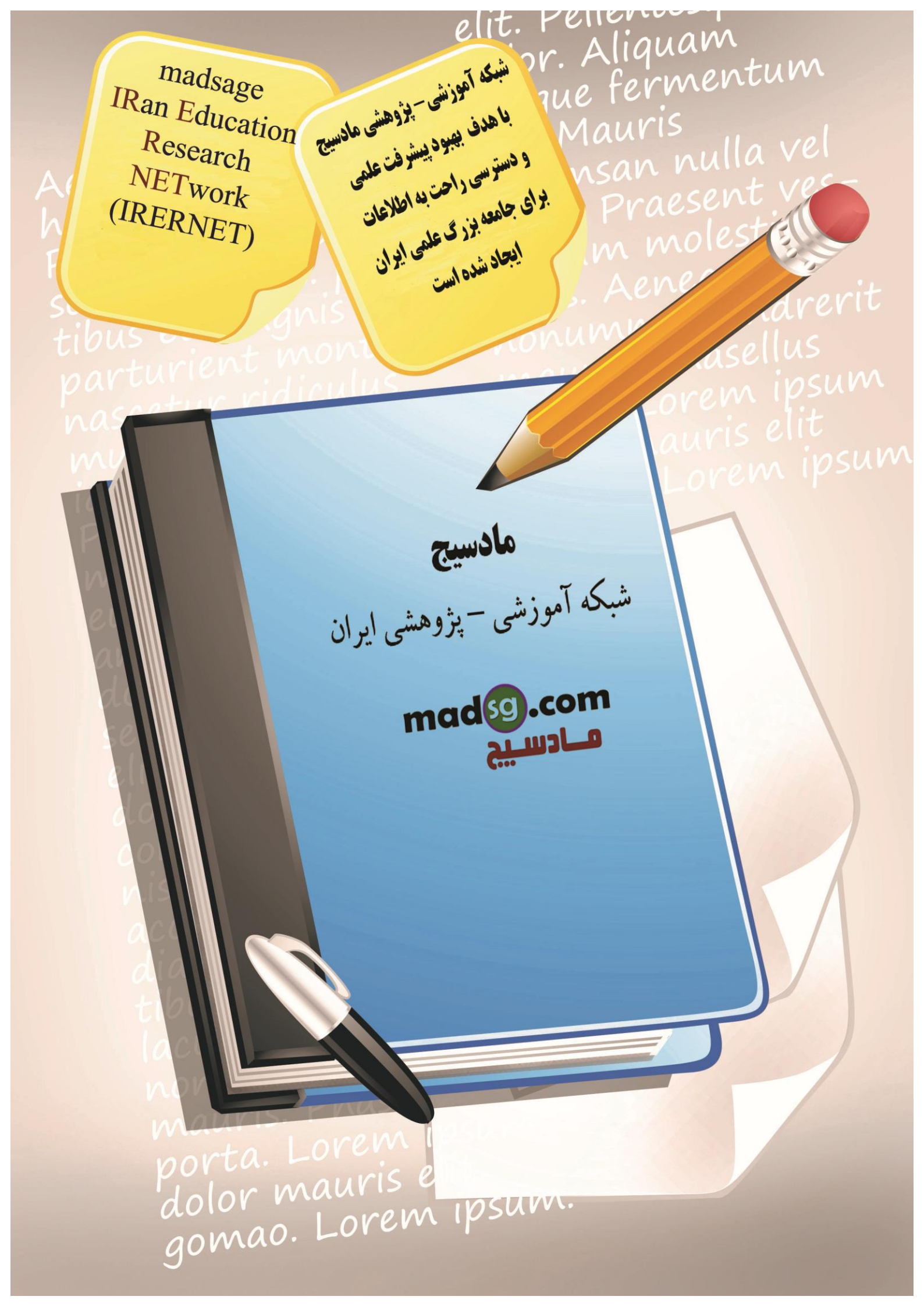

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

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 گیری 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 شبكه های اطلاعاتی و دنیای مجازی به رفاه، آسایش و انجام کارها با سرعت و دقت بیشتر کمك می کند، از سوی دیگر چالشها و موانعی نیز در به کارگیری فناوری اطلاعات و شبکه‌های اطلاعاتی رخ می دهد که یکی از مقوله‌ها 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 استفاده‌هايي كه ار عرضه تبادل اطلاعات می شود، هستیم از جمله هك شدن سایتها توسط نفوذگران، انتشار ویروسهای رایانه ای جدید و سرقت از حسابهای مشتریان بانکها، شکسته شدن قفلهای نرم‌افزاری و.... در دنیای امروز با واگذاری کارهای مالی، اداری و اطلاعاتی به شبکه های رایانه‌ای و همچنین وسعت زیاد تبادل اطلاعات بین نقاط مختلف در کشورهای جهان، باید نسبت به هشدارهای موجود در زمینه امنیت اطلاعات و امن بودن این حوزه بیش از پیش توجه شود.

در امور تجاري ، تجارتي موفق محسوب مي‌گردد كه در آن بسياري از ملاحظات امنيتي مد نظر قرارگرفته باشد براي يك سازمان تجاري موفق اطلاعات دارايي اصلي است همانطور كه در امر تجارت سنتي مجموعه‌اي از تمهيدات وجود دارد، در شكل پيچيده‌تر آن هم در محيط الكترونيكي وجود دارد امنيت اطلاعات كمك مي‌كند كه آسيبها كمينه، سرمايه اطلاعاتي بيشينه، و فرصتهاي تجاري از دست اندازي رقبا محافظت گردد

1-1) امنیت فناوری اطلاعات

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

ایمن از این فناوری و اطمینان از وجود محیطی عاری از هرگونه تهدید 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 یك 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 یك شبکه ارتباطی که دارای نام و آدرس دهی خاص می باشد. فرآیند: عملیاتی که برروی 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 خواهیم‌کرد.

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 هوائی) ، تغییرات اساسی در روش خرید و فروش کالا (فروشگاههای online ، کارت های اعتباری) ، پیشرفت های برجسته در عرصه پزشکی ، صرفا" نمونه هائی اندک در این زمینه می باشد .

اجازه دهید به منظور آشنائی 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 درشبکه 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) برخي 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 ایمن سازی اطلاعات ، شناخت تهدیدات و آگاهی لازم در خصوص برخی مفاهیم اولیه در خصوص ایمن سازی اطلاعات است که در امتداد بیان میگردد.

- Hacker , Attacker **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 صرفا" کنجکاوی باشد، ماحصل عملیات آنان می تواند اثرات جانبی منفی را به دنبال داشته باشد .
- **کد مخرب :** 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 هائی 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 ، عموما" 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 .

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

1-2-4) سابقه امنيت در شبكه اينترنت

اينترنت در سال 1969 بصورت شبكه‌هاي بنام آرپانت كه مربوط به وزارت دفاع آمريكا بود راه‌اندازي شد. هدف اين بود كه با استفاده از رايانه‌هاي متصل به هم، شرايطي ايجاد شود كه حتي اگر، بخشهاي عمده‌اي از سيستم اطلاعاتي به هر دليلي از كار بيفتد، كل شبكه بتواند به كار خود ادامه دهد، تا اين اطلاعات حفظ شود. از همان ابتدا، فكر ايجاد شبكه، براي جلوگيري از اثرات مخرب حملات اطلاعاتي بود.
در سال 1971 تعدادي از رايانه‌هاي دانشگاهها و مراكز دولتي به اين شبكه متصل شدند و محققين از اين طريق شروع به تبادل اطلاعات كردند.

با بروز رخدادهاي غيرمنتظره در اطلاعات، توجه به مسأله امنيت بيش از پيش اوج گرفت. در سال 1988، آرپانت براي اولين بار با يك حادثه امنيتي سراسري در شبكه، مواجه شد كه بعداً، «كرم موريس» نام گرفت. رابرت موريس كه يك دانشجو در نيويورك بود، برنامه‌هايي نوشت كه مي‌توانست به يك رايانه‌اي ديگر راه يابد و در آن تكثير شود و به همين ترتيب به رايانه‌هاي ديگر هم نفوذ كند و بصورت هندسي تكثير شود. آن زمان 88000 رايانه به اين شبكه وصل بود. اين برنامه سبب شد طي مدت كوتاهي ده درصد از رايانه‌هاي متصل به شبكه در آمريكا از كار بيفتد.

به دنبال اين حادثه، بنياد مقابله با حوادث امنيتي (IRST) شكل گرفت كه در هماهنگي فعاليتهاي مقابله با حملات ضد امنيتي، آموزش و تجهيز شبكه‌ها و روشهاي پيشگيرانه نقش مؤثري داشت. با رايجتر شدن و استفاده عام از اينترنت، مسأله امنيت خود را بهتر و بيشتر نشان داد. از جمله اين حوادث، اختلال در امنيت شبكه، WINK/OILS WORM در سال 1989، Sniff packet در سال 1994 بود كه مورد اخير از طريق پست الكترونيك منتشر مي‌شد و باعث افشاي اطلاعات مربوط به اسامي شماره رمز كاربران مي‌شد. از آن زمان حملات امنيتي- اطلاعاتي به شبكه‌ها و شبكه جهاني روزبه‌روز افزايش يافته است.
گرچه اينترنت در ابتدا، با هدف آموزشي و تحقيقاتي گسترش يافت، امروزه كاربردهاي تجاري، پزشكي، ارتباطي و شخصي فراواني پيدا كرده است كه ضرورت افزايش ضريب اطمينان آن را بيش از پيش روشن نموده است.

1-3) فرايند توسعه امنيت 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 (ریسك) بین خطر آفرینی یك 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 برگیرنده 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.

يك سياست امنيتي، اعلاميه‌اي رسمي مشتمل بر مجموعه‌اي از قوانين است كه مي‌بايست توسط افرادي كه به يك تكنولوژي سازمان و يا سرمايه‌هاي اطلاعاتي دستيابي دارند، رعايت و به آن پايبند باشند. به منظور تحقق اهداف امنيتي، مي‌بايست سياست‌هاي تدوين شده در رابطه با تمام كاربران، مديران شبكه و مديران عملياتي سازمان، اعمال گردد. مهمترين هدف يك سياست امنيتي، آگاهي دادن لازم به كاربران، مديران شبكه و مديران عملياتي يك سازمان در رابطه با امكانات و تجهيزات لازم، به منظور حفظ و صيانت از تكنولوژي و سرمايه‌هاي اطلاعاتي است. در ادامه ويژگي‌هاي يك سياست امنيتي خوب و يك مثال از سياست امنيتي، تعريف رمز عبور، بيان مي‌گردد.

- **تعريف رمز عبور به عنوان يك مثال از سياست امنيتي**

- حداقل طول رمز عبور، دوازده و يا بيشتر باشد.
- در رمز عبور از حروف كوچك، اعداد، كاراكترهاي خاص و زيرخط[1] استفاده شود.
- از كلمات موجود در ديكشنري استفاده نگردد.
- رمزهاي عبور، در فواصل زماني مشخصي (سي و يا نود روز) به صورت ادواري تغيير داده شوند.

كاربراني كه رمزهاي عبور ساده و قابل حدسي را براي خود تعريف نموده‌اند، تشخيص و به آنها تذكر داده شود (عمليات فوق به صورت متناوب و در فواصل زماني يك ماه انجام گردد).

[1]- 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، صحتداده، احراز هویت، پوشش ترافیك، کنترل مسیر یابی و تأیید توسط عامل سوم.

به طور کلی نگاه به مقوله امنیت نمی تواند یك 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 یك نگرش سیستماتیك و استفاده مداوم از یك چرخه ایمن سازی شامل طراحی، پیاده سازی، ارزیابی و اصلاح، ضریب امنیتی سیستم های رایانه ای خود را بالا ببریم.

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

- احراز هویت – Authentication:
فرستنده یا گیرنده هویت واقعي خود را براي طرف مقابل اثبات مي‌كند.
- كنترل اختيارات – Authorization:
يعني هر طرف فعاليت به چه سطح از اطلاعاتي دسترسي داشته و چه نوع ازعمل(رويت، حذف، تغيير، اضافه) برايش مقدور باشد.
- در دسترس بودن – Availability:
خدمات بايد هميشه در دسترس افراد مجاز باشد.
- محرمانگي اطلاعات – Confidentiality:
فقط فرستنده و گيرنده مورد نظر قابل به درك پيام باشند.
- بازرسي – Auditing:
امكان بررسي داده‌ها و اطلاعات موجود در سيستم ظبط رويدادها (Log File) موجود باشد.
- صحت داده‌ها (تماميت و جامعيت) – Integrity:
يعني عدم امكان دستكاري داده‌ها توسط افراد يا نرم افزارهاي غير مجاز.به بياني ديگر اطلاعاتي كه درون

پيغام و يا تبادلات وجود دارد در طول مسير به طور اتفاقي يا عمدي مورد دستبرد قرار نمي‌گيرند

- انكار ناپذيري – Non-Repudiation:

يعني هيچ‌كدام از طرفين (فرستنده و گيرنده پيام)، امكان انكار عملكرد خود (ارسال پيام) را نداشته باشد. يا به عبارت ديگر ارسال‌كننده نمي‌تواند منكر ارسال پيام يا تبادل مالي شود و دريافت‌كننده هم نمي‌تواند منكر دريافت 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 سرویس‌های فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطیمنان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین) . در زمان ارائه، سرویس دهندگان مجموعه‌ای از سرویس‌ها و پروتکل‌ها را به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال کرده‌اند. این موضوع ارتباط مستقیمی با سیاست‌های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهائی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند.

اولین مرحله در خصوص ایمن سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص ایمن 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 سرویس‌ها ، پروتکل‌ها و برنامه‌های نصب شده با خواسته‌های یک سازمان
- ✓ بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس‌ها و پروتکل‌های غیرضروری ، تنظیم دقیق امنیتی سرویس‌ها 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 . متاسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری‌ها 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 سرویس‌ها ، پروتکل‌ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل‌های آنان در جهت افزایش کارائی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه‌های 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 .

2-1) وظیفه یک سرویس دهنده

پس از شناسائی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس‌ها و پروتکل‌های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم‌گیری 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 شناسائی 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 سرویس‌های 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)

- (Simple Network Management Protocol) SNMP

- Application Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن برنامه ها ی 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 سایت‌های داخلی و یا خارجی را برعهده دارند .
- FTP Server : این نوع سرویس دهندگان مسئولیت ذخیره‌سازی 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 پروتکل‌های 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 پروتکل‌های ضروری و حذف و غیر فعال نمودن سرویس‌ها و پروتکل‌های 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 مکانیزم‌هاي جلوگيري از حملات امنيتي و سياست‌هاي امنيتي محقق اهداف امنيت اطلاعات هستند. حملات امنيتي مي‌تواند شامل؛ قطع (Interruption)، دسترسي غيرمجاز (Interception)، دستكاري داده ها (Modification) و ساخت پيغام (Fabrication) باشد.

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی 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 ؟ شناسائی 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 رویاروئی 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	
Back Door	Spoofing
Middle Man in the	Replay
Hijacking TCP/IP	Brute Force
Dictionary	Password Guessing

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

1-2-2) حملات DoS

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoS قرار گرفته است . این نوع از حملات صرفا" 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 ممانعت 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 پاسخگوئی 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 ، قطعا" 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 ، عملا" 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 عملا" امکان دریافت email های معتبر را از account فوق سلب نمایند

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

در یک تهاجم از نوع DDoS ، یک مهاجم ممکن است از کامپیوتر شما برای تهاجم 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 بالائی داده از طریق کامپیوتر شما برای یک وب سایت و یا ارسال نامه های الکترونیکی ناخواسته برای آدرس های Email خاصی ، نمونه هائی 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

متاسفانه 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 سیاستهای 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 معمولا" چنین پتانسیلهائی 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 داراي اين مشكل مي‌باشد.

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 صرفا" از منابع و سایت‌های 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 افزارهائی (نظیر : Back Orifice, NetBus, and Sub7) را به دنبال داشته باشد . برنامه های آنتی ویروس می بایست به صورت مستمر بهنگام شده تا امکان شناسائی نرم افزارهای جدید ، فراهم گردد .

3-2-2) حملات از نوع Spoofing – ره‌گيري

تكنيكي است براي دسترسي غير مجاز به كامپيوترها .هكر ابتدا آدرس IP يك كامپيوتر مورد اعتماد را پيدا مي كند. پس از به دست آوردن اين اطلاعات هكر شروع ارسال اطلاعات به سيستم قرباني كرده و خود را مورد اعتماد وانمود مي كند (خود را به جاي يك كامپيوتر مورد اعتماد جا مي زند!) ، پس از برقراري ارتباط شروع به دريافت اطلاعاتي مي كند كه در حالت معمول ، مجاز به دسترسي به آنها نيست.

اين حمله عمدتا متكي است بر ضعف پروتكل IP و ضعفهاي ساختاري اينترنت براي دسترسي كاربران بر روي لايه Application. در اين حمله معمولا دو تكنيك معرفي مي‌گردد:

- جعل هويت Impersonation
- تغيير قيافه Masquerading

در روش تغيير قيافه فرض مي‌شود كه فرد حمله كننده قبلا User Id. و Pass Word فردي را دزديده و حال با تغيير قيافه خود را به عنوان يك كاربر معتبر جا مي‌زند.

اما در روش جعل هويت معمولا به طور مثال سناريوي زير كه نسبتا ساده ولي خطرناك مي‌باشد انجام مي‌گيرد:

در اين روش مثلا وقتي يك كاربر معتبري مي‌خواهد به سرور دانشگاه متصل گردد، قبلا دانشجوها به DNS دانشگاه حمله كرده‌اند و اين سرور را به شكلي مختل كرده‌اند كه بسته‌هاي اطلاعاتي به جاي آنكه بين سرور دانشگاه و كلاينت جابجا شوند، بين كلاينت متقاضي و سرور جعلي مهاجم جابجا مي‌شوند. يعني اولين پيغام (Prompt) كه بر روي صفحه كاربر ظاهر مي شود دقيقا مشابه پيغامي است كه سرور دانشگاه براي دريافت User Id. و Pass Word به كلاينت مي‌دهد و از او خواسته مي‌شود Id. و P/W خود را وارد نمايد و آنگاه اين مشخصات به سرقت مي‌رود و در ادامه بلافاصله پيغام " User Id. or Pass Word Incorrect " بر روي صفحه ظاهر مي‌شود و كاربر هم بدون اينكه احساس بدي پيدا كند، با تصور آنكه مشخصه يا كلمه خود را اشتباه وارد كرده مجددا آنها را وارد كرده و وارد سيستم دانشگاه مي‌شود.

4-2-2) حملات از نوع Man in the Middle

نفوذگر بين دو كامپيوتر Client و Server كه در حال تبادل اطلاعات هستند قرار مي گيرد. نفوذگر ترتيبي را اتخاذ مي كند كه دو كامپيوتر از وجود او بي اطلاع باشند. به اين ترتيب دسترسي كاملي به اطلاعات بين دو نقطه پاياني دارد. در اين حملع عمدتا هدف بدست آوردن كلمه عبور و رمز عبور مي‌باشد.

سيستم هاي Wireless در معرض اين حمله قرار دارند.

5-2-2) حملات از نوع Replay

وقتي يك هكر به وسيله ابزار Sniffer (بو كشيدن) بسته هاي اطلاعاتي را از روي سيم بر مي دارد ، يك حمله Replay رخ داده است. وقتي بسته‌ها دزديده شدند ، هكر اطلاعات مهم و نامهاي كاربري و كلمات عبور را از درون آن استخراج مي كند. وقتي كه اطلاعات ازبسته‌ها استخراج شدند ، دوباره بسته‌ها روي خط قرار مي گيرند و يا بدانها به صورت دروغين پاسخ داده مي شود.

يا به عبارت ديگر وقتي بين يك سرويس‌دهنده و سرويس‌گيرنده مجاز بر اساس سطوح دسترسي موردنظر يك تماس(Session) اتفاق مي‌افتد، اين جلسه ذخيره گرديده و مجددا توسط كاربر غير مجاز اين جلسه تكرار ميگردد. لذا اگر به‌گونه‌اي ترتيب و توالي اين جلسات(sessions) مجددا مورد بررسي قرار نگيرد مي‌تواند يك حمله انجام پذيرد.

6-2-2) حملات از نوع TCP/IP Hijacking

معمولا به آن جعل نشست (Session Hijacking) نيز گفته مي شود. هكر مي تواند نشست TCP بين دو ماشين را به دست آورد. يك روش مشهور استفاده از Source-rout كردن IP ها مي باشد. Source-rout كردن يعني بسته هاي IP را طوري تغيير دهيم كه از مسيري خاص بگذرند.

7-2-2) حملات از نوع DNS Poisoning (مسموميتDNS)

اين حمله هنگامي است كه فايل DNS شما با اطلاعات ناجوري پر شود. به صورت ساده تر هنگامي مي باشد كه نفوذگر ركوردهاي DNS را كه به Host هاي صحيحي اشاره دارند ، به Host مورد نظر خود تغيير مي دهد.

8-2-2) حملات از نوع Social Engineering (مهندسي اجتماعي)

بيشتري زماني رخ مي دهد كه هكر به سيستم هاي واقعي قصد نفوذ دارد. راه ديگر هنگامي مي باشد كه نفوذگر با استفاده از نقاط ضعف كاربر انتهايي (End User) راه نفوذ به شبكه را پيدا مي كند. سوءاستفاده از نقاط ضعف افراد با به دست آوردن عادت هاي شخصيتي افراد براي اغفال آنها و يا تحت فشار قرار دادن آنها تا اطلاعات مورد نياز براي نفوذ به شبكه را در اختيار فرد هكر قرار دهد.

9-2-2) حملات از نوع Brute Force

يك روش براي به شكستن كلمات رمز و به دست آوردن آنهاست. حمله Brute-force حروف را به صورت تركيبي استفاده مي كند و با تست كردن آنها رمز عبور را پيدا مي كند.

براي مقابله با اين روش بايد كلمات رمز با طول زياد انتخاب كرد و يا كلمات رمز را هر دفعه تغيير داد.

10-2-2) حملات از نوع Dictionary

يك روش براي به دست آوردن كلمات رمز عبور است. كلمه Dictionary در اصل لغتنامه اي از كلمات معروف مي باشد كه در يك فايل ذخيره شده اند و به وسيله يك ابزار براي شكستن كلمات رمز ، مورد استفاده قرار مي گيرند.

براي مقابله با اين حمله بايد از كلماتي استفاده كرد كه در لغتنامه وجود ندارد. البته امروزه راه ديگر مقابله با

تهديدات از نوع Brute Force و Dictionary استفاده از يك فعاليت انساني است. مثلا يك شكل گرافيكي با اشكالي كه توسط سيستمهاي الكترونيكي قابل تشخيص نيستند ، شما را مجبور به تايپ مي‌كنند.

2-2-11) حملات از نوع Software Exploitation

حمله عليه سوراخها و باگهاي موجود در كدهاي سيستم. براي اصلاح آنها بايد از Hotfix ها و Service Pack ها استفاده كرد.

2-2-12) حملات از نوع Sniffing

اطلاعاتي مانند نام عبور (U/Id) و رمز عبور (P/W) توسط هكر بر روي خط شنود شده و يا اينكه با حمله به ديتابيس‌ها و به دست آوردن اين اطلاعات، هكر ميتواند خود را به جاي كاربر مجاز معرفي كرده و سوء استفاده نمايد.

فصل سوم: روش‌ها و سيستم‌هاي كنترل دسترسي

مقدمه

در اين بحث تلاش مي‌كنيم از دسترسي‌هاي غير مجاز (Unauthorized Access) جلوگيري نماييم. اين محافظت اطلاعات 3 وجه دارد:

- محرمانگي (Confidentiality)
- تماميت و صحت داده ها (Integrity)
- در دسترس بودن (Availability)

در بحث محرمانگي هدف اصلي آن است كه دسترسي به اطلاعات و خواندن آنها بدون مجوز انجام نپذيرد.

در بحث صحت داده‌ها هدف آن است كه اجازه ندهيم تغييرات هوشمندانه‌اي در مجموعه اطلاعات انجام گيرد. يعني اجازه نوشتن اطلاعات را بدون مجوز ندهيم.

در بحث در دسترس بودن اين انتظار را داريم در زمان‌هاي مشخص شده كه به كاربر اجازه دسترسي داده مي‌شود ، و با وجود پهناي باندي كه بايد در اختيارش باشد، هميشه اين امكان يعني دسترسي به منابع و اطلاعات برايش مقدور باشد.

براي مدلسازي بحث كنترل دسترسي دو مفهوم كلي بايد مورد نظر قرار گيرد:

- Subject: يك موجود فعال است، مانند يك كاربر، يا مثل يك برنامه ، يك پروسس ، يا يك كامپيوتر، و يا حتي يك ديتابيس كه تلاش و فعاليت آنها در راستاي دسترسي به يك منبع اطلاعاتي مي‌باشد.
- Object: منظور همان منبع اطلاعاتي مي‌باشد كه مي‌تواند يك برنامه ديگر، يك فايل ديگر، يك كامپيوتر ديگر، و يا اطلاعات مربوط به كاربري ديگر باشد. Objectها ماهيت غير فعال (Passive) دارند.در واقع عمل انتقال اطلاعات از Object به سمت Subject مي‌باشد. و ما در بحث كنترل دسترسي سعي مي‌كنيم براي اين انتقال اطلاعات رويه و روش خاصي را تعريف كنيم.

3-1) تكنيك‌هاي كنترل دسترسي

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

يكي از مهمترين تكنيكهاي كنترل دسترسي كنترل حداقل اجازه مي باشد. ديدگاه اصلي حاكم بر اين تكنيك اين است كه در يك شبكه متشكل از تجهيزات و منابع اعم از كامپيوترها ، ديتابيس‌ها، فايل‌ها، چاپگرها و ... كاربر به هيچ عنوان نتواند اجازه دسترسي عمومي داشته باشد. يعني به هيچ كس اجازه دسترسي عمومي (Global Access) داده نشود. به عبارت ديگر به هر Subject اجازه دسترسي به Objectهايي را مي‌دهيم كه براي آن درخواست دارد براي انجام كار مشخصي كه از قبل تعريف شده است. لازم به توجه است كه اين اصل با ماهيت اينترنت كه به همه كس بصورت پيش‌فرض اجازه دسترسي عمومي به همه سرويسها را داده است، در تضاد مي‌باشد. لذا براي رسيدن به اين هدف لازم است كه زير ساخت‌هاي امنيتي را بر روي اينترنت به‌گونه‌اي شكل دهيم كه ضمن استفاده اينترنت در دسترسي‌هاي عمومي قانون"حداقل اجازه" رعايت گردد.

براي انجام اين منظور يك راه حل آن است كه هنگاميكه براي مجموعه كاربران يك شبكه سطوح دسترسي ايجاد مي‌شود، ابتدا كليه اجازه‌هاي دسترسي لغو گردد و آنگاه مورد به مورد با توجه به صلاحديد مدير سيستم (Admin)، Objectها براي Subjectها فعال كردد.

3-1-2) حسابرسي كاربران (Accountability)

از جمله محوري‌ترين پايه‌هاي مبحث كنترل دسترسي مي‌باشد. در واقع اين امكان با اضافه كردن لايه‌هايي به سازمان ITمان بوجود مي‌آيد، اين لايه باعث مي‌گردد كه اطلاعات هر گونه دسترسي يك Subject و اقدام بر روي يك Object بر روي سيستم ذخيره(log) گردد. در نتيجه مدير سيستم ميتواند با مراجعه به اين فايل ثبت وقايع (Log File) بررسي نمايد كه آيا Subjectها در مجموعه شرايط و قوانين امنيتي مورد نظر مدير سيستم عمل كرده‌اند يا خير.

اين عمل به خودي خود در صورتي كه كاربران از آن اطلاع داشته باشند، باعث كاهش تخلفات در سيستم مي‌گردد.

فرآيند حسابرسي در اصل با يك عمل شناسايي (Identification) هويت Subject آغاز مي‌گردد. در اين مرحله كاربر با ارايه كلمه عبور و رمز عبور و يا بهره‌گيري از كارتهاي هوشمند(Smart Card) كه در آن اطلاعات مربوط به هويت صاحب آن مي‌باشد، خودش را به سيستم معرفي مي‌كند.

3-1-3) كنترل Objectها

در واقع جهت كنترل در محيطهاي فنآوري اطلاعات 3 لايه داريم:

- كنترل دسترسي فيزيكي (Physical Access Control)
- كنترل دسترسي اجرايي (Administrative Access Control)
- كنترل دسترسي منطقي (Logical Access Control)

و بطور كلي هدف جلوگيري و امن سازي يك Object توسط تهديدات مي‌باشد.

در كنترل دسترسي به روش فيزيكي هدف ايجاد حدود دسترسي‌ها به منابع (عمدتا سخت‌افزاري) مي‌باشد. اين روش مشابه انواع روش‌هاي ممانعت فيزيكي ورود و خروج افراد به محيط و سازمان مي‌باشد(استفاده از ديوار ، قفل در، و يا فنس‌كشي). مثلا در مراكز حياتي IT كه اطلاعات بانكي نگه‌داري مي‌شود يا مراكز صدور گواهي ديجيتال، آيين‌نامه‌هاي مشخص و پيچيده‌اي براي ورود از يك اطاق به اطاق ديگر وجود دارد. بطور مثال از سيستمهاي شناسايي به روش زيست‌سنجي (بيومتريك) مثلا اثر انگشت استفاده مي‌گردد. و يا كابل‌هاي انتقال اطلاعات را از هرگونه برونداد يا شنود توسط مهاجمين محفوظ گردد.

اما در بحث كنترل دسترسي اجرايي، تكيه بر سياستها (Policy) مي‌باشد كه براي امنيت سازمان تعريف گرديده و مدير سيستم (Admin) بر اساس اين قوانين سطوح دسترسي هر فرد از سازمان را به اطلاعات، معين مي‌نمايد. و يا اينكه در استخدام افراد براي اينگونه محيطها بايستي ملاحظات امنيتي مورد توجه قرار گيرد. همچنين توجه به آموزشهاي لازم امنيتي در اين محيطها در حوزه كنترل دسترسي اجرايي قرار مي‌گيرد.

در بحث كنترل منطقي تكيه بر تكنيك‌هاي فني و مهندسي است. يعني با بهره‌گيري از روشهاي مهندسي بتوانيم اطلاعات سازمان‌مان را از دسترسي‌هاي بدون مجوز محفوظ نگه داريم.

در بخش كنترل دسترسي منطقي 3 روش مهندسي مورد استفاده قرار مي‌گيرد:

1- محدود سازي دسترسي به Object ها (Object Access Restriction)
2- رمزنگاري (Encryption)
3- معماري دسترسي شبكه‌اي تفكيك شده (Network Architecture/Segregation)

در بخش اول (محدود سازي دسترسي به Object ها) هدف ايجاد محدوديت براي دسترسي به يك Object توسط Subject هاي مختلف مي‌باشد. يعني تنها Subjectهايي كه در يك فرآيند شناسايي (Authentication) احراز هويت گرديده‌اند و بر اساس رويه‌هاي امنيتي سيستم اجازه و حد دسترسيشان به منابع تاييد گرديده، قادر به دسترسي به Object خاصي را داشته باشند.

در بخش دوم يعني رمزنگاري هدف محرمانه كردن اطلاعات با بهره‌گيري از تكنيك‌هاي رمزنگاري مي‌باشد. با بهره‌گيري از اين روش حتي اگر فرد غير مجازي به اطلاعات سازمان ما دسترسي پيدا نمايد به دليل اينكه همه اطلاعات به صورت رمز درآمده اند، اين دستيابي برايش ثمري نخواهد داشت، چرا كه قادر به فهم آن اطلاعات نخواهد بود.

در بخش سوم (معماري دسترسي شبكه‌اي تفكيك شده)، جداسازي حداكثري در شبكه مد نظر مي‌باشد. مثلا در يك محيط نظامي كه اطلاعات بسيار محرمانه‌اي بر روي يك كامپيوتر وجود دارد، اگر ضرورتي براي حضور اين كامپيوتر در شبكه وجود ندارد، لازم نيست اين كامپيوتر حتما به محيط شبكه متصل گردد. و يا اينكه مثلا بخشهاي مختلف شبكه‌اي با توجه به اهداف آنها از همديگر جدا شوند.

2-3) انواع كنترل‌ها (Control Types)

حال در اين مرحله سوالي مطرح مي‌شود كه چطور اين كنترل‌هاي دسترسي را بكار گيريم. و يا به عبارت ديگر استراتژي كنترلي ما چگونه مي‌تواند باشد.

اصولا در اين مبحث 5 نوع استراتژي كنترلي معرفي مي‌گردد:

1- پيشگيرانه (Preventative)
2- نمايان سازي و كشف (Detective)
3- بازدارنده و تنبيه كننده (Deterrent)
4- تصحيح كننده (Corrective)
5- بازگشت و بازيابي (Recovery)

در تكنيك پيشگيرانه جلوگيري از رخداد يك حمله انجام مي‌گيرد. در واقع از ابتدا اجازه نمي‌دهيم كه يك Subject به يك Object غير مجاز دسترسي داشته باشد.

در تكنيك نمايان سازي و كشف ، استراتژي را به شكلي تعريف مي كنيم كه پس از وقوع يك حمله موفق، اولا وقوعش اعلام شود و ثانيا اينكه توسط چه كسي حمله انجام پذيرفته مشخص شود.

در روش بازدارنده و تنبيه كننده ما براي Subject مهاجم طبعاتي تعريف مي‌كنيم . مثلا در سياستهاي امنيتي تعريف مي‌كنيم كه چنانچه يك دسترسي به Object بدون اجازه انجام پذيرد، Subject مهاجم شناسايي مي‌گردد و بر اساس تصميمات سازمان كه در بخش مديريت سيستم تعريف گرديده با او (Subject متخاصم)برخورد مي‌گردد.

در روش تصحيح در واقع هدف آن است به محض بروز يك حمله بلافاصله سيستم را به وضعيت مناسب آن برگردانيم. بطور مثال فرض كنيد به سرور پست الكترونيك يك سازمان يك حمله به منظور پر كردن حجم آن انجام گرفته است. در اين روش(تصحيح سازي) براي برخورد با اين حمله ، مثلا تمام ميل باكس‌ها را پاك (Delete) مي‌كنيم، خواه اين Mail Box مربوط به افراد باشد و در آن نامه‌هاي درست باشد، و يا خواه مربوط به فرد حمله كننده باشد.

3-3) بخش‌بندي تكنيك‌هاي كنترل دسترسي

همانطور كه در صفحات گذشته مطرح گرديد بعد از انجام مرحله احراز هويت، (Authentication) و شروع مرحله ثبت وقايع و حسابداري(Accounting) ، مرحله بررسي كنترل حدود اختيارات دسترسي (Authorization) آغاز مي‌گردد. و اين بدان معنا است كه بررسي شود هر Subject اختيار دسترسي به چه Objectهايي را دارا مي‌باشد.

اين مرحله _ يعني Authorization – توسط تكنيك‌هاي كنترل دسترسي انجام مي‌پذيرد.

بدين معنا تكنيك‌هاي كنترل دسترسي را مي‌توان را مي‌توان به دو بخش تقسيم‌بندي نمود:

1) بصيرتي (Discretionary)
2) غير بصيرتي (Non Discretionary)

3-3-1) كنترل دسترسي بصيرتي (Discretionary Access Control - DAC)

در اين روش ايجاد كننده يا اصطلاحا مالك (Owner) هر Object ميتواند برروي آن Object تغييري دهد، آن را حذف كند، يا دوباره بنويسد و همينطور به ديگر Subject ها اجازه دسترسي و يا عدم دسترسي و همينطور نوع اختيارات (ديدن، تغيير، حذف، ...) را تفويظ نمايد. پس با توضيحات بالا ميتوان به اين نتيجه هم رسيد كه اين روش متكي است بر شناسايي (Identify) هر Subject.

بدين دليل اين روش با عنوان: Identity- Based Access Control نيز شناخته ميشود.

اين نوع از كنترل دسترسي بيشتر ماهيت غير متمركز دارد، يعني هر كسي كه Objectاي را ايجاد ميكند، خودش اقدام به صدور مجوز به Subjectهاي ديگر براي دسترسي به آن Object مينمايد.

اين Subject ها ميتوانند يك كاربر باشند يا در شكل عامتر آن نقش و وظيفه(Role) يك كاربر باشند. بطور مثال يك كاربر ميتواند يك مدير باشد كه در يك نقش وظيفه مدير سيستم (Admin) را ايفا مينمايد و در نقش ديگر ممكن است وظيفه بررسي و محاسبه حقوق كارمندان را انجام دهد.

براي انجام اين نوع از كنترل دسترسي بايد "ليست كنترل دسترسي" ايجاد گردد. اين ليست مطابق شكل 3-1 در بردارنده جزئياتي در خصوص اينكه چه كاربري ميتواند به چه Objectاي دسترسي پيدا كند ميباشد. بايد توجه داشت كه در اين روش Subject ميتواند يك كاربر، يا يك نقش و وظيفه، يا يك 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

شكل3-1) ليست كنترل دسترسي (Access Control List)

بايد توجه داشت اين روش كنترل دسترسي بيشتر در محيطهاي تجاري استفاده مي‌گردد.

3-3-2) كنترل دسترسي الزامي (Mandatory Access Control - MAC)

در اين روش سيستم به صورت غير متمركز نمي‌باشد. بلكه بر اساس قوانين مشخصي(Rules) كه توسط مديريت سازمان مشخص گرديده است، تعريف مي‌گردد. يعني همه بايد از تعدادي قوانين مشخص تبعيت كنند. اين روش به نام Rule-Based Access Control نيز شناخته مي‌شود. و براي اين منظور براي هر كاربر يك برچسب(Label) امنيتي توليد مي‌شود. در محيطهاي تجاري اين برچسبها بر اساس طبقه‌بندي زير انجام مي‌گيرد:

- عمومي (Public)
- حساس در سطح ديپارتمان (Sensitive)
- شخصي (Private)
- داراي مالكيت معنوي (Confidential)

همانطور كه گفته شد براي هر كدام از Subjectها و Objectها يك برچسب امنيتي اختصاص مي‌دهيم.

يك مثال از اين كاربرد در سيستمهاي فايروال (Fire Wall) مي‌باشد. همانطور كه مي‌دانيم اين سيستم‌ها يك سري قوانين مشخصي دارند. مثلا آنهايي كه در لايه IP قرار مي‌گيرند، بر اساس اطلاعاتي مانند IP گيرنده ، IP فرستنده، و ... كه به صورت قانون از قبل در آنها بارگزاري شده، تصميم مي‌گيرند كه يك اتصال بين فضاي بيرون فايروال و درون آن انجام شود يا نه. همانطور كه ملاحظه مي‌كنيد در اينجا مهم نيست كه اگر فردي مي‌خواهد به Objectاي دسترسي پيدا كند آيا مالك آن مي‌باشد يا نه ، بلكه اطلاعات مربوط به اين درخواست با قوانين مشخص تعريف شده تطابق داده مي‌شود.

3-3-3) كنترل دسترسي غير بصيرتي (Non Discretionary Access Control - NDAC)

اين روش به دو شيوه زير انجام مي‌پذيرد

- كنترل دسترسي بر اساس نقش و وظيفه (Role-Based Access Control)
- كنترل دسترسي بر اساس شبكه‌بندي(Lattice-Based Access Control)

در شيوه اول به هر مشخصه كاربر (User ID.) مجموعه‌اي از اجازه‌هاي دسترسي را صادر نمي‌كنيم بلكه بر اساس شرح خدمات هر كاربر اين كار انجام مي‌شود. در سازمانهايي كه موقعيت شغلي افراد به سرعت تغيير مي‌كند، افراد ممكن است داراي چندين مسئوليت گردند. بطور مثال در داخل يك پروژه، چندين زير پروژه در بخشهاي مختلف زماني تعريف مي‌گردد و وظايف فرد تغيير مي‌كند. پس در اين روش اجازه دسترسي بر اساس شرح وظايف كاري يك كاربر انجام مي‌پذيرد.

در شيوه دوم، از تركيب دو روش بر مبناي نقش و وظيفه (Role-Based) ، و بر مبناي قوانين (Rule-Based) استفاده مي‌شود. در اين روش براي وظيفه افراد برچسبهاي امنيتي تعريف مي‌گردد. مثلا كسي كه مدير سيستم است برچسب شخصي (Private) مي‌گيرد. لذا اين فرد اجازه دسترسي به اطلاعات سطح Private و بالطبع آن اجازه دسترسي با سطوح پايينتر امنيتي يعني Sensitive و Public را نيز دارا مي‌باشد. اما در بعضي از مواقع لازم است بر اساس سياستنامه امنيتي سازمان و قوانين پيشبيني شده در آن (Rules) ، فقط به بعضي از Objectها در سطوح پايين‌تر امكان دسترسي داشته باشد.

همانطور كه در بالا اشاره شد اين روش براي محيطهاي با تغييرات زياد و دوره‌اي در پرسنل آن (مانند محيطهاي پروژه‌اي) مناسب مي‌باشد.

4-3) تعيين هويت (Identification) و احراز و تصديق هويت (Authentication)

تاكنون در مورد نحوه Authorization مبتني بر روشهاي كنترل دسترسي مطالعه كرديم. اما قبل از اينكه يك Subject مجاز يا غير مجاز شناخته شود بايد تعيين هويت يا اصطلاحا Identify شود. يعني اسمش مورد شناسايي قرار گيرد. و سپس اين اسم احراز هويت يا اصطلاحا Authenticate گردد.

در مرحله Identification، سيستمي كه در واقع ايجاد كننده يا مالك و يا محفظه قرارگيري يك Object مي‌باشد، بر اساس تكنيكهاي موجود از Subject تقاضاي دادن اطلاعات منحصر بفردي مي‌كند كه مي‌تواند اين شناسه يك نام كاربري (User ID.) باشد يا يك كارت

هوشمند(Smart Card) باشد و يا مثلا يك نشانه (Token) باشد. پس از اين مرحله سيستم شروع به مرحله احراز هويت مي‌كند.

3-4-1) تكنيك‌هاي احراز هويت (Authentication)

روش‌هاي احراز هويت به سه نوع تقسيم مي‌گردد كه هر كدام مبتني بر يك خاصيت مربوط به Subject مي‌باشد.

- نوع اول: What You Know
كه يك اطلاع خاص منحصر بفردي است كه تنها كاربر مي‌داند. كه معمولا يك كلمه عبور (Pass Word) مي‌باشد. P/Wها يك رشته اي از كاراكترها مي‌باشند كه مي‌تواند بصورت يك سري رقم يا اصطلاحا PIN باشد يا اينكه بصورت تركيبي از اعداد و حروف باشند. معمولا يك P/W خوب داراي شرايطي است. مثل حداقل طول، تاريخ انقضاء، تصادفي، عدم انتخاب اسامي مشخص و آشكار، نگهداري محرمانه، غير قابل حدس.
از جمله نمونه‌هاي P/Wهاي ضعيف انتخاب نام همسر، فرزند، و حيواناتمان و يا انتخاب تاريخ تولد مي‌باشد.
از آنجا كه اطلاعات مربوط به P/Wها در داخل يك پايگاه داده نگه‌داري مي‌شود و هميشه امكان حمله به اين پايگاه وجود دارد، لذا اين روش احراز هويت جزء روش‌هاي ضعيف محسوب مي‌شود.
- نوع دوم: What You Have
چيز منحصر بفردي كه كاربر براي اثبات هويت خودش به همراه مي‌برد. مثل كارت هوشمند(Smart Cart) و يا يك نشانه(Token).
بايد توجه داشت در سيستم‌ها عمدتا براي بالا بردن سطح امنيتي احراز هويت از روش چند فاكتوري (Multiple Factors) استفاده مي‌شود. يعني از ميان نوع‌هاي 1 يا 2 و يا 3 حداقل از دو نوع بطور همزمان استفاده مي‌گردد. بطور نمونه در سيستم‌هاي خودپرداز بانكي از دو نوع اول(pass Word) و دوم (Smart Card) به صورت تركيبي استفاده مي‌شود.
همچنين بايد به اين نكته توجه كرد كه اگر چه استفاده از روش Multiple Factors باعث بالا رفتن سطح امنيتي سيستم مي‌شود، اما اين بدان معنا نمي‌باشد كه استفاده از دو

عنصر در يك نوع از انواع تكنيكهاي احراز هويت – مثلا استفاده همزمان از دو P/W– نيز 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 بكند.

- نوع سوم: What You Are

به معناي ويژگي‌هاي منحصر بفرد افراد مي‌باشد (ويژگي‌هاي بيومتريك افراد). در اين نوع تكنيك كه بهترين اما گرانترين روش نيز مي‌باشد، Subject كه معمولا يك عامل انساني است با توجه به مشخصات منحصر بفرد خودش شناسايي مي شود. از جمله اين مشخصات مي‌توان به تصوير عنبيه، شبكيه، اثر انگشت دست، الگوي صدا، الگوي زدن كليد در صفحات كليد، و يا امضاء فيزيكي اشاره كرد.
روش بيومتريك هم در مرحله Identification و هم در نوع سوم Authentication مي‌تواند مورد استفاده قرار گيرد.
اگر روش بيومتريك در Identification استفاده شده باشد، يعني بدون استفاده از ابزار نوع اول مستقيما از ابزار نوع سوم استفاده شده باشد، كار بسيار پيچيده مي‌گردد. چرا كه مشخصات دريافتي از دستگاه بيومتريك بايد با ديتابيس بسيار بزرگي شامل همه Subject ها مقايسه شود. به اين دليل بهتر است براي افزايش كارايي سيستم حتما از نوع اول و يا نوع دوم روشهاي احراز هويت در كنار نوع سوم احراز هويت – بيومتريك- بهره‌گيري شود.

2-4-3) خطاهاي نوع سوم احراز هويت _ بيومتريك

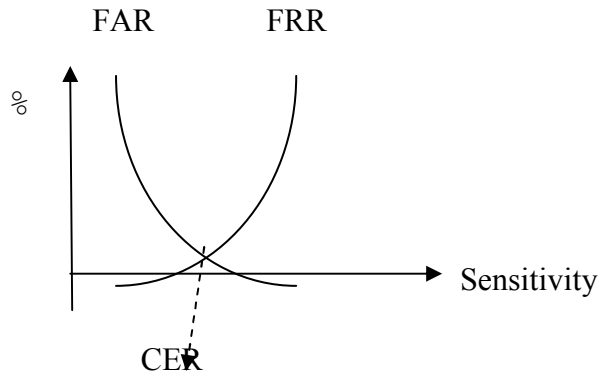
در دستگاههاي ميتني بر بيومتريك به دليل ميزان حساسيت دستگاه ما مواجه با دو نوع خطا مي باشيم:

- False Rejection Rate: يعني ميزان عدم تشخيص درست فرد داراي اعتبار براي سيستم. يعني مثلا اثر انگشت فردي كه در

سيستم به عنوان فرد معتبر مي‌باشد به دليل آلودگي محيطي تشخيص داده نشود.

- False Acceptance Rate: يعني ميزان پذيرفته شدن افراد غير معتبر به عنوان فرد معتبر در سيستم مي‌باشد. كه عمدتا بدليل كافي نبودن حساسيت سيستم مي‌باشد.

حال اگر به منحني ميزان حساسيت دستگاه بيومتريك با دو ميزان FAR و FRR توجه كنيم (شكل 3-2)، اين نكته مشهود مي‌باشد هرچه حساسيت دستگاه بالا رود FAR پايين مي‌آيد ولي در مقابل FRR بالا مي‌رود. نقطه‌اي كه اين دو (FAR و FRR) برابر شوند، آن نقطه به عنوان Crossover Error Rate شناخته مي‌شود، كه ملاكي است براي اندازه‌گيري اين نوع از دستگاه‌ها.



شكل 3-2) ميزان حساسيت حساسيت دستگاه‌هاي بيومتريك

3-5) روشهاي پياده‌سازي احراز هويت

براي پياده‌سازي احراز هويت معمولا از سه روش به شرح زير استفاده مي‌شود:

- متمركز (Centralized)
- غير متمركز (Decentralized)
- تركيبي (Hybrid)

در روش اول يعني روش متمركز، عمليات احراز هويت بطور متمركز بر روي يك سرور انجام مي‌پذيرد. حسن اين روش آنست كه چون كليه احراز هويت براي دسترسي به Objectها در يك نقطه واحد انجام مي‌گيرد، مديريت آن براحتي انجام مي‌گيرد. و ضعف اين روش در زماني است كه امنيت آن سرور دچار اخلال شود، آنگاه امنيت كل

سيستم مختل مي‌شود. ضعف ديگر آن اين است كه در صورت بالا رفتن بار كاري كارايي اين سرور پايين آيد، سرعت كل سيستم مختل مي‌شود. و مشكل ديگر مساله نقطه خرابي واحد يا باصطلاح Single Point of Failure است، يعني در صورت خرابي اين سرور كل سيستم از كار مي‌افتد.

در روش دوم يعني روش غير متمركز، در واقع عمل احراز هويت از راه دور مي‌باشد. مثلا وقتي از بيرون يك سازمان بخواهند عمل احراز هويت انجام دهند و به سرورهاي مختلف آن سازمان دسترسي پيدا كنند، معمولا از اين روش استفاده مي‌كنند. در اين شكل از كار معمولا مديريت دسترسي در نزديكي Object هاي مورد كنترل اعمال مي‌شوند نه در مركز اصلي IT سازمان. بطور مثال اگر دانشجويان نتايج كنكور را از سايت ببينند، عمل احراز هويت بر روي سرور نتايج كنكور انجام مي‌گيرد نه بر روي سرور كل سازمان سنجش. در اين روش چون در ذات خودش حالت توزيع شوندگي دارد، لذا نياز به يك هارموني يا هماهنگي بين سرورهايي كه بصورت مشترك عمليات احراز هويت را انجام مي‌دهند دارد، كه اين خود عاملي است براي افزايش پردازش‌هاي لازم (Overhead).

در روش سوم يعني روش تركيبي، در واقع هدف استفاده از مزاياي دو روش قبلي بطور همزمان مي‌باشد. براي بعضي از منابع حياتي سيستم مثل فايل‌هاي مهم و ديتابيس‌هاي فيزيكي بهتر است از روش متمركز استفاده شود. و براي ساير Objectها كه از حساسيت كمتري برخوردار هستند مي‌توان از روش غير متمركز استفاده كرد.

6-3) تكنيك‌هاي كاربردي براي مقابله با حملات عليه سيستم كنترل دسترسي

در اين قسمت دو طرح اصلي را مورد بررسي قرار مي‌دهيم:

- Monitoring
- Intrusion Detection System (IDS)

از جمله تكنيك‌هاي مورد استفاده در مقابل حملات در سيستمهاي Authentication روش مانيتورينگ مي‌باشد. هدف اصلي كه در اين روش تعقيب مي‌گردد اين است كه در قدم اول تمامي فعاليت Subject قابل حسابرسي باشد. و در قدم دوم كه استفاده امنيتي دارد هدف آن

است كه كليه فعاليتهاي غير مجاز و تلاش براي نفوذ در سيستم و يا خرابكاري آن مورد شناسايي قرار گيرد. مانيتورينك بسيار وابسته به دو مبحث ثبت وقايع (Log) و حسابرسي (Auditing) مي‌باشد. در بخش ثبت وقايع كليه فعاليتهاي مهم قبل شروع يك نشست – مثل فعاليت درخواست شده توسط يك كاربر – در فايلي ثبت مي‌گردد. معمولا در فايلهاي ثبت وقايع، رخدادهاي مربوط به سه بخش : سيستم، برنامه كاربردي، و كاربر ثبت و ضبط مي‌گردد.

اما در مبحث IDS هدف جستجو و بازرسي در فايلهاي ثبت شده و همچنين اتفاقاتي كه بصورت زنده در سيستم در حال انجام مي‌باشد بمنظور شناسايي تلاشهاي نفوذگران به سيستم مي‌باشد. در سيستمهاي كشف نفوذگر (IDS) معمولا دو شكل معرفي مي‌گردد:

- بخشي از شبكه را بطور كامل تحت سرويس‌هاي امنيتي خود قرار دهد.
- تنها ماشين و يا Host خاصي را كه عمليات با حساسيت بالايي را انجام مي دهد، تحت پوشش سيستم كشف نفوذگر قرار دهد

3-6-1) سرويس‌هاي اصلي IDS

خدماتي كه يك IDS در مقابل نفوذگران مي‌دهد به سه دسته تقسيم مي‌شود:

- فعال (Active)
- غير فعال (Passive)
- مركب (Hybrid)

در نوع فعال سيستم هاي كشف نفوذ، بلافاصله بعد از شناسايي يك نفوذ و تجاوز (Violation)، با استفاده از سياستهاي امنيتي يك اقدام و واكنش جدي صورت مي‌گيرد. مثلا اگر IDS متوجه شود يك مجموعه از حملات DoS براي يك سرور در داخل شبكه تحت پوشش تدارك ديده شده، بلافاصله مي‌تواند آن ارتباط را قطع كند.

اما در نوع دوم IDS كه به عنوان روش غير فعال شناخته مي‌شود، در صورت انجام چنين اتفاقي واكنش سريعي انجام نمي‌گيرد و IDS فقط اين رخداد را در فايل اتفاقات (Log File) ثبت مي‌كند تا بعدا مدير سيستم بر اساس اطلاعات ثبت و ضبط شده تصميمات لازم را اتخاذ نمايد.

اما در نوع سوم IDS يعني روش تركيبي، هر دو كار بطور همزمان انجام ميگيرد. يعني هم اتفاقات ثبت و ضبط ميشود و هم عكس‌العمل مناسب انجام ميگيرد.

2-6-3) نحوه شناسايي فعاليت‌هاي غير مجاز (Intrusion Detection Methods)

شناسايي فعاليت‌هاي غير مجاز در سيستم‌هاي IDS به دو طريق انجام ميگيرد:

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

در روش مبتني بر نشانه ما از قبل براي وقوع حملات سناريوهايي را در نظر ميگيريم. مثلا مدير امنيت سيستم تجسم ميكند كه اگر فردي بخواهد به فايل حاوي رمزهاي عبور(Pass Word) حمله كند چه كارهايي را انجام خواهد داد و از چه راههايي خواهد گذشت. و براي اين سناريوي حمله يك سري نشانه را براي ورودي IDS قرار ميدهد. آنگاه زماني كه IDS متوجه ميشود كه يك كاربر رفتار نامناسب انجام ميدهد، اطلاعات مربوط به رفتار كاربر را با اطلاعات درون ديتابيسي كه حاوي ترتيب رفتاري نامناسب ميباشد و از قبل تدارك ديده شده است، مطابقت ميدهد. و در صورت بروز تطابق مشخص ميشود كه حمله‌اي تدارك ديده شده و يا در حال تدارك است، آنوقت IDS به صورت اتوماتيك پيغام هشداري براي يك عكس‌العمل مناسب (فعال، غير فعال، و يا تركيبي) ميفرستد.

اما در شكل دوم يعني مبتني بر رفتار ، رفتارهاي كاربران را در طي دورانهاي زماني شناسايي و دسته‌بندي ميكنند. بدين شكل الگوهاي رفتاري هر كاربر مجاز به دست آمده و در درون ديتابيس نگه داري ميشود. و در صورتي كه يك كاربر رفتار متفاوت با الگوهاي شناسايي شده رفتاريش انجام دهد، معلوم ميگردد كه اين فرد كه خود را به عنوان يك كاربر مجاز معرفي كرده، همان فرد مجاز نمي باشد، بلكه يك نفوذگر ميباشد.

روش مبتني بر رفتار گاهي اوقات با نام Expert System هم معرفي ميگردد.

فصل چهارم: مقدمه‌اي بر رمزنگاري (Cryptography)

مقدمه

تاكنون امنيت را از مجموعه سرويس‌هايي مانند كنترل دسترسي، احراز هويت، در دسترس بودن معرفي كرديم و متوجه شديم كه چطور با تكنيك‌هايي مانند مانيتورينگ و سيستمهاي كشف نفوذ مي‌توانيم امنيت سيستم را در مورد اين سرويس‌هاي پايه بهبود بخشيم. در ادامه در اين فصل به موضوع رمزنگاري مي‌پردازيم.

به طور سنتي ورود به مبحث امنيت از طريق رمزنگاري بوده است، وليكن اين مورد به نوعي باعث خلط مبحث از منظر بسيار از كارشناسان و مديران شده است. اين دو مقوله نزديك به هم ولي متفاوت از هم مي‌باشند. در واقع رمزنگاري يكي از سنگ‌هاي زير بنايي امنيت اطلاعات مي‌باشد.

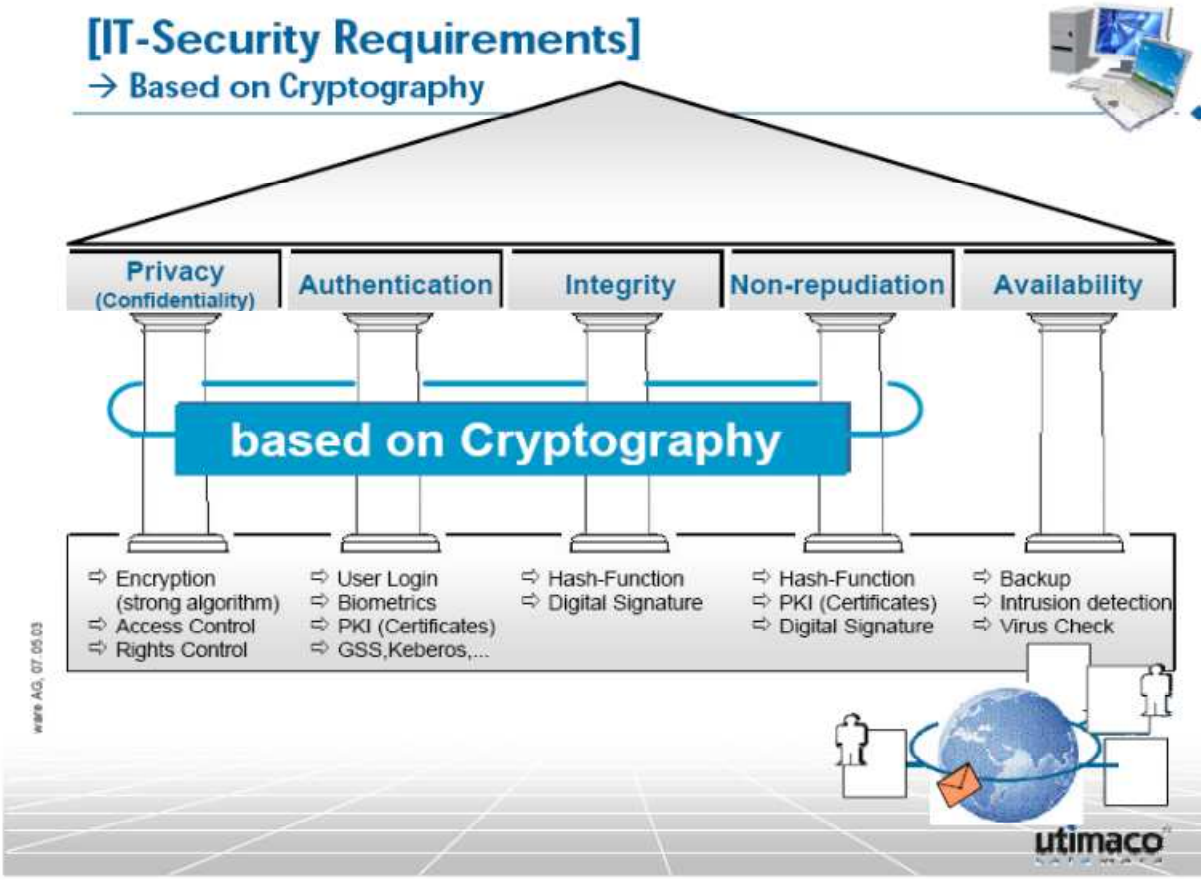
گسترش و رشد بي سابقه اينترنت باعث ايجاد تغييرات گسترده در نحوه زندگی و فعاليت شغلی افراد ، سازمانها و موسسات شده است . امنيت اطلاعات يكی از مسائل مشترك شخصيت های حقوقی و حقيقی است . كاربران اينترنت در زمان استفاده از شبكه، اطلاعات حساس و مهمی را بدفعات ارسال و يا دريافت می دارند. اطمينان از عدم دستيابی افراد غير مجاز به اطلاعات حساس از مهمترين چالش های امنيتی در رابطه با توزيع اطلاعات در اينترنت است. اطلاعات حساس كه ما تمايلی به مشاهده آنان توسط ديگران نداريم ، موارد متعددی را شامل می شود. برخی از اينگونه اطلاعات بشرح زير می باشند:

- اطلاعات كارت اعتباری
- شماره های عضويت در انجمن ها
- اطلاعات خصوصی
- جزئيات اطلاعات شخصی
- اطلاعات حساس در يك سازمان
- اطلاعات مربوط به حساب های بانكی

تاكنون برای امنيت اطلاعات بر روی كامپيوتر و يا اينترنت از روشهای متعددی استفاده شده است. ساده‌ترين 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 صرفا" افرادیکه دارای کلید رمز می باشند، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند.

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



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

همانطور كه در شكل 4-1 مشاهده مي‌شود امنيت در محيطهاي فن‌آوري اطلاعات به مثابه يك ساختمان مي‌باشد و سرويس‌هاي پايه‌اي لازم براي ايجاد امنيت در محيطهاي فن‌آوري اطلاعات مانند احراز هويت، صحت اطلاعات ، انكار ناپذيري، و محرمانگي مي‌توانند بر اساس رمز نگاري اجرا گردند.

به طور ساده مي‌توان گفت رمزنگاري عبارت است از انجام محاسبات بر روي متن داده‌اي ورودي به منظور تبديل كردن آن به يك متن غير واضح و غير قابل آشكارسازي توسط افراد غير مجاز.

در اين فصل در ابتدا نكاتي در مورد تاريخچه رمزنگاري، مفاهيم اوليه رمزنگاري، و حملات محتمل بر سيستم‌هاي رمزنگاري مطرح كرده ، و در امتداد مروري كوتاه بر الگوريتم‌هاي رمزنگاري خواهيم داشت، و در انتها فصل را با توضيح مختصري از زيرساخت‌هاي كليد عمومي به پايان خواهيم برد.

4-1) تاريخچه رمزنگاري

علم رمزنگاري داراي سابقه‌اي طولاني است. شايد بتوان گفت اولين سيستم رمز نگاري سيستمي باشد كه توسط ژوليت سزار(پادشاه رم باستان) در جنگهاي بيش از دو هزار سال قبل مورد استفاده قرار داده شده است. در اين روش رمز نگاري الفباي رومي را 3 حرف به سمت راست مي‌چرخاندند. (مانند شكل 4-2) .

و دانش رمزنگاري در طول زمان گسترش يافت بطوريكه در طول جنگ جهاني دوم از آن بصورت گسترده‌اي استفاده گرديد.

متن رمزشده	متن اصلي
DEF	ABC
Khoor	Hello
Dwwdfn	Attack

شكل 4-2) روش رمزنگاري سزار

مانند بقيه علوم، دانش رمزنگاري هم توسط نيروهاي مسلح به ويژه در هنگام جنگها پيشرفت قابل ملاحظه‌اي داشته است. در

زمان سزار به طور سنتي در طي سال‌ها از سيستم رمزي كه به‌صورت جايگشتي عمل مي‌كرده است استفاده شده است

2-4) مفاهيم رمزنگاري

در دانش رمزنگاري از مفاهيم پايه‌اي به كرات استفاده مي‌گردد كه برخي از آن عبارتند از:

متن واضح(Plain Text)

آن پيغام يا داده اوليه است كه به سهولت قابل خواندن است.

متن رمزشده (Cipher Text)

بعد از انجام يك عمل رمزنگارانه متن واضح اوليه را به يك متن رمز شده تبديل مي‌كنيم. اين متن (متن رمز شده) تنها زماني قابل خواندن است كه توسط الگوريتم رمزگشايي از حالت رمز خارج گردد. بايد توجه داشت كه كه الگوريتم رمزنگاري و الگوريتم رمزگشايي بايد با هم رابطه داشته باشند، به گونه‌اي كه بتوان با داشتن اطلاع خاصي (كه معمولا از آن به عنوان كليد ياد مي‌شود) بتوان متن رمز شده را به متن واضح برگرداند.

رمزنگاري (Cryptography)

به فرآيندي كه در آن متن واضح با اعمالي همچون آرايش مجدد، و يا جايگزين كردن علامت، كاراكتر يا نشانه و يا علامت ديگري، از حالت قابل خواندن به متن غير قابل خواندن تبديل مي‌شود، رمز نگاري اطلاق مي‌گردد.

الگوريتم (Algorithm)

عبارت است از قدم‌هاي متوالي و از پيش تعيين شده‌اي كه بر روي متن واضح انجام مي‌شود و در خروجي آن متن رمز شده حاصل مي‌گردد. بايد توجه داشت كه اين تعريف شامل الگوريتم‌هاي رمزگشايي (Decryption) هم مي‌شود، يعني آنكه متن رمز شده را به الگوريتم رمزگشايي مي‌دهيم و الگوريتم مي‌تواند متن واضح را ايجاد كند.

كليد (Key)

يك تفاوت عمده بين الگوريتم‌هاي رمزنگاري و الگوريتم‌هاي متعارف كدينگ در بهره‌گيري الگوريتمهاي رمزنگاري از كليد است. در واقع بخش عمده‌اي از الگوريتم‌هاي متعارف رمزنگاري ارايه و منتشر (Publish) شده‌اند. يعني همه مي‌دانند كه ساختار و نحوه انجام عمل الگوريتم (مثلا الگوريتم‌هاي DES و RSA) به چه ترتيبي مي‌باشد، و اينكه اين الگوريتم‌ها در طي چه مراحلي يك متن واضح را مي‌گيرند و به يك متن رمزنگاري تبديل مي‌كنند و همينطور بالعكس. اما با اين توصيفات چرا اين متن رمز شده توسط افراد غير مجاز قابل خواندن نمي‌باشد، در حاليكه فرد غير مجاز هم ممكن است الگوريتم را بداند؟ دليل اين موضوع مفهوم كليد است. در واقع هر الگوريتم به‌ازاي كليد متفاوت خروجي متفاوتي توليد مي‌كند.

نكته بسيار مهم در بحث رمزنگاري مديريت كليد است، به‌نحوي كه كه اطلاعات به سادگي افشا نگردد. بالاخص در محيطهاي تجارت الكترونيك و دولت الكترونيك نمي‌توان به سمت الگوريتم‌هاي خاصي كه در صنايع نظامي است و توسط افراد خاص استفاده مي‌شود رفت. در اين چنين محيطهايي بايد سراغ الگوريتم‌هاي منتشر شده رفت. و لذا آنچيزي كه به صورت محرمانه و مخفي بين طرفهاي مجاز جابجا مي‌شود كليد است.

4-3) انواع حملات به سيستم‌هاي رمزنگاري

حمله عبارت است از هر نوع تلاشي كه توسط مهاجم انجام مي‌گيرد كه فضاي جستجو را در بين متن‌هاي واضح براي يك متن رمز شده و يا در بين تمام فضاي جستجو براي كليد، محدود مي‌سازد.

بطور مثال در مورد يك كليد n بيتي تمامي حالات ممكن اين كليد مي‌تواند فضاي جستجو باشد. يعني مثلا اگر يك كليد 4 بيتي داشته باشيم، حمله كننده مواجه با يك فضاي جستجوي $2^4 =16$ تايي است. لذا هر چه تعداد بيت‌هاي كليد اضافه شود فضاي جستجوي مهاجم به روش نمايي اضافه مي‌شود.

اما در واقع اين روش جستجو و حمله براي كليد ساده‌ترين شكل مي‌باشد و به نام جستجوي فراگير(Exhaustive Search) ناميده مي‌شود. معمولا براي حمله به يك سيستم رمزنگاري از انواع تكنيك‌هاي زير استفاده مي‌شود.

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

در اين خانواده از حملات فرد مهاجم فقط يك متن رمز شده دارد و از روي آن مي‌خواهد كليد استفاده شده براي رمزنگاري را بدست آورد. در اين حالت به‌طور طبيعي براي حمله كننده اطلاع خاصي وجود ندارد و بايد سراغ روشهاي جستجوي فراگير(Exhaustive Search) برود.

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

در اين روش حمله فرد مهاجم يك متن واضح و يك متن رمز شده متعارف با آن را دارد. پس در اين حالت به نوعي مي‌تواند تشخيص دهد چه كاراكتري از متن واضح به چه كاراكتري از متن رمز شده مبدل گرديده است. در اين روش هدف مهاجم مشخص سازي كليد مي‌باشد. اين روش نسبت به روش قبلي(فقط متن رمز شده) داراي فضاي جستجوي كمتري است.

4-3-3) متن واضح انتخاب شده (Chosen Plain text)

در اين روش مهاجم اين امكان را دارد كه براي تعدادي متن واضح كه در اختيار دارد، متن رمز شده آن را توليد كند. در اين روش نيز هدف مهاجم مشخص كردن كليد است. مثالي براي اين روش آن است كه مثلا فرد مهاجم منشي و يا كارمند يك دفتر است و يا دشمن در اين دفتر جاسوس دارد، و از طريق اين جاسوس مي‌تواند با دستگاه رمزنگاري اين دفتر كار كند ولي نمي‌تواند كليد را تغيير دهد و يا تنظيم كند و يا بخواند و فقط مي‌تواند به دستگاه رمزنگاري متن واضح را وارد كند و متن رمز شده را بدست آورد.

در اين روش فرد مهاجم اين امكان را دارد كه دائما تحليل كند و الگوهاي واضح مورد نظر خودش را توليد كند و براي نزديك شدن به كليد آنها را به دستگاه رمزنگار بدهد و دستگاه رمزنگار نيز با محاسبات دروني كه انجام مي‌دهد متن رمز شده را ارائه دهد. به اين ترتيب در دفعات متوالي اطلاعات مهاجم نسبت به كليد اضافه مي‌شود. و به اين ترتيب فضاي جستجو و آناليز براي بدست آوردن كليد مرتبا براي مهاجم كاهش پيدا مي‌كند.

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

اين روش چيزي شبيه روش قبلي است با اين تفاوت كه در اين حالت فرد مهاجم مي‌تواند متون رمز شده را به دستگاه رمزگشا بدهد و متون واضح را بدست آورد(عكس روش قبلي).

4-3-5) متن انتخاب شده (Chosen text)

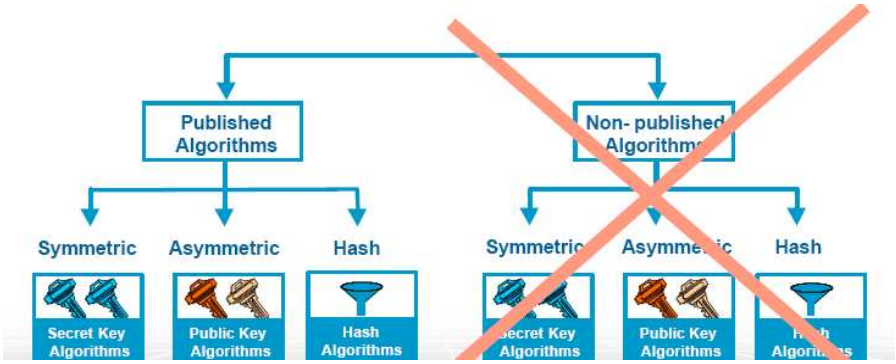
اين روش تركيب دو روش قبلي است. يعني فرد مهاجم مي‌تواند به تعداد نامحدود متن واضح به دستگاه رمزنگار بدهد و متن رمز شده بدست آورد و هم عكس عمل را انجام دهد، يعني تعدادي متن رمز شده را به‌دستگاه رمزگشا بدهد و متن واضح آن را بدست آورد. و به اين ترتيب فضاي جستجو براي بدست آوردن كليد را مرتبا كاهش دهد.

4-4) انواع الگوريتم‌هاي رمزنگاري

همانطور كه در قبل مطرح گرديد الگوريتم‌هاي رمزنگاري به دو دسته كلي تقسيم مي‌گردند:

- الگوريتم‌هاي منتشر شده (Published Algorithms)
- الگوريتم‌هاي منتشر نشده (Non-Published Algorithms)

گروه الگوريتم‌هاي منتشر شده الگوريتم‌هايي هستند كه توسط گروه‌هاي تحقيقاتي طراحي گرديده و به بازار تجاري ارائه مي‌گردد و توسط گروه‌هاي مختلف مورد آزمايش و بررسي قرار گرفته و معايب آن مرتفع مي‌گردد. در اين الگوريتم‌ها، اطلاعات مرتبط با ساختار الگوريتم، و اقداماتي كه بطور متوالي بر روي متن ورودي انجام مي‌دهد به صورت عمومي منتشر مي‌گردد.



شكل 4-3) انواع الگوريتم‌هاي رمزنگاري

اما در مقابل الگوريتم‌هاي منتشر نشده وجود دارند كه معمولا در صنايع مخابراتي و نظامي مورد استفاده قرار مي‌گيرند. بايد توجه داشت از آنجا كه اين الگوريتم‌ها براي مراكز خاصي طراحي مي‌شوند و كاربرد عمومي ندارند، ساختار اين

الگوريتم‌ها هيچگاه مورد انتشار عمومي قرار نمي‌گيرند و لذا مديريت آنها در مقابل تهاجمات آسانتر است..

همانطور كه در شكل 4-3 مشاهده مي‌گردد هدف ما در اين درس الگوريتم‌هاي منتشر شده مي‌باشد.

4-5) انواع الگوريتم‌هاي منتشر شده

الگوريتم‌هاي منتشر شده به 3 دسته كلي تقسيم مي‌شوند

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

4-5-1) الگوريتم‌هاي متقارن (Symmetric Algorithms)

الگوريتم متقارن يا الگوريتم كليد خصوصي (Secret Key Algorithm) الگوريتمي است كه در آن كليد رمزنگاري و كليد رمزگشايي در هر دو طرف گيرنده و فرستنده يا با هم برابرند، يا به سهولت توسط توابع ساده رياضي مي‌توان از روي كليد رمزنگاري كليد رمز گشايي را استحصال كرد.

4-5-1-1) الگوريتم جايگشتي

يكي از الگوريتم‌هاي متقارن الگوريتم جايگشتي (Transposition Algorithm) مي‌باشد. كه در ادامه به توضيح آن مي‌پردازيم. براي توضيح اين موضوع مي‌توان به شكل 4-4 توجه كرد.

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

شكل 4-4) مثالي از الگوريتم جايگشتي

فرض كنيد متن واضحي بدين شكل داريم : "I LIKE LEARN KEY"

و مي‌خواهيم توسط كليد خصوصي "ISAAC" اين متن واضح را به متن رمز شده تبديل كنيم.

با توجه به اين كه كليد خصوصي ما پنج حرفي است، جدولي با 5 ستون تشكيل مي‌دهيم و حروف كليد خصوصي‌مان را در سطر اول جدول قرار مي‌دهيم و آنگاه در سطر دوم جدول شماره هر كدام از حروف مربوط به كليد را با توجه به جايگاه آن در حروف الفبا قرار مي‌دهيم. در ادامه كليه حروف مربوط به متن واضح را در خانه‌هاي مختلف جدول مي‌چينيم. حال براي بدست آوردن متن رمز شده، ابتدا نگاه مي‌كنيم به ستون با كمترين شماره. اين ستون در اين جدول ستون شماره 3 مي‌باشد، آنگاه حروف مربوط به ان ستون را پشت سر هم قرار مي‌دهيم(IAY). ستون بعدي ستون شماره 4 مي‌باشد(KR)، دقت كنيد كه با توجه به آگاهي از طول متن واضح از اينكه آخرين خانه اين ستون خالي است مطلع مي‌باشيم. در ادامه نوبت حروف ستون 5 مي‌باشد(EN) و بعد ستون شماره 1 (ILK) و در نهايت ستون 2 (LEE).

در نهايت متن رمز شده روبرو به‌دست مي‌آيد: IAYKR ENILK LEE

حال بطور معكوس در طرف گيرنده براي تبديل متن رمز شده به متن واضح، مجددا اين جدول را داريم. در اين جدول 2 سطر اول باز براي طرف گيرنده مشخص است. يعني طرف گيرنده به كليد (ISAAC) آگاهي دارد، و بر اين اساس مي‌تواند شماره ستون‌ها را بچيند(توجه كنيد كه كليد ISAAC كه يك كليد متقارن مي‌باشد بين دو طرف گيرنده و فرستنده محرمانه مي‌باشد و فرد ديگري نسبت به آن اطلاع ندارد. حال بعد از چيدن حروف كليد در جدول، گيرنده شروع مي‌كند به چيدن حروف در ستون شماره 3، كه سه حرف مي‌باشد. دقت كنيد با توجه به اينكه طول متن رمز مشخص مي‌باشد، گيرنده مي‌تواند تشخيص دهد تعداد سطرهاي جدول چه ميزان است، پس به سادگي مي‌تواند تعداد سلول‌هاي خالي را تشخيص دهد. و در ادامه مابقي حروف را نيز در جدول قرار مي‌دهد. در نهايت براي بدست آوردن متن واضح به جاي آنكه آن‌را ستوني بخواند به صورت سطري مي‌خواند.

4-5-1-2) الگوريتم جانشيني

نوع ديگر الگوريتم‌هاي متقارن الگوريتم مبتني بر جانشيني(Substitution) مي‌باشد. كه در ادامه به توضيح اين روش خواهيم پرداخت.

در الگوريتم جانشيني بطور كلي هر حرف مربوط به متن واضح را با يك مقدار حرف جديد جايگزين مي‌كنيم. در واقع ما به جدولي نياز داريم كه در آن جدول مشخص مي شود كه بازاي هر كاراكتر چه كاراكتري بايد جايگزين شود. مثال ساده آن الگوريتم رمز سزار يا روتيشن 3 بود كه در گذشته از آن سخن به ميان آورديم. در اين نوع رمزنگاري هم فرستنده و هم گيرنده از يك جدول جانشيني (Substitution Table) استفاده مي‌كنند كه اين جدول است كه بايد به صورت محرمانه بين اين دو باقي بماند. بايد توجه داشت كه اين دست از الگوريتم‌ها در ذات خود به صورت تئوريك قابل شكستن مي‌باشند.

اما يك الگوريتم جانشيني كه در ذات خود به صورت تئوريك غير قابل شكستن است الگوريتم One-Time-Pad (OTP) مي‌باشد. اين الگوريتم مبتني بر اعداد واقعا تصادفي مي‌باشد. در اين الگوريتم ما يك جدول خواهيم داشت و در اين جدول يك تعداد حرف را بصورت تصادفي توليد مي‌كنيم و اين حروف به مجموعه‌اي از حروف جديد نشانه‌گذاري مي‌شوند. در اين روش پيغام را رمز كرده و ارسال مي‌كنيم و طرف گيرنده عمل عكس را انجام مي‌دهد. دقت كنيد چون در هر بار عمل رمزنگاري يك OTP جديد توليد مي‌كنيم، پي بردن به اين OTPها كه بصورت كاملا تصادفي ايجاد مي‌گردد براي حمله كننده غير ممكن مي‌باشد. پس در اين روش كانال ارسال اين OTPها بين گيرنده و فرستنده بايد كاملا امن باشد ولي متن رمز شده مي تواند از كانال نا امن نيز ارسال گردد.

يكي ديگر از الگوريتم‌هاي جانشيني، رمز جانشيني ويگنر Substitution (Cipher-Vigenere) مي‌باشد كه به شكلي رمز چند الفبايي است. بدين معني كه به‌ازاي هر كاراكتر در متن واضح چندين كاراكتر به عنوان كاراكتر رمز شده قرار مي دهيم و به اين دليل حمله كننده ديگر با حملاتي مثل حملات تكرار و تعداد كاراكترهاي رمز شده در متن رمز شده به اطلاعات متن واضح دسترسي پيدا كند.

همانطور كه در شكل 4-5 مشهود است جدول ويگنر جدولي است كه در اولين سطر آن حروف انگليسي به ترتيب الفبا و در هر سطر يك حرف الفباي انگليسي به سمت راست شيفت پيدا كرده است. روش كار براي به رمز درآوردن متون واضح بين فرستنده و گيرنده متن با بهره‌گيري از اين جدول بدين شكل است كه اين جدول به‌صورت ثابت بين گيرنده و فرستنده تبادل شده است. ارسال كننده اطلاعات يك متن را به عنوان كليد در نظر گرفته و تلاش مي‌كند

اين متن را به تعدادي كه كل حروف متن واضح را پوشش دهد در زير متن واضح تكرار كند بطور مثال فرض كنيد متن واضح جمله: "ATTACK AT DOWN" باشد و متن كليد كلمه "SECRET" باشد. پس متن جمله واضح و جمله كليد به شكل زير مي‌باشد:

متن واضح: ATTACKATDOWN

متن كليد: SECRETSECRET

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

شكل4-5) جدول جانشيني ويگنر

حال مي‌خواهيم طبق جدول حروف متن واضح را به حروف رمز درآوريم. همانطور كه مي‌بينيم اولين حرف ما در متن واضح حرف "A" مي‌باشد، و اولين حرف مطابق با آن در متن كليد حرف "S" مي‌باشد. طبق جدول مكان تلاقي ستوني كه با حرف "A" شروع شده و سطري كه با "S" شروع شده پيدا مي‌كنيم. مي‌بينيم كه محل تلاقي اين سطر و ستون حرف "S" است، پس اولين حرف جمله رمز ما حرف "S" مي‌شود. بهمين ترتيب حرف دوم متن واضح ما حرف "T" و دومين حرف جمله كليد حرف "E" مي‌باشد كه محل تلاقي ستون وسطر مربوطه در

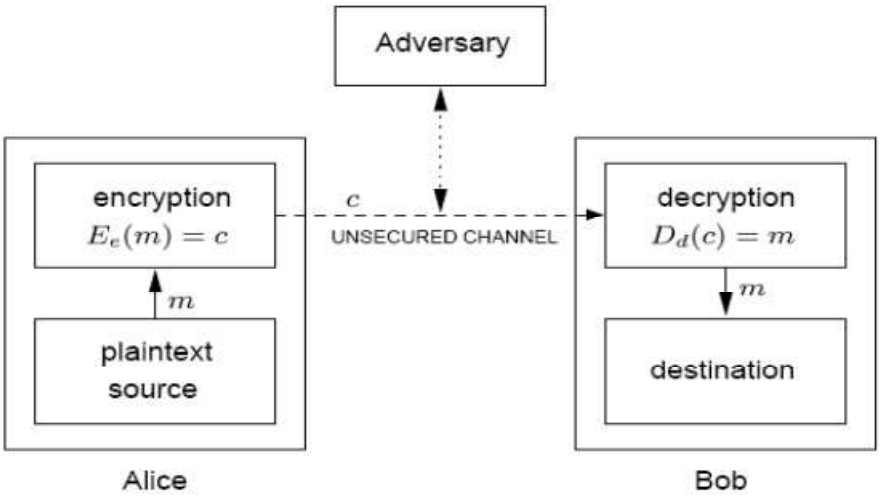
جدول حرف "X" مي‌باشد كه دومين حرف جمله رمز شده ما مي‌شود. و به همين ترتيب مراحل را براي ديگر حروف متن واضح به‌انجام مي‌رسانيم. متن رمز شده نهايي به شكل زير است:

متن رمز شده : s x v r g d s x f r a g

همانطور كه در روش‌هاي رمزنگاري كه تاكنون بيان گرديد مشاهده كرديد يكي از محدوديت‌هايي كه باعث مي‌شود سطح اعتماد روش رمزنگاري پايين بيايد طول كليد است. به‌صورت كلي هرچه طول كليد كمتر باشد افراد مهاجم با عمليات ساده‌تري را براي شناسايي كليد رمزنگاري و شكستن رمز مواجه هستند.

اين نكته حائز اهميت مي‌باشدكه روش‌هاي رمزنگاري كه تاكنون مطرح گرديده است مبتني بر رمزنگاري رشته‌اي بودند. در واقع در اين روش رمزنگاري هر بيت اطلاعات بطور جداگانه مورد پردازش قرار مي‌گيرند. اما نوع ديگر روش‌هاي رمزنگاري مبتني بر بلوكي از بيت‌ها مي‌باشند. در اين روش يك بلوك از بيت‌هاي متن واضح با يك بلوك از بيت‌هاي متن كليد در طي پردازشهايي متن رمز شده را توليد مي‌كنند. لذا تغيير در يك بيت متن واضح تغييرات گسترده‌اي را در متن رمز شده ايجاد مي‌كند.

بطور كلي عمل رمزنگاري را مي‌توان مطابق شكل 4-6 توصيف كرد



شكل 4-6) مدل رمزنگاري

همانطور كه در شكل بالا مشهود است فرستنده‌اي به نام Alice در صدد ارسال پيام به سمت گيرنده‌اي به‌نام Bob مي‌باشد. فرستنده متن واضحي را از منبع متون واضح خودش مثل m انتخاب مي‌كند.

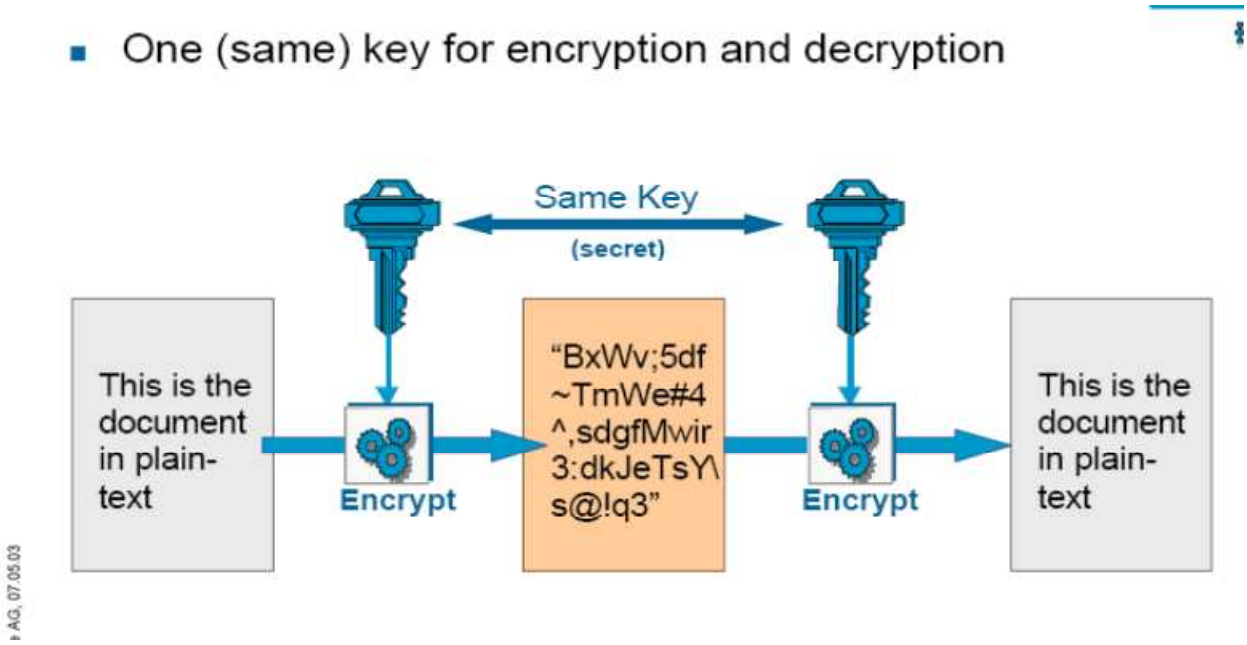
آنگاه يك تبديل رمزنگارانه مبتني بر كليد e را بر رويش انجام مي‌دهد. نتيجه متن رمز شده c مي‌باشد كه فرستنده مي‌تواند از طريق كانال ناامني براي گيرنده ارسال نمايد. گيرنده نيز با دريافت متن رمز شده c و اعمال الگوريتم رمزگشايي مبتني بر كليد d به متن واضح m دست پيدا مي‌كند. همانطور كه در شكل مشهود است دشمنان و رقبا به كانال لرسال متن رمز شده دسترسي دارند ولي بدليل آنكه متن رمز شده مي‌باشد، امكان استفاده از آن برايشان مقدور نمي‌باشد. توجه نماييد كه اين نوع از رمز نگاري مبتني بر زوج كليد مي‌باشد.

حال در ادامه نحوه عملكرد الگوريتمهاي رمزگذاري متقارن را بيشتر توضيح مي دهيم.

4-5-1-3) توضيحات تكميلي در مورد الگوريتم‌هاي رمزگذاري متقارن

اين الگوريتم ها، الگوريتم هاي كليد مخفي (secret Key Algorithm) نيز ناميده مي شوند. در اين الگوريتم، كليد رمزنگاري و كليد رمزگشايي مشابه هم مي‌باشد، و يا اينكه به سهولت و از طريق محاسبات نسبتا ساده از روي همديگر قابل محاسبه مي‌باشند. مثلا يك كليد عكس كليد ديگر مي‌باشد.

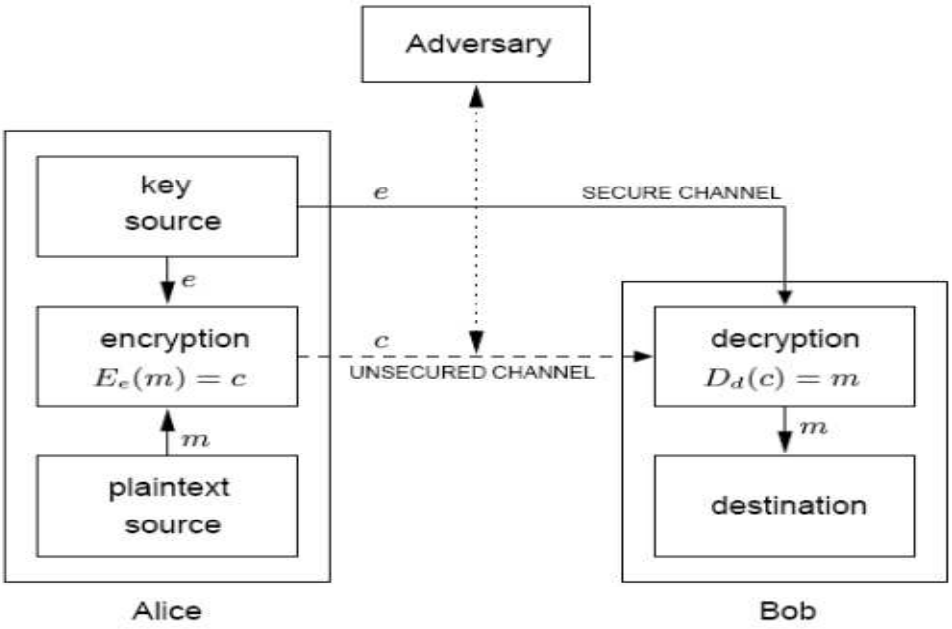
اين الگوريتم داراي نقاط ضعفي مي‌باشد، از جمله اينكه توزيع كليد بين طرفين مبادله كليد به خودي خود كاري مشكل و پر مخاطره مي باشد. و اين بدان معني است كه كليد رمز نگاري و يا رمزگشايي بايد از كانال امني انتقال يابد. مشكل ديگر اين الگوريتم ها اين است كه سرويس انكارناپذيري را پوشش نمي‌دهند. و همچنين اين نوع از رمز نگاري مقياس پذير نمي‌باشد، يعني آنكه نمي‌توان اين نوع از رمزنگاري را بصورت بلوكي و بازاي طول بلوك‌هاي مختلف انجام داد. البته در مقابل اين نقاط ضعف، اين الگوريتم ها در مقايسه با الگوريتم هاي نامتقارن، بسيار سريع هستند.



شكل 4-7) شمايي از الگوريتم رمزنگاري متقارن

همانطور كه در شكل 4-7 مشاهده مي‌شود در الگوريتم رمزنگاري متقارن گيرنده و فرستنده براي اعمال رمزنگاري و رمزگشايي از يك كليد مشابه استفاده مي‌كنند.

در شكل 4-8 روش توزيع كليد در الگوريتم متقارن به تصوير كشيده شده است. آليس به عنوان فرستنده متن با استفاده از كليد رمزنگاري e كه توسط يك توليدكننده كليد دريافت كرده، متن واضح m را به متن رمز شده c با بهره‌گيري از الگوريتم رمزنگاري E، رمزنگاري مي‌كند. بايد توجه داشت در اين راستا كليد رمز نگاري بايستي از طريق يك كانال امن به گيرنده پيام يعني باب فرستاده شود، ولي براي ارسال پيام رمز شده c، نيازي به كانال ارسال امن نمي‌باشد.



شكل 4-8) روش توزيع كليد در الگوريتم متقارن

توجه كنيد در اين روش رمزنگاري بدليل امكان لو رفتن كليد رمزنگاري، طرفين رمزنگاري بايد به صورت دوره اي كليد رمزنگاري را تغيير دهند.

مشكل ديگر در اين روش رمزنگاري اين است كه با بالا رفتن طرفين تبادل اطلاعات، تعداد كليد رمزنگاري به صورت نمايي افزايش مي‌يابد يعني اگر به جاي آنكه فقط دو نفر آليس و باب تبادل اطلاعات كنند، سه نفر به تبادل اطلاعات بين يكديگر بپردازند، آنوقت براي رمز نگاري نياز به 3 كليد رمزنگاري مي‌باشد. و به اين ترتيب با بالا رفتن نفرات، تعداد كليد افزايش پيدا مي‌كند (تعداد كليد از فرمول $n(n-1)/2$ تبعيت مي‌كند، كه در اين فرمول n تعداد نفرات مي‌باشد). بدين ترتيب حفظ امنيت كليد و مديريت اين كليدها در يك شبكه به يك كار بسيار پيچيده اي تبديل مي‌گردد.

از جمله الگوريتم هاي رمزنگاري مي‌توان به الگوريتم هاي: DES, Triple DES, AES, IDEA, Blowfish اشاره كرد. بعضي از مشخصات اين الگوريتم ها عبارتند از:

DES: داراي كليد با طول 65 بيت، تا سال 1998 استاندارد دولتي آمريكا بود. ولي امروزه به اندازه كافي قدرتمند نمي‌باشد، كه به عنوان استاندارد دولتي محسوب گردد.

Triple DES: سه بار عمليات الگوريتم DES را انجام مي‌دهد. داراي كليدي با طول 168 بيت مي‌باشد. كاربرد وسيعي دارد. نسبت به DES امن‌تر است. اما كند است.

AES: طول كليد متغير دارد. آخرين استاندارد دولتي آمريكا مي‌باشد، و جاي الگوريتم DES را گرفته است.

IDEA: داراي كليد 128 بيتي مي‌باشد. براي استفاده نياز به مجوز دارد.

Blowfish: طول كليد متغير دارد. الگوريتم آن مجاني و در اختيار عموم است. بسيار سريع مي‌باشد.

2-5-4) الگوريتم‌هاي نامتقارن (Asymmetric Algorithms)

با توجه به مشكلاتي كه در مساله توزيع كليد در الگوريتم‌هاي رمزنگاري متقارن يا مبتني بر كليد خصوصي داريم، به تدريج در دنياي رمزنگاري مبحثي به نام الگوريتم‌هاي كليد عمومي يا Public Key Algorithm و يا باصطلاح الگوريتم‌هاي نامتقارن، شكل گرفت.

در اين روش، در واقع فرستنده اطلاعات يك زوج كليد را توليد مي‌كند. يكي از كليدها مخفي و خصوصي است (Private Key)، و ديگري كليد عمومي است كه آن را در اختيار عموم افراد قرار مي‌دهد. براي انجام رمزنگاري، فرستنده اطلاعات ، متن مورد نظر خود را با كليد عمومي گيرنده متن به رمز در آورده و اين متن رمز شده را از طريق كانال ناامني براي گيرنده ارسال مي‌دارد. گيرنده هم با استفاده از كليد خصوصي خود اين متن را رمزگشايي كرده و به متن اصلي و واضح دست پيدا مي‌كند.

نكته حائز اهميت آن است كه با انتشار كليد عمومي، هكرها و كاربران غير مجاز هم قادر به آن مي‌باشند كه اطلاعاتي را رمزگذاري كرده و به سمت گيرنده ارسال دارند، و با اينكه هكر به كليد عمومي و هم به الگوريتم رمزگذاري دسترسي دارند، اما نمي‌توانند كليد خصوصي دريافت كننده پيام را كشف و شناسايي كنند.

اين نوع الگوريتم‌ها در انجام سرويس‌هاي امنيتي كاربرد وسيعي دارند. اين الگوريتم‌ها براي انجام سرويس‌هاي امنيتي محرمانگي، احراز هويت، و انكار ناپذيري، استفاده مي‌گردد. اين

الگوريتم ها در دنياي امنيت به عنوان الگوريتمهاي كليد عمومي نيز ناميده مي‌شود.

4-2-5-1) انجام سرويس محرمانگي با بهره‌گيري از الگوريتم‌هاي نامتقارن

براي تحقق سرويس محرمانگي كه هدف محرمانه نگه‌داشتن اطلاعات انتقالي بين طرفين مبادله پيغام مي‌باشد، روش انجام كار بدين شكل مي‌باشد:

كه فرد دريافت كننده پيام از قبل زوج كليد رمزنگاري را براي خود تدارك ديده است(يك كليد به عنوان كليد خصوصي و يك كليد به عنوان كليد عمومي). و اين گيرنده پيام كليد عمومي خود را براي اطلاع ديگران منتشر كرده است، مثلا آن را براي اطلاع ديگران بر روي وب سايت خود قرار داده و يا آن را طريق نشريات تبليغاتي به اطلاع ديگران رسانده است. البته لازم به توجه است كه كليد دوم يعني كليد خصوصي را تنها پيش خود بصورت محرمانه نگه داشته است. حال فرستنده پيام با آگاهي از كليد عمومي فرستنده، متن مورد نظر را با كليد عمومي گيرنده رمز كرده و از طريق كانال ناامني براي گيرنده ارسال مي‌كند. گيرنده هم با دريافت متن رمز شده با بهره‌گيري از كليد خصوصي خود، اين متن رمز شده را از رمز خارج كرده و به يك متن واضح تبديل مي‌كند. روشن است كهفرد مهاج و دشمن علي‌الرغم اطلاع از كليد رمزنگاري عمومي و دستيابي به متن رمز شدهف چون از كليد خصوصي آگاهي ندارد، قادر به اطلاح از متن واضح نمي‌باشد.

از جمله نقاط قوت اين روش اين مي‌باشد كه سرويس انكارناپذيري را پشتيباني مي‌كند، مديريت كليدها راحت مي‌باشد، چرا كه تعداد كليدها به تعداد كاربران مي‌باشد. و همچنين توزيع كليد راحت مي‌باشد. اما نقطه ضعف آن هم پايين بودن سرعت آن مي‌باشد، چرا كه ميزان محاسبات در الگوريتم هاي نامتقارن بيشتر از الگوريتم هاي متقارن مي‌باشد.

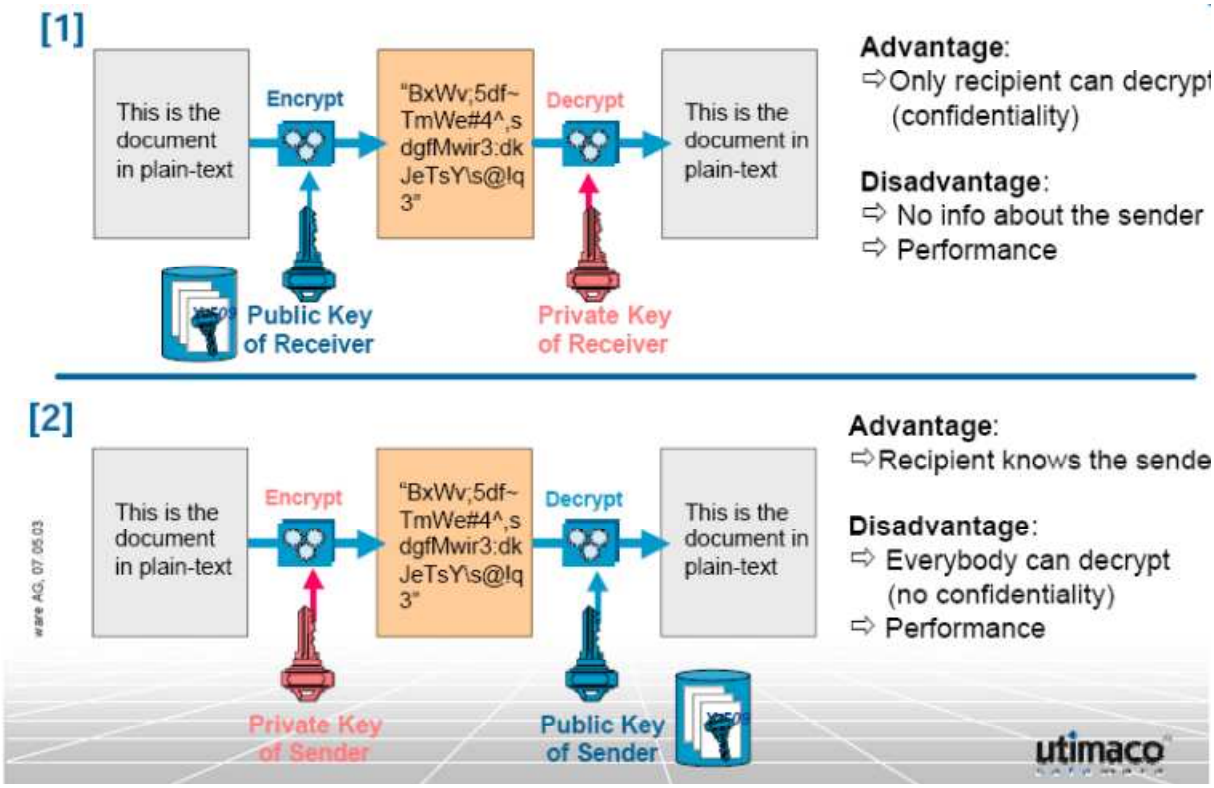
4-2-5-2) انجام سرويس احراز هويت با بهره‌گيري از الگوريتم‌هاي نامتقارن

اما در ابتدا اين پاراگراف اشاره داشتيم به اينكه يكي از سرويس‌هاي امنيتي ديگر كه توسط الگوريتم هاي نامتقارن پشتيباني مي‌شوند، سرويس احراز هويت يا Authentication مي‌باشد.

براي انجام اين سرويس فرستنده با كليد خصوصي خودش يك متن معني‌دار را به يك متن رمز شده تبديل كرده و آن را منتشر مي‌نمايد. در اينجا تمام كساني كه به كليد عمومي او دسترسي دارند مي‌توانند روي متن رمز شده عمل رمزگشايي را انجام داده و متن واضح را شناسايي كنند. بايد توجه داشت در اين سرويس هدف محرمانگي اين اطلاعات نمي‌باشد، بلكه احراز هويت فرستنده پيام مي‌باشد. با اين ترتيب گيرنده پيام با بدست آوردن متن واضح و داراي معنا با استفاده از كليد عمومي فرستنده كه بر روي متن رمز شده اعمال كرده است، مي‌تواند از صحت ارسال كننده آن مطمئن شود.

در امتداد اين نكته قابل توجه است كه كه ما مي‌توانيم با بهره برداري از الگوريتم كليد عمومي، دو سرويس محرمانگي و احراز هويت را در كنار هم داشته باشيم. يعني با استفاده از كليد منتشر شده يك گيرنده مي‌توانيم برايش متن رمز شده و محرمانه ارسال كنيم، و همچنين فرد فرستنده مي‌تواند با رمز كردن اين متن رمز شده با كليد خصوصي خودش و ارسال آن به گيرنده، گيرنده در ابتدا با كليد عمومي فرستنده مرحله اول رمزگشايي را انجام دهد و در نتيجه مي‌تواند به صحت فرستنده پي ببرد(Authenticate)، و آنگاه با رمزگشايي مجدد با كليد خصوصي خودش به متن واضح اصلي دست پيدا كند.

در شكل 4-9 شمايي از دو سرويس امنيتي محرمانگي و احراز هويت با استفاده از الگوريتم كليد عمومي ، در دو بخش 1 و 2 آورده شده است.

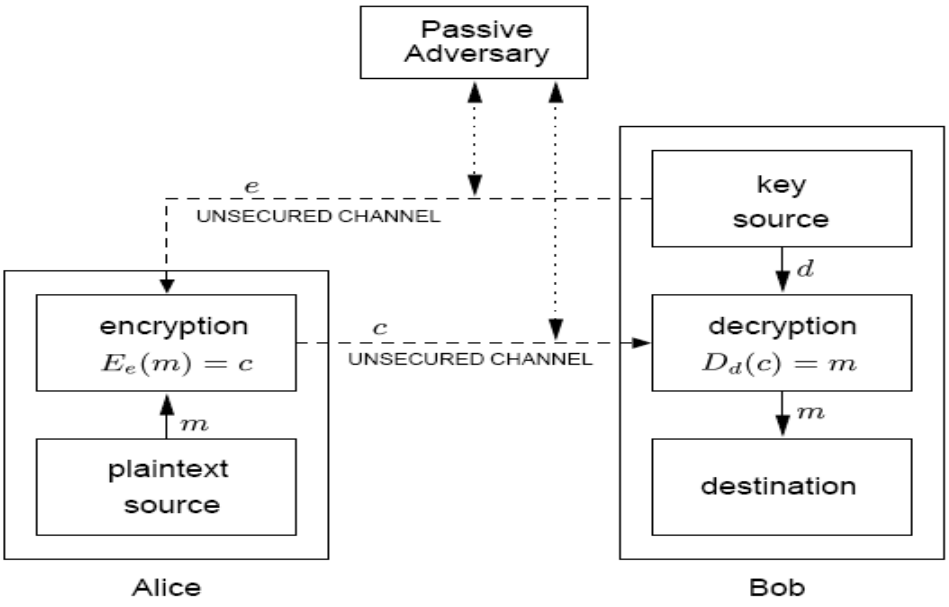


شكل 4-9) شمايي از دو سرويس محرمانگي و احراز هويت با استفاده از الگوريتم كليد عمومي

همچنين با توجه به شكل 4-10 مي‌توان از نحوه توزيع كليد در الگوريتم متقارن مطلع گرديد. همانطور كه در شكل ملاحظه مي‌كنيد گيرنده ،يعني باب، از يك منبع محاسباتي ايجاد و توزيع كليد، زوج كليد خود را دريافت مي‌كند. باب كليد خصوصي خودش(يعني d) را بصورت محرمانه نزد خود نگه داشته، ولي كليد عمومي خود(يعني e) را براي ديگران از طريق كانال ناامن منتشر مي‌كند. توجه كنيد كه در طرح نسبت به الگوريتم سيميتريك، ما اين آزادي عمل را داريم كه از يك كانال ناامن براي توزيع كليد عمومي هم استفاده كنيم. و اين بدان معني است كه دشمن اجازه دارد هم كليد عمومي را ببيند هم متن رمز شده ارسالي را.

آليس به عنوان ارسال كننده، متن واضح(يعنيm) را با كليد رمزگذاري عمومي باب(e) – كه توسط باب منتشر شده و در اختيار دارد- از طريق الگوريتم رمزنگاري E، به متن رمز شده تبديل مي‌كند. و اين متن رمز شده را باز ازطريق كانال ناامن براي باب مي‌فرستد. باب هم پس از دريافت متن رمز شده (يعنيc)، با اعمال كليد رمزگشاي شخصي خود (يعنيd) و استفاده از الگوريتم

رمزگشايي (يعنيD)، از حالت رمز شده خارج كرده و به يك متن واضح تبديل مي‌كند.



شكل 4-10) روش توزيع كليد در الگوريتم نامتقارن

براي درك بهتر تفاوتهاي دو نوع الگوريتم متقارن و نامتقارن جدول 4-1 در زير آورده شده است .

همانطور كه در جدول ملاحظه مي‌كنيد:

در روش سيمتريك كليد منحصر بفرد بين دو طرف به اشتراك گذاشته مي‌شود. ولي در الگوريتم آسيمتريك از دو كليد عمومي و خصوصي استفاده مي شود.

عمل جابجايي كليد در سيمتريك بايد در كانال جدا از كانال ارسال پيام‌ها انجام گيرد، و اين در حالي است كه در آسيمتريك عمل انتقال كليد در همان كانال در نظر گرفته شده براي انتقال متن، منتقل مي‌گردد.

الگوريتم‌هاي رمزگذاري سيمتريك مقياس پذير نيستند، يعني آنكه قابليت اعمال بر روي بلوك‌هاي مختلف داده‌اي با اندازه‌هاي مختلف را ندارند. ولي در آسيمتريك اين كار امكان‌پذير است.

سيمتريك‌ها داراي سرعت بالاتر اجرايي نسبت به آسيمتريك‌ها هستند.

سيمتريك‌ها براي اجراء بر روي حجم بالاي داده مناسب مي‌باشند. در حاليكه آسيمتريك‌ها بيشتر براي اعمال بر روي حجم كوچكتر داده بكار مي‌روند. و براي توليد امضاي الكترونيكي، گواهي ديجيتالي، پاكت ديجيتالي استفاده مي‌شوند.

سيمتريك صرفا براي سرويس محرمانگي بكار مي‌رود، در حاليكه آسيمتريك علاوه بر سرويس محرمانگي، سرويس‌هاي احراز هويت، و انكارناپذيري را هم پشتيباني مي‌كند.

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 سيمتريك و آسيمتريك

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

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

تابع درهم‌ريزي را مي‌توان با اثر انگشت مقايسه كرد. همانطور كه اثر انگشت هركس انحصاري است و داراي اندازه ثابتي است. نتيجه تابع درهم‌ريزي هم انحصاري است و نمي‌توان مقادير يكسان از داده‌هاي متفاوت بدست آورد. بعضي از مشخصات توابع درهم‌ريزي MD-4, MD-5, SHA-1 عبارتند از:

MD-4: خروجي آن يك مقدار 128 بيتي است. خيلي سريع مي‌باشد. براي اهداف امنيتي سطح متوسط مناسب مي‌باشد.

MD-5: خروجي آن يك مقدار 128 بيتي است. سريع مي‌باشد(اما نه به اندازه MD-4). از MD-4 امن‌تر است. در بسياري از مكان‌ها استفاده مي‌شود.

SHA-1: خروجي آن يك مقدار 160 بيتي است. استاندارد دولتي آمريكا مي‌باشد. اما از MD-5 كندتر مي‌باشد.

4-6) معرفي اجزاء زيرساخت كليد عمومي

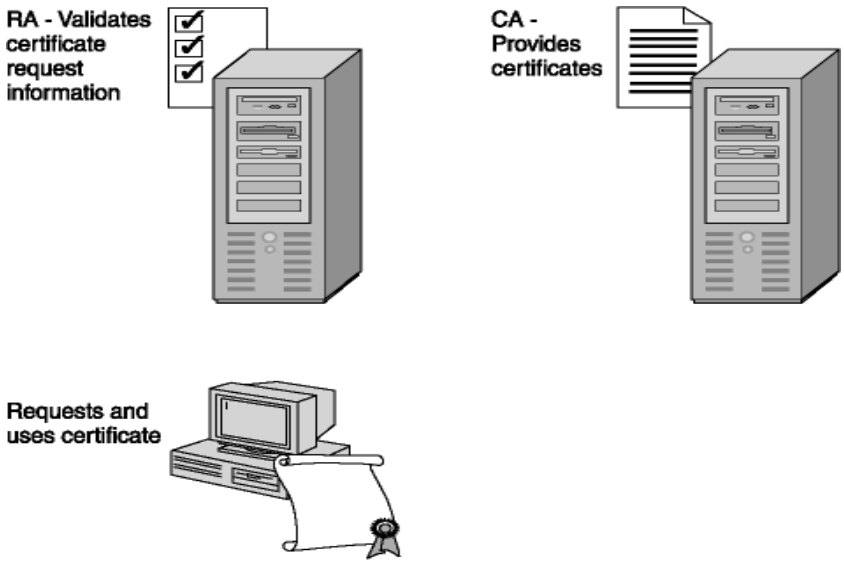
استفاده از زوج كليد در الگوريتم آسيمتريك براي پياده‌سازي در محيطهاي كوچك و افراد كم، كاري ساده است. اما در محيطهاي بزرگ با كاربردهاي وسيع، توزيع كليد عمومي و مديريت كليد خصوصي كاري بس دشوار مي‌گردد. زماني كه يك كليد خصوصي مورد هجوم قرار مي‌گيرد، پاك كردن آن و جايگذاري آن سخت مي‌باشد.

براي اين منظور زيرساخت‌هاي امنيتي با نام زيرساخت‌هاي كليد عمومي (Public Key Infrastructure) يا باختصار PKI، بوجود آمده‌اند. PKI از زوج كليد آسيمتريك، نرم‌افزارهاي تركيبي، و تكنولوژي‌هاي رمزنگاري، براي ايجاد امنيت ارتباطات و تراكنشهاي تجاري استفاده مي‌كنند. استاندارد PKI كه در محيطهاي اينترنتي مورد استفاده قرار مي‌گيرد، استاندارد X.509 مي‌باشد. اين استاندارد شامل: تاييديه، تاييد كننده تاييديه، ابزار مديريتي تاييديه‌ها، و برنامه‌هاي كاربردي كه تاييديه‌ها را بكار مي‌گيرند، مي‌باشد.

1-6-4) اجزاء PKI

همانطور كه در شكل 4-11 مشاهده ميكنيد اجزاء اصلي اين زيرساخت عبارتند از:

- **تاييديه ديجيتالي(Digital Certificate)**. كه يك اعتبارنامه الكترونيكي براي احراز هويت كاربر ميباشد.
- **مركز قانوني صدور تاييديه (Certification Authority - CA)**. يك كامپيوتر كه تاييديه ديجيتالي را صادر ميكند، يك ليست تاييديه‌هاي معتبر را نگه‌داري ميكند، و همچنين يك ليست از تاييديه‌هايي كه به دلايلي اعتبار آن باطل شده را هم نگه‌داري ميكند.
- **مركز قانوني ثبت نام (Registration Authority - RA)**. مركزي كه براي رسيدگي به شرايط ثبتنامي و ثبت نام از متقاضيان در خواست تاييديه‌هاي ديجيتالي، و ارسال درخواستها به CA، فعاليت ميكنند.
- **ابزار مديريت تاييديه‌ها و كليدها (Key and Certification Management Tools)**. ابزار براي حسابرسي و مديريت تاييديه‌هاي ديجيتالي.
- **نقطه انتشار تاييديه‌ها (Certificate Publication Point)**. مكاني كه تاييديه‌ها ذخيره و منتشر ميشوند.
- **سرويس‌ها و برنامه‌هاي فعال‌ساز كليد عمومي (Public Key-Enabled Applications and Services)**. برنامه‌هاي كاربردي و سرويس‌هايي كه استفاده از تاييديه را پشتيباني ميكنند.



شكل 4-11) اجزاء اصلي PKI

4-6-2) تاييديه (Certificate)چه مي‌باشد؟

تاييديه يك معرف ديجيتالي مي‌باشد كه شما را معرفي كرده و توسط CA صادر مي‌گردد. اين CA معمولا به عنوان سوم شخص قابل اعتماد يا Trusted Third Party (TTP) هم شناخته مي‌شود. در هر تاييديه مشخصات سوم شخص معتمد صادر كننده آن، تاريخ اعتبار تاييديه، و امضاء تاييديه سوم شخص معتمد براي تاييد صدور آن، وجود دارد.

تاييديه مي‌تواند توسط برنامه‌هاي كاربردي و سرويس‌هاي امنيتي مختلف براي انجام مواردي همچون احراز هويت، صحت و يكپارچگي داده‌ها، و امنيت بكار رود. كاربردهاي تاييديه شامل موارد زير است:

- **امن‌سازي ايميل.** از پروتكل S/MIME براي اطمينان از صحت و جامعيت، مبداء‌ف و محرمانگي ايميل استفاده مي‌شود.
- **امن‌سازي ارتباطات وب.** استفاده از تاييديه در پروتكل SSL/TLS براي احراز هويت و رمزنگاري ارتباطات ميان سرور و كلاينت.
- **امن‌سازي سرور وب.** استفاده از تاييديه براي احراز هويت دسترسي به وي سايت‌هاي امن.
- **راه‌حلهاي امنيت مشتريان.** استفاده از تاييديه براي اجراي محرمانگي، صحت، احراز هويت، و انكار ناپذيري در برنامه‌هاي كاربردي مشتريان.

فصل پنجم: امن‌سازي زيرساخت‌هاي شبكه

مقدمه

در اين فصل به بحث امنيت در زيرساخت‌هاي شبكه از سه بعد كانال‌هاي ارتباطي و تجهيزات ارتباطي و منابه شبكه‌اي خواهيم پرداخت. سازمان‌ها و اشخاص علاقه‌مند به محافظت از داده‌ها،تجهيزات، اسرار تجاري، و حفظ حريم شركاي خود مي‌باشند. يك حمله موفق‌آميز به شبكه ممكن است عاملي براي به مخاطره درآمدن هريك از ابعاد فوق باشد. براي محافظت از زيرساخت‌هاي شبكه خود در مقابل حملات در ابتدا بايد نسبت به انواع حملات ممكن فرا روي اين زير ساخت آگاه باشيد. بعضي از اين تهديدات عبارتند از:

- تخريب فيزيكي تجهيزات
- شنود بسته هاي اطلاعاتي
- اسكن پورت‌هاي شبكه و نقشه شبكه براي شناسايي اهداف جهت تدارك حمله
- چيدمان مجدد و يا غير فعال كردن ارتباطات تجهيزات امنيتي
- استفاده از تجهيزات شبكه براي تدارك حمله به شبكه‌اي ديگر
- استفاده از شبكه شما براي ميزباني سرويس هاي غيرقانوني، مخريف و ناشناخته
- پاك كردن و تخريب داده‌ها

در راستاي نيل به اهداف امنيتي بعضي از راه‌ها براي براي امن نمودن فيزيكي تجهيزات به قرار زير است:

- استخدام گارد حفاظتي
- نصب سنسور، و تلويزيون‌هاي مدار بسته براي نظارت بر تجهيزات
- استفاده از كارت‌هاي امن براي دسترسي قيزيكي
- نصب سيستم برق اضطراري
- پوشش كابل‌هاي شبكه و يا قرار دادن آنها درون ديوارها
- قفل نمودن دري اطاق سرور

- قرار دادن تجهيزات در پوششهاي مناسب و مهر و موم كردن آنها
- نصب فنس و گيتهاي ورود و خروج
- نصب سيستم ضد حريق
- اطمينان از استانداردهاي نصب و پيادهسازي تجهيزات.

5-1) امنيت در كانالهاي ارتباطي شبكه

بسياري از شبكههاي كامپيوتري از انواع مختلف كابل براي ارتباطاتشان استفاده ميكنند.در اين درس شما با بعضي از اين كابلها و نحوه حمله به آنان آگاه ميشويد. كابلهاي اساسي در شبكه عبارتند از : كابلهاي كواكسيال، كابلهاي زوج سيم مسي، كابل فيبر نوري. البته لازم به ذكر است كه خطوط بيسيم نيز از انواع خطوط ارتباطي مي باشد.

5-1-1) كابلهاي كواكسيال

كابلهاي كواكسيال داراي انواع مختلف ولي داراي ساختار نسبتا يكسان ميباشد. هر كابل كواكسيال شامل: رشته سيم رساناي مركزي، يك رشته سيم رساناي بيروني، و يك پوشش بيروني است. انتقال الكترونيكي(دادههاي در حال انتقال) از ميان رشته سيم رساناي مركزي عبور ميكند.

5-1-1-1) حملات عليه كابلهاي كواكسيال

كابلهاي كواكسيال معمولا از دو جنبه تخريب و يا استراق سمع اطلاعات مورد تهاجم قرار ميگيرند.اين كابلها معمولا براي نصب شبكه با توپولوژي باس(Bus) مورد استفاده قرار ميگيرند، به اين دليل قطع شدن بخشي از آن باعث قطعي كل شبكه ميشود.

يكي از تخريبهايي كه عليه اين كابلها انجام ميگيرد برش آنها بوسيله قيچيهاي فلزبر(عليرغم محكم بودن اين كابلها) ميباشد. همچنين منبع گرمايي شديد در مجاورت اين كابلها عامل ديگري براي تخريب آنها ميباشد.

اما از بعد فركانسي هم اين كابلها آسيبپذير ميباشند. اين كابلها در مقابل امواج راديويي و امواج مغناطيس دچار آشفتگي اطلاعاتي ميشوند. همچنين جداسازي قطعه

تمام‌كننده (Terminator) در قسمت انتهايي خطوط در اين كابل‌ها باعث قطعي شبكه مي‌شود.

اما از بعد استراق سمع ، چون اين كابل‌ها معمولا در توپولوژي باس مورد استفاده قرار مي‌گيرند و در اين توپولوژي سيگنال‌هاي اطلاعاتي در كل شبكه به انتقال در مي‌آيند، پس هر نود متصل به اين شبكه در صورت لحاظ نشدن موارد امنيتي در شبكه، امكان استراق سمع اطلاعات را دارا مي‌باشد. همچنين هر بخش از كابل شبكه مكان مناسبي براي يك اتصال جديد به شبكه توسط مهاجمين مي‌باشد. البته لازم بذكر است براي ايجاد اتصال به شبكه در اين كابلها توسط مهاجمين بايد قسمتي از كابل قطع شود، و بدليل نوع توپولوژي شبكه‌هايي كه از كابل‌هاي كواكسيال استفاده مي‌كنند (توپولوژي باس)، انگاه كل شبكه در آن زمان از كار مي‌افتد.

5-1-1-2) امن‌سازي كابل‌هاي كواكسيال

از روش‌هاي زير براي امن سازي كابل‌هاي كواكسيال در برابر تخريب و شنود استفاده مي‌شود:

- قرار دادن اين كابل‌ها در زير سطح زمين، قرار دادن آن‌ها در ديوارها، و پوشش‌گذاري حداكثري آنها براي جلوگيري از استراق سمع.
- مستندسازي كابل كشي‌ها
- وارسي كردن تمامي راه‌هاي خروجي شبكه كابل كواكسيال.
- بازرسي فيزيكي به صورت دوره‌اي از تمامي زير ساخت‌هاي كابل.
- وارسي كردن تمامي تجهيزات ميزبان و اتصالات مستند نشده.

5-1-2) زوج سيم مسي

هر كابل زوج سيم مسي داراي يك يا بيشتر زوج سيم تابيده شده بهم قرار گرفته در يك غلاف پلاستيكي مي‌باشند..هر سيم از جنس مسي مي‌باشد كه توسط لايه پلاستيكي به عنوان پوشش در دور آن جهت عدم اتصال الكتريكي سيم‌ها به يكديگر محافظت مي‌شود. هر زوج تك سيم بدور يكديگر جهت جلوگيري از هرز رفتن سيگنال‌هاي الكتريكي درونشان، بهم تابيده شده‌اند.

5-1-2-1) حملات عليه زوج سيم مسي

اين سيم ها به دليل جنس نازكشان براحتي قابل تخريب و بريده شدن مي‌باشند. همچنين حرارت گرمايي نيز بر روي آنها تاثير مخربي دارد. اما بدليل آنكه اينگونه كابل ها عمدتا در شبكه‌هاي مبتني بر توپولوژي ستاره(Star) استفاده مي‌شوند، لذا قطع شدن يكي از اين سيم ها باعث قطعي كل شبكه نمي‌شود.

اما از بعد استراق سمع، اين كابل‌ها به 3 شكل مورد تهاجم قرار مي‌گيرند:

- اتصال فيزيكي يك پروتكل آناليزر به يك نقطه اتصال از اين زوج سيم هاي مسي. پروتكل آناليزر يك دستگاه و يايك برنامه نرم افزاري كامپيوتري مي‌باشدكه به مهاجم اجازه تصرف و ورمزگشايي ترافيك موجود بر روي شبكه را مي‌دهد. يا باصطلاح ديگر امكان بو كشيدن اطلاعات را مي‌دهد.
- بهم تابيدن به داخل كابل زوج سيم مسي.
- استفاده از سيگنال‌هاي الكترومغناطيسي براي استراق سيگنال‌هاي عبوري از ميان زوج سيم مسي.

5-1-2-2) امن‌سازي زوج سيم مسي

- محافظت فيزيكي كابل بالاخص در مراكز حساس آن مثل محل اتصالات به هاب و سوييچ و ...
- استفاده از سوييچ به‌جاي هاب، چرا كه سوييچ ترافيك مورد نظر را مستقيما به ميزبان مورد نظر اصلي مي‌فرستد، در حاليكه هاب ترافيك را به سمت تمامي ميزبان‌هاي موجود در شبكه گسيل مي‌دارد.
- مديريت سوييچ‌ها، هاب‌ها، و روترها به شكلي كه در صورت صدمه ديدن بخشي از شبكه و يا ورود يك اتصال جديد به شبكه، به مدير شبكه پيغام دهد.

5-1-3) فيبر نوري

كابل فيبر نوري از يك رشته و تار شيشه‌اي يا پلاستيكي براي انتقال پالس‌هاي نوري تشكيل شده است.

كابل هاي فيبر نوري بسيار امن‌تر از انواع ديگر كابل‌ها مي‌باشند، چرا كه توسط امواج راديويي و مغناطيس تحت تاثير

قرار نمي‌گيرند. اين كابل‌ها گران‌تر و نصب آنها نيز سخت‌تر مي‌باشد.

5-1-3-1) حملات عليه فيبر نوري

خرابي بر روي اين كابل‌ها بسيار راحت‌تر مي‌باشد. اين كابل‌ها براحتي مي‌توانند آسيب ديده، مچاله شده، و يا شكسته شوند. اما شنود بر روي كابل فيبر نوري غير ممكن است، مگر آنكه فرد مهاجم بخشي از فيبر نوري را بريده و يك كارت قرائتگر فيبر نوري وارد مسير شبكه نمايد.

5-1-3-2) امن‌سازي فيبر نوري

مهمترين عاملي كه جهت امن سازي اين كابل‌ها ذكر مي‌شود محافظت فيزيكي از آنها و همينطور پيكر بندي شبكه به شكلي كه در صورت قطعي در شبكه، بدليل تلاش مهاجم براي وارد كردن يك كارت قرائتگر فيبر نوري در بخشي از شبكه، فورا هشدارهاي لازم به مديران شبكه داده شود.

5-2) امنيت در تجهيزات ارتباطي شبكه

بسياري از تجهيزات ارتباطي در شبكه داراي بخش‌هاي سخت افزاري و پيكربندي منطقي مي باشندكه فرد مهاجم مي‌تواند از ضعف در هر يك از اين دو بخش براي تدارك حمله بهره‌برداري نمايد. اين تجهيزات به شرح زير مي‌باشند:

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

5-2-1) Hubs

همانطور كه مي دانيد هاب يك وسيله ارتباط و اتصال در شبكه‌هاي از نوع اترنت مي‌باشد. كه داراي دو نوع فعال و غير

فعاي مي‌باشد. در نوع فعال ان سيگنال‌هاي شبكه تكرار و تقويت مي‌گردد. و چون هاب محل ارتباط اصلي در شبكه مي‌باشد لذا مورد توجه مهاجمين براي تدارك حمله مي‌باشد.

4-2-1-1) تخريب هاب

هاب به راحتي قابل تخريب است اگر مهاجم به آن دسترسي فيزيكي داشته باشد. هاب به راحتي ميتواند از اتصال خارج و يا خراب شود، و يا اگر از نوع فعال آن باشد، به راحتي خاموش شود. در اين صورت تجهيزات متصل به شبكه امكان ارتباطي خودشان با يكديگر را از دست مي‌دهند.

شنود بر روي هاب نيز امكان پذير مي‌باشد. اگر يك پورت بر روي هاب آزاد باشد و يا اگر امگان جداسازي يك دستگاه تاييد شده متصل به هاب براي حمله كننده وجود داشته باشد، آنوقت فرد حمله كننده مي‌تواند از آن پورت براي دستيابي به اطلاعات و يا تخريب بر روي ديگر تجهيزات متصل در شبكه سود برد.

5-2-1-2) امن سازي هاب

به دليل خاصيت فيزيكي هاب، امكان حفاظت فيزيكي آن هم وجود دارد. تلاش گردد هاب درون محفظه‌اي امن قرار داده شود. اگر هاب درون اطاق يا محفظه‌اي قفل شده نمي‌باشد، تلاش شود توسط ديگر بسته‌بندي‌ها محافظتي امت گردد. حداقل به صورت دوره‌اي هاب مورد بازديد قرار گيرد تا از امن بودن اتصالات آن و عدم اتصال يك فرد غير مجاز به آن مطمئن شويم. هاب‌هاي قابل مديريت مي‌توانند براي آشكارسازي تغييرات فيزيكي در بهم‌بنديشان بكار گرفته شوند. هاب‌هاي قابل مديريت اطلاعات آماري و اطلاعات اتصاليشان را براي مديريت نرم افزار ارسال مي‌كنند. لذا شما مي توانيد هاب را براي اعلام خطر به هنگام تغيير در بهم بنديش مجهز كنيد. اما از آنجا كه اين روش مديريت موقعيت و بهم‌بندي به شكل نرم افزاري انجام ميگيرد، فرد مهاجم مي‌تواند چيدمان نرم افزاري را تخريب و يا تدارك حمله‌اي ديگر از اين ناحيه را ببيند.

5-2-2) Switches and Bridges

سويیچ و بريج در لايه دوم شبكه (در مدل استاندارد OSI) متصل مي‌گردد. آنها عمل سويیچينگ و پل‌بندي را بر مبناي آدرس كنترل دسترسي كانال‌هاي ارتباطي (MAC) هريك از اتصالات شبكه، انجام مي‌دهند. سوويچ و بريج جدولي را براي كمك به ارسال بسته‌هاي اطلاعاتي به بخش‌هاي مناسب شبكه، ايجاد مي‌كنند. پل يا باصطلاح بريج نوعا يك شبكه را به دو بخش تقسيم ميسازند ولي سويیچ‌ها نوعا هر بخش از شبكه را به چندين قسمت كوچكترتقسيم مي‌كنند، و هر قسمت براي هر پورت سويیچ مي‌باشد. اين تجهيزات عمدتا تنها براي انتقال اطلاعات تك مقصده (Unicast) مورد استفاده قرار مي‌گيرند و اطلاعاتي كه براي همزمان چند مقصد(Multicast) ارسال ميشوند از اين تجهيزات گذر مي‌كنند.

توجه: ممكن است در كاتالوگهاي بازاريابي كاركرد اين تجهيزات در لايه‌هاي 3 و 4 شبكه را هم ملاحظه كرده باشيد. كه در اين صورت ديگر نام اين تجهيزات "روتر با كارايي بالا" مي‌باشد.

5-2-2-1) تخريب سويیچ و پل

همانطور كه ديديد سويیچ‌ها و پل‌ها حدولي به نام MAC براي نشان دادن اتصالات به هر نقطه اتصالي ايجاد مي‌كنند. اين جدول امكان ارتباط با بخش صحيح شبكه يا پورتي را براي سويیچ و يا پل در لايه دوم شبكه امكان پذير مي‌سازد، كه اين موضوع پتانسيل خوبي را براي حمله كنندگان براي تدارك حمله‌اي به ارمغان مي‌آورد. همچنين يك سويیچ مركزي مكان مناسبي براي هدفگذاري يك حمله مي‌باشد. خراب كردن يك سويیچ مركزي، يا قطع برق آن، يا قطع كردن كابل‌هاي متصل به آن باعث از كار افتادن تمام ارتباطات عبوري از آن مي‌شود. به موازات اين تخريب‌هاي فيزيكي غرق‌سازي جدول MAC با آدرس‌هاي بي‌مقصد در سويیچ و بريج (البته آندسته از سويیچها و پل‌هايي كه قابليت آموزش دارند) باعث كند شدن كار شبكه مي‌گردد. ديگر تخريب‌هاي ممكن به اشكال زير اتفاق مي‌افتد:

الف) تمليك دسترسي مديريت شبكه

اگر فرد مهاجم بتواند امكان دسترسي مديريتي شبكه را به دست آورد، او مي‌تواند ارتباطات شبكه را مسيردهي مجدد كند. اين ارتباطات مي‌تواند به سمت ماشيني كه تحت كنترل حمله كننده مي‌باشد مسيردهي شود. آنگاه تا زمانيكه مهاجم امكان اتصال مديريتي به

شبكه را دارا باشد مي‌تواند شبكه را تخريب نمايد. اينكار با دسترسي به شناسه و كلمه عبور مدير سيستم انجام مي‌گيرد. سويچها بالاخص فانكشني به نام "معكوس سازي پورت" (Mirroring Port) دارند، كه مدير سيستم را قادر به نگاشت ورودي و خروجي از يك يا چند پورت سويچ به يك پورت خاص مي‌سازند. اين به منزله روشي براي عيبزدايي مشكلات ارتباطي در شبكه مي‌باشد. حال اگر مهاجمي امكان دسترسي به اين فانكشن را داشته باشد، او مي‌تواند تمام ترافيك عبوري از شبكه را مشاهده نمايد. به اين شكل او مي‌تواند تمام اطلاعات رمز نشده در شبكه مثل اطلاعات شناسه و كلمه عبور ديگر سيستم‌هاي متصل به شبكه را به دست آورد.

ب) مسموم سازي حافظه ARP (ARP Cache Poisoning)

اگرچه سويچ و پل شبكه را بخش‌بندي مي‌كنند، اين امكان وجود دارد كه فرد مهاجم حافظه پروتكل تجزيه و تحليل (ARP) را مسموم نمايد. و بدين شكل ترافيك شبكه را در شبكه پخش نمايد. كش ARP براي نگهداري اطلاعات نگاشت پروتكل اينترنت(IP) به آدرس MAC بكار مي‌رود.

براي اينكه حمله كننده اين مسموميت را انجام بدهد، ابتدا بايد به صورت فيزيكي به يك بخش داخلي از شبكه دسترسي پيدا كند. آنگاه تخريبگر بايد كش ARP مربوط به ماشين‌هاي آن قسمت شبكه را تخريب نمايد. به اين ترتيب مي‌تواند تمام ترافيك ماشين‌هاي آن بخش شبكه را به سمت كامپيوتر خودش روان سازد.

5-2-2-2) امن‌سازي سويچ‌ها و پل‌ها

مانند ديگر تجهيزات شبكه حفاظت فيزيكي از آنها شرط اوليه مي‌باشد. اما ديگر راه‌ها به نحو زير مي‌باشد:

- امن كردن كليه اتصالات فيزيكي در شبكه. اطمينان از امكان پذير نبودن ارتباط افراد تعريف نشده جهت اتصال به اين تجهيزات. همچنين محدودسازي دسترسي به مكان اين تجهيزات و نظارت بر تجهيزات از جهت اطمينان از امن بودن اتصالات.
- استفاده از كلمات عبور مركب و پيچيده براي كنسول‌هاي مديريتي. در اختيار داشتن اين كلمات عبور تنها توسط افراد خاصي و تغييرات آنها بصورت دوره‌اي و تغيير آن در صورت تعويض

افراد، از جمله ديگر مواردي است كه بايد مورد توجه قرار گيرد.

- ورود دستي نگاشتهاي ARP در تجهيزات بحراني، همچون سرورها، سويچها، و پلهاي مركزي . اگر كليه آدرسهاي MAC بصورت دستي در جداول وارد شوند، اين عمل از يادگيري آدرسهاي جديد بصورت اتوماتيك توسط سويچها و پلها جلوگيري مي‌كند.
- سويچها و پلها را توسط آخرين نسخه‌هاي وصله‌هاي امنيتي طراحي شده توسط سازندگان آنها مجهز نماييم.
- مستندسازي نحوه بهم‌بندي دستگاه براي يادآوري ارتباطات نرمال و مجاز در آينده.
- مانيتور كردن شبكه با ابزارهاي مديريتي براي آگاهي از اتصالات غيرمجاز. ابزاري به نام ARPWATCH مي‌تواند فعاليت‌ها برروش شبكه را مانيتور كرده و يك ديتابيس از اطلاعات نگاشت MAC به IP را در خود نگه دارد. همچنين اين ابزار مي‌تواند شما را از تغييرات ايجاد شده در اين بخش مطلع سازد.

Routers (3-2-5

همانطور كه مي‌دانيد مسيرياب (Router) ارتباطات را در لايه سوم مدل مرجع شبكه (OSI)، يعني لايه شبكه، به عهده دارد. روتر همچنين از ARP Cache و جدول مسيردهي(Routing table) براي انجام وظيفه مسيردهي در شبكه بهره مي‌گيرد.

1-3-2-5) تخريب مسيريابها

همانطور كه گفتيم روترها هر دوي ARP Cache و جدول مسيردهي (Routing table) را براي انتقال و مسيردهي مناسب ارتباطات استفاده مي‌كند. و اين خود نقطه‌اي براي تدارك حمله مي تواند باشد. روتر مركزي همچنين مي‌تواند مكان مناسبي براي تخريب باشد. خراب كردن روتر مركزي، قطع كردن برق، و يا قطع كردن اتصالات كابل‌هاي روتر مي‌تواند عاملي براي جلوگيري از گذر اطلاعات در بين دستگاه در شبكه باشد.

از آنجا كه روترها از ARP Cache استفاده مي‌كند، آنها مي‌توانند مستعد حمله مسموم‌سازي ARP Cache باشند. بعلاوه، روترها از Routing table، كه مي‌تواند از طريق اتصال از راه دور و يا اتصال

كنسول مديريت از طريق كابل تغيير يابد، استفاده مي‌كنند. اگر مهاجمي بتواند اين جدول را تغيير دهد، ترافيك شبكه مي‌تواند به صورت ناصحيح به سمت يك كامپيوتر كه تحت كنترل مهاجم مي‌باشد مسيردهي شود. همانطور كه در گذشته هم ديديد شما مي‌توانيد با نظارت بر نقاط اتصال فيزيكي در شبكه‌تان از اين حمله پيشگيري نماييد.

اگر يك حمله كننده بتواند دسترسي مديريتي به روتر پيدا كند، او مي‌تواند مسيردهي مجدد در شبكه را انجام دهد. اين ارتباطات مي‌تواند به سمت يك ميزبان تحت كنترل مهاجم در شبكه مسيردهي مجدد شود.

همچنين مهاجم مي‌تواند پروتكل اطلاعات مسيردهي (RIP) را براي بروزسازي اطلاعات جدول مسيريابي با اطلاعات نادرست مورد استفاده قرار دهد.. اين عمل RIP Spoofing ناميده مي‌شود، و مربوط به تجهيزاتي است كه از روايه يكم آن (RIPv1) استفاده مي‌كنند. به هر حال روايه دوم آن (RIPv2)، روتر را براي تنظيم كلمه عبور مجاز مي‌سازد. بنابراين در اين نسخه فرد مهاجم بايد براي قرار دادن اطلاعات نادرست روتينك حتما كلمه عبور را داشته باشد.

همانطور كه در بخشهاي قبل گفته شده دستگاه‌هاي ارتباطي ممكن است مشكلات بهم‌بندي نرم افزاري و يا نقاط آسيب‌پذيري امنيتي داشته باشند. بطور مثال، ممكن است شخصي دريابد كه يك روتر مي‌تواند بروز و يا غيرفعال شود بدون مجوز مديريت(به اين معني كه در صورت دسترسي به شبكه مي‌تواند آن روتر را تخريب نمايد). فروشنگان اين تجهيزات در صورت اطلاع از اين ضعفها غالبا قادر به حل آن مي‌باشند، لذا براي محافظت از تجهيزات ارتباطي حتما پيگيري از فروشندگان آنها را براي دريافت وصله‌هاي مرتفع كننده مشكل، فراموش نكنيد.

5-2-3-2) امن‌سازي مسيريابها

يك روتر مركزي هدف مناسبي براب مهاجمين مي باشد. تخريب يك روتر مركزي، قطع برق آن و يا قطع نمودن كليه كابل‌هاي ارتباطي آن ممكن است كليه ارتباطات متصل به اين دستگاه را مختل سازد. براي امن‌سازي آن بايد مراقبت‌هاي زير را انجام داد:

- اطمينان از نگه‌داري روتر در اطاق قفل‌دار يا در پوشش مناسب.
- امتحان امنيت تمامي اتصالات ورودي و خروجي.
- محدودسازي دسترسي فيزيكي به تجهيزات زيربنايي شبكه كابل، و اطاق‌هاي سرور.
- مانيتورينگ تجهيزات براي حفاظت از نقاط اتصال و تجهيزات.
- بكارگيري كلمات عبور تركيبي براي كنسول هاي مديريتي. در اختيار داشتن اين كلمات عبور تنها توسط افراد خاصي و تغييرات آنها بصورت دوره‌اي و تغيير آن در صورت تعويض افراد، از جمله ديگر مواردي است كه بايد مورد توجه قرار گيرد.
- بهنگام نگه‌داري روترها با آخرين نسخه وصله هاي(Patches) امنيتي ارائه شده توسط فروشندگان.
- اطمينان از مستندسازي و نظارت مجدد بر چيدمان و بهم‌بندي شبكه.
- غيرفعال سازي RIPv1 و بكارگيريRIPv2 و يا ديگر پروتكل‌هاي مسيردهي كه امكان تغييرات در روتر را تنها با ارائه كلمات عبور ميسر مي‌سازند.

Firewalls (4-2-5

كلمه ديواره آتش بصورت عمومي براي توضيح تجهيزاتي بكار مي‌رود كه براي محافظت از يك شبكه داخلي(يا يك ميزبان) در مقابل مهاجمين يا كدهاي مخرب از شبكه خارجي (يا شبكه‌اي كه آن ميزبان به آن متصل است) بكار مي‌رود. ديواره‌هاي آتش معمولا از اعمال متفاوتي براي فيلتر كردن ترافيك‌هاي ورودي و يا خروجي مضر و مخرب، استفاده مي‌كنند. آنها اغلب براي پياده‌سازي بين ارتباط شبكه داخلي سازمان و اينترنت بكار مي‌روند. البته گاها بعضي از ديواره‌هاي آتش براي جداسازي شبكه داخلي و يا حتي محافظت از يك كامپيوتر تنها نيز بكار مي‌رود.

ديواره های آتش يک زير سيستم از نرم افزار وسخت افزار كامپيوتری اند كه از ورود ويا خروج داده ها به /از شبكه داخلی (LAN) جلوگيری می كنند. اين ديواره ها هستند كه بر اساس مقررات امنيتی موجود تصميم می گيرند كدام داده ها وارد شبكه شوند يا ازشبكه 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[2] 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 افزاریست 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 آتشهای 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

[2] 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 معمولا 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، معمولا 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، معمولا 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، اولا هیچ گونه نیازی به تغییر نرم افزاری توپولوژی شبکه نیست، ثانیا هیچ کدام از برنامه های کاربردی نیازی به پیکربندی خاص (معرفی دیواره آتش به عنوان default gateway ، proxy و ...) ندارند.

5-2-4-2) فوائد 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 می کند.

2. دیواره آتش، خواه نا خواه برای کاربران قانونی هم محدودیت‌های دسترسی ایجاد می کند.

3. دیواره آتش حملات Back Door را نمی تواند 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 می گذرد، این مساله می تواند به یک معضل برای throughput سیستم تبدیل شود.

6. نفوذهايي كه از درون شبكه داخلی و به قصد ماشيني در همان شبكه انجام مي شود، از ديد ديواره آتش پنهان مي ماند، چرا كه اصولا بسته‌های مربوطه از ديواره آتش عبور نمي‌كنند. يكي از دلايل لزوم استفاده از سيستم‌های مهاجم‌ياب [3] نيز همين است.

5-2-4-3) تخريب ديواره‌هاي آتش

پياده‌سازي و نصب ضعيف ديواره‌هاي آتش يك دليل اساسي براي تخريب ديواره‌هاي آتش مي‌باشد. ديواره‌هاي آتش مي‌توانند به دو شكل " قوانين اجازه به صورت پيش‌فرض" و " قوانين عدم اجازه به صورت پيش‌فرض" پيكربندي شوند. در شكل قوانين اجازه پيش‌فرض، ديواره آتش به تمام بسته‌هاي اطلاعاتي ورودي به شبكه به جزء آنهايي كه ممنوع شده‌اند اجازه ورود مي‌دهند، در حاليكه در روش دوم يعني قوانين عدم اجازه پيش‌فرض، به هيچ بسته اطلاعاتي ورودي به شبكه به جزء آنهايي كه اجازه داده شده اجازه ورود نمي‌دهد. معمولا مديران امنيتي شبكه روش اول را بعنوان يك روش سهل‌انگارانه مي‌دانند و معمولا اين روش را قابل اعتماد نمي‌دانند.

[3] Intrusion Detection System

نقص و عيب در بخش نرم افزاري ديواره آتش ديگر دليل براي رخداد تخريب در آنها مي‌باشد. معمولا 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 مي‌كنند.

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

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

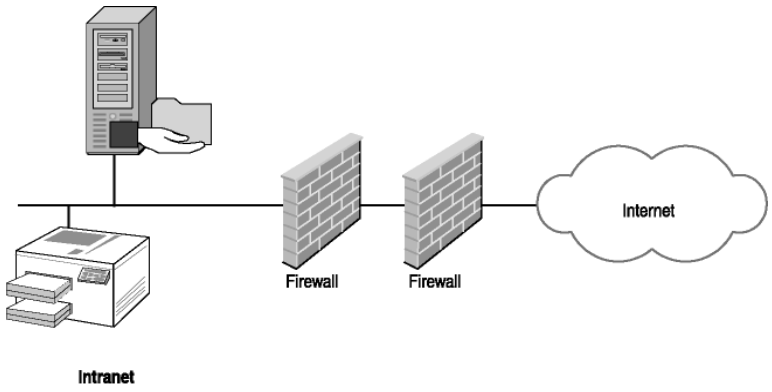
و در انتها امكان دسترسي فيزيكي به فايروال توسط مهاجمين مي‌تواند شرايط را براي خراب كردن و يا قطع كردن ارتباطات سيستم فايروال را براي مهاجمين به ارمغان آورد.

5-2-4-4) 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.
- بروزسازي فايل‌هاي شناسايي ويروسها
- حفاظت فيزيكي از فايروال‌ها.
- مستندسازي نحوه بهم‌بندي سيستم‌هاي فايروال و بررسي مجدد آن بصورت دوره اي.
- 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 سيستم فايروال توسط مديران شبكه- حتما از روشهاي احراز هويت مطمئن استفاده شود.
- استفاده از رمزهاي عبور تركيبي براي دسترسي به فايروالها. وتغيير اين رمز عبور بصورت دوره اي توسط مديران شبكه.
- اطمينان از عدم وجود راههاي دسترسي به شبكه كه تحت مديريت فايروال نباشد.
- استفاده از چند فايروال بصورت پشت سرهم، بالاخص استفاده پشت سرهم فايروالهاي شركتهاي سازنده مختلف، كمك زيادي به امن سازي شبكه ما ميكند. (همانطور كه در شكل 5-1 مشاهده ميشود)



شكل 5-1) استفاده از فايروال چندگانه

Modems (5-2-5

مودمها امكان اتصال كامپيوترها به اينترنت و يا شبكه داخلي را فراهم ميسازند. اما آنها ممكن است توسط مهاجمين تخريب گردند. مودمها ميتوانند امكان دسترسي به يك سيستم در شبكه و همچنين بصورت بالقوه امكان دسترسي به ديگر تجهيزات در شبكه را فراهم ميسازد. لذا از همين امكان فرد مهاجم ميتواند براي نفوذ به شبكه سوء استفاده كند.

براي محافظت از مودمها در مقابل حملات تخريبگرايانه بايد اعمال زير را انجام داد:

- جداسازي همه مودمهاي غيرضروري از كامپيوترهاي داخل شبكه
- بررسي بروز بودن همه نرم افزارهاي موجود بر روي كامپيوترهاي شبكه كه نياز به مودم دارند. مثلا بروزسازي

آنتي‌ويروسها و يا بروزسازي وصله‌هاي رفع عيب همه نرم افزارهاي موجود بر روي اين كامپيوترها.
- پيگيري از فروشندگان مودم‌ها براي دريافت وصله‌هاي برطرف كننده نقائص مودم‌ها و بروزسازي آنها.
- نظارت دوره‌اي بر كامپيوترهاي داراي مودم براي آنكه مورد تخريب قرار نگرفته باشند.

Wireless (6-2-5

بسياري از توليدكنندگان نقاط دسترسي بيسيم (APs) را كه بوسيله كارت‌هاي شبكه‌اي بيسيم قابل دسترسي است، بر روي تجهيزات خود تدارك ديده‌اند. ارتباطات مابين نقاط دسترسي و كارت‌هاي شبكه از طريف سيگنال هاي راديويي و سيگنال‌هاي مادون قرمز در فضا انجام مي‌گيرد. مهاجمين كه ممكن است از اين تجهيزات حتي مايل‌ها دور باشند، مي‌توانند بصورت بالقوه اين سيگنال‌ها را استراق سمع كنند. لذا براي فرد مهاجم نيازي به اتصال فيزيكي و يا برش بر روي سيم‌ها جهت اتصال به شبكه وجود ندارد. اين نقاط دسترسي همچنين مي‌توانند مانند هابها، سوييچ‌ها، و يا روترها عمل نمايند. بنابراين تمام حملاتي كه در گذشته بر روي اين تجهيزات مطرح گرديده بر روي نقاط دسترسي هم متصور مي‌باشد.

امروزه در بسياري از سازمان‌ها در كنار شبكه داخلي‌شان، امكان اتصال به شبكه اينترنت در اطراف فضاي اداري‌شان براي اتصال عموم مردم به شبكه اينترنت هم پيش‌بيني مي‌شود، كه اين خود نقطه بسيار خطرناكي براي نفوذ مهاجمين به شبكه داخلي‌شان مي‌باشد. لذا استفاده از روشهاي احراز هويت و همچنين رمزگذاري اطلاعات مهم، راه مناسبي براي جلوگيري بسياري از تخريب‌ها در اين شبكه‌ها مي‌باشد. اما بايد توجه داشت در كنار استفاده از اين روشهاي پيش رفته احراز هويت و رمزگذاري، امكانات، روشها و ابزارهاي پيشرفته‌اي نيز براي كمك به مهاجمين بصورت روزانه وارد بازار مي‌گردد. لذا بروز نگه‌داشتن تجهيزات امنيتي و استفاده از آخرين وصله‌هاي بر طرف كننده عيوب اين تجهيزات كه توسط توليد كنندگان آنها به بازار عرضه مي‌شود، مي‌تواند كمك شاياني براي مقابله با مهاجمين در اختيار ما قرار دهد.

راه حل ديگر براي جلوگيري از پراكندگي سيگنال‌هاي سيستم‌هاي بيسيم، پياده‌سازي اين تجهيزات در بخش‌هاي زيرين زمين و استفاده ازديوارهاي ضخيم مي‌باشد.

همچنين امواج تجهيزات بيسيم ممكن است در مقابل امواج راديويي و مغناطيس ديگر آسيب‌پذير باشند، لذا بالا بردن توان سيگنالينگ اين تجهيزات راه حل مناسبي براي اين مشكل مي‌باشد. همچنين در حين نصب تجهيزات بيسيم مطمئن گرديد مه نقاط دسترسي آنها در كنار منابع امواج راديويي و مغناطيسي ديگر مانند آسانسور، ماشين‌هاي كپي، فرستنده‌هاي راديويي، و يا تجهيزات صنعتي نمي‌باشد.

3-5) امنيت در منابع شبكه‌اي

در اين بخش اطلاعاتي در خصوص محافظت تجهيزات زير بنايي شبكه شما با توجه ويژه بر منابع شبكه‌اي و مانيتورينگ آنها ارائه خواهد گرديد.

1-3-5) امن‌سازي و مانيتورينگ ايستگاه‌هاي كاري (work Stations security)

ايستگاه‌هاي كاري در شبكه شما جهت مقاصد كاربردي مي‌باشد اما اين ايستگاه‌ها مي‌توانند آسيب‌پذير در مقابل مهاجمين باشند. تخريب ايستگاه‌هاي كاري در شبكه باعث اتلاف وقت كاربران آنها و همچنين از دست رفتن اطلاعات ذي‌قيمت مي‌شوند. اگر يك مهاجم بتواند به يك ايستگاه كاري در شبكه شما وارد شود و اخلالي را ايجاد نمايد، احتمالا مي‌تواند به ديگر تجهيزات در شبكه نيز دست‌اندازي كند. در زير بعضي از روش‌ها براي محافظت اين ايستگاه‌ها ذكر مي گردد:

- نصب آنتي ويروس‌ها و بروز نگه داشتن آنها
- مانيتورينگ فايل‌هاي ثبت وقايع(Log File) براي ايرادات بوجود آمده
- نصب سيستم ثبت اطلاعات و حسابرسي براي سيستم‌ها و منابع داده‌اي حساس در شبكه

- محدود سازي دسترسي به هر ايستگاه كاري توسط يك كاربر يا گروه مشخصي از كاربران
- كنترل دسترسي به منابع داخلي و يا منابع به اشتراك گذاشته شده در شبكه
- برداشتن برنامه‌ها و سرويس‌ها غير ضروري بر روي آنها
- نصب سيستم‌هاي اتوماتيك يا مركزي تهيه نسخه پشتيبان
- اطمينان از نصب بروزترين تعميركنندگان امنيتي(وصله) بر روي سيستم‌هاي عامل، و برنامه‌هاي كاربردي

همچنين سيستم‌هاي مانيتورينگ و سيستم‌هاي كشف نفوذ كه بعدا توضيح داده خواهد شد، مي‌تواند به حفظ امنيت ايستگاه‌هاي كاري در شبكه شما كمك كند.

از جمله مواردي كه در مانيتورينگ ايستگاه‌هاي كاري مي‌تواند مورد توجه قرار گيرند عبارتند از:

- سيستم ثبت وقايع: نظارت بر پيغام‌هاي خطا در باره تغييرات در سيستم فايلها، تغيير اجازه‌هاي دسترسي، سرويس‌هايي كه ديگر امكان شروع و انجام آنها وجود ندارد، و يا ديگر تغغيرات در سيستم.
- فضاي هارد ديسك: ايستگاه‌هاي كاري ممكن است از انجام ثبت وقايع، ثبت خطاها، كشف حملات و ديگر موارد به شكل صحيح، بدليل پر شدن فضاي هارد ديسكشان باز بمانند. پس مانيتورينگ ميزان فضاي خالي هارد ديسك ضروري است.

5-3-2) محافظت تجهيزات سيار (Mobile Device)

لپتاپ، نوتبوك، دستيار ديجيتالي شخصي(PDA) و ديگر تجهيزات سيار امروزه به شكل فزاينده‌اي در بسياري از شبكه‌هاي كامپيوتري بكار گرفته مي‌شود. حفاظت از اين تجهيزات نيز در شبكه امري ضروري است. البته مانيتورينگ اين تجهيزات سختتر از مانيتورينگ ايستگاه‌هاي كاري است.

تمامي مواردي كه براي امن‌سازي ايستگاه‌هاي كاري مطرح گرديد براي امنيت تجهيزات سيار نيز در صورت امكان ضروري است. اما ديگر موارد براي برقراري امنيت در خصوص اين تجهيزات عبارتند از:

- تجهيزات ضد سرقت: كاربرد تجهيزات هشداردهي و آلارم‌هاي تغيير جا براي اين تجهيزات، كابل‌هاي قفل‌شده
- استفاده از علائم و رنگ‌هاي شناسايي اضافي: اگر اين تجهيزات داراي رنگ‌هاي خاصي باشند و يا بر روي آنها علائم شناسايي و حتي نام سازمان حك شده باشد، پيگيري آنها را در بيرون سازمان هم مقدورتر مي‌سازد. از طرفي بكار گيري اين روش سارقان را در سرقت آنها بي‌ميل‌تر مي‌سازد.
- رمزگذاري داده‌ها: اگر تجهيزات موبايل شما براي نگهداري و يا انتقال داده‌هاي سري و مهم بكار گرفته مي‌شود، حتما اين گونه داده‌ها توسط الگوريتم‌هاي پيشرفته رمزنگاري بصورت رمز شده در آورده شود، تا در صورت دستيابي توسط مهاجمين به اين تجهيزات، اطلاعات درون آنها قابليت استفاده براي مهاجم را نداشته باشد.

5-3-3) امن‌سازي و مانيتورينگ سرورها (Servers security)

شما بايد همان عملكردها كه براي امن سازي ايستگاه‌هاي كاري انجام داده‌ايد، براي سرورها هم انجام دهيد. البته سرورها نياز به مراقبت بيشتري نسبت به يك ايستگاه كاري دارند، چرا كه تخريب يك سرور افراد بيشتري را تحت شعاع خود قرار مي‌دهد. از بعضي جهات حفاظت از سرورها راحت‌تر از حفاظت ايستگاه‌هاي كاري مي‌باشد، چرا كه آنها نيازي به دستيابي فيزيكي يا ورود بوسيله كاربران عادي ندارند. بعضي ديگر از راه‌هاي امنيتي براي محافظت از سرورها به شرح زير مي‌باشد:

- امن‌سازي فيزيكي سرورها از طريق قرار دادن آنها در اطاق‌هاي قفل‌دار
- جلوگيري از ورود كاربران بوسيله كنسول‌ها به آنها
- كنترل دقيق و مانيتورينگ دسترسي به منابع، از جمله سيستم فايل‌ها، داده‌هاي به اشتراك گذاشته شده، و چاپگرها
- كنترل دقيق و مانيتورينگ دسترسي به كليه سرويس‌ها. سرويس‌هاي اضافي همچون ديتابيس كاربران، سرويس وب، و ديگر سرويس‌هاي ارائه شده توسط سرور. همچنين شما بايد خطاهاي ايجاد شده در دسترسي به سرويس‌ها، خطا در اجراي سرويس‌ها، و هر تغييري در اجراي سرويس‌ها را رهگيري كنيد.
- ايجاد نسخه‌هاي پشتيبان بصورت دوره‌اي از بهم‌بندي سرورها، داده‌هاي به اشتراك گذاشته شده، و ديگر داده‌ها كه نياز

به حفاظت از آنها وجود دارد. همچنين بايد از حفاظت فيزيكي از اين نسخه هاي پشتيبان مطمئن گرديد. قرار دادن رمز عبور بر روي آنها و رمزگذاري آنها و قرار دادن آنها در گاوصندوق‌هاي ضد حريق از ديگر موارد مهم امنيتي مي‌باشد.

همچنين بايد از مانيتورينگ دسترسي‌ها و و در دسترس بودن منابع بر روي سرورها مطمئن گرديد. بطور مثال شما بايد از امكان پذير بودن سرويس HTTP براي دسترسي به وب سايت‌ها بر روي سرور خود اطمينان حاصل كنيد.

5-3-3) مانيتورينگ تجهيزات اتصال

امروزه سيستم‌هاي مديريت شبكه ارائه شده توسط بسياري از فروشندگان كه اطلاعات از تجهيزات اتصال را جمع‌آوري مي‌كنند، در دسترس مي‌باشند. بطور مثال، اگر يك روتر يا سوييچ بعضي ازفريم‌هاي اطلاعاتي را بدليل حجم بالاي ديتاهاي ورودي از دست بدهد، يك هشدار مي‌تواند به سمت كنسول مديريت شبكه و يا ديگر مكان‌هاي بالقوه مثل پيجر مدير شبكه ارسال گردد. بسياري از سيستم‌هاي مديريت شبكه از پروتكل (SNMP – Simple Network Management Protocol) براي جمع‌آوري اطلاعات از سيستم‌هاي مختلف، شامل ميزبان‌هاي انفرادي موجود در شبكه، استفاده مي‌كنند. بعضي از شركت‌هايي مانند: Cisco, IBM و Hewlett-Packard سيستم‌هاي مديريت شبكه‌اي را پيشنهاد مي‌دهند كه مي‌توانند تجهيزات شبكه را مانيتور كنند.

فصل ششم : امن‌سازي برنامه‌هاي كاربردي

مقدمه

همانطور كه در فصول پيشين ديديد راه‌هاي متفاوتي براي تخريب يك شبكه توسط مهاجمين وجود دارد. در اين فصل تلاش مي‌شود بر روي راه‌هاي تخريب از طريق برنامه‌هاي كاربردي موجود در شبكه، و همچنين روش‌هاي جلوگيري از اين حملات مطالبي ارائه گردد. البته توجه شود كه تمركز اصلي اين فصل بر روي بررسي برنامه‌هاي كاربردي در سمت كاربر(Client) مي‌باشد. البته در برنامه‌هاي كاربردي سمت سرويس‌دهنده (Server) نيز امكانات تخريبي وجود دارد كه در صورت داشتن زمان در اين ترم تحصيلي در فصل جداگانه‌اي مطالب مربوط به اين بخش نيز توضيح داده خواهد شد.

در اين فصل بر روي 2 برنامه اصلي شامل پست الكترونيكي(Email)، و تارنماي وب(Web)، توضيحات لازم ارائه خواهد گرديد.

6-1) امنيت بر روي پست الكترونيكي

اتصال بين يك كاربر و سرويس دهنده در شبكه جهاني اينترنت از ميان تعدادي سيستم غير مرتبط به طرفين اين ارتباط گذر مي كند. لذا در هر نقطه اتصالي از اين ارتباط، ترافيك در حال گذر قابل مانيتور مي‌باشد. انتقال اطلاعات رمزگذاري نشده در اينترنت عاملي است براي ناديده گرفتن محرمانگي.

امروزه پست الكترونيكي يكي از روش‌هاي ارتباطي متداول مي‌باشد. در اين قسمت بعضي از موضوعات وابسته به امنيت در پست الكترونيكي مورد توجه قرار مي‌گيرد.بعضي از مهمترين سرفصل‌هاي اين قسمت عبارتند ازك رمزگذاري ايميل، ابعاد آسيب‌پذيري ايميل، ايميل‌هاي ناخواسته، و ايميل‌هاي گول زننده (Hoaxes)، و ايميل‌هاي اسكم (Scam).

6-1-1) امن‌سازي پيغام‌هاي الكترونيكي

شبيه ارسال كارت پستال از طريق پست معمولي، ايميل‌هاي استاندارد اوليه نيز داراي نقاط آسيب‌پذيري از آن جهت كه توسط افراد غير هم خوانده شود وجود دارد. ايميل‌ها مي‌توانند توسط تجهيزاتي مانند پروتكل آنالايزر در طول مسير انتقالشان

مورد شنود قرار گيرند. طبق آمار تيم امنيتي CERT، در سال 1994 بيش از يك درصد ماشين‌هاي موجود بر روي اينترنت مورد تعرض شنود ايميل‌ها براي دستيابي به موضوعات مهم درون آنها مانند كلمه و رمز عبور توسط پروتكل آنالايزرها قرار گرفته‌اند. از طرفي به دليل فقدان محرمانگي، ايميل‌ها براحتي قابل جعل مي‌باشند. يك فرد حمله‌كننده مي‌تواند با تغيير فيلد ارسال‌كننده در ايميل‌ها، آنها را به شكلي كه از طرف فرد مطمئن و معتبري ارسال شده‌اند جلوه دهد.

لذا امن‌سازي انتقال اطلاعات مي‌تواند اين ابعاد ايمني را لحاظ كند. رمزگذاري ايميلها اين امكان را مي‌دهد كه تنها توسط افراد مورد نظر شما قابل فهم باشد. همچنين امن سازي پيغام‌هاي الكترونيكي مي‌تواند شامل امضاء الكترونيكي ايميل‌ها هم شود. با اين كار گيرنده نامه هم مطمئن مي‌گردد كه اين ايميل از جانب شخص شما مي‌باشد.

PGP (2-1-6

Pretty Good Privacy مجموعه‌اي از ابزارهاي نرم‌افزاري است كه به شما امكان رمزگذاري، رمزگشايي، و امضاء الكترونيكي بر روي اطلاعات ذاخل كامپيوترتان و همچنين ايميل‌ها را مي‌دهد. روش رمزگذاري و رمزگشايي در PGP بصورت نامتقارن(Asymmetric) مي‌باشد. PGP براي رمزگذاري و امضاء الكترونيكي اعمال زبر را انجام مي‌دهد:

- توليد كليدها: PGP زوج كليد عمومي و خصوصي را براي شما ايجاد مي‌كند.
- مديريت كليدها: PGP امكان نگهداري كليد عمومي ديگران را بصورت محلي براي شما امكان پذير مي‌سازد.
- رمزگذاري و رمزگشايي ايميل‌ها: دوستان شما مي‌توانند با كليد عمومي شما پبغام‌ها را رمزگذاري كنند، و شما هم مي‌توانيد با كليد خصوصي خودتان اين پيغام‌ها را از رمز در آوريد.
- امضاء ايميل‌ها: شما مي‌توانيد با استفاده از كليد خصوصي خودتان پيغام‌هاي ارسالي به دوستانتان را امضاء كنيد. و دوستانتان هم با داشتن كليد عمومي شما مي‌توانند اين امضاء را رمزگشايي كنند و از اينكه شما ارسال كننده واقعي ايميل هستيد مطمئن گردند.

- شما بايد كليد عمومي خود را بر افرادي كه علاقه‌منديد براي شما نامه بصورت رمزگذاري شده بفرستند يا اينكه بتوانند نامه‌هاي شما را كه امضاء ديجيتالي كرده‌ايد دريافت دارند، بفرستيد كليد خصوصي‌شما هم در كامپيوتر شخصي شما مورد استفاده شخص شما مي‌باشد. شما همچنين مي‌توانيد كليد خصوصي‌تان را در تجهيزات قابل حمل مانند فلاپي ديسك نيز قرار دهيد. كليد خصوصي با قرار دادن رمز عبور كه شما هنگام نصب PGP قرار مي‌دهيد، محافظت مي‌گردد. اين رمز عبور هر زمان كه از كليد خصوصي براي رمزنگاري يا امضاء استفاده مي‌كنيد از شما خواسته مي‌شود.
- توجه: PGP مي‌تواند با برنامه‌هاي كاربردي ايميل زير مجتمع گردد: Qualcomm Eudora, Microsoft Exchange, Microsoft Outlook, Microsoft Outlook Express, Lotus Notes.

S/MIME (3-1-6

اين نرم افزار هم شبيه PGP مي‌باشد، با اين تفاوت كه كاربران به تاييديه‌هاي ايجاد شده توسط PKI اعتماد مي‌كنند.

شما براي استفاده از S/MIMEبايد از برنامه‌هاي كاربردي كه S/MIME را قادر به استفاده مي‌كنند و همچنين دسترسي به يك تاييديه PKI ، استفاده كنيد. اين تاييديه مي‌تواند توسط يك PKI داخلي سازمان در اختيار شما قرار گيرد و يا اينكه توسط يك زيرساخت‌هاي توليد كليد خارجي (PKI عمومي) در اختيار شما قرار گيرد. دو نوع از اين PKIهاي عمومي، شركت Verisign با آدرس *(http:/www.virisign.com)* و شركت Thwate با آدرس *(http://www. Thwate.com)* مي‌باشد. البته در كشور ما ايران نيز به تازگي يكي از شركت‌هاي وابسته به وزارت بازرگاني در حال ارائه امضاء الكترونيكي و كليد عمومي و خصوصي مي‌باشد.

معروفترين برنامه‌هاي كاربردي كه S/MIME را قادر به استفاده مي‌كنند عبارتند از: Microsoft Outlook, Microsoft Outlook Express و Netscape.

نقاط آسيب‌پذيري پست الكترونيك (4-1-6

نقاط آسيب پذيري اغلب بر روي نرم‌افزارها ديده مي‌شود، و ايميل هم يك مستثناء نمي‌باشد. علاوه براينكه ايميل داراي نقاط آسيب‌پذيري براي تخريب خودش مي‌باشد، بلكه بسياري از مهاجمين از

اين نقاط آسيب براي تخريب ديگر امكانات سيستم مثل پاك كردن اطلاعات بر روي كامپيوتر شما، سوء اسفاده مي‌كنند.

براي محافظت از شبكه و سازمان‌تان در مقابل نقاط آسيب‌پذيري پست الكترونيكي، شما بايد در مقابل هشدارهاي امنيتي سيستم هشيار بوده و همچنين از ويروسيابهاي بروز شده استفاده نماييد. سرور درگاه ايميل مي‌تواند با اسكن ايميل‌هاي ورودي اين درگاه را ايزوله كرده و يا ويروس‌هاي متصل به ايميل‌ها را اجازه ورود به شبكه ندهد. اين يك راه عمومي براي بسياري از سازمان‌ها براي دفاع مي‌باشد. اما تك تك كامپيوترهاي موجود در شبكه شما هم مي‌توانند از ويروسيابها براي دفاع محكم‌تر استفاده كنند. اين كار علاوه بر جلوگيري از ورود ويروس‌هاي بيرون از شبكه به كامپيوتر شما، از ويروس‌هاي ايجاد شده توسط كاربران داخل شبكه شما نيز براي ورود به كامپيوتر شما جلوگيري مي‌نمايد.

شما همچنين بايد كاربران شبكه‌تان را در خصوص نقاط احتمالي حمله به وسيله ايميل‌ها آموزش دهيد. بطور مثال بسياري از كدهاي مخرب بصورت فايل‌هاي متصي به ايميل‌ها براي شما مي‌ايد، لذا كاربران بايد آموزش‌هاي لازم براي باز نكردن اين ايميل‌هاي مزاحم را ديده باشند.

هر زماني كه تخريبي بر روي يك نرم‌افزار ايميل اتفاق مي‌افتد، فروشندگان اين نرم‌افزارها نسبت به رفع نقاط آسيب آنها از طريق وصله‌هاي امنيتي مبادرت مي‌كنند، لذا ارتباط با فروشندگان و ره‌گيري اين وصله‌ها و نصب آنها بر روي كامپيوترهاي شبكه‌تان كمك شاياني به حفاظت از آنها در مقابل تهديدات ناشي از ايميل‌ها مي‌كند.

6-1-5) انواع ايميل‌هاي مخرب

در اين بخش ما انواع ايميل‌هاي مخرب را به سه دسته كلي:

- Spams
- Scams
- Hoaxes

تقسيم‌كرده ايم.

Spams (1-5-1-6

اين عنوان براي آندسته از ايميل هاي ناخواسته (مانند تبليغات تجاري) كه به آدرس‌هاي زيادي ارسال مي‌گردند اطلاق مي‌شود. در سال 2002 سايت آنلاين Business Week اعلام كرد نزديك به نيمي از ايميل‌هاي بعضي از سرويس‌دهندگان اينترنتي و ايميل مربوط به اين نوع از ايميل‌ها مي باشد.

براي محافظت سازمان‌تان در مقابل اين نوع از ايميل‌هاي مزاحم، شما بايد از نرم افزارهاي فيلتر كننده در درگاه سرور ايميلتان و همچنين تك تك كاپيوترهاي شبكه‌تان استفاده نماييد. بعضي از اين فيلترها عبارتند از: SpamAssassin, BrightMail, Cloudmark, DigiPortal's ChoiceMail, Mailshell . شما همچنين بايد كاربرانتان را براي برخورد با اين ايميل‌ها آموزش دهيد. بعضي از اين آموزش‌ها عبارتند از:

- *عدم پاسخگويی به Spamها*. پاسخگويي به ايجاد كنندگان Spamها باعث مي‌شود كه آنان از فعال بودن آدرس ايميل شما مطمئن گرديده و حتي آدرس ايميل شما را به ديگر توليدكنندگان Spam بفروشند.
- *آدرس ايميلتان را در داخل صفحات وب سايت‌ها پست نكنيد*. آدرس ايميل قرار داده شما در داخل صفحات اختصاصي وب شما و يا ديگران مي‌توانند كمك شاياني براي شناسايي آدرس ايميل شما توسط نرم افزارهاي اسكنري كه توسط توليدكنندگان Spam بطور دائم بر روي اينترنت و صفحات وب براي پيدا كردن آدرس‌هاي ايميل جستجو مي‌كنند، نمايد.
- *براي استفاده از گروه‌هاي خبري از آدرس ايميل دومی استفاده كنيد*. گروه‌هاي خبري مكان مناسبي براي جمع‌اوري آدرسهاي ايميل توسط توليدكنندگان Spam مي‌باشد. لذا براي اينكه آدرس ايميل اصلي شما لو نرود حتما براي ورود به گروه‌هاي خبري از آدرس ايميل دوم استفاده نماييد.
- *هرگز آدرس ايميل خود را، بدون دانست دليل اصلي براي خواستن آن، در جايی عرضه نكنيد*. بسياري از سايت‌ها براي اينكه بتوانيد وارد آنها شويد از شما آدرس ايميلتان و يك كلمه عبور را در خواست مي‌كنند. حتما قبل از ورود آدرس ايميلتان از "عبارات رعايت حريم ايميل" درخواستي توسط آن سايت مطمئن گرديد.

- *از فيلترهاي Spam* استفاده كنيد. بعضي از اين فيلترها به شما اجازه مي‌دهند بر اساس قوانيني كه توسط شما تعريف مي‌گردد عمل فيلترينگ انجام گيرد. مثل قوانيني بر مبناي عنوان ايميل، فرستنده، يا بدنه متن ايميل.
- *هيچگاه چيزي را كه در يك Spam* تبليغ شده را خريداري نكنيد.

Scams (2-5-1-6

شبيه مورد قبلي اين ايميل‌ها هم ناخواسته مي‌باشند. تفاوت ايندو در آن است كه Scamها محصولات و كالايي را براي فروش ارائه نمي دهند، بلكه بطور خاص هدفشان سرقت پول، كالاها، و سرويس‌ها مي باشد. اغلب آنها از قرباني تقاضاي ارسال پول، يا ارائه مشخصات حساب بانكي، و يا اطلاعات كارت اعتباري مي‌كنند. يكي از معروفترين اين ايميل‌ها، با نام ايميل پولشويي نيجريه‌اي معروف مي‌باشد. اگرچه محل ارسال حتمي اين ايميلهل كشور نيجريه نمي‌باشد، ولي اين ايميل‌ها به اين نام شهرت گرفته‌اند. در اين ايميل‌ها مثلا از فرد مورد تهاجم درخواست مي‌گردد براي اينكه پولي كه از طرف فردي كه از دنيا رفته و آن پول به شما به ارث رسيده، به حساب شما واريز گردد، مشخصات حساب بانكي‌تان را بدهيد و يا اينكه حسابي مثلا در فلان بانك افتتاح كنيد. بدبن طريق فرد طمعكار قرباني اهداف پولشويي باندهاي تبهكاري قرار گرفته و از طريق حساب بانكي اين فرد اعمال خلاف قانون پولشويي انجام مي‌گيرد.

براي محافظت كامپيوترتان يا شبكه‌تان از سوء استفاده اين ايميل‌ها، تنظيم سياستنامه امنيتي و قرار دادن مطالبي در خصوص رعايت محرمانگي اطلاعات ويژه مانند شماره حساب بانكي و يا شماره بيمه‌نامه و ... در آن امري لازم مي‌باشد. شما بايد در اين سياستنامه مشخص سازيد چه اطلاعاتي حساس مي‌باشند. همچنين بايد در اين سياستنامه كانال‌هاي امن ارسال داده و كانال‌هاي ناامن مشخص گردند. همچنين آموزش اين نكات امنيتي به كاربران شبكه‌تان لازم مي‌باشد. همچنين آموزش اينكه چه ايميل‌هايي مي‌توانند يك ايميل Scam باشد به كاربران ضروري است. بعضي از مشخصه‌هايي موجود در يك ايميل كه مي‌تواند بيانگر يكScam باشد بشرح زير است:

- فرصت‌هاي تجاري(Business Opportunity Scams)

- پولسازي از طريق ارسال ايميل‌هاي عمده (Make Money by Sending Bulk E-Mail)
- نامه هاي زنجيره اي (Chain Email)
- برنامه كار در خانه (Work-at-Home Scheme)
- سلامتي و رژيم (Health and Diet Scams)
- درآمد بدون تلاش(Effortless Income)
- كالاي مجاني(Free Goods)
- فرصت‌هاي سرمايه‌گذاري(Investment Opportunities)
- وام ها و يا اعتبارهاي تضمين شده (Guaranteed Loans or Credit)
- اصلاح اعتبار (Credit Repair)

Hoaxes (3-5-1-6

يك ايميل از نوع Hoaxes مانند يك نامه زنجيره‌اي در شبكه پخش مي‌گردند. آنها حاوي اطلاعات غلط ولي قابل باوري مي‌باشند. اين ايميلها معمولا از سوي يك شخص به تعداد زيادي از افراد براي اينكه ايده يا ديدگاهي را در افراد به باور برسانند ارسال مي‌گردد. معمولا در اين ايميل‌ها از گيرنده درخواست مي‌شود كه آن را براي دوستانش هم ارسال كند. يكي از معروفترين اين ايميلها ايميلي با عنوان Good Time استكه به سرعت در شبكه پخش گرديد و با داشتن كد مخرب درون خود باعث تخريب اطلاعات درون هارد ديسك‌هاي بسياري از كامپيوترها گرديد.

بعضي از اين ايميلها به شما اعلام مي‌كنند كه مثلا كامپيوتر شما توسط يك نامه كه از طرف دوستتان ارسال گرديده ويروسي شده و نام فايل ويروس را هم اعلام مي‌كنند. در حاليكه اين فايل يكي از فايلهاي اصلي سيستم شما مثلا Sulfnbk.exe , jdbgmgr.exe مي‌باشد و شما به تصور اينكه اين فايل‌ها ويروس مي‌باشند نادانسته آن را از روي سيستم‌تان پاك كرده و ادامه كار كامپيوترتان را دچار اخلال مي‌نماييد.

براي محافظت از شبكه‌تان در مقابل اين نوع از ايميل‌ها بايد سياستنامه امنيتي مبني بر شناسايي اين نامه‌ها و نحوه برخورد با انها را در سازمانتان تنظيم كرده و آن را به كاربران شبكه‌تان هم آموزش دهيد. بعضي از عناوين در اين نوع ايميل‌ها كه كمك به شناسايي آنها مي‌كند عبارتند از:

- *فوري(Urgent)* . كلماتي مانند فوري، مهم، خطر، هشدار ويروس معمولا در عنوان اين ايميل‌ها وجود دارند
- *به دوستان خود بگوييد (Tell all Your Friens)*. معمولا اين درخواست در داخل ايميل مي‌تواند وجود داشته باشد.
- *اين يك Hoax نيست(This isn't a Hoax)*. اين پيغام‌ها معمولا شامل معرفي افرادي به عنوان تاييد كننده آن هست كه افراد قابل اعتمادي مي‌باشند. بطور مثال فرستنده اصلي آن مي‌تواند عبارتي مانند" اين هشدار توسط فلان مقام قانوني و يا فلان ايستگاه خبري تاييد شده" را براي فريب افراد در آن قرار دهد.
- *پي‌آمد ناگوار(Dire Consequence)*. اين ايميل‌ها مي‌تواند حاوي اخطارهاي بسيار فوري مبني بر اينكه مثلا اطلاعات در كامپيوتر شما در حال تخريب ميباشد، باشند.
- *تاريخچه (History)*. اگر يك پيغام حاوي"FW" در قسمت موضوع خود باشد، و يا تعداد زيادي پرانتز زاويه‌دار(شبيه <<<<<<) در عنوان خود باشد، اين پيغام احتمالا چندين بار فوروارد(Forward) شده است، و مي‌توان احتمال داد اين يك ايميل Hoax مي‌باشد.

6-2) امنيت بر روي وب

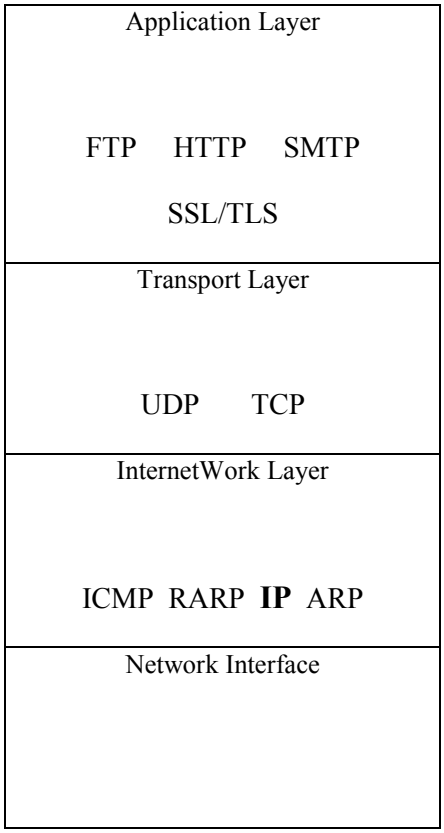
همانطور كه در گذشته گفته شد سرقت بسته‌هاي اطلاعاتي عاملي است براي اينكه فرد مهاجم بتواند شبكه و كامپيوترهاي يك سازمان را تخريب كند. معمولا اين حمله متكي بر ضعف‌هاي برنامه‌هاي كاربردي است كه ناشي از ضعف در مرحله طراحي و برنامه‌نويس آنها مي‌باشد. حتي مهاجمين مي‌توانند كاربران را براي دريافت برنامه‌هايي كه حاوي ويروس مي‌باشند فريب دهند. . در اين بخش هدف بيان مخاطرات و نحوه مقابله با اين مخاطرات در محيط وب مي‌باشد.

6-2-1) SSL/TLS

پروتكل‌هاي لايه سوكت امن (Secure Sockets Layer) و امنيت لايه انتقال (Transport Layer Security) براي پياده‌سازي امنيت در تبادلات كلاينت/سرور در اينترنت بكار برده مي‌شود.

در سال 1994 شركت نتاسكيپ پروتكلي به نام SSL را ارائه كرد. اساس اين پروتكل مبتني بر رمزگذاري بوسيله كليدهاي غيرمتقارن كه توسط شركت RSA ارائه مي‌گردد، بود. در سال 1999 سازمان IETF پروتكل جديدي را ارائه كرد كه مبتني بر SSL بود كه آن را TLS ناميد. امروزه بسياري از توليدكنندگان نرمافزار در دنيا محصولاتي ارائه مي‌دهند كه اين پروتكل هاي امنيتي را پشتيباني مي‌كنند. علاوه بر اين از اين دو پروتكل در اكثر مواقع بصورت متشابه در غالب عنوان مشترك SSL/TLS ياد مي‌شود.

SSL/TLS ارتباطات اينترنتي را در مقابل استراق سمع، مداخله، و جعل محافظت مي‌كنند. كلاينت و سرور مي‌توانند با استفاده از آن همديگر را احراز هويت كرده و پيغام‌ها را به شكل رمزگذاري شده در اينترنت انتقال دهند. SSL/TLS پروتكل غير وابسته به لايه‌اي در شبكه مي‌باشد كه طبق شكل 6-1 مابين دو لايه كاربردي و انتقال قرار مي‌گيرد. هر برنامه كاربردي در شبكه مبتني بر IP كه بطور خاص پروتكل SSL/TLS را در خود پيشبيني كرده باشد، مي‌تواند از اين پروتكل به نحو احسن براي امن‌سازي انتقال اطلاعات بين كلاينت و سرور بهره برداري كند.



شكل 6-1) SSL/TLS در پشته پروتكل TCP/IP

- **احراز هويت سرور براي كلاينت .** زماني كه يك مشتري قصد خريد كالايي از يك فروشنده بر روي وب سايت را دارد، مشتري ميخواهد از اينكه اين وبسايت توسط يك فروشنده واقعي جهت فروش محصولاتش ايجاد شده است مطمئن گردد. SSL/TLS اين امكان را براي كامپيوترهاي مشتريان فراهم ميآورد كه از مطمئن بودن سرويس فروش و تعلق آن به فروشنده واقعي آن محصول مطمئن گردد.(و اينكه اين سايت فروش از جانب يك سارق براي به سرقت بردن اطلاعات كارت فروش مشتري تدارك ديده نشده است). براي اين منظور اين سرور بايد يك گواهينامه از يك CA قابل اعتماد براي كاربر، دريافت كرده باشد.
- **مبادله الگوريتم رمزگذاري مشترك.** كلاينت و سرور ميتوانند الگوريتم رمزگذاري مورد استفادهشان را مبادله كنند. اينكار طرفين كلاينت و سرور را براي پشتيباني از تكنيك رمزگذاري قلدر ميسازد.
- **احراز هويت كلاينت براي سرور(اختياري).** وقتي كه محدودسازي دسترسي به سرور توسط كلاينتها مورد نظر باشد، كامپيوترهاي كلاينت بايستي گواهينامه معتبري از يك CA را بر روي خود نصب كرده باشند. البته در بسياري از خريدهاي اينترنتي اين كار انجام نميگيرد چرا كه بسياري از خريداران گواهينامه معتبري در دست ندارند. لذا براي شناسايي كلاينتها در تجارت الكترونيكي معمولا از مشخصاتي مثل شماره كارت اعتباري، تاريخ اعتبار آن، و آدرس صدور صورتحساب براي شناسايي كلاينتها توسط سرورها استفاده ميشود.
- **استفاده از رمزگذاري غيرمتقارن براي ارسال رمزهاي اشتراكي.** رمزگذاري غيرمتقارن (يا كليد عمومي) براي شكسته شدن سخت ميباشد. و رمزگذاري متقارن براي انتقال دادههاي حجيم بسيار كارآ ميباشد. SSL/TLS از رمزگذاري غير متقارن براي ارسال رمزهاي اشتراكي(كليد متقارن) استفاده ميكند، بنابراين رمزگذاري داده واقعي بسيار سريعتر ميشود، و در عين حال روش برقراري ارتباطات رمزگذاري شده نيز بسيار امن ميباشد.
- **برقراري يك اتصال رمزگذاري شده.** در انتها، و البته بسيار مهم، تمام ارتباطات ميان كلاينت و سرور رمزگذاري شده ميباشد.

HTTPS (2-2-6

ارتباطات وب با بكارگيري HTTP اجرا مي‌گردد. ارتباطات وبي كه بوسيله SSL/TLS امن شده است با عنوان HTTPS ناميده مي‌شود. مرورگرهاي وب كه ارتباطات HTTPS را نشان مي‌دهند از علامت https:// (به جاي http://) در بخش آدرس وب استفاده مي‌كنند.

اگرچه HTTPS ارتباط بين كلاينت و سرور را رمزگذاري مي‌كنند، اما قابل اعتماد بودن فروشنده يا امن بودن سرور فروشنده را تضمين نمي‌كند.

SSL/TLS جهت شناسايي سرور فروشنده و رمزگذاري ارتباطات بين كلاينت و سرور طراحي شده است. SSL/TLS قادر به جلوگيري از اعمال غير اخلاقي بر روي اطلاعات جمع‌آوري شده از كارت‌هاي اعتباري توسط فروشنده ، نمي‌باشد. همچنين SSL/TLS قادر به محافظت از اطلاعات ذخيره شده بر روي كامپيوتر سرور فروشنده نمي‌باشد. متاسفانه بسياري از كامپيوترهاي سرور سمت فروشنده مورد تعرض قرار مي‌گيرند (و مشخصات كارت اعتباري خريداران سرقت مي شود). به اين دليل بسياري از فروشندگان اطلاعات كارت اعتباري خريدارانشان را ير روي سرور خود ذخيره نمي كنند.

Buffer Overflows (3-2-6

بافر به فضاي داده‌اي اطلاق مي‌شود كه بوسيله هر دو عنصر تجهيزات سخت افزاري و پروسس‌هاي نرم افزاري به اشتراك گذاشته مي‌شود. در اين بخش تمركز ما بر روي بافرهاي برنامه‌اي، كه اجازه اجراي برنامه‌هاي مختلف با اولويت‌هاي مختلف را مي‌دهند، مي‌باشد. هر بافر داراي سطح مشخص و يك مرز مي‌باشد.

سرريزي بافر زماني اتفاق مي‌افتد كه يك برنامه تلاش مي‌كند داده‌هاي بيشتر از ظرفيت بافر را وارد آن كند. اين كار گاها باعث آن مي‌شود كه حجم داده اضافي بر روي بافرهاي كناري ريزش كرده و باعث خرابي داده‌هاي موجود در آنها شود. سرريزي بافر ممكن است بدليل ضعف در ساختار برنامه و يا ناشي از يك حمله تخريب آميز باشد. يك مهاجم از اين روش براي در اختيار گرفتن كامپيوتر قرباني استفاده مي‌كند. در يك حمله، سرريز بافر ممكن است باعث خراب شدن فايل‌ها، تغييرات داده‌ها، استحصال اطلاعات محرمانه، و يا اجراي كد بر روي ماشين هدف گردد.

بهترين راه در برخورد با اين مشكل اين‌استكه پيادەكنندگان نرم افزار از روشهاي برنامەنويسي امن طبعيت كنند. اجراي عمليات امن برنامه نويسي به معناي طراحي برنامەنويسي به طرق امن آن در ذهن برنامەنويس مي‌باشد. توجه به اينكه چگونه اين برنامه مي‌تواند تخريب و يا جهت تخريب ديگر برنامه‌ها استفاده شود، از راهكارهاي اجرايي مي‌باشد. بسياري از پيشنهادات مربوط به طراحي امن يك برنامه را در كيت پيادەسازي برنامه (SDKs) مي‌توان يافت. اين كيت يك راهنماي برنامه نويسي است كه در آن موضوعاتي از قبيل ساختار يك برنامه، فانكشن‌ها، و روشهاي پيادەسازي يك برنامه بر روي پلتفرمي خاص بيان گرديده است.

يكي ديگر از راه‌هاي برخورد صحيح با اين پديده، رەگيري از فروشندگان برنامه‌ها براي بهره برداري از وصله‌هايي است كه در مرور زمان براي حل مشكلات اين نرم افزارها توسط فروشندگان آن به بازار عرضه مي‌گردد.

Active Content (4-2-6

در راستاي تلاش براي اينكه مرور صفحات وب مهيج، كاربردي، ومفيد گردند، توليدكنندگان و فروشندگان نرم افزارها محتواهاي فعال(Active Content) را ايجاد مي‌كنند. مواد محتواهاي فعال برنامه اجرايي كوچك و يا كدهاي اسكريپت مي باشند كه به داخل مرورگرهاي وب ارائه مي‌گردند. بطور مثال، بعضي از بانكها حسابگرهايي براي محاسبه ميزان پرداخت رهن را در داخل وب سايتهايشان پيشنهاد مي‌دهند. اين ماشين‌حسابهاي محاسب رهن به عنوان محتواي فعال شناخته مي‌شوند. به عنوان مثال‌هاي ديگر مي‌توان ازبعضي از محتواهاي ويدئويي و انيميشني بر روي صفحات وب نام برد. دو نوع مرسوم محتواهاي فعال جاوا اسكريپتها(JavaScript) و اكتيوكس (ActiveX) مي‌باشند. محتواهاي فعال براي اجراي يك اسكريپت در داخل سيستم كلاينت طراحي شده‌اند. متاسفانه، اين امكان باعث ايجاد ريسك‌هاي امنيتي در سيستم‌ها هم مي‌شود: بعضي از اين اسكريپتها باعث ايجاد عملكردهاي مخرب در ماشين كلاينت هم مي‌شوند. در اين فصل تمركز اصلي ما بر روي اين محتواهاي فعال در سمت كلاينت و امكانات تخريب آميز ممكنه آنها مي‌باشد.

Java Applets (1-6-2-4

جاوا زبان برنامه نويسي ارائه شده توسط شركت سان (Sun Microsystems) مي‌باشد كه داراي امكاناتي است كه استفاده از آن را براي محيط وب مناسب مي‌سازد. برنامه‌هاي كوچك كامل در اين زبان Java Applets ناميده مي‌شود، كه بر روي بيشتر مرورگرهاي سمت كلاينت اجرا مي‌گردد. بطور مثال نت اسكيپ و اينترنت اكسپلورر اين برنامه‌هاي كوچك را پشتيباني مي‌كنند.

اين برنامه‌هاي كوچك از داخل يك صفحه وب توسط برچسب‌هاي اپلت (APPLET tag) آدرس دهي مي‌شوند. اين برچسب‌ها براي بارگذاري فايل‌هاي مربوط به متن كد جاوا استفاده مي‌شوند. كد متن جاوا توسط موتوري بر روي كلاينت به نام ماشين مجازي جاوا *(Java Virtual Machine)* اجراء مي‌شوند. اين VMها بر روي بسياري از سيستم‌هاي عامل مانند يونيكس، مكينتاش، و ويندوز اجراء مي‌شوند.

توجه: سيستم عامل Windows XP به همراه خود اين VM را ندارد، و اين بدان معناست كه به خودي خود امكان اجراي Java Appletها را ندارد. لذا در صورت نياز به اجراي اين اپلت‌ها بر روي اين سيستم عامل حتما نرم افزار ماشين مجازي جاوا *(Java Virtual Machine)* را بر روي كامپيوتر خود دريافت كنيد.

متاسفانه مهاجمين مي‌توانند از اين امكان براي حمله به سيستم‌هاي سمت كلاينت استفاده كنند. شما براي اينكه خود وسازمان‌تان را در مقابل حملات از طريق Java Appletها محافظت كنيد، مي‌توانيد امكان پشتيباني جاوا را بر روي ماشين‌تان غير فعال كنيد. بسياري از مرورگرها (مثل نت اسكيپ و اينترنت اكسپلورر) امكان غير فعال كردن جاوا را به شما مي‌دهند.

Java Script (2-6-2-4

شركت نت‌اسكيپ جاوا اسكريپت را بوجود آورد، يك زبان اسكريپت كه تعداد زيادي از استراكچرها و ويژگي‌هاي جاوا را به مشاركت مي‌گذارد. به هر حال، جاوا و جاوا اسكريپت به صورت مستقل از هم پياده‌سازي شده‌اند و دو زبان مستقل از هم تلقي مي‌شوند.

بسياري از مرورگرهاي وب، شامل نت اسكيپ و اينترنت اكسپلورر، جاوا اسكريپت را پشتيباني مي‌كنند. جاوا اسكريپت نوعا در داخل صفحات HTML قرار داده مي‌شود و توسط مرورگر وب در سمت كلاينت خوانده مي‌شود. يك برچسب اسكريپت (SCRIPT tag) در داخل

كدهاي HTML براي نشانه گذاري جاوا اسكريپت قرار داده مي‌شود. جاوا اسكريپت معمولا براي ارتباط با ديگر اجزاء (مانند برنامه‌هاي CGI كه بعدا توضيح داده خواهد شد) و يا دريافت اطلاعات ورودي از كاربران مورد استفاده قرار مي‌گيرد.

توجه: جاوا اسكريپت مي‌تواند براي باز كردن جاوا اپلت‌ها هم مورد استفاده قرار گيرد. بطور مثال، جاوا اسكريپت و جاوا اپلت ممكن است به همراه هم براي ايجاد يك محاسب ميزان رهن ، نقشه‌هاي تعاملي، و بسياري از موارد ديگر استفاده شوند.

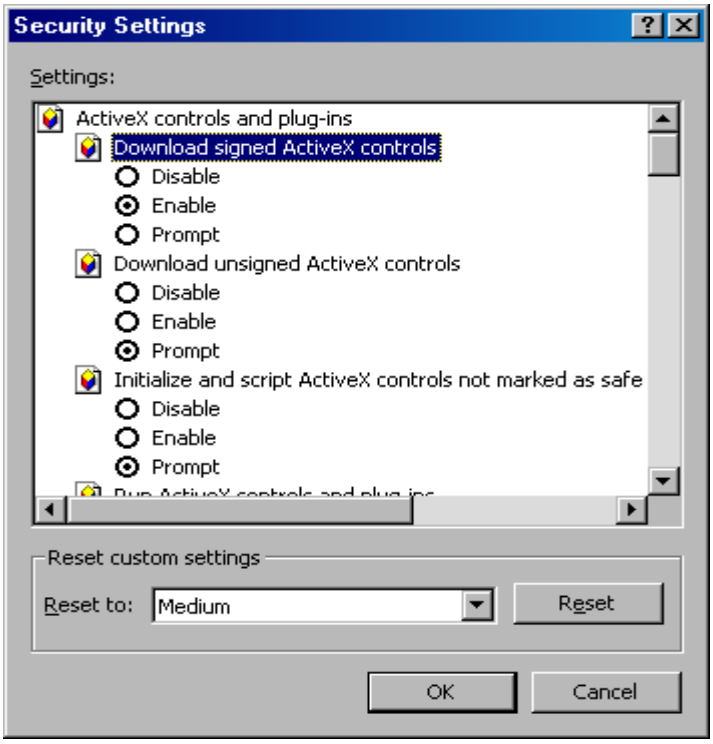
مهاجمين مي‌توانند از جاوا اسكريپت‌ها براي حمله به سيستم كلاينت‌ها سوء استفاده كنند. براي محافظت از خودتان و سازمان‌تان در مقابل جاوا اسكريپت‌هاي مخرب، شما مي‌توانيد جاوا اسكريپت را بر روي كامپيوترتان غير فعال كنيد. اگر چه غير فعال سازي جاوا اسكريپت بر روي كامپيوترتان شما را در مقابل اين نوع حملات بيمه مي‌كند، اما شما را هم از بهره‌گيري استفاده‌هاي مفيد از محتواهاي فعال محروم مي‌سازد. به هر حال، شما مي توانيد بصورت انتخابي در مورد سايت‌هايي كه به آنها وارد مي‌شويد و داراي اپلت‌هاي جالب و قابل اعتمادي هستند، جاوا اسكريپت خود را فعال كنيد. به هر صورت، در صورتيكه شما علاقه‌مند باشيد كه جاوا اسكريپت خود را فعال نگه داريد، حتما بايد مرورگر وب خود را با آخرين نسخه‌هاي وصله‌هاي نرم افزاري بروز نگه داريد. در صورت غير فعال كردن جاوا اسكريپت بر روي مرورگر خودف در صورتيكه وبسايتي بخواهد به روي كامپيوتر شما محتواي فعالي بفرستد، شما بر روي صفحه كامپيوتر خود جملات زير را مشاهده خواهيد كرد كه در صورت كليك بر روي اين جملات راه فعال سازي مرورگر وب شما براي دريافت محتواي فعال را به شما نشان مي‌دهد.

"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

اين تكنولوژي هم براي فراهم‌سازي محتواي فعال بوجود آمده است. لازم به توجه است كه اين تكنولوژي توسط شركت مايكروسافت تنها براي استفاده در مرورگرهاي اينترنت اكسپلورر طراحي گرديده و در حال حاضر در هيچ مرورگر ديگري

پشتيباني نمي‌شود. شبيه جاوا اسكريپت، اكتيوكس هم مي‌تواند با ديگر برنامه‌هاي كاربردي ارتباط برقرار كرده، داده‌هاي ورودي توسط كاربران را دريافت دارد، و سرويس‌هاي كاربردي را براي كاربران تدارك ببيند. همچنين مانند جاوا اسكريپت در معرض سوء استفاده توسط مخربين براي حملات مي‌باشد.



شكل 6-2) تنظيمات ActiveX در اينترنت اكسپلورر

براي كمك به حفاظت سيستم‌ها از تخريب‌هاي ناشي از سوء استفاده از اكتيوكس، اينترنت اكسپلورر به شما امكان انتخاب دريافت و اجراي كنترل‌هاي اكتيوكس مطابق شكل 6-2 را مي‌دهد. شما مي‌توانيد اينترنت اكسپلورر را به شكلي تنظيم نماييد كه به صورت اتوماتيك كنترل اكتيوكس را دريافت نمايد، يا قبل از دريافت به شما پيغامي مبني بر دريافت يا عدم دريافت دهد، و يا بطور كلي دريافت هر گونه كنترل اكتيوكس را غير فعال نمايد.

اگر شما لازم است از كنترل اكتيوكس استفاده كنيد، شما بايد بطور دائمي سايت فروشنده نرم افزار را براي هشدارهاي امنيتي و اطلاعاتي در مورد احتمالات تخريب مورد مطالعه قرار دهيد. اگر شما متوجه شديد كه يك كنترل كننده خاص اكتيوكس دچار مخاطراتي براي امكان حمله مي‌باشد، شما بايد آنرا غير فعال كرده تا وصله امنيتي آن ارائه گردد.

Signing Active Content (4-6-2-4

در تلاش براي افزايش امنيت محتواهاي فعال، بعضي از فروشندگان فرآيندي را براي انجام امضاي ديجيتالي قبل از نصب محتواهاي فعال، پيادهسازي كردهاند. توليد كنندگان محتواهاي فعال قبل از ارسال اين محتواهاي فعال آنها را امضاي ديجيتالي مينمايند اين ارائه دهندگان تاييديه امضاء براي امضا نمودن محصولاتشان را از يك CA قابل اعتماد(مانند Verisign) دريافت ميكنند. امضاء الكترونيكي كمك به ايجاد اعتماد از آن جهت كه محتواي فعال ارائه شده از يك فروشنده معتبر ميباشد، ميكند.

مايكروسافت از يك تكنولوژي در اينترنت اكسپلورر به نام *Authenticode* براي يررسي صحت امضاء قبل از دريافت محتواي فعال از يك فروشنده، استفاده ميكند.

بايد توجه داشت اگر چه اين كار امنيت زيادي را براي دريافت محتواهاي الكترونيكي به ارمغان ميآورد، اما در مقابل مشكلاتي كه ممكن است از طرف يك فروشنده مورد اعتماد بوجود آيد، و يا در مورد حفرههاي امنيتي كه ممكن است در نرمافزاري در آينده مشخص شود، قادر به عملكرد پيشگيرايانه نميباشد. لذا هميشه توجه داشته باشيد كه آخرين وصلههاي امنيتي را هم از فروشندگان براي رفع عيوب دريافت داريد.

Cookies (5-2-6

كوكي عبارت است از مقدار كوچكي از اطلاعات كه يك وب سرور در مورد يك كاربر بر روي كامپيوتر خود كاربر ذخيره ميكند. بطور مثال، كوكي ممكن است تبليغات مختلفي كه يك مرورگر كلاينت دريافت كرده است را ضبط نمايد. اين امر به وب سرور كمك ميكند تبليغات متفاوتي غير از تبليغاتي كه براي كاربر در گذشته نشان داده است را به نمايش گذارد.

مرورگر سمت كلاينت معمولا به سرورها اجازه ذخيره سازي كوكيها را ميدهند. بسياري از مرورگرها به اين دليل اين اجازه را صادر ميكنند كه امروزه كوكيها در حجم بالايي مورد استفاده ميباشند، و بسياري ار وب سرورها قادر به انجام فعاليت صحيح خود بدون آنها نمي باشند. كوكيها بسته به مرورگر وب مورد استفاده در مكانهاي مختلفي ذخيره مِي شوند. بطور مثال نت

اسكيپ كوكي‌ها در فايلي به نام Cookies.txt و اينترنت اكسپلورر هر كوكي را در فايل‌هاي جداگانه‌اي در پوشه‌اي به نام Temporery Internet Files\ %windir% ثبت مي‌نمايد.

كوكي‌ها به دلايل مختلف استفاده مي‌شوند. بطور مثال، بعضي از كوكي‌ها براي ثبت علايق كاربران وقتي به وب سايتي متصل مي‌شوند، بكار مي‌روند. ديگر كوكي‌ها براي پشتيباني از وضعيت اطلاعات بكار مي‌روند(وضعيت اتصال بين كلاينت و سرور). بعضي از سرورها هم از كوكي‌ها براي مقاصد احراز هويت كلاينت‌ها استفاده مي‌كنند. متاسفانه كوكي‌ها هم مي‌توانند توسط مهاجمين به طرق زير براي مقاصد سوء مورد استفاده قرار گيرند:

- كوكي‌ها مي توانند اداره شوند و يا دزديده شوند. حمله كننده مي‌تواند كوكي‌ها را براي بدست آوردن اطلاعات مهم در مورد كاربران شبكه، سازمان، و مسائل امنيتي در شبكه داخلي شما به سرقت ببرد.
- مهاجم مي‌تواند با قرار دادن يك اسكريپت به داخل كامپيوتر كلاينت، كوكي‌ها داخل سيستم كلاينت را به طرف سيستم خودش انتقال دهد. حتي احتمال استراق سمع كوكي توسط مهاجمين در حين انتقال وجود دارد.

براي محافظت سازمان و كلاينت‌هاي سازمان‌تان در برابر تخريب هاي ناشي از سوء استفاده از كوكي‌ها، مي‌بايست از روشهاي زير بهره ببريد.

- وب سرور خود را با اتكا و اعتماد بر اطلاعات ذخيره شده در كوكي‌هاي سمت كلاينت جهت كنترل دسترسي به منابع يا ارائه هر سرويس اضافه، پيكربندي نكنيد. چرا كه ممكن است از اين طريق توسط مهاجمي كه بر روي كوكي‌ها دسترسي داشته، تخريبي بر روي وب سرور شما انجام گيرد.
- از كوكي‌ها براي نگهداري اطلاعات محرمانه و مهم مانند كد شماره حساب بانكي، و گواهينامه‌هاي احراز هويت (مانند كلمه عبور)، استفاده نكنيد.
- اگر لازم است كه اطلاعات مهمي در كوكي‌ها نگه‌داري شود، حتما از SSL/TLS براي محافظت از اطلاعات داخل كوكي‌ها استفاده شود.

CGI (6-2-6

برنامه‌هاي CGI معمولا براي توليد محتواهاي فعال در وب سرورها مورد استفاده قرار مِي گيرد. CGIها معمولا براي ارسال اطلاعات ميان برنامه]كاربردي و وب سرورها مي‌باشند. بطور مثال، آنها معمولا براي انجام كارهايي مانند وارد كردن داده، جستجو، فانكشن‌هاي بازيابي در ديتابيس‌ها، مورد استفاده قزار مي‌گيرند.

با زبانهاي مختف برنامه نويسي مي‌توان CGIها را ايجاد كرد، زبان‌هايي همچون C, C++, Visual Basic, Fortran, PERL.

اين برنامه‌ها مي‌توانند هدف حمله براي تخريب وب سرورها قرار گيرند. بر خلاف Java Script و ActiveX، كه بر روي كامپيوتر كلاينت اجرا مي‌شوند، بر روي كامپيوتر وب سرور اجراء مي‌گردد. البته شبيه ديگر برنامه‌ها ، اين برنامه هم مي‌تواند داراي حفره‌هاي امنيتي باشد كه توسط مخربين سوء استفاده شود. در زير برخي از تخريب‌هاي ممكنه بر اساس اين برنامه‌ها آورده شده است.

- اجراي چندين باره يك برنامه CGI از طريق مرورگرهاي چندگانه وب. هر گاه كه يك برنامه CGI توسط مرورگري اجراء مي‌گردد، بخشي از ظرفيت منابع سيستمي بر روي وب سرور را براي اجراء در اختيار مي‌گيرد، حال اگر مهاجمي به كرات دستور اجراي اين برنامه را بر روي مرورگر خود بدهد، ظرفيت منابع وب سرور مورد استفاده قرار مي‌گيرد، و اين عاملي است براي پايين آمدن سرعت سرويس‌دهي وب سرور.
- تهديد از طريق برنامه‌هاي CGI كه بعضا در كنار خود وب سرور به صورت پيش فرض ارائه مي‌گردد. اين برنامه‌ها ممكن است داراي حفره‌هاي امنيتي باشند، و بدين شكل مخربين از آن سوء استفاده نمايند.
- تهديد از طريق برنامه‌هاي مجاني CGI، اين برنامه‌ها هم ممكن است داراي حفره‌هاي امنيتي باشند.
- ارسال داده‌هاي جعلي به سمت برنامه‌هاي CGI، كه مي‌تواند باعث تخريب برنامه گردد.

براي اينكه يك سرور قادر به اجراي يك برنامه‌هاي CGI باشد، شما بايد به وب سرور اجازه خواندن و اجراء را در دايركتوري برنامه‌هاي CGI بدهيد. اما بايد مطمئن گرديد كه امكان نوشتن در اين دايركتوري را غير فعال كنيد. بدين روش امكان وارد كردن اطلاعات مخرب به اين دايركتوري از طرف فرد مخرب را هم سلب مي‌كنيد.

براي حفاظت از وي سرور در مقابل مخاطرات ناشي از برنامه‌هاي CGI، بايد روش‌هاي زير را بكار بنديد.

- ايجاد محدوديت در كاربرد برنامه‌هاي CGI. به اين طريق از ايجاد بار زياد بر روي وب سرور و نتيجتا كاهش سرعت آن، مي‌كاهيد.
- نصب برنامه‌هاي CGI به شكلي كه در شرايط قانون حداقل اجازه (Least Privileged User) اجراء گردد.
- پاك كردن تمام برنامه‌هاي CGI بصورت پيش فرض موجود در درون وب سرور.
- بررسي برنامه‌هاي CGI در جهت پيدا كردن حفره‌هاي امنيتي آنان. استفاده از برنامه‌هايي كه از مراحل تست لازم عبور كرده باشند.

Instant Messaging (7-2-6

پيغام‌گذاري لحظه‌اي يا IM، روشي است كه امروزه براي انتقال صحبت، فايل، صدا بين كاربران مختلف بصورت مستقيم بر روي وب، مورد استفاده قرار مي‌گيرد. اين برنامه‌ها براي اجرا و بهره‌برداري بسيار راحت مي‌باشند، اما متاسفانه داراي شرايطي مي‌باشند كه توسط مهاجمين براي تدارك حمله مورد استفاده قرار مي‌گيرند. از جمله مشكلات مي‌توان به موارد زير اشاره كرد:

- انتقال داده‌هاي رمز نشده. مردم اغلب داده‌هاي مهم مثل كلمه عبور و رمز عبور را از اين طريق براي افراد مورد اعتمادشان ارسال مي‌كنند. غافل از اينكه اين ارتباط مي‌تواند توسط هكر با استفاده از پروتكل آنالايزر مورد استراق سمع قرار گيرد.
- فايل‌هاي ارسالي ممكن است ويروسي‌ها را دور بزنند. IM به كاربران اجازه انتقال فايل، جدا از سيستم ايميل كه داراي ويروسي‌اب مي‌باشد را مي‌دهد. وچون فايل ارسالي از

طريق ايميل ارسال نمي‌شود، لذا مورد بررسي ويروسياب ايميل قرار نمي‌گيرد. پس انتقال ويروس از اين طريق امكان پذير مي‌باشد.

- هكر مي‌تواند نقاط ضعف اين سيستم را شناسايي كند، مواردي همچون سرريز بافر. شبيه ديگر برنامه‌هاي كاربردي، IMها هم مي‌توانند داراي حفره‌هاي امنيتي باشند، اما اين حفره‌هاي امنيتي بطور بالقوه خطرناكتر مي‌باشد، چرا كه اتصال بصورت مستقيم بين كاربران مي باشد. همچنين اشكال برنامه‌اي در يك طرف ارتباط مي‌تواند عاملي گرد كه طرف مقابل ارتباطي، كنترل كامپيوتر ديگري را در اختيار گيرد.
- هكر مي‌تواند طرف مقابل ارتاطي خود را با استفاده از اطلاعات دروغ فريب داده، و اورا مجاب ابه افشاي اطلاعات محرمانه كند. (حملاتي از نوع مهندسي اجتماعي).

بعضي از سازمان‌ها خود را در مقابل تهديدات ناشي از IM با جلوگيري از استفاده از IM در سازمان خود، بيمه كرده اند. بعضي از سازمان‌ها اجازه استفاده از IM هاي را كه امن باشد را مي‌دهند. اگر امكان حذف كامل سيستم IM در سازمان‌تان نمي‌باشد، حتما موارد امنيتي زير را مد نظر داشته باشيد:

- انحصار در استفاده از IM هاي كه براي استفاده شما مجاز مي‌باشند. اين عمل شما را از پشتيباني، امن‌سازي، مشكلات ممكنه چندگانه ناشي از IMهاي مختلف خلاص مي‌كند.
- اگر اطلاعات انتقالي بين كلاينت‌ها بايد امن باشد، از برنامه IMاي استفاده كنيد كه قابليت رمزگذاري داشته باشد.
- تنظيم نظام‌نامه امنيتي براي استفاده از IM. مثلا اينكه از طريق IM انتقال فايل انجام نگيرد.
- آموزش كاربران براي آگاهي آنان از خطرات ممكن IM.به آنها توضيح دهيد كه انتقال فايل از اين طريق چقدر خطرناك مي‌باشد، و اينكه يك هكر ممكن است براي فاش شدن اطلاعات محرمانه او تلاش كند.
- اطمينان از اينكه تمامي استفاده كنندگان از IM، از ويروسيابهاي بروز شده استفاده مي‌كنند.
- پيگيري از فروشندگان نرم افزارهاي IM براي دريافت آخرين وصله هاي امنيتي

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)