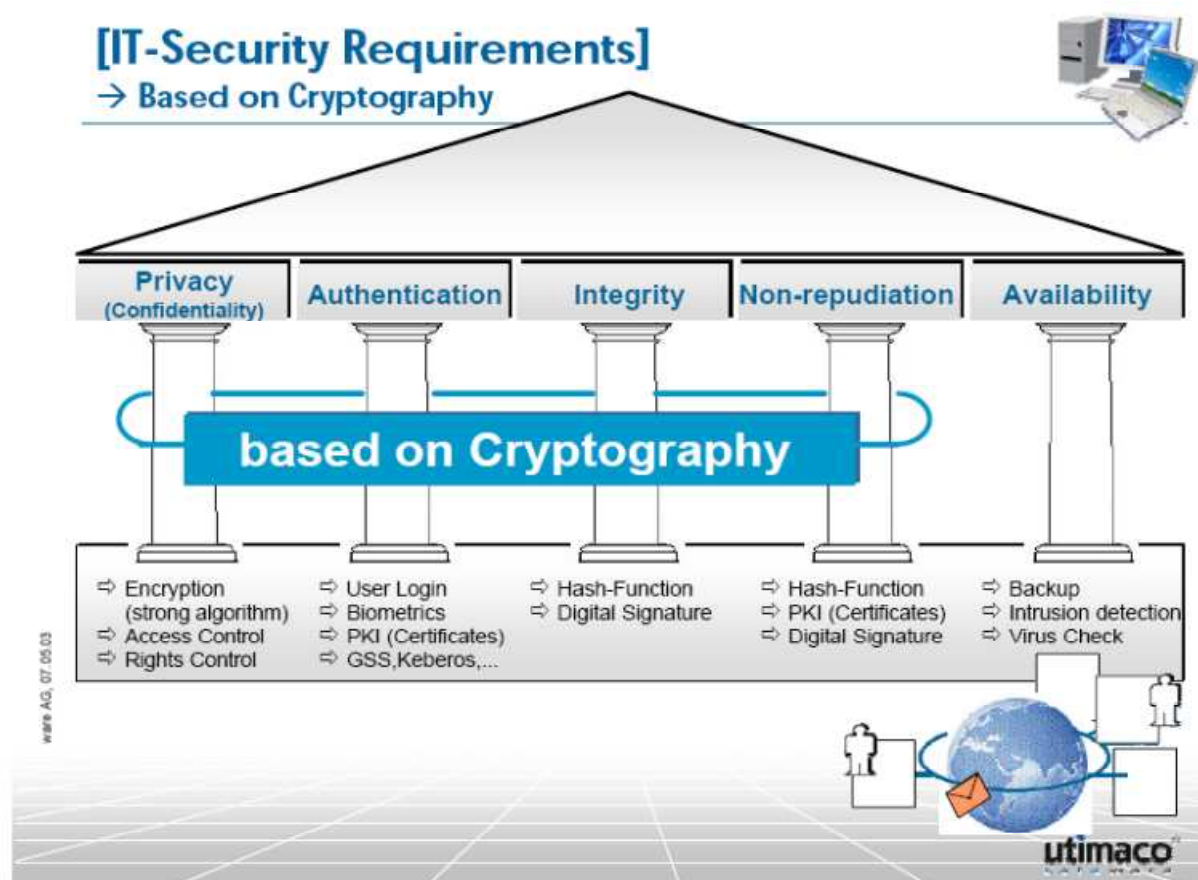
گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است. امنیت اطلاعات یکی از مسائل مشترک شخصیت‌های حقوقی و حقیقی است. کاربران اینترنت در زمان استفاده از شبکه، اطلاعات حساس و مهمی را بدفعات ارسال و یا دریافت می‌دارند. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش‌های امنیتی در رابطه با توزیع اطلاعات در اینترنت است. اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم، موارد متعددی را شامل می‌شود. برخی از اینگونه اطلاعات بشرح زیر می‌باشند:

- 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 ذخیره سازی قابل انتقال نظیر فلاپی دیسکها است. متداولترین روش حفاظت اطلاعات رمز نمودن آنها است. دستیابی به اطلاعات رمز شده برای افراد غیر مجاز امکان پذیر نبوده و صرفاً "افرادیکه دارای کلید رمز می باشند، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند.

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، دولت ها و مخصوصاً "در موارد نظامی بوده است. سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می گردد. امروزه اغلب روشها و مدل های رمزنگاری اطلاعات در رابطه با کامپیوتر به خدمت گرفته می شود. کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت.



شکل 4-1) شرایط لازم برای امنیت فن آوری اطلاعات - بر اساس رمزنگاری

همانطور که در شکل 4-1 مشاهده می‌شود امنیت در محیط‌های فن‌آوری اطلاعات به مثابه یک ساختمان می‌باشد و سرویس‌های پایه‌ای لازم برای ایجاد امنیت در محیط‌های فن‌آوری اطلاعات مانند احراز هویت، صحت اطلاعات، انکار ناپذیری، و محرمانگی می‌توانند بر اساس 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 غیر واضح و غیر قابل آشکارسازی توسط افراد غیر مجاز.

در این فصل در ابتدا نکاتی در مورد تاریخچه رمزنگاری، مفاهیم اولیه رمزنگاری، و حملات محتمل بر سیستم‌های 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.

## 4-1) تاریخچه رمزنگاری

علم رمزنگاری دارای سابقه‌ای طولانی است. شاید بتوان گفت اولین سیستم رمزنگاری سیستمی باشد که توسط ژولیت سزار (پادشاه رم باستان) در جنگ‌های بیش از دو هزار سال قبل مورد استفاده قرار داده شده است. در این روش رمزنگاری الفبای رومی را 3 حرف به سمت راست می‌چرخانند. (مانند شکل 4-2).

و دانش رمزنگاری در طول زمان گسترش یافت بطوریکه در طول جنگ جهانی دوم از آن بصورت گسترده‌ای استفاده گردید.

| متن رمز شده | متن اصلی |
|-------------|----------|
| DEF         | ABC      |
| Khoor       | Hello    |
| Dwwdfn      | Attack   |

شکل 4-2) 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 است استفاده شده است

## 4-2) مفاهیم رمزنگاری

در دانش رمزنگاری از مفاهیم پایه‌ای به کرات استفاده می‌گردد که برخی از آن 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 (متن رمز شده) 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 معمولاً از آن به عنوان کلید یاد می‌شود) بتوان متن رمز شده را به متن واضح برگرداند.

### رمزنگاری (Cryptography)

به فرآیندی 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 آنکه متن رمز شده را به الگوریتم رمزگشایی می‌دهیم و الگوریتم می‌تواند متن واضح را ایجاد کند.

### کلید (Key)

يك تفاوت عمده بين الگوریتم‌هاي رمزنگاري و الگوریتم‌هاي متعارف كدینگ در بهره‌گيري الگوریتم‌هاي رمزنگاري از كلید است. در واقع بخش عمده‌اي از الگوریتم‌هاي متعارف رمزنگاري ارایه و منتشر (Publish) شده‌اند. یعنی همه می‌دانند كه ساختار و نحوه انجام عمل الگوریتم (مثلا الگوریتم‌هاي DES و RSA) به چه ترتیبی می‌باشد، و اینكه این الگوریتم‌ها در طی چه مراحل يك متن واضح را می‌گیرند و به يك متن رمزنگاري تبدیل می‌کنند و همینطور بالعكس. اما با این توصیفات چرا این متن رمز شده توسط افراد غیر مجاز قابل خواندن نمی‌باشد، در حالیکه فرد غیر مجاز هم ممكن است الگوریتم را بداند؟ دلیل این موضوع مفهوم كلید است. در واقع هر الگوریتم به ازاي كلید متفاوت خروجی متفاوتی تولید می‌کند.

نکته بسیار مهم در بحث رمزنگاري مدیریت كلید است، به نحوی كه كه اطلاعات به سادگی افشا نگردد. بالاخص در محیط‌هاي تجارت الکترونیک و دولت الکترونیک نمی‌توان به سمت الگوریتم‌هاي خاصی كه در صنایع نظامی است و توسط افراد خاص استفاده می‌شود رفت. در این چنین محیط‌هایی باید سراغ الگوریتم‌هاي منتشر شده رفت. و لذا آنچیزی كه به صورت محرمانه و مخفی بین طرف‌هاي مجاز جابجا می‌شود كلید است.

### (3-4) انواع حملات به سیستم‌هاي رمزنگاري

حمله عبارت است از هر نوع تلاشی كه توسط مهاجم انجام می‌گیرد كه فضاي جستجو را در بین متن‌هاي واضح برای يك متن رمز شده و یا در بین تمام فضاي جستجو برای كلید، محدود می‌سازد.

بطور مثال در مورد يك كلید  $n$  بیتی تمامی حالات ممكن این كلید می‌تواند فضاي جستجو باشد. یعنی مثلا اگر يك كلید 4 بیتی داشته باشیم، حمله كننده مواجه با يك فضاي جستجوی  $2^4 = 16$  تایی است. لذا هر چه تعداد بیت‌هاي كلید اضافه شود فضاي جستجوی مهاجم به روش نمایی اضافه می‌شود.

اما در واقع این روش جستجو و حمله برای كلید ساده‌ترین شكل می‌باشد و به نام جستجوی فراگیر (Exhaustive Search) نامیده می‌شود. معمولا برای حمله به يك سیستم رمزنگاري از انواع تکنیک‌هاي زیر استفاده می‌شود.

### (1-3-4) فقط متن رمز شده (Cipher Text Only)

در این خانواده از حملات فرد مهاجم فقط يك متن رمز شده دارد و از روی آن می‌خواهد کلید استفاده شده برای رمزنگاری را بدست آورد. در این حالت به‌طور طبیعی برای حمله کننده اطلاع خاصی وجود ندارد و باید سراغ روشهای جستجوی فراگیر (Exhaustive Search) برود.

#### **(2-3-4) متن واضح دانسته شده (Known Plain Text)**

در این روش حمله فرد مهاجم يك متن واضح و يك متن رمز شده متعارف با آن را دارد. پس در این حالت به نوعی می‌تواند تشخیص دهد چه کاراکتری از متن واضح به چه کاراکتری از متن رمز شده مبدل گردیده است. در این روش هدف مهاجم مشخص سازی کلید می‌باشد. این روش نسبت به روش قبلی (فقط متن رمز شده) دارای فضای جستجوی کمتری است.

#### **(3-3-4) 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 مثلاً فرد مهاجم منشی و یا کارمند يك دفتر است و یا دشمن در این دفتر جاسوس دارد، و از طریق این جاسوس می‌تواند با دستگاه رمزنگاری این دفتر کار کند و می‌تواند کلید را تغییر دهد و یا تنظیم کند و یا بخواند و فقط می‌تواند به دستگاه رمزنگاری متن واضح را وارد کند و متن رمز شده را بدست آورد.

در این روش فرد مهاجم این امکان را دارد که دائماً 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. و به این ترتیب فضای جستجو و آنالیز برای بدست آوردن کلید مرتباً برای مهاجم کاهش پیدا می‌کند.

#### **(4-3-4) متن رمز شده انتخاب شده (Chosen Cipher text)**

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

#### (5-3-4) متن انتخاب شده (Chosen text)

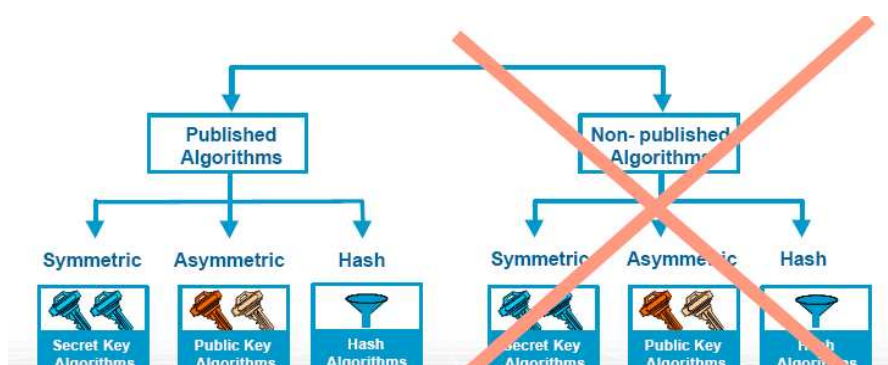
این روش ترکیب دو روش قبلی است. یعنی فرد مهاجم می‌تواند به تعداد نامحدود متن واضح به دستگاه رمزنگار بدهد و متن رمز شده بدست آورد و هم عکس عمل را انجام دهد، یعنی تعدادی متن رمز شده را به دستگاه رمزگشا بدهد و متن واضح آن را بدست آورد. و به این ترتیب فضای جستجو برای بدست آوردن کلید را مرتباً کاهش دهد.

#### (4-4) انواع الگوریتم‌های رمزنگاری

همانطور که در قبل مطرح گردید الگوریتم‌های رمزنگاری به دو دسته کلی تقسیم می‌گردند:

- 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 می‌گردد 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 بطور متوالی بر روی متن ورودی انجام می‌دهد به صورت عمومی منتشر می‌گردد.



شکل (3-4) انواع الگوریتم‌های رمزنگاری

اما در مقابل الگوریتم‌های منتشر نشده وجود دارند که معمولاً در صنایع خابراتی 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 3-4 مشاهده می‌گردد هدف ما در این درس الگوریتم‌های منتشر شده می‌باشد.

#### 4-5) انواع الگوریتم‌های منتشر شده

الگوریتم‌های منتشر شده به 3 دسته کلی تقسیم می‌شوند

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

#### 4-5-1) 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.

#### 4-5-1-1) الگوریتم جایگشتی

یکی از الگوریتم‌های متقارن الگوریتم جایگشتی (Transposition Algorithm) می‌باشد. که در ادامه به توضیح آن می‌پردازیم. برای توضیح این موضوع می‌توان به شکل 4-4 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 4-4) 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 این که کلید خصوصی ما پنج حرفی است، جدولی با 5 ستون تشکیل می‌دهیم و حروف کلید خصوصی‌مان را در سطر اول جدول قرار 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 بدست آوردن متن رمز شده، ابتدا نگاه می‌کنیم به ستون با کمترین شماره. این ستون در این جدول ستون شماره 3 می‌باشد، آنگاه حروف مربوط به آن ستون را پشت سر هم قرار می‌دهیم (IAY). ستون بعدی ستون شماره 4 می‌باشد (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 حروف ستون 5 می‌باشد (EN) و بعد ستون شماره 1 (ILK) و در نهایت ستون 2 (LEE).

در نهایت متن رمز شده روبرو به دست می‌آید: IAYKR ENILK LEE

حال بطور معکوس در طرف گیرنده برای تبدیل متن رمز شده به متن واضح، مجدداً این جدول را داریم. در این جدول 2 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 می‌باشد 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 3، 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. و در ادامه مابقی حروف را نیز در جدول قرار می‌دهد. در نهایت برای بدست آوردن متن واضح به جای آنکه آن را ستونی بخواند به صورت سطری می‌خواند.

#### 4-5-1-2) الگوریتم جانشینی

نوع دیگر الگوریتم‌های متقارن الگوریتم مبتنی بر جانشینی (Substitution) می‌باشد. که در ادامه به توضیح این روش خواهیم پرداخت.

در الگوریتم جانشینی بطور 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 بازای هر کاراکتر چه کاراکتری باید جایگزین شود. مثال ساده آن الگوریتم رمز سزار یا روتیشن 3 بود که در گذشته از آن سخن به میان آوردیم. در این نوع رمزنگاری هم فرستنده و هم گیرنده از یک جدول جانشینی (Substitution Table) 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) می‌باشد. این الگوریتم مبتنی بر اعداد واقعا تصادفی می‌باشد. در این الگوریتم ما یک جدول خواهیم داشت و در این جدول یک تعداد حرف را بصورت 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 OTP‌ها که بصورت کاملا تصادفی ایجاد می‌گردد برای حمله کننده غیر ممکن می‌باشد. پس در این روش کانال ارسال این OTP‌ها بین گیرنده و فرستنده باید کاملا امن باشد و لی متن رمز شده می‌تواند از کانال ناامن نیز ارسال گردد.

یکی دیگر از الگوریتم‌های جانشینی، رمز جانشینی ویگنر Substitution (Cipher-Vigenere) می‌باشد که به شکلی 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 حمله کننده دیگر با حملاتی مثل حملات تکرار و تعداد کاراکترهای رمز شده در متن رمز شده به اطلاعات متن واضح دسترسی پیدا کند.

همانطور که در شکل 4-5 مشهود است جدول ویگنر جدولی است که در اولین سطر آن حروف انگلیسی به ترتیب الفبا و در هر سطر یک حرف الفبایی 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. ارسال کننده 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 بطور 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:

ATTACKATDOWN

متن واضح:

SECRETSECRET

متن کلید:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 4-5) 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" می‌باشد، 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 "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. بهمین ترتیب حرف دوم متن واضح ما حرف "T" و دومین حرف جمله کلید حرف "E" می‌باشد که محل تلاقی ستون وسطی و سطر مربوطه در

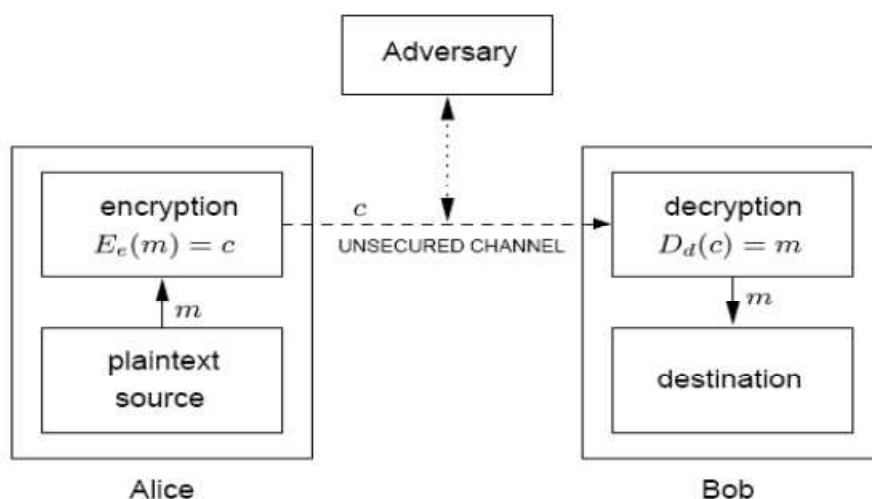
جدول حرف "X" می‌باشد که دومین حرف جمله رمز شده ما می‌شود. و به همین ترتیب مراحل را برای دیگر حروف متن واضح به انجام می‌رسانیم. متن رمز شده نهایی به شکل زیر است:

متن رمز شده : `sxvrgdsxfrag`

همانطور که در روش‌های رمزنگاری که تاکنون بیان گردید مشاهده کردید یکی از محدودیتهایی که باعث می‌شود سطح اعتماد روش رمزنگاری پایین بیاید طول کلید است. به صورت کلی هرچه طول کلید کمتر باشد افراد مهاجم با عملیات ساده‌تری را برای شناسایی کلید رمزنگاری و شکستن رمز مواجه هستند.

این نکته حائز اهمیت می‌باشد که روش‌های رمزنگاری که تاکنون مطرح گردیده است مبتنی بر رمزنگاری رشته‌ای بودند. در واقع در این روش رمزنگاری هر بیت اطلاعات بطور 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.

بطور کلی عمل رمزنگاری را می‌توان مطابق شکل 4-6 توصیف کرد



شکل 4-6 مدل رمزنگاری

همانطور که در شکل بالا مشهود است فرستنده‌ای به نام Alice در صدد ارسال پیام به سمت گیرنده‌ای به نام Bob می‌باشد. فرستنده متن واضحی را از منبع متون واضح خودش مثل  $m$  انتخاب می‌کند.

آنگاه يك تبدیل رمزنگارانه مبتني بر کلید e را بر رويش انجام مي‌دهد. نتیجه متن رمز شده c مي‌باشد که فرستنده مي‌تواند از طريق کانال ناامني براي گيرنده ارسال نمايد. گيرنده نیز با دریافت متن رمز شده c و اعمال الگوریتم رمزگشایی مبتني بر کلید d به متن واضح m دست پیدا مي‌کند. همانطور که در شکل مشهود است دشمنان و رقبا به کانال لرسال متن رمز شده دسترسی دارند ولي بدليل آنکه متن رمز شده مي‌باشد، امکان استفاده از آن برايشان مقدور نمي‌باشد. توجه نماييد که اين نوع از رمز نگاري مبتني بر زوج کلید مي‌باشد.

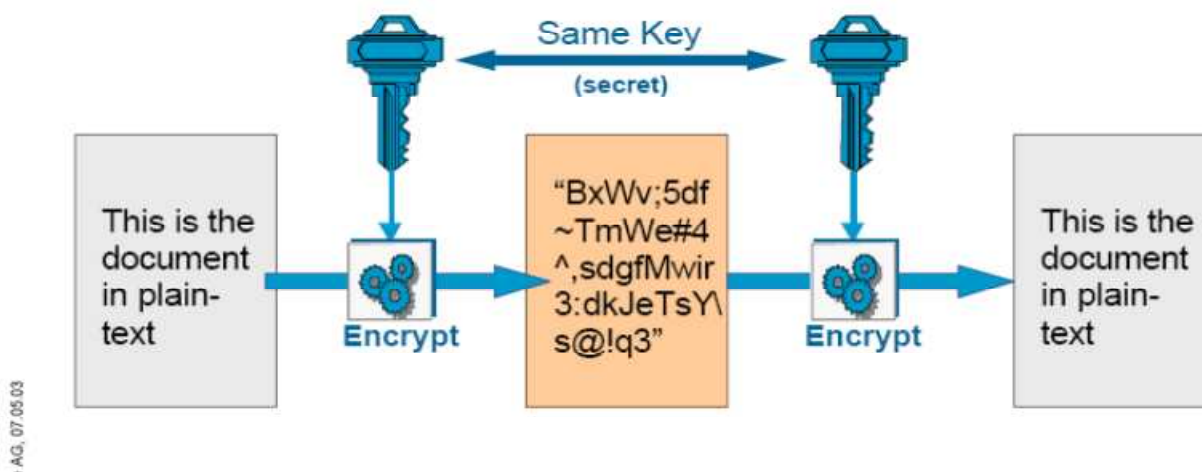
حال در ادامه نحوه عملکرد الگوریتمهاي رمزگذاري متقارن را بيشتر توضيح مي دهيم.

#### 3-1-5-4 توضیحات تکمیلی در مورد الگوریتم‌های رمزگذاری متقارن

اين الگوریتم‌ها، الگوریتم‌هاي کلید مخفي (secret Key Algorithm) نیز ناميده مي شوند. در اين الگوریتم، کلید رمزنگاري و کلید رمزگشایی مشابه هم مي‌باشد، و يا اينکه به سهولت و از طريق محاسبات نسبتا ساده از روي همدیگر قابل محاسبه مي‌باشند. مثلا يك کلید عكس کلید ديگر مي‌باشد.

اين الگوریتم داراي نقاط ضعفي مي‌باشد، از جمله اينکه توزيع کلید بين طرفين مبادله کلید به خودي خود کاري مشکل و پر مخاطره مي باشد. و اين بدان معني است که کلید رمز نگاري و يا رمزگشایی بايد از کانال امني انتقال يابد. مشکل ديگر اين الگوریتم‌ها اين است که سرويس انکارناپذيري را پوشش نمي‌دهند. و همچنين اين نوع از رمز نگاري مقياس پذير نمي‌باشد، يعني آنکه نمي‌توان اين نوع از رمزنگاري را بصورت بلوکی و بازاي طول بلوك‌هاي مختلف انجام داد. البته در مقابل اين نقاط ضعف، اين الگوریتم‌ها در مقايسه با الگوریتم‌هاي نامتقارن، بسيار سريع هستند.

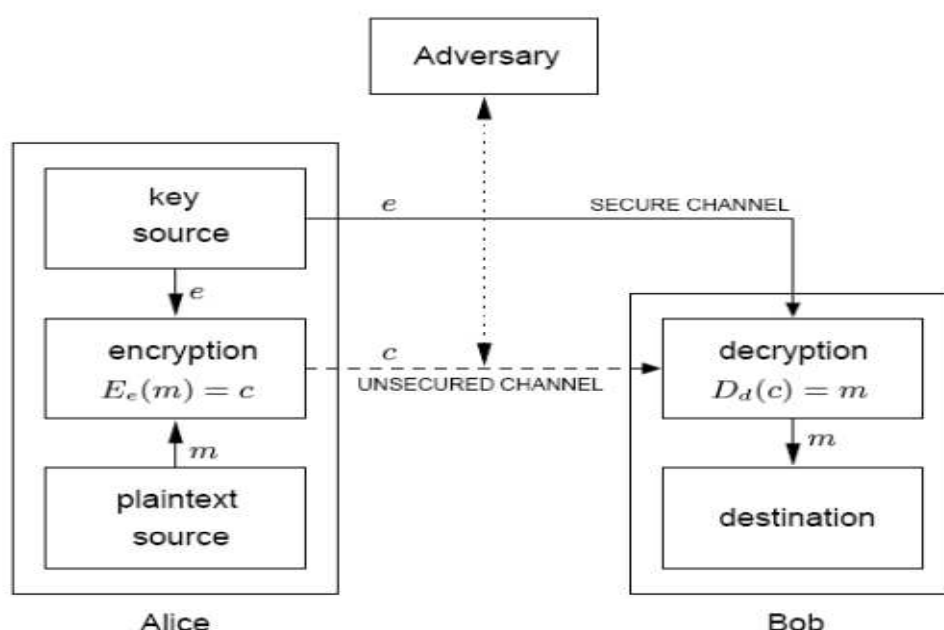
## ■ One (same) key for encryption and decryption



شکل 4-7) شمایی از الگوریتم رمزنگاری متقارن

همانطور که در شکل 4-7 مشاهده می‌شود در الگوریتم رمزنگاری متقارن گیرنده و فرستنده برای اعمال رمزنگاری و رمزگشایی از یک کلید مشابه استفاده می‌کنند.

در شکل 4-8 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 رمزنگاری  $E$ ، رمزنگاری می‌کند. باید توجه داشت در این راستا کلید رمزنگاری بایستی 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 4-8) روش توزیع کلید در الگوریتم متقارن

توجه کنید در این روش رمزنگاری بدلیل امکان لو رفتن کلید رمزنگاری، طرفین رمزنگاری باید به صورت دوره ای 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 می یابد یعنی اگر به جای آنکه فقط دو نفر آلیس و باب تبادل اطلاعات کنند، سه نفر به تبادل اطلاعات بین یکدیگر پردازند، آنوقت برای رمز نگاری نیاز به 3 کلید رمزنگاری می باشد. و به این ترتیب با بالا رفتن نفرات، تعداد کلید افزایش پیدا می کند (تعداد کلید از فرمول  $n(n-1)/2$  تبعیت می کند، که در این فرمول  $n$  تعداد نفرات می باشد). بدین ترتیب حفظ امنیت کلید و مدیریت این کلیدها در یک شبکه به یک کار بسیار پیچیده ای تبدیل می گردد.

از جمله الگوریتم های رمزنگاری می توان به الگوریتم های: DES, Triple DES, AES, IDEA, Blowfish اشاره کرد. بعضی از مشخصات این الگوریتم ها عبارتند از:

DES: دارای کلید با طول 65 بیت، تا سال 1998 استاندارد دولتی آمریکا بود. ولی امروزه به اندازه کافی قدرتمند نمی باشد، که به عنوان استاندارد دولتی محسوب گردد.

**Triple DES:** سه بار عملیات الگوریتم DES را انجام می‌دهد. دارای کلیدی با طول 168 بیت می‌باشد. کاربرد وسیعی دارد. نسبت به DES امن‌تر است. اما کند است.

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

**IDEA:** دارای کلید 128 بیتی می‌باشد. برای استفاده نیاز به مجوز دارد.

**Blowfish:** طول کلید متغیر دارد. الگوریتم آن جهانی و در اختیار عموم است. بسیار سریع می‌باشد.

#### **(2-5-4) 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 Public Key Algorithm و یا باصطلاح الگوریتم‌های نامتقارن، شکل گرفت.

در این روش، در واقع فرستنده اطلاعات یک زوج کلید را تولید می‌کند. یکی از کلیدها مخفی و خصوصی است (Private Key)، 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 در آورده و این متن رمز شده را از طریق کانال ناامنی برای گیرنده ارسال می‌دارد. 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 می‌باشند که اطلاعاتی را رمزگذاری کرده و به سمت گیرنده ارسال دارند، و با اینکه هکر به کلید عمومی و هم به الگوریتم رمزگذاری دسترسی دارند، اما نمی‌توانند کلید خصوصی دریافت کننده پیام را کشف و شناسایی کنند.

این نوع الگوریتم‌ها در انجام سرویس‌های امنیتی کاربرد وسیعی دارند. این الگوریتم‌ها برای انجام سرویس‌های امنیتی محرمانگی، احراز هویت، و انکار ناپذیری، استفاده می‌گردد. این

الگوریتم‌ها در دنیای امنیت به عنوان الگوریتم‌های کلید عمومی نیز نامیده می‌شود.

#### 4-5-2-1) انجام سرویس حرمانگی با بهره‌گیری از الگوریتم‌های نامتقارن

برای تحقق سرویس حرمانگی که هدف حرمانه نگه داشتن اطلاعات انتقالی بین طرفین مبادله پیغام می‌باشد، روش انجام کار بدین شکل می‌باشد:

که فرد دریافت کننده 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). و این گیرنده پیام کلید عمومی خود را برای اطلاع دیگران منتشر کرده است، مثلاً آن را برای اطلاع دیگران بر روی وب سایت خود قرار داده و یا آن را طریق نشریات تبلیغاتی به اطلاع دیگران رسانده است. البته لازم به توجه است که کلید دوم یعنی کلید خصوصی را تنها پیش خود بصورت حرمانه 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 مهاج و دشمن علی‌الرغم 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 می‌باشد که سرویس انکارناپذیری را پشتیبانی می‌کند، مدیریت کلیدها راحت می‌باشد، چرا که تعداد کلیدها به تعداد کاربران می‌باشد. و همچنین توزیع کلید راحت می‌باشد. اما نقطه ضعف آن هم پایین بودن سرعت آن می‌باشد، چرا که میزان محاسبات در الگوریتم‌های نامتقارن بیشتر از الگوریتم‌های متقارن می‌باشد.

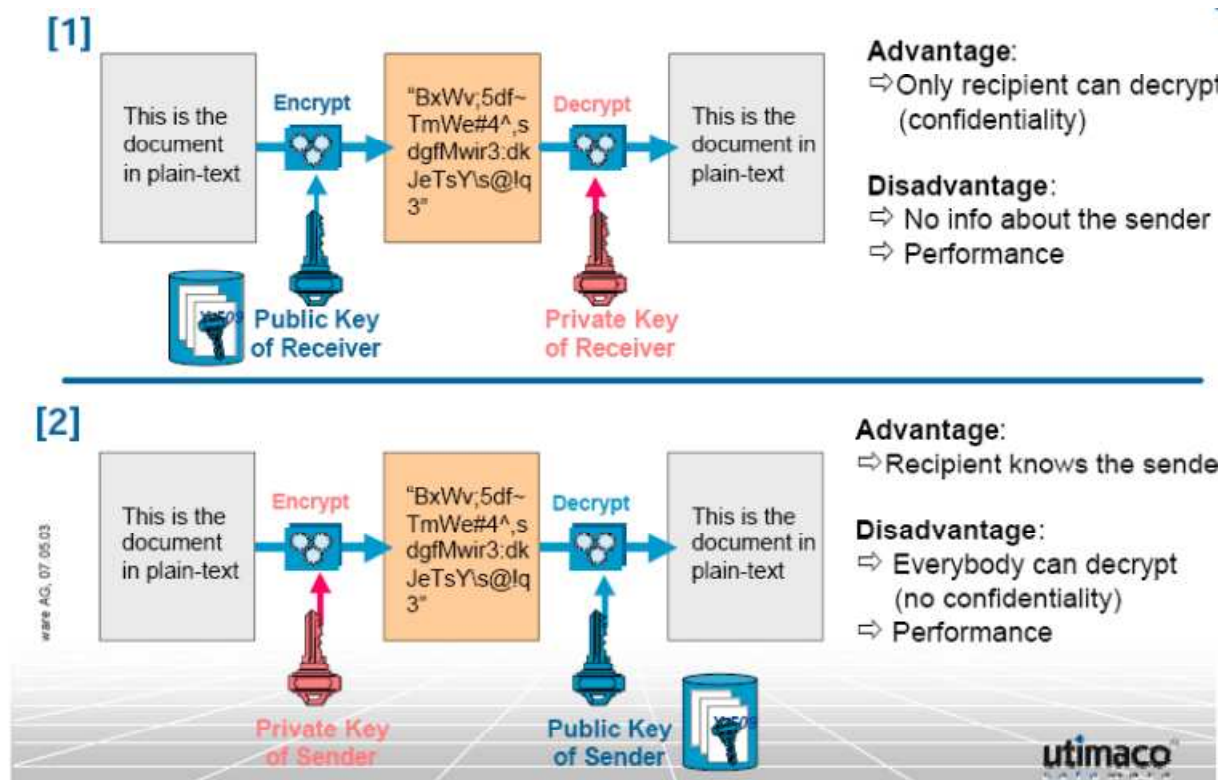
#### 4-5-2-2) انجام سرویس احراز هویت با بهره‌گیری از الگوریتم‌های نامتقارن

اما در ابتدا این پاراگراف اشاره داشتیم به اینکه یکی از سرویس‌های امنیتی دیگر که توسط الگوریتم‌های نامتقارن پشتیبانی می‌شوند، سرویس احراز هویت یا Authentication می‌باشد.

برای انجام این سرویس فرستنده با کلید خصوصی خودش يك متن معني‌دار را به يك 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 در این سرویس هدف محرمانگی این اطلاعات نمی‌باشد، بلکه احراز هویت فرستنده پیام می‌باشد. با این ترتیب گیرنده پیام با بدست آوردن متن واضح و دارای معنا با استفاده از کلید عمومی فرستنده که بر روی متن رمز شده اعمال کرده است، می‌تواند از صحت ارسال کننده آن مطمئن شود.

در امتداد این نکته قابل توجه است که ما می‌توانیم با بهره برداری از الگوریتم کلید عمومی، دو سرویس محرمانگی و احراز هویت را در کنار هم داشته باشیم. یعنی با استفاده از کلید منتشر شده يك گیرنده می‌توانیم برایش متن رمز شده و محرمانه ارسال کنیم، و 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 (Authenticate)، و آنگاه با رمزگشایی مجدد با کلید خصوصی خودش به متن واضح اصلی دست پیدا کند.

در شکل 4-9 شمایی از دو سرویس امنیتی محرمانگی و احراز هویت با استفاده از الگوریتم کلید عمومی، در دو بخش 1 و 2 آورده شده است.

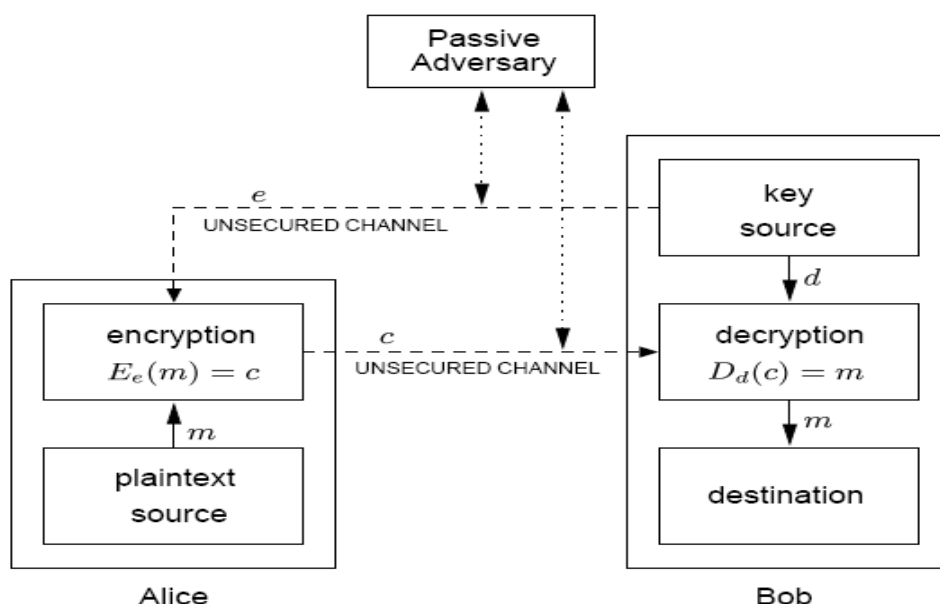


شک 4-9) شمایی از دو سرویس محرمانگی و احراز هویت با استفاده از الگوریتم کلید عمومی

همچنین با توجه به شکل 4-10 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 خودش (یعنی d) را بصورت 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 سیمتیک، ما این آزادی عمل را داریم که از یک کانال ناامن برای توزیع کلید عمومی هم استفاده کنیم. و این بدان معنی است که دشمن اجازه دارد هم کلید عمومی را ببیند هم متن رمز شده ارسالی را.

آلیس به عنوان ارسال کننده، 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 (یعنی c)، با اعمال کلید رمزگشایی شخصی خود (یعنی d) و استفاده از الگوریتم

رمزگشایی ( یعنی D )، از حالت رمز شده خارج کرده و به يك متن واضح تبدیل می‌کند.



شکل 4-10) روش توزیع کلید در الگوریتم نامتقارن

برای درک بهتر تفاوت‌های دو نوع الگوریتم متقارن و نامتقارن جدول 4-1 در زیر آورده شده است.

همانطور که در جدول ملاحظه می‌کنید:

در روش سیمتریک کلید منحصر بفرد 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 مقیاس پذیر نیستند، یعنی آنکه قابلیت اعمال بر روی بلوک‌های مختلف داده‌ای با اندازه‌های مختلف را ندارند. ولی در آسیمتریک این کار امکان‌پذیر است.

سیمتريکها داراي سرعت بالاتر اجرايي نسبت به آسيمتريکها هستند.

سیمتريکها براي اجراء بر روي حجم بالاي داده مناسب ميباشند. در حالیکه آسيمتريکها بيشتر براي اعمال بر روي حجم کوچکتر داده بکار ميروند. و براي توليد امضاي الکترونيکي، گواهي ديжитالي، پاکت ديжитالي استفاده ميشوند.

سيمتريک صرفا براي سرويس محرمانگي بکار ميروند، در حالیکه آسيمتريک علاوه بر سرويس محرمانگي، سرويسهاي احراز هويت، و انکارناپذيري را هم پشتيباني ميکند.

| 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 (4-1) مقايسه الگوريتمهاي رمزنگاري سيمتريک و آسيمتريک

#### (3-5-4) توابع درهمريزي (Hash Algorithms)

الگوريتم درهمريزي با هدف تامين سرويس امنيتي صحت و جامعيت داده بکار گرفته ميشود. درهمريزي يك تابع يك طرفه ميباشد که سايزي ثابت از مقادير مبتي بر اندازههاي مختلف از حجم داده ورودي را توليد ميکند. يك تابع درهمريزي در هر بار اجراء بر روي ديتاي مشخصي، خروجي ثابت دارد، و اين بدان معني ميباشد که با اجراء مختلف بر روي داده مشخصي خروجي متفاوتي نميدهد. بعضي از الگوريتمهاي درهمريزي معروف عبارتند از: MD-4, MD-5, SHA-1.

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

MD-4: خروجی آن یک مقدار 128 بیتی است. خیلی سریع می‌باشد. برای اهداف امنیتی سطح متوسط مناسب می‌باشد.

MD-5: خروجی آن یک مقدار 128 بیتی است. سریع می‌باشد (اما نه به اندازه MD-4). از MD-4 امن‌تر است. در بسیاری از مکان‌ها استفاده می‌شود.

SHA-1: خروجی آن یک مقدار 160 بیتی است. استاندارد دولتی آمریکا می‌باشد. اما از MD-5 کندتر می‌باشد.

#### 4-6) معرفی اجزاء زیرساخت کلید عمومی

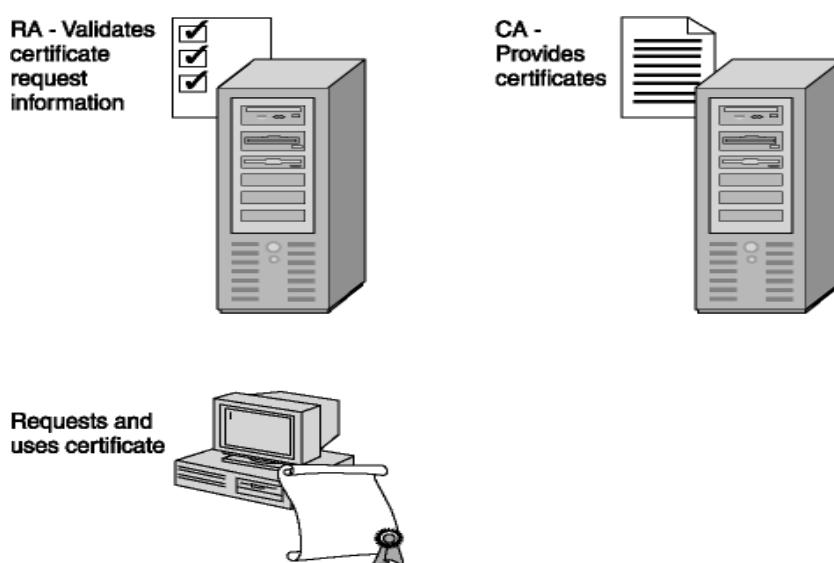
استفاده از زوج کلید در الگوریتم آسیمتริก برای پیاده‌سازی در محیط‌های کوچک و افراد کم، کاری ساده است. اما در محیط‌های بزرگ با کاربردهای وسیع، توزیع کلید عمومی و مدیریت کلید خصوصی کاری بس دشوار می‌گردد. زمانی که یک کلید خصوصی مورد هجوم قرار می‌گیرد، پاک کردن آن و جایگذاری آن سخت می‌باشد.

برای این منظور زیرساخت‌های امنیتی با نام زیرساخت‌های کلید عمومی (Public Key Infrastructure) یا باختصار PKI، بوجود آمده‌اند. PKI از زوج کلید آسیمتริก، 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 X.509 می‌باشد. این استاندارد شامل: تاییدیه، تایید کننده تاییدیه، ابزار مدیریتی تاییدیه‌ها، و برنامه‌های کاربردی که تاییدیه‌ها را بکار می‌گیرند، می‌باشد.

#### 4-6-1) اجزاء PKI

همانطور که در شکل 4-11 مشاهده میکنید اجزاء اصلی این زیرساخت عبارتند از:

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



شکل 4-11) اجزاء اصلی PKI

#### 4-6-2) تاییدیه (Certificate) چه می‌باشد؟

تاییدیه یک معرف دیجیتالی می‌باشد که شما را معرفی کرده و توسط CA صادر می‌گردد. این CA معمولاً به عنوان سوم شخص قابل اعتماد یا Trusted Third Party (TTP) هم شناخته می‌شود. در هر تاییدیه مشخصات سوم شخص معتمد صادر کننده 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 بکار رود. کاربردهای تاییدیه شامل موارد زیر است:

- **امن‌سازی ایمیل.** از پروتکل S/MIME برای اطمینان از صحت و جامعیت، مبداء 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 وی سایت‌های امن.
- **راه‌حلهای امنیت مشتریان.** استفاده از تاییدیه برای اجرای محرمانگی، صحت، احراز هویت، و انکار ناپذیری در برنامه‌های کاربردی مشتریان.

## فصل پنجم: امن سازی زیرساخت های شبکه

### مقدمه

در این فصل به بحث امنیت در زیرساخت های شبکه از سه بعد کانال های ارتباطی و تجهیزات ارتباطی و منابه شبکه ای خواهیم پرداخت. سازمان ها و اشخاص علاقه مند به محافظت از داده ها، تجهیزات، اسرار تجاری، و حفظ حریم شرکای خود می باشند. یک حمله موفق آمیز به شبکه ممکن است عاملی برای به مخاطره درآمدن هریک از ابعاد فوق باشد. برای محافظت از زیرساخت های شبکه خود در مقابل حملات در ابتدا باید نسبت به انواع حملات ممکن فرا روی این زیر ساخت آگاه باشید. بعضی از این تهدیدات عبارتند از:

- تخریب فیزیکی تجهیزات
  - شنود بسته های 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 شبکه ای دیگر
  - استفاده از شبکه شما برای میزبانی سرویس های غیرقانونی، مخریف و ناشناخته
  - پاک کردن و تخریب داده ها
- در راستای نیل به اهداف امنیتی بعضی از راه ها برای برای امن نمودن فیزیکی تجهیزات به قرار زیر است:
- استخدام گارد حفاظتی
  - نصب سنسور، و تلویزیون های مدار بسته برای نظارت بر تجهیزات
  - استفاده از کارتهای امن برای دسترسی فیزیکی
  - نصب سیستم برق اضطراری
  - پوشش کابل های شبکه و یا قرار دادن آنها درون دیوارها
  - قفل نمودن 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.

## (1-5) امنیت در کانال‌های ارتباطی شبکه

بسیاری از شبکه‌های کامپیوتری از انواع مختلف کابل برای ارتباطاتشان استفاده می‌کنند. در این درس شما با بعضی از این کابل‌ها و نحوه حمله به آنان 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 می‌باشد.

### (1-1-5) کابل‌های کواکسیال

کابل‌های کواکسیال دارای انواع مختلف ولی دارای ساختار نسبتاً یکسان می‌باشد. 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 عبور می‌کند.

### (1-1-1-5) حملات علیه کابل‌های کواکسیال

کابل‌های کواکسیال معمولاً از دو جنبه تخریب و یا استراق سمع اطلاعات مورد تهاجم قرار می‌گیرند. این کابل‌ها معمولاً 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 بوسیله 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 می‌باشند. این کابل‌ها در مقابل امواج رادیویی و امواج مغناطیس دچار آشفته‌گی اطلاعاتی می‌شوند. همچنین جداسازی قطعه

تمام‌کننده (Terminator) در قسمت انتهایی خطوط در این کابل‌ها باعث قطعی شبکه می‌شود.

اما از بعد استراق سمع، چون این کابل‌ها معمولاً در توپولوژی باس مورد استفاده قرار می‌گیرند و در این توپولوژی سیگنال‌های اطلاعاتی در کل شبکه به انتقال در می‌آیند، پس هر نود متصل 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 می‌باشد. البته لازم بذکر است برای ایجاد اتصال به شبکه در این کابل‌ها توسط مهاجمین باید قسمتی از کابل قطع شود، و بدلیل نوع توپولوژی شبکه‌هایی که از کابل‌های کواکسیال استفاده می‌کنند (توپولوژی باس)، انگاه کل شبکه در آن زمان از کار می‌افتد.

#### 2-1-1-5) 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، و 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.

#### 2-1-5) زوج سیم مسی

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

#### 1-2-1-5) حملات علیه زوج سیم مسی

این سیم‌ها به دلیل جنس نازکشان براحتی قابل تخریب و بریده شدن می‌باشند. همچنین حرارت گرمایی نیز بر روی آنها تاثیر مخربی دارد. اما بدلیل آنکه اینگونه کابل‌ها عمدتاً در شبکه‌های مبتنی بر توپولوژی ستاره (Star) استفاده می‌شوند، لذا قطع شدن یکی از این سیم‌ها باعث قطعی کل شبکه نمی‌شود.

اما از بعد استراق سمع، این کابل‌ها به 3 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 ورمزگشایی ترافیک موجود بر روی شبکه را می‌دهد. یا باصطلاح دیگر امکان بو کشیدن اطلاعات را می‌دهد.
- بهم تابیدن به داخل کابل زوج سیم مسی.
- استفاده از سیگنال‌های الکترومغناطیسی برای استراق سیگنال‌های عبوری از میان زوج سیم مسی.

### 5-1-2) امن‌سازی زوج سیم مسی

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

### 5-1-3) فیبر نوری

کابل فیبر نوری از یک رشته و تار شیشه‌ای یا پلاستیکی برای انتقال پالس‌های نوری تشکیل شده است.

کابل‌های 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 می‌باشد.

### 5-1-3-1 حملات علیه فیبر نوری

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

### 5-1-3-2 امن‌سازی فیبر نوری

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

## 5-2 امنیت در تجهیزات ارتباطی شبکه

بسیاری از تجهیزات ارتباطی در شبکه دارای بخش‌های سخت افزاری و پیکربندی منطقی می‌باشند که فرد مهاجم می‌تواند از ضعف در هر یک از این دو بخش برای تدارک حمله بهره‌برداری نماید. این تجهیزات به شرح زیر می‌باشند:

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

### 5-2-1 Hubs

همان‌طور که می‌دانید هاب یک وسیله ارتباط و اتصال در شبکه‌های از نوع اترنت می‌باشد. که دارای دو نوع فعال و غیر

فعالی می‌باشد. در نوع فعال آن سیگنال‌های شبکه تکرار و تقویت می‌گردد. و چون هاب محل ارتباط اصلی در شبکه می‌باشد لذا مورد توجه مهاجمین برای تدارک حمله می‌باشد.

#### 4-1-2-1) 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، و یا اگر از نوع فعال آن 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 امکان پذیر می‌باشد. اگر یک پورت بر روی هاب آزاد باشد و یا اگر امکان جداسازی یک دستگاه تایید شده متصل به هاب برای حمله کننده وجود داشته باشد، آنوقت فرد حمله کننده می‌تواند از آن پورت برای دستیابی به اطلاعات و یا تخریب بر روی دیگر تجهیزات متصل در شبکه سود برد.

#### 5-1-2-2) امن سازی هاب

به دلیل خاصیت فیزیکی هاب، امکان حفاظت فیزیکی آن هم وجود دارد. تلاش گردد هاب درون محفظه‌ای امن قرار داده شود. اگر هاب درون اتاق یا محفظه‌ای قفل شده نمی‌باشد، تلاش شود توسط دیگر بسته‌بندی‌ها محافظتی امت گردد. حداقل به صورت دوره‌ای هاب مورد بازدید قرار گیرد تا از امن بودن اتصالات آن و عدم اتصال یک فرد غیر مجاز به آن مطمئن شویم. هاب‌های قابل مدیریت می‌توانند برای آشکارسازی تغییرات فیزیکی در بهم‌بندی‌شان بکار گرفته شوند. هاب‌های قابل مدیریت اطلاعات آماری و اطلاعات اتصالاتشان را برای مدیریت نرم افزار ارسال می‌کنند. لذا شما می‌توانید هاب را برای اعلام خطر به هنگام تغییر در بهم‌بندی مجهز کنید. اما از آنجا که این روش مدیریت موقعیت و بهم‌بندی به شکل نرم افزاری انجام می‌گیرد، فرد مهاجم می‌تواند چیدمان نرم افزاری را تخریب و یا تدارک حمله‌ای دیگر از این ناحیه را ببیند.

#### 5-2-2) Switches and Bridges

سوییچ و بریج در لایه دوم شبکه (در مدل استاندارد OSI) متصل می‌گردد. آنها عمل سوییچینگ 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 باصطلاح بریج نوعاً یک شبکه را به دو بخش تقسیم می‌سازند ولی سوییچ‌ها نوعاً هر بخش از شبکه را به چندین قسمت کوچکتر تقسیم می‌کنند، و هر قسمت برای هر پورت سوییچ می‌باشد. این تجهیزات عمدتاً تنها برای انتقال اطلاعات تک مقصده (Unicast) مورد استفاده قرار می‌گیرند و اطلاعاتی که برای همزمان چند مقصد (Multicast) ارسال میشوند از این تجهیزات گذر می‌کنند.

توجه: ممکن است در کاتالوگ‌های بازاریابی کارکرد این تجهیزات در لایه‌های 3 و 4 شبکه را هم ملاحظه کرده باشید. که در این صورت دیگر نام این تجهیزات "روتر با کارایی بالا" می‌باشد.

#### 5-2-2-1) تخریب سوییچ و پل

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

#### الف) تخلیک دسترسی مدیریت شبکه

اگر فرد مهاجم بتواند امکان دسترسی مدیریتی شبکه را به دست آورد، او می‌تواند ارتباطات شبکه را مسیّردهی مجدد کند. این ارتباطات می‌تواند به سمت ماشینی که تحت کنترل حمله کننده می‌باشد مسیّردهی شود. آنگاه تا زمانی که مهاجم امکان اتصال مدیریتی به

شبکه را دارا باشد می‌تواند شبکه را تخریب نماید. اینکار با دسترسی به شناسه و کلمه عبور مدیر سیستم انجام می‌گیرد. سوییچها بالاخص فانکشنی به نام "معکوس سازی پورت" (Mirroring Port) دارند، که مدیر سیستم را قادر به نگاشت ورودی و خروجی از یک یا چند پورت سوییچ به یک پورت خاص می‌سازند. این به منزله روشی برای عیبزدایی مشکلات ارتباطی در شبکه می‌باشد. حال اگر مهاجمی امکان دسترسی به این فانکشن را داشته باشد، او 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) مسموم سازی حافظه ARP (ARP Cache Poisoning)

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

برای اینکه حمله کننده این مسمومیت را انجام بدهد، 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.

#### 5-2-2-2) امن‌سازی سوییچ‌ها و پل‌ها

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

- امن کردن کلیه اتصالات فیزیکی در شبکه. اطمینان از امکان پذیر 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 توسط افراد خاصی و تغییرات آنها بصورت دوره‌ای و تغییر آن در صورت تعویض

افراد، از جمله دیگر مواردی است که باید مورد توجه قرار گیرد.

- ورود دستی نگاشته‌های ARP در تجهیزات بحرانی، همچون سرورها، سویچ‌ها، و پل‌های مرکزی. اگر کلیه آدرس‌های MAC بصورت دستی در جداول وارد شوند، این عمل از یادگیری آدرس‌های جدید بصورت اتوماتیک توسط سویچ‌ها و پل‌ها جلوگیری می‌کند.

- سویچ‌ها و پل‌ها را توسط آخرین نسخه‌های وصله‌های امنیتی طراحی شده توسط سازندگان آنها مجهز نماییم.

- مستندسازی نحوه بهم‌بندی 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 روی شبکه را مانیتور کرده و یک دیتابیس از اطلاعات نگاشت MAC به IP را در خود نگه دارد. همچنین این ابزار می‌تواند شما را از تغییرات ایجاد شده در این بخش مطلع سازد.

### Routers (3-2-5)

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 مسیره‌ی (Routing table) برای انجام وظیفه مسیره‌ی در شبکه بهره می‌گیرد.

#### 1-3-2-5 (تخریب مسیریاب‌ها)

همانطور که گفتیم روترها هر دوی ARP Cache و جدول مسیره‌ی (Routing table) را برای انتقال و مسیره‌ی مناسب ارتباطات استفاده می‌کند. و این خود نقطه‌ای برای تدارک حمله می‌تواند باشد. روتر مرکزی همچنین می‌تواند مکان مناسبی برای تخریب باشد. خراب کردن روتر مرکزی، قطع کردن برق، و یا قطع کردن اتصالات کابل‌های روتر می‌تواند عاملی برای جلوگیری از گذر اطلاعات در بین دستگاه در شبکه باشد.

از آنجا که روترها از ARP Cache استفاده می‌کند، آنها می‌توانند مستعد حمله مسموم‌سازی ARP Cache باشند. بعلاوه، 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 مهاجم بتواند این جدول را تغییر دهد، ترافیک شبکه می‌تواند به صورت ناصحیح به سمت یک کامپیوتر که تحت کنترل مهاجم می‌باشد مسیردهی شود. همانطور که در گذشته هم دیدید شما می‌توانید با نظارت بر نقاط اتصال فیزیکی در شبکه‌تان از این حمله پیشگیری نمایید.

اگر یک حمله کننده بتواند دسترسی مدیریتی به روتر پیدا کند، او 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 بروزرسانی 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 (RIPv1) استفاده می‌کنند. به هر حال روایه دوم آن (RIPv2)، روتر را برای تنظیم کلمه عبور مجاز می‌سازد. بنابراین در این نسخه فرد مهاجم باید برای قرار دادن اطلاعات نادرست روتینگ حتما کلمه عبور را داشته باشد.

همانطور که در بخش‌های قبل گفته شده دستگاه‌های ارتباطی ممکن است مشکلات بهم‌بندی نرم افزاری و یا نقاط آسیب‌پذیری امنیتی داشته باشند. بطور مثال، ممکن است شخصی دریابد که یک روتر می‌تواند بروز 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.

### 5-2-3-2) امن‌سازی مسیریاب‌ها

یک روتر مرکزی هدف مناسبی برای مهاجمین می‌باشد. 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 پوش 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.
- بکارگیری کلمات عبور ترکیبی برای کنسول‌های مدیریتی. در اختیار داشتن این کلمات عبور تنها توسط افراد خاصی و تغییرات آنها بصورت دوره‌ای و تغییر آن در صورت تعویض افراد، از جمله دیگر مواردی است که باید مورد توجه قرار گیرد.
- بهنگام نگهداری روترها با آخرین نسخه وصله‌های (Patches) امنیتی ارائه شده توسط فروشندگان.
- اطمینان از مستندسازی و نظارت مجدد بر چیدمان و بهم‌بندی شبکه.
- غیرفعال سازی RIPv1 و بکارگیری RIPv2 و یا دیگر پروتکل‌های مسيردهی که امکان تغییرات در روتر را تنها با ارائه کلمات عبور میسر می‌سازند.

## Firewalls (4-2-5)

کلمه دیواره آتش بصورت عمومی برای توضیح تجهیزاتی بکار می‌رود که برای محافظت از یک شبکه داخلی (یا یک میزبان) در مقابل مهاجمین یا کدهای مخرب از شبکه خارجی (یا شبکه‌ای که آن میزبان به آن متصل است) بکار می‌رود. دیواره‌های آتش معمولاً 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 بکار می‌روند. البته گاهی بعضی از دیواره‌های آتش برای جداسازی شبکه داخلی و یا حتی محافظت از یک کامپیوتر تنها نیز بکار می‌رود.

دیواره‌های آتش یک زیر سیستم از نرم افزار و سخت افزار کامپیوتری اند که از ورود و یا خروج داده‌ها به / از شبکه داخلی (LAN) جلوگیری می‌کنند. این دیواره‌ها هستند که بر اساس مقررات امنیتی موجود تصمیم می‌گیرند کدام داده‌ها وارد شبکه شوند یا از شبکه خارج شوند.

تحول و پیشرفت سیستمهای اطلاعات در سالهای اخیر به مرحله ای رسیده است که دیگر اتصال به اینترنت، یک گزینه اختیاری نیست، بلکه نیازی ضروری به نظر می رسد. اتصال به اینترنت، چه از طریق یک شبکه محلی و چه به وسیله خط تلفن، به دنیای بیرون امکان دسترسی به شبکه داخلی را می دهد. این مساله، حفاظت از داده ها را در برابر دسترسیهای غیر مجاز، الزامی کرده است. اولین راه حلی که به نظر می رسد، تجهیز کلیه دستگاه ها به ابزارهای امنیتی از قبیل سیستم مهاجم یاب<sup>2</sup> و ... است که بدون شک راه حل کارآ و مفیدی نیست.

راه حل مورد قبول امروزی، استفاده از دیواره آتش یا Firewall است. امروزه دیواره آتش از اجزای اصلی و ضروری شبکه های 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 می کند.

دیواره آتش در ساده ترین حالت، نرم افزار است که روی یک کامپیوتر شخصی نصب می شود، اما می تواند یک سیستم سخت افزار - نرم افزار ویژه هم باشد.

## 5-2-4-1) وظایف کلی دیواره آتش:

1. **فیلترینگ** : اصلی ترین وظیفه دیواره آتش، محافظت از شبکه داخلی در برابر نفوذهای بیرونی است. این کار بر اساس مجموعه قواعدی معروف به rule set که توسط مدیر دیواره آتش تنظیم می شود، انجام می گیرد. در ساده ترین حالت، بر اساس مقادیر فیلدهای مختلف header یک بسته، فیلترینگ انجام می شود. به این نوع دیواره آتش، packet filter گفته می شود. در اغلب دیواره آتشیهای فعلی، فیلترینگ در لایه 2 (بر اساس آدرس های فیزیکی یا MAC) هم قابل انجام است. نوع پیشرفته تر فیلترینگ، علاوه بر header هر بسته، به ارتباط بسته ها با یکدیگر هم توجه و بر اساس آن تصمیم گیری می کند. به این نوع فیلترینگ، stateful

<sup>2</sup> Intrusion Detection System

inspection گفته می شود، که در آن state هر connection نگهداری و برای انجام فیلترینگ استفاده می شود. در برخی دیگر از آنها، امکان فیلتر کردن محتوای بسته ها (content filtering) هم وجود دارد.

2. **Network Address Translation** : دیواره آتش معمولاً در نقش دروازه (Gateway) برای شبکه داخلی عمل می کند. لذا کل ترافیک ورودی و خروجی از آن می گذرد. به دلایل مختلف امنیتی و اقتصادی، معمولاً ماشین های شبکه داخلی را از دید بیرون پنهان می کنند. این کار در اغلب موارد (نه همه 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 می گیرد. این عمل ترجمه، معمولاً درون دیواره آتش که همان دروازه شبکه به بیرون است، انجام می گیرد.

3. کلیه امکانات یک دیواره آتش می تواند در حالت شفاف ارائه شود. در این حالت، هنگام قرار دادن دیواره آتش در شبکه، اولاً هیچ گونه نیازی به تغییر نرم افزاری توپولوژی شبکه نیست، ثانیاً هیچ کدام از برنامه های کاربردی نیازی به پیکربندی خاص (معرفی دیواره آتش به عنوان default gateway ، proxy و ...) ندارند.

#### (2-4-2-5) فواید و ضعفهای دیواره آتش

برخی از فواید استفاده از دیواره آتش عبارت است از:

1. توانایی کنترل ترافیک در هر دو جهت ورودی و خروجی.
2. قابلیت اعمال کنترل متمرکز و یکپارچه به جای کنترل توزیع شده.
3. قابلیت محدود کردن دسترسی به سرویسهای غیر امن.
4. توانایی انجام فیلترینگ در لایه های مختلف (Data Link تا Application) .
5. هزینه کمتر جهت امن کردن شبکه، در مقایسه با امن کردن مستقل هر یک از host ها.
6. پیچیدگی کمتر در مقایسه با امن کردن host ها، به خاطر نداشتن سیستم عامل و برنامه های کاربردی پیچیده.

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

1. دیواره آتش کانون نفوذهای امنیتی است، و در صورتی که مهاجم به آن راه پیدا کند، به احتمال قریب به یقین دسترسی نامحدود به کل منابع شبکه پیدا می‌کند.
2. دیواره آتش، خواه نا خواه برای کاربران قانونی هم محدودیت‌های دسترسی ایجاد می‌کند.
3. دیواره آتش حملات Back Door را نمی‌تواند تشخیص دهد.
4. دیواره آتش در برابر بسیاری از نقاط ضعف امنیتی در سطح application راه حلی ندارد.
5. به خاطر اینکه تمام ترافیک از دیواره آتش می‌گذرد، این مساله می‌تواند به یک معضل برای throughput سیستم تبدیل شود.
6. نفوذهایی که از درون شبکه داخلی و به قصد ماشینی در همان شبکه انجام می‌شود، از دید دیواره آتش پنهان می‌ماند، چرا که اصولاً بسته‌های مربوطه از دیواره آتش عبور نمی‌کنند. یکی از دلایل لزوم استفاده از سیستم‌های مهاجم‌یاب<sup>3</sup> نیز همین است.

### 5-2-4-3) تخریب دیواره‌های آتش

پیاده‌سازی و نصب ضعیف دیواره‌های آتش یک دلیل اساسی برای تخریب دیواره‌های آتش می‌باشد. 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 جزء 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 جزء آنهایی که اجازه داده شده اجازه ورود نمی‌دهد. معمولاً مدیران امنیتی شبکه روش اول را بعنوان یک روش سهل‌انگارانه می‌دانند و معمولاً این روش را قابل اعتماد نمی‌دانند.

<sup>3</sup> Intrusion Detection System

نقص و عیب در بخش نرم افزار ديواره آتش ديگر دليل براي رخداد تخريب در آنها مي‌باشد. معمولاً فروشندگان ديواره‌هاي آتش پس از پي بردن به اين نقائص براي رفع آنها، بالاخص براي خريداران قبلي، وصله‌هايي را براي نصب بر روي آنها و رفع عيب طراحي مي‌کنند.

دليل ديگر براي تخريب ديواره‌هاي آتش دسترسي مهاجم به رمز عبور كنسول مديريت ديواره آتش مي‌باشد. معمولاً اين كنسول‌ها در يكي از دو شكل ارتباط نزديك و از طريق كابل و يا ارتباط از راه دور بوسيله ارتباطات بيسيم بوسيله مديران شبکه قابليت دسترسي به سيستم فايروال را ايجاد مي‌کنند.

راه ديگر براي تخريب ديواره‌هاي آتش، راه دسترسي مستقل ديگر براي شبکه مي‌باشد. به طور مثال امكان تماس از طريق شماره‌گيري (DialUp Connection) براي سرور به خارج از شبکه كه اين امكان تحت نظارت فايروال نباشد، مي‌تواند به عنوان نقطه‌اي براي حمله به فايروال توسط مهاجمين باشد.

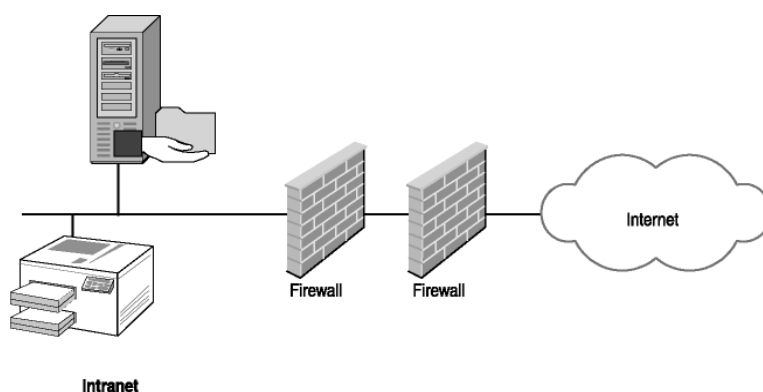
و در انتها امكان دسترسي فزيكي به فايروال توسط مهاجمين مي‌تواند شرايط را براي خراب كردن و يا قطع كردن ارتباطات سيستم فايروال را براي مهاجمين به ارمغان آورد.

#### 5-4-2-4 امن‌سازي ديواره‌هاي آتش

همانطور كه توضيح داده شد روش‌هاي متفاوتي براي تخريب ديواره‌هاي آتش بوسيله مهاجمين وجود دارد كه براي جلوگيري از اين روش‌ها بايد از راه‌هاي زير بهره برد:

- زير نظر داشتن و پي‌گيري از فروشندگان فايروال براي دريافت وصله‌هاي رفع خطاي بروز از آنها.
- بروzsازي فايل‌هاي شناسايي ويروس‌ها
- حفاظت فزيكي از فايروال‌ها.
- مستندسازي نحوه بهم‌بندي سيستم‌هاي فايروال و بررسي مجدد آن بصورت دوره‌اي.
- محدودسازي روش‌هاي مديريت فايروال‌ها تا حد ممكن. بطور مثال اگر نياز زيادي به دسترسي مديريتي به فايروال از راه دور نمي‌باشد، اين امكان را غير فعال سازيم، و در غير اينصورت در صورت لزوم به اين امكان ارتباطي- 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 بصورت دوره‌ای توسط مدیران شبکه.
- اطمینان از عدم وجود راه‌های دسترسی به شبکه که تحت مدیریت فایروال نباشد.
- استفاده از چند فایروال بصورت پشت سرهم، بالاخص استفاده پشت سرهم فایروال‌های شرکت‌های سازنده مختلف، کمک زیادی به امن سازی شبکه ما می‌کند. (همانطور که در شکل 1-5 مشاهده می‌شود)



شکل 1-5 استفاده از فایروال چندگانه

## Modems (5-2-5)

مودم‌ها امکان اتصال کامپیوترها به اینترنت و یا شبکه داخلی را فراهم می‌سازند. اما آنها ممکن است توسط مهاجمین تخریب گردند. مودم‌ها می‌توانند امکان دسترسی به یک سیستم در شبکه و همچنین بصورت 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 بروز بودن همه نرم افزارهای موجود بر روی کامپیوترهای شبکه که نیاز به مودم دارند. مثلا بروزرسانی

- آنتی‌ویروسها و یا یروzsازي وصله‌هاي رفع عيب همه نرم افزارهاي موجود بر روي اين کامپیوترها.
- پیگیری از فروشندگان مودم‌ها برای دریافت وصله‌هاي برطرف کننده نقائص مودم‌ها و بروzsازي آنها.
  - نظارت دوره‌اي بر کامپیوترهاي داراي مودم برای آنکه مورد تخريب قرار نگرفته باشند.

## Wireless (6-2-5)

بسیاري از تولیدکنندگان نقاط دسترسی بیسیم (APs) را که بوسیله کارت‌هاي شبکه‌اي بیسیم قابل دسترسی است، بر روي تجهیزات خود تدارك دیده‌اند. ارتباطات مابین نقاط دسترسی و کارت‌هاي شبکه از طریق سیگنال‌هاي رادیویی و سیگنال‌هاي مادون قرمز در فضا انجام می‌گیرد. مهاجمین که ممکن است از این تجهیزات حتي مایل‌ها دور باشند، می‌توانند بصورت بالقوه این سیگنال‌ها را استراق سمع کنند. لذا برای فرد مهاجم نیازی به اتصال فیزیکی و یا برش بر روي سیم‌ها جهت اتصال به شبکه وجود ندارد. این نقاط دسترسی همچنین می‌توانند مانند هاب‌ها، سویچ‌ها، و یا روترها عمل نمایند. بنابراین تمام حملاتی که در گذشته بر روي این تجهیزات مطرح گردیده بر روي نقاط دسترسی هم متصور می‌باشد.

امروزه در بسیاری از سازمان‌ها در کنار شبکه داخلی‌شان، امکان اتصال به شبکه اینترنت در اطراف فضای اداری‌شان برای اتصال عموم مردم به شبکه اینترنت هم پیش‌بینی می‌شود، که این خود نقطه بسیار خطرناکی برای نفوذ مهاجمین به شبکه داخلی‌شان می‌باشد. لذا استفاده از روش‌هاي احراز هویت و همچنین رمزگذاری اطلاعات مهم، راه مناسبی برای جلوگیری بسیاری از تخریب‌ها در این شبکه‌ها می‌باشد. اما باید توجه داشت در کنار استفاده از این روش‌هاي پیش‌رفته احراز هویت و رمزگذاری، امکانات، روش‌ها و ابزارهاي پیشرفته‌اي نیز برای کمک به مهاجمین بصورت روزانه وارد بازار می‌گردد. لذا بروز نگه‌داشتن تجهیزات امنیتی و استفاده از آخرین وصله‌هاي بر طرف کننده عیوب این تجهیزات که توسط تولید کنندگان آنها 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 بخش‌های 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 یا تجهیزات صنعتی نمی‌باشد.

### 5-3) امنیت در منابع شبکه‌ای

در این بخش اطلاعاتی در خصوص محافظت تجهیزات زیر بنایی شبکه شما با توجه ویژه بر منابع شبکه‌ای و مانیتورینگ آنها ارائه خواهد گردید.

#### 5-3-1) امن‌سازی و مانیتورینگ ایستگاه‌های کاری (work Stations 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 آنها و همچنین از دست رفتن اطلاعات ذی‌قیمت می‌شوند. اگر یک مهاجم بتواند به یک ایستگاه کاری در شبکه شما وارد شود و اخلاقی را ایجاد نماید، احتمالاً می‌تواند به دیگر تجهیزات در شبکه نیز دست‌اندازی کند. در زیر بعضی از روش‌ها برای محافظت این ایستگاه‌ها ذکر می‌گردد:

- نصب آنتی ویروس‌ها و بروز نگه داشتن آنها
- مانیتورینگ فایل‌های ثبت وقایع (Log File) برای ایرادات بوجود آمده
- نصب سیستم ثبت اطلاعات و حسابرسی برای سیستم‌ها و منابع داده‌ای حساس در شبکه

- محدود سازی 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 سرویس‌ها غیر ضروری بر روی آنها
  - نصب سیستم‌های اتوماتیک یا مرکزی تهیه نسخه پشتیبان
  - اطمینان از نصب بروزترین تعمیرکنندگان امنیتی (وصله) بر روی سیستم‌های عامل، و برنامه‌های کاربردی
- همچنین سیستم‌های مانیتورینگ و سیستم‌های کشف نفوذ که بعداً توضیح داده خواهد شد، می‌تواند به حفظ امنیت ایستگاه‌های کاری در شبکه شما کمک کند.
- از حمله مواردی که در مانیتورینگ ایستگاه‌های کاری می‌تواند مورد توجه قرار گیرند عبارتند از:
- سیستم ثبت وقایع: نظارت بر پیغام‌های خطا در باره 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، بدلیل پر شدن فضای هارد دیسکشان باز بمانند. پس مانیتورینگ میزان فضای خالی هارد دیسک ضروری است.

### 5-3-2) محافظت تجهیزات سیار (Mobile Device)

لپ‌تاپ، نوت‌بوک، دستیار دیجیتالی شخصی (PDA) و دیگر تجهیزات سیار امروزه به شکل فزاینده‌ای در بسیاری از شبکه‌های کامپیوتری بکار 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 در خصوص این تجهیزات عبارتند از:

- تجهیزات ضد سرقت: کاربرد تجهیزات هشداردهی و آلام‌های تغییر جا برای این تجهیزات، کابل‌های قفل‌شده
- 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 بکارگیری این روش سارقان را در سرقت آنها بی‌میل‌تر می‌سازد.
- رمزگذاری داده‌ها: اگر تجهیزات موبایل شما برای نگهداری و یا انتقال داده‌های سری و مهم بکار گرفته می‌شود، حتماً این گونه داده‌ها توسط الگوریتم‌های پیشرفته رمزنگاری بصورت رمز شده در آورده شود، تا در صورت دستیابی توسط مهاجمین به این تجهیزات، اطلاعات درون آنها قابلیت استفاده برای مهاجم را نداشته باشد.

### 5-3-3 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 بوسیله 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 اتاق‌های قفل‌دار
- جلوگیری از ورود کاربران بوسیله کنسول‌ها به آنها
- کنترل دقیق و مانیتورینگ دسترسی به منابع، از جمله سیستم فایل‌ها، داده‌های به اشتراک گذاشته شده، و چاپگرها
- 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 بصورت دوره‌ای از بهم‌بندی سرورها، داده‌های به اشتراک گذاشته شده، و دیگر داده‌ها که نیاز

به حفاظت از آنها وجود دارد. همچنین باید از حفاظت فیزیکی از این نسخه های پشتیبان مطمئن گردید. قرار دادن رمز عبور بر روی آنها و رمزگذاری آنها و قرار دادن آنها در گاوصندوق های ضد حریق از دیگر موارد مهم امنیتی می باشد.

همچنین باید از مانیتورینگ دسترسی ها و و در دسترس بودن منابع بر روی سرورها مطمئن گردید. بطور مثال شما باید از امکان پذیر بودن سرویس HTTP برای دسترسی به وب سایت ها بر روی سرور خود اطمینان حاصل کنید.

### 5-3-3) مانیتورینگ تجهیزات اتصال

امروزه سیستم های مدیریت شبکه ارائه شده توسط بسیاری از فروشندگان که اطلاعات از تجهیزات اتصال را جمع آوری می کنند، در دسترس می باشند. بطور مثال، اگر یک روتر یا سویچ بعضی از فریم های اطلاعاتی را بدلیل حجم بالای دیتاهای ورودی از دست بدهد، یک هشدار می تواند به سمت کنسول مدیریت شبکه و یا دیگر مکان های بالقوه مثل پیجر مدیر شبکه ارسال گردد. بسیاری از سیستم های مدیریت شبکه از پروتکل (SNMP – Simple Network Management Protocol) برای جمع آوری اطلاعات از سیستم های مختلف، شامل میزبان های انفرادی موجود در شبکه، استفاده می کنند. بعضی از شرکت هایی مانند: Cisco, IBM و Hewlett-Packard سیستم های مدیریت شبکه ای را پیشنهاد می دهند که می توانند تجهیزات شبکه را مانیتور کنند.

## فصل ششم : امن سازی برنامه های کاربردی

### مقدمه

همانطور که در فصول پیشین دیدید راه های متفاوتی برای تخریب یک شبکه توسط مهاجمین وجود دارد. در این فصل تلاش می شود بر روی راه های تخریب از طریق برنامه های 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 برنامه های کاربردی در سمت کاربر (Client) می باشد. البته در برنامه های کاربردی سمت سرویس دهنده (Server) نیز امکانات تخریبی وجود دارد که در صورت داشتن زمان در این ترم تحصیلی در فصل جداگانه ای مطالب مربوط به این بخش نیز توضیح داده خواهد شد.

در این فصل بر روی 2 برنامه اصلی شامل پست الکترونیکی (Email)، و تارنمای وب (Web)، توضیحات لازم ارائه خواهد گردید.

### (1-6) امنیت بر روی پست الکترونیکی

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

امروزه پست الکترونیکی یکی از روش های ارتباطی متداول می باشد. در این قسمت بعضی از موضوعات وابسته به امنیت در پست الکترونیکی مورد توجه قرار می گیرد. بعضی از مهمترین سرفصل های این قسمت عبارتند از: رمزگذاری ایمیل، ابعاد آسیب پذیری ایمیل، ایمیل های ناخواسته، و ایمیل های گول زننده (Hoaxes)، و ایمیل های اسکم (Scam).

### (1-1-6) امن سازی پیغام های الکترونیکی

شبهه ارسال کارت پستال از طریق پست معمولی، ایمیل های استاندارد اولیه نیز دارای نقاط آسیب پذیری از آن جهت که توسط افراد غیر هم خوانده شود وجود دارد. ایمیل ها می توانند توسط تجهیزاتی مانند پروتکل آنالایزر در طول مسیر انتقالشان

مورد شنود قرار گیرند. طبق آمار تیم امنیتی CERT، در سال 1994 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 براحتی 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 (2-1-6)

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 بصورت نامتقارن (Asymmetric) می‌باشد. PGP برای رمزگذاری و امضاء الکترونیکی اعمال زبر 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 بصورت محلی برای شما امکان پذیر 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 در آورید.
- 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 بر افرادی که علاقه‌مندید برای شما نامه بصورت رمزگذاری شده بفرستند یا اینکه بتوانند نامه‌های شما را که امضاء دیجیتالی کرده‌اید دریافت دارند، بفرستید کلید خصوصی شما هم در کامپیوتر شخصی شما مورد استفاده شخص شما می‌باشد. شما همچنین می‌توانید کلید خصوصی‌تان 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.

### S/MIME (3-1-6)

این نرم افزار 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 اینکه توسط یک زیرساخت‌های تولید کلید خارجی (PKI عمومی) در اختیار شما قرار گیرد. دو نوع از این PKI‌های 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: Microsoft Outlook, Microsoft Outlook Express و Netscape.

### (4-1-6) نقاط آسیب‌پذیری پست الکترونیک

نقاط آسیب‌پذیری اغلب بر روی نرم‌افزارها دیده می‌شود، و ایمیل هم یک مستثناء نمی‌باشد. علاوه براینکه ایمیل دارای نقاط آسیب‌پذیری برای تخریب خودش 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 سازمانتان در مقابل نقاط آسیبپذیری پست الکترونیکی، شما باید در مقابل هشدارهای امنیتی سیستم هشیار بوده و همچنین از ویروس‌یابهای بروز 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 شما جلوگیری مینماید.

شما همچنین باید کاربران شبکه‌تان را در خصوص نقاط احتمالی حمله به وسیله ایمیل‌ها آموزش دهید. بطور مثال بسیاری از کدهای مخرب بصورت فایل‌های متصی به ایمیل‌ها برای شما مینماید، لذا کاربران باید آموزش‌های لازم برای باز نکردن این ایمیل‌های مزاحم را دیده باشند.

هر زمانی که تخریبی بر روی یک نرم‌افزار ایمیل اتفاق مینماید، 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 شبکه‌تان کمک شایانی به حفاظت از آنها در مقابل تهدیدات ناشی از ایمیل‌ها میکند.

## 6-1-5) انواع ایمیل‌های مخرب

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

- Spams
- Scams
- Hoaxes

تقسیم کرده ایم.

## Spams (1-5-1-6)

این عنوان برای آندسته از ایمیل های ناخواسته (مانند تبلیغات تجاری) که به آدرسهای زیادی ارسال میگردند اطلاق میشود. در سال 2002 سایت آنلاین Business Week اعلام کرد نزدیک به نیمی از ایمیل های بعضی از سرویسدهندگان اینترنتی و ایمیل مربوط به این نوع از ایمیل ها می باشد.

برای محافظت سازمانتان در مقابل این نوع از ایمیل های مزاحم، شما باید از نرم افزارهای فیلتر کننده در درگاه سرور ایمیلتان و همچنین تک تک کاپیوترهای شبکهتان استفاده نمایید. بعضی از این فیلترها عبارتند از: SpamAssassin, BrightMail, Cloudmark, DigiPortal's . شما همچنین باید کاربران را برای برخورد با این ایمیل ها آموزش دهید. بعضی از این آموزشها عبارتند از:

- عدم پاسخگویی به Spam ها. پاسخگویی به ایجاد کنندگان Spam ها باعث میشود که آنان از فعال بودن آدرس ایمیل شما مطمئن گردیده و حتی آدرس ایمیل شما را به دیگر تولیدکنندگان Spam بفروشند.
- آدرس ایمیلتان را در داخل صفحات وب سایتها پست نکنید. آدرس ایمیل قرار داده شما در داخل صفحات اختصاصی وب شما و یا دیگران میتواند کمک شایانی برای شناسایی آدرس ایمیل شما توسط نرم افزارهای اسکری که توسط تولیدکنندگان Spam بطور دائم بر روی اینترنت و صفحات وب برای پیدا کردن آدرسهای ایمیل جستجو میکنند، نماید.
- برای استفاده از گروه های خبری از آدرس ایمیل دومی استفاده کنید. گروه های خبری مکان مناسبی برای جمع آوری آدرسهای ایمیل توسط تولیدکنندگان Spam میباشد. لذا برای اینکه آدرس ایمیل اصلی شما لو نرود حتما برای ورود به گروه های خبری از آدرس ایمیل دوم استفاده نمایید.
- هرگز آدرس ایمیل خود را، بدون دانست 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 را در خواست میکنند. حتما قبل از ورود آدرس ایمیلتان از "عبارات رعایت حریم ایمیل" درخواستی توسط آن سایت مطمئن گردید.

- از فیلترهای Spam استفاده کنید. بعضی از این فیلترها به شما اجازه می‌دهند بر اساس 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 Spam تبلیغ شده را خریداری نکنید.

## Scams (2-5-1-6)

شبهه مورد قبلی این ایمیل‌ها هم ناخواسته می‌باشند. تفاوت ایندو در آن است که Scam ها محصولات و کالایی را برای فروش ارائه نمی‌دهند، بلکه بطور خاص هدفشان سرقت پول، کالاهای 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 می‌باشد. اگرچه محل ارسال حتمی این ایمیل‌ها کشور نیجریه نمی‌باشد، ولی این ایمیل‌ها به این نام شهرت گرفته‌اند. در این ایمیل‌ها مثلاً 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 بانکی‌تان را بدهید و یا اینکه حسابی مثلاً 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 کامپیوترتان یا شبکه‌تان 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 می‌باشد. شما باید در این سیاستنامه مشخص سازید چه اطلاعاتی حساس می‌باشند. همچنین باید در این سیاستنامه کانال‌های امن ارسال داده و کانال‌های ناامن مشخص گردند. همچنین آموزش این نکات امنیتی به کاربران شبکه‌تان لازم می‌باشد. همچنین آموزش اینکه چه ایمیل‌هایی می‌توانند یک ایمیل Scam باشد به کاربران ضروری است. بعضی از مشخصه‌هایی موجود در یک ایمیل که می‌تواند بیانگر یک Scam باشد بشرح 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)

### Hoaxes (3-5-1-6)

یک ایمیل از نوع Hoaxes مانند یک نامه زنجیره‌ای در شبکه پخش می‌گردند. آنها حاوی اطلاعات غلط و قابل باوری می‌باشند. این ایمیل‌ها معمولاً از سوی یک شخص به تعداد زیادی از افراد برای اینکه ایده یا دیدگاهی را در افراد به باور برسانند ارسال می‌گردد. معمولاً در این ایمیل‌ها از گیرنده درخواست می‌شود که آن را برای دوستانش 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 هارد دیسک‌های بسیاری از کامپیوترها گردید.

بعضی از این ایمیل‌ها به شما اعلام می‌کنند که مثلاً کامپیوتر شما توسط یک نامه که از طرف دوستان ارسال گردیده ویروسی شده و نام فایل ویروس را هم اعلام می‌کنند. در حالیکه این فایل یکی از فایل‌های اصلی سیستم شما مثلاً `Sulfnbk.exe`, `jdbgmgr.exe` می‌باشد و شما به تصور اینکه این فایل‌ها ویروس می‌باشند نادانسته آن را از روی سیستم‌تان پاک کرده و ادامه کار کامپیوترتان را دچار اختلال می‌نمایید.

برای محافظت از شبکه‌تان در مقابل این نوع از ایمیل‌ها باید سیاستنامه امنیتی مبني بر شناسایی این نامه‌ها و نحوه برخورد با آنها را در سازمانتان تنظیم کرده و آن را به کاربران شبکه‌تان 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 و ویروس معمولاً در عنوان این ایمیل‌ها وجود دارند
- به دوستان خود بگویید (Tell all Your Friends). معمولاً این درخواست در داخل ایمیل می‌تواند وجود داشته باشد.
- این یک Hoax نیست (This isn't a Hoax). این پیغام‌ها معمولاً شامل معرفی افرادی به عنوان تایید کننده آن هست که افراد قابل اعتمادی می‌باشند. بطور 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.
- پی‌آمد ناگوار (Dire Consequence). این ایمیل‌ها می‌تواند حاوی اظهارهای بسیار فوری مبنی بر اینکه مثلاً 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 ( >>>>>> ) شبیه >>>>>> در عنوان خود باشد، این پیغام احتمالاً چندین بار فوروارد (Forward) شده است، و می‌توان احتمال داد این یک ایمیل Hoax می‌باشد.

## 6-2) امنیت بر روی وب

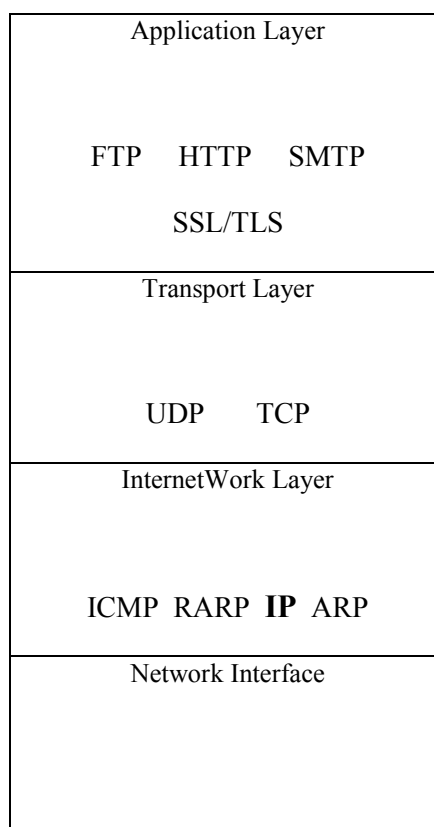
همانطور که در گذشته گفته شد سرقت بسته‌های اطلاعاتی عاملی است برای اینکه فرد مهاجم بتواند شبکه و کامپیوترهای یک سازمان را تخریب کند. معمولاً این حمله متکی بر ضعف‌های برنامه‌های کاربردی است که ناشی از ضعف در مرحله طراحی و برنامه‌نویس آنها می‌باشد. حتی مهاجمین می‌توانند کاربران را برای دریافت برنامه‌هایی که حاوی ویروس می‌باشند فریب دهند. در این بخش هدف بیان مخاطرات و نحوه مقابله با این مخاطرات در محیط وب می‌باشد.

### 6-2-1) SSL/TLS

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

در سال 1994 شرکت نتاسکیپ پروتکل به نام SSL را ارائه کرد. اساس این پروتکل مبتنی بر رمزگذاری بوسیله کلیدهای غیرمتقارن که توسط شرکت RSA ارائه می‌گردد، بود. در سال 1999 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 پروتکل های امنیتی را پشتیبانی می‌کنند. علاوه بر این از این دو پروتکل در اکثر مواقع بصورت 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 همدیگر را احراز هویت کرده و پیغام‌ها را به شکل رمزگذاری شده در اینترنت انتقال دهند. SSL/TLS پروتکل غیر وابسته به لایه‌ای در شبکه می‌باشد که طبق شکل 1-6 مابین دو لایه کاربردی و انتقال قرار می‌گیرد. هر برنامه کاربردی در شبکه مبتنی بر IP که بطور 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 بهره برداری کند.



شکل 1-6 SSL/TLS در پشته پروتکل TCP/IP

- **احراز هویت سرور برای کلاینت .** زمانی که يك مشتري قصد خرید كالايي از يك فروشنده بر روي وب سايت را دارد، مشتري ميخواهد از اينكه اين وبسایت توسط يك فروشنده واقعي جهت فروش محصولاتش ایجاد شده است مطمئن گردد. SSL/TLS این امکان را برای کامپیوترهای مشتریان فراهم می‌آورد که از مطمئن بودن سرویس فروش و تعلق آن به فروشنده واقعي آن محصول مطمئن گردد. ( و اینکه این سایت فروش از جانب يك سارق برای به سرقت بردن اطلاعات کارت فروش مشتري تدارك دیده نشده است). برای این منظور این سرور باید يك گواهینامه از يك CA قابل اعتماد برای کاربر، دریافت کرده باشد.
- **مبادله الگوریتم رمزگذاری مشترك.** کلاینت و سرور می‌توانند الگوریتم رمزگذاری مورد استفاده‌شان را مبادله کنند. این کار طرفین کلاینت و سرور را برای پشتیبانی از تکنیک رمزگذاری قلدر می‌سازد.
- **احراز هویت کلاینت برای سرور (اختیاری).** وقتی که محدودسازی دسترسی به سرور توسط کلاینت‌ها مورد نظر باشد، کامپیوترهای کلاینت بایستی گواهینامه معتبري از يك CA را بر روي خود نصب کرده باشند. البته در بسیاری از خریدهای اینترنتی این کار انجام نمی‌گیرد چرا که بسیاری از خریداران گواهینامه معتبري در دست ندارند. لذا برای شناسایی کلاینت‌ها در تجارت الکترونیکی معمولاً 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 کارآمدتر می‌باشد. SSL/TLS از رمزگذاری غیر متقارن برای ارسال رمزهای اشتراکی (کلید متقارن) استفاده می‌کند، بنابراین رمزگذاری داده واقعي بسیار سریعتر می‌شود، و در عین حال روش برقراری ارتباطات رمزگذاری شده نیز بسیار امن می‌باشد.
- **برقراری يك اتصال رمزگذاری شده.** در انتها، و البته بسیار مهم، تمام ارتباطات میان کلاینت و سرور رمزگذاری شده می‌باشد.

## HTTPS (2-2-6)

ارتباطات وب با بکارگیری HTTP اجرا می‌گردد. ارتباطات وبی که بوسیله 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 وب استفاده می‌کنند.

اگرچه HTTPS ارتباط بین کلاینت و سرور را رمزگذاری می‌کند، 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. متأسفانه 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 (3-2-6)

بافر به فضای داده‌ای اطلاق می‌شود که بوسیله هر دو عنصر تجهیزات سخت افزاری و پروسس‌های نرم افزاری 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 گاهی باعث آن می‌شود که حجم داده اضافی بر روی بافرهای کناری ریزش کرده و باعث خرابی داده‌های موجود در آنها شود. سرریزی بافر ممکن است بدلیل 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 نرم افزار از روش‌های برنامه‌نویسی امن طبیعت کنند. اجرای عملیات امن برنامه نویسی به معنای طراحی برنامه‌نویسی به طرق 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 بهره برداری از وصله‌هایی است که در مرور زمان برای حل مشکلات این نرم افزارها توسط فروشندگان آن به بازار عرضه می‌گردد.

#### Active Content (4-2-6)

در راستای تلاش برای اینکه مرور صفحات وب مهیج، کاربردی، و مفید گردند، تولیدکنندگان و فروشندگان نرم افزارها محتوای فعال (Active Content) را ایجاد می‌کنند. مواد محتوای فعال برنامه اجرایی کوچک و یا کدهای اسکریپت می‌باشند که به داخل مرورگرهای وب ارائه می‌گردند. بطور مثال، بعضی از بانک‌ها حسابگرهایی برای محاسبه میزان پرداخت رهن را در داخل وب سایت‌هایشان پیشنهاد می‌دهند. این ماشین‌حساب‌های محاسب رهن به عنوان محتوای فعال شناخته می‌شوند. به عنوان مثال‌های دیگر می‌توان از بعضی از محتوای ویدئویی و انیمیشنی بر روی صفحات وب نام برد. دو نوع مرسوم محتوای فعال جاوا اسکریپت‌ها (JavaScript) و اکتیوکس (ActiveX) می‌باشند. محتوای فعال برای اجرای یک اسکریپت در داخل سیستم کلاینت طراحی شده‌اند. متأسفانه، 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 محتوای فعال در سمت کلاینت و امکانات تخریب آمیز ممکنه آنها می‌باشد.

#### Java Applets (1-6-2-4)

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

این برنامه های کوچک از داخل یک صفحه وب توسط برچسب های اپلت (APPLET tag) آدرس دهی میشوند. این برچسب ها برای بارگذاری فایل های مربوط به متن کد جاوا استفاده میشوند. کد متن جاوا توسط موتور بر روی کلاینت به نام ماشین مجازی جاوا (Java Virtual Machine) اجرا میشوند. این VM ها بر روی بسیاری از سیستم های عامل مانند یونیکس، مکینتاش، و ویندوز اجرا 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 اپلت ها بر روی این سیستم عامل حتما نرم افزار ماشین مجازی جاوا (Java Virtual Machine) را بر روی کامپیوتر خود دریافت کنید.

متأسفانه مهاجمین میتوانند از این امکان برای حمله به سیستم های سمت کلاینت استفاده کنند. شما برای اینکه خود و سازمانتان را در مقابل حملات از طریق Java Applet ها محافظت کنید، میتوانید امکان پشتیبانی جاوا را بر روی ماشینتان غیر فعال کنید. بسیاری از مرورگرها (مثل نت اسکپ و اینترنت اکسپلورر) امکان غیر فعال کردن جاوا را به شما میدهند.

#### Java Script (2-6-2-4)

شرکت نت اسکپ جاوا اسکریپت را بوحود 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 پیاده سازی شده اند و دو زبان مستقل از هم تلقی میشوند.

بسیاری از مرورگرهای وب، شامل نت اسکپ 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 میشود. یک برچسب اسکریپت (SCRIPT tag) در داخل

کدهای HTML برای نشانه گذاری جاوا اسکریپت قرار داده می‌شود. جاوا اسکریپت معمولاً برای ارتباط با دیگر اجزاء (مانند برنامه‌های CGI که بعداً 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. بطور 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.

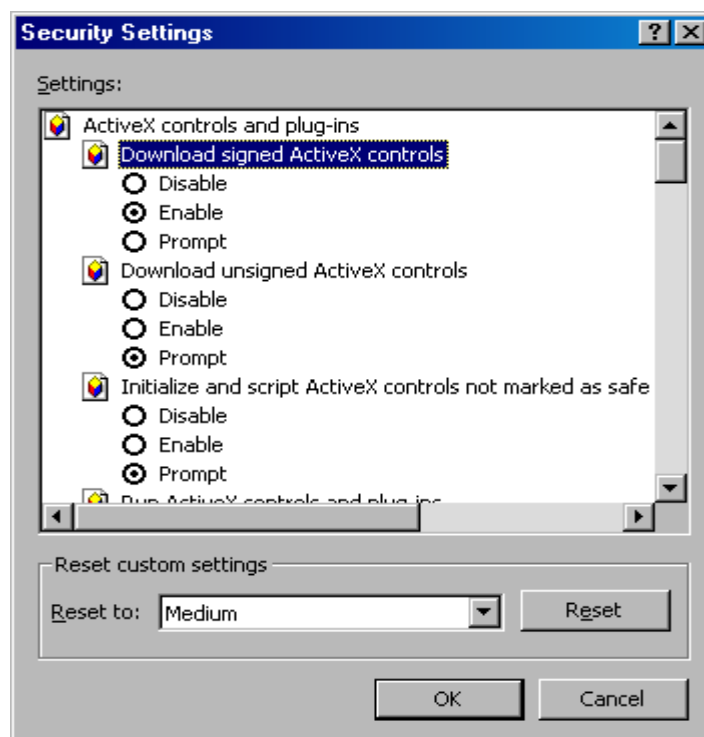
مهاجمین می‌توانند از جاوا اسکریپت‌ها برای حمله به سیستم کلاینت‌ها سوء استفاده کنند. برای محافظت از خودتان و سازمان‌تان در مقابل جاوا اسکریپت‌های مخرب، شما می‌توانید جاوا اسکریپت را بر روی کامپیوترتان غیر فعال کنید. اگر چه غیر فعال سازی جاوا اسکریپت بر روی کامپیوترتان شما را در مقابل این نوع حملات بیمه می‌کند، اما شما را هم از بهره‌گیری استفاده‌های مفید از محتوای فعال محروم می‌سازد. به هر حال، شما می‌توانید بصورت انتخابی در مورد سایت‌هایی که به آنها وارد می‌شوید و دارای اپلت‌های جالب و قابل اعتمادی هستند، جاوا اسکریپت خود را فعال کنید. به هر صورت، در صورتیکه شما علاقه‌مند باشید که جاوا اسکریپت خود را فعال نگه دارید، حتماً باید مرورگر وب خود را با آخرین نسخه‌های وصله‌های نرم افزاری بروز نگه دارید. در صورت غیر فعال کردن جاوا اسکریپت بر روی مرورگر خود در صورتیکه وبسایتی بخواهد به روی کامپیوتر شما محتوای فعالی بفرستد، شما بر روی صفحه کامپیوتر خود جملات زیر را مشاهده خواهید کرد که در صورت کلیک بر روی این جملات 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..."](#)

#### ActiveX (3-6-2-4)

این تکنولوژی هم برای فراهم‌سازی محتوای فعال بوجود 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 دارد، و سرویس‌های کاربردی را برای کاربران تدارک ببیند. همچنین مانند جاوا اسکریپت در معرض سوء استفاده توسط مخربین برای حملات می‌باشد.



شکل 6-2) 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 6-2 را می‌دهد. شما می‌توانید اینترنت اکسپلورر را به شکلی تنظیم نمایید 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 بطور کلی دریافت هر گونه کنترل اکتیوکس را غیر فعال نماید.

اگر شما لازم است از کنترل اکتیوکس استفاده کنید، شما باید بطور دائمی سایت فروشنده نرم افزار را برای هشدارهای امنیتی و اطلاعاتی در مورد احتمالات تخریب مورد مطالعه قرار دهید. اگر شما متوجه شدید که یک کنترل کننده خاص اکتیوکس دچار خطراتی برای امکان حمله می‌باشد، شما باید آنرا غیر فعال کرده تا وصله امنیتی آن ارائه گردد.

**Signing Active Content (4-6-2-4)**

در تلاش برای افزایش امنیت محتوای فعال، بعضی از فروشندگان فرآیندی را برای انجام امضای دیجیتالی قبل از نصب محتوای فعال، پیاده‌سازی کرده‌اند. تولید کنندگان محتوای فعال قبل از ارسال این محتوای فعال آنها را امضای دیجیتالی می‌نمایند این ارائه دهندگان تاییدیه امضاء برای امضا نمودن 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 محتوای الکترونیکی به ارمغان می‌آورد، اما در مقابل مشکلاتی که ممکن است از طرف یک فروشنده مورد اعتماد بوجود آید، و 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 دارید.

**Cookies (5-2-6)**

کوکی عبارت است از مقدار کوچکی از اطلاعات که یک وب سرور در مورد یک کاربر بر روی کامپیوتر خود کاربر ذخیره می‌کند. بطور مثال، کوکی ممکن است تبلیغات مختلفی که یک مرورگر کلاینت دریافت کرده است 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 معمولاً به سرورها اجازه ذخیره سازی کوکی‌ها را می‌دهند. بسیاری از مرورگرها به این دلیل این اجازه را صادر می‌کنند که امروزه کوکی‌ها در حجم بالایی مورد استفاده می‌باشند، 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. بطور مثال نت

اسکیپ کوکی‌ها در فایلی به نام Cookies.txt و اینترنت اکسپلورر هر کوکی را در فایل‌های جداگانه‌ای در پوشه‌ای به نام %windir%\Internet Files ثبت می‌نماید.

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

- کوکی‌ها می‌توانند اداره شوند و یا دزدیده شوند. حمله کننده می‌تواند کوکی‌ها را برای بدست 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، کوکی‌ها داخل سیستم کلاینت را به طرف سیستم خودش انتقال دهد. حتی احتمال استراق سمع کوکی توسط مهاجمین در حین انتقال وجود دارد.

برای محافظت سازمان و کلاینت‌های سازمان‌تان در برابر تخریب‌های ناشی از سوء استفاده از کوکی‌ها، می‌بایست از روشهای زیر بهره ببرید.

- وب سرور خود را با اتکا و اعتماد بر اطلاعات ذخیره شده در کوکی‌های سمت کلاینت جهت کنترل 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، حتماً از SSL/TLS برای محافظت از اطلاعات داخل کوکی‌ها استفاده شود.

## CGI (6-2-6)

برنامه‌های CGI معمولاً برای تولید محتوای فعال در وب سرورها مورد استفاده قرار می‌گیرد. CGI‌ها معمولاً برای ارسال اطلاعات میان برنامه [کاربردی و وب سرورها می‌باشند. بطور مثال، آنها معمولاً برای انجام کارهایی مانند وارد کردن داده، جستجو، فانکشن‌های بازیابی در دیتابیس‌ها، مورد استفاده قرار می‌گیرند.

با زبانهای مختلف برنامه نویسی می‌توان CGI‌ها 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 حفره‌های امنیتی باشد که توسط مخربین سوء استفاده شود. در زیر برخی از تخریب‌های ممکنه بر اساس این برنامه‌ها آورده شده است.

- اجرای چندین باره یک برنامه CGI از طریق مرورگرهای چندگانه وب. هر گاه که یک برنامه CGI توسط مرورگری اجرا می‌گردد، بخشی از ظرفیت منابع سیستمی بر روی وب سرور را برای اجرا در اختیار می‌گیرد، 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 بعضاً در کنار خود وب سرور به صورت پیش فرض 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 برنامه‌های 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 غیر فعال کنید. بدین روش امکان وارد کردن اطلاعات مخرب به این دایرکتوری از طرف فرد مخرب را هم سلب می‌کنید.

برای حفاظت از وی سرور در مقابل مخاطرات ناشی از برنامه‌های CGI، باید روش‌های زیر را بکار بندید.

- ایجاد محدودیت در کاربرد برنامه‌های CGI. به این طریق از ایجاد بار زیاد بر روی وب سرور و نتیجتاً 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 بصورت پیش فرض موجود در درون وب سرور.
- بررسی برنامه‌های CGI در جهت پیدا کردن حفره‌های امنیتی آنان. استفاده از برنامه‌هایی که از مراحل تست لازم عبور کرده باشند.

## Instant Messaging (7-2-6)

پیغام‌گذاری لحظه‌ای یا IM، روشی است که امروزه برای انتقال صحبت، فایل، صدا بین کاربران مختلف بصورت مستقیم بر روی وب، مورد استفاده قرار می‌گیرد. این برنامه‌ها برای اجرا و بهره‌برداری بسیار راحت می‌باشند، اما متأسفانه دارای شرایطی می‌باشند 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 اعتمادشان 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 نمی‌شود، لذا مورد بررسی و ویروسیاب ایمیل قرار نمی‌گیرد. پس انتقال ویروس از این طریق امکان پذیر می‌باشد.

- هکر می‌تواند نقاط ضعف این سیستم را شناسایی کند، مواردی همچون سرریز بافر. شبیه دیگر برنامه‌های کاربردی، IMها هم می‌توانند دارای حفره‌های امنیتی باشند، اما این حفره‌های امنیتی بطور بالقوه خطرناکتر می‌باشد، چرا که اتصال بصورت مستقیم بین کاربران می‌باشد. همچنین اشکال برنامه‌ای در یک طرف ارتباط می‌تواند عاملی گرد 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 کرده اند. بعضی از سازمان‌ها اجازه استفاده از IM های را که امن باشد را می‌دهند. اگر امکان حذف کامل سیستم IM در سازمان‌تان نمی‌باشد، حتما موارد امنیتی زیر را مد نظر داشته باشید:

- انحصار در استفاده از IM های که برای استفاده شما مجاز می‌باشند. این عمل شما را از پشتیبانی، امن‌سازی، مشکلات ممکنه چندگانه ناشی از IMهای مختلف خلاص می‌کند.
- اگر اطلاعات انتقالی بین کلاینت‌ها باید امن باشد، از برنامه IM ای 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 آنان از خطرات ممکن IM. به آنها توضیح دهید که انتقال فایل از این طریق چقدر خطرناک می‌باشد، و اینکه یک هکر ممکن است برای فاش شدن اطلاعات محرمانه او تلاش کند.
- اطمینان از اینکه تمامی استفاده کنندگان از IM، از ویروسیاب‌های بروز شده استفاده می‌کنند.
- پی‌گیری از فروشندگان نرم افزارهای IM برای دریافت آخرین وصله‌های امنیتی