امنیت در تجارت الکترونیک

یکی از مقوله‌ها امنیت فناوری اطلاعات یا امن بودن فضای تبادل اطلاعات است

هک شدن سایتها توسط نفوذگران، انتشار ویروسهای رایانه ای جدید و سرقت از حسابهای مشتریان بانکها، شکسته شدن قفلهای نرم‌افزاری و....

تجارتی موفق محسوب می‌گردد که در آن بسیاری از ملاحظات امنیتی مد نظر قرارگرفته باشد. برای یک سازمان تجاری موفق اطلاعات دارایی اصلی است

امنیت فناوری اطلاعات

امنیت فناوری اطلاعات به استفاده ایمن از این فناوری و اطمینان از وجود محیطی عاری از هرگونه تهدید باز می گردد.

فناوری اطلاعات شامل فناوریهایی است که در خدمت ذخیره سازی، پردازش، انتقال و مدیریت اطلاعات است

1. **امنیت رایانه (Computer Security)** هدف از امنیت رایانه نگهداری از منابع اطلاعاتی در مقابل
   - استفاده غیر مجاز (Anauthorized)،
   - سوء استفاده (Abuse)
   - حفاظت در مقابل صدمات عمدی یا غیر عمدی، افشا (Disclosure)
   - تغییر و اصلاح (Modification) است.
2. **امنیت ارتباطات (Communication Security)** حفاظت از اطلاعات در طی انتقال بین سیستم های رایانه ای و شبکه ها را امنیت ارتباطات گویند

   در یک شبکه ارتباطی برای ارائه خدمات مورد نیاز می تواند همراه با خطرات امنیتی متعددی باشد
   - کاربران انسانی **(Human user)** کاربر: موجودیتی جوابگو و مسئول در قبال فعالیتهای خود در تعامل با رایانه و شبکه است
   - ماشین **(Host)** ماشین: موجودیتی دارای آدرس در یک شبکه ارتباطی که دارای نام و آدرس دهی خاص می باشد
   - فرآیندهای رایانه ای **(Process)** 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

امنیت شبکه و اینترنت

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

برخی از انواع تهدیدات در اینترنت

- 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

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

Attacker , Hacker **و یا** Intruder . اسامی فوق به افرادی که همواره در صدد استفاده از نقاط ضعف و آسیب پذیر موجود در نرم افزارها می باشند ، اطلاق می گردد

کد مخرب : این نوع کدها شامل ویروس ها ، کرم ها و برنامه های تروجان می باشد.

ویروس‌ها (Virus) 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.

کرم ها (Worm) بدون نیاز به دخالت کاربر ، توزیع و گسترش می یابند 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

تروجان (Trojan) 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 .

سابقه امنیت در شبکه اینترنت

اینترنت در سال ۱۹۶۹ بصورت شبکه‌های بنام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد

اگر، بخشهای عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد

در سال ۱۹۷۱ تعدادی از رایانه‌های دانشگاهها و مراکز دولتی به این شبکه متصل شدند

در سال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که بعداً «کرم موریس» نام گرفت

ویروس می‌توانست به یک رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و بصورت هندسی تکثیر شود. در آن زمان ۸۸۰۰۰ رایانه متصل به شبکه وجود داشت

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت

اختلال در امنیت شبکه، WINK/OILS WORM در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می شود.

فرایند توسعه امنیت سازمان

الف) تجزیه و تحلیل خطرات مطرح در سازمان یا سیستم

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

ب) تدوین سیاستها و خدمات امنیتی

یک سیاست امنیتی، اعلامیه‌ای رسمی مشتمل بر مجموعه‌ای از قوانین است که می‌بایست توسط افرادی که به یک تکنولوژی سازمان و یا سرمایه‌های اطلاعاتی دستیابی دارند، رعایت و به آن پایبند باشند

در ادامه ویژگی‌های یک سیاست امنیتی خوب و یک مثال از سیاست امنیتی، تعریف رمز عبور، بیان می‌گردد.

رمز عبور

حداقل طول رمز عبور، دوازده و یا بیشتر باشد.

در رمز عبور از حروف کوچک، اعداد، کاراکترهای خاص و زیرخط[1] استفاده شود.

از کلمات موجود در دیکشنری استفاده نگردد.

رمزهای عبور، در فواصل زمانی مشخصی (سی و یا نود روز) به صورت ادواری تغییر داده شوند.

ج) تعیین مکانیزمهای امنیتی

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

انواع ویژگیها و سرویس‌های امنیتی در محیطهای تجاری

۱-احراز هویت (Authentication)

فرستنده یا گیرنده هویت واقعی خود را برای طرف مقابل اثبات می‌کند.

۲-کنترل اختیارات (Authorization)

یعنی هر طرف فعالیت به چه سطح از اطلاعاتی دسترسی داشته و چه نوع ازعمل(رویت، حذف، تغییر، اضافه) برایش مقدور باشد

۳-در دسترس بودن (Availability)

خدمات باید همیشه در دسترس افراد مجاز باشد.

٤-محرمانگی (Confidentiality)

فقط فرستنده و گیرنده مورد نظر قابل به درک پیام باشند.

٥-بازرسی (Auditing)

امکان بررسی داده‌ها و اطلاعات موجود در سیستم ظبط رویدادها (Log File) موجود باشد

٦-صحت داده ها (تمامیت و جامعیت) (Auditing)

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

۷-انکار ناپذیری (Non-Repudiation)

یعنی هیچکدام از طرفین (فرستنده و گیرنده پیام)، امکان انکار عملکرد خود (ارسال پیام) را نداشته باشد.یا به عبارت دیگر ارسال‌کننده نمی‌تواند منکر ارسال پیام یا تبادل مالی شود و دریافت‌کننده هم نمی‌تواند منکر دریافت آن شود

ایمن سازی یک شبکه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم **سرویس‌های فعال ، پروتکل های استفاده شده و پورت های باز** می باشد .

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

برنامه ریزی

- ✓ 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

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 .

هر سیستم عامل دارای مجموعه‌ای 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

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

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 .

وظایف سرویس دهنده های مختلف

(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 .

- **DHCP (Dynamic Host Configuration Protcol)**
- **WINS (Windows Internet Name Service)**
- **DNS (Domain Name System)**
- **SNMP (Simple Network Management Protocol)**

(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

(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 . **(News/Usenet)**

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

حملات (Attacks)

چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد.

توجه به مکانیزم‌های جلوگیری از حملات امنیتی و سیاست‌های امنیتی محقق اهداف امنیت اطلاعات هستند.

انواع حملات امنیتی

1. قطع (Interruption)
2. دسترسی غیرمجاز (Interception)
3. دستکاری داده ها (Modification)
4. ساخت پیام (Fabrication)

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.

TCP/IP Hijacking		Sniffing	Spoofing	Man in the Middle	Denial of Service (DoS)
Brute Force	DNS Poisoning	Dictionary	Trojan	Auditing	(Distributed Denial of Service (DDoS)
Replay		Password Guessing	HorsesWorms	Social Engineering	Back Door

1 Denial of Service (DoS)

- 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 و اتصالات شبکه ای آن و یا کامپیوترها و شبکه ای از سایت هائی که مورد استفاده قرار میگیرد ، باعث سلب دستیابی به سایت های Email ، وب سایت‌ها ، account های online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد
- 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
- 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
- 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

2 (Distributed Denial of Service (DDoS)

- 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 .

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoS و یا DDoS وجود ندارد

- 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

3 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 دارای این مشکل می‌باشد

روش پیشگیری

- آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود .
- 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 Subv۷) را به دنبال داشته باشد

4 Spoofing رهگیری

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

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

برای پیشگیری بهتر است از تایید گواییهای ملی یا بین المللی مانند versign استفاده شود.

● **تغییر قیافه Masquerading**

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

● **جعل هویت Impersonation**

در این روش مثلا وقتی یک کاربر معتبری می‌خواهد به سرور دانشگاه متصل گردد، قبلا دانشجوها به DNS دانشگاه حمله کرده‌اند و این سرور را به شکلی مختل کرده‌اند که بسته‌های اطلاعاتی به جای آنکه بین سرور دانشگاه و کلاینت جابجا شوند، بین کلاینت متقاضی و سرور جعلی مهاجم جابجا می‌شوند. یعنی اولین پیغام (Prompt) که بر روی صفحه کاربر ظاهر می شود دقیقا مشابه پیغامی است که سرور دانشگاه برای دریافت .User Id و Pass Word به کلاینت می‌دهد و از او خواسته می‌شود .Id و P/W خود را وارد نماید و آنگاه این مشخصات به سرقت می‌رود و در ادامه بلافاصله پیغام " User Id. or Pass Word Incorrect " بر روی صفحه ظاهر می‌شود و کاربر هم بدون اینکه احساس بدی پیدا کند، با تصور آنکه مشخصه یا کلمه خود را اشتباه وارد کرده مجددا آنها را وارد کرده و وارد سیستم دانشگاه می‌شود

5 Man in the Middle

● نفوذگر بین دو کامپیوتر Client و Server که در حال تبادل اطلاعات هستند قرار می گیرد. نفوذگر ترتیبی را اتخاذ می کند که دو کامپیوتر از وجود او بی اطلاع باشند. به این ترتیب دسترسی کاملی به اطلاعات بین دو نقطه پایانی دارد. در این حملع عمدتا هدف بدست آوردن کلمه عبور و رمز عبور می‌باشد. ، سیستم های Wireless در معرض این حمله قرار دارند. هدف شنود اطلاعات است (Interception) ، از شار مغناطیسی ایجاد شده در خطوط باسیم و Decode کردن آن نیز میتوان استراق سمع نمود.

یکی از روشهای پیشگیری رمز نگاری اطلاعات می باشد.

6 Replay

● وقتی یک هکر به وسیله ابزار Sniffer (بو کشیدن) بسته های اطلاعاتی را از روی سیم بر می دارد ، یک حمله Replay رخ داده است. وقتی بسته‌ها دزدیده شدند ، هکر اطلاعات مهم و نامهای کاربری و کلمات عبور را از درون آن استخراج می کند. وقتی که اطلاعات ازبسته‌ها استخراج شدند ، دوباره بسته‌ها روی خط قرار می گیرند و یا بدانها به صورت دروغین پاسخ داده می شود. حمله در بخش Authenticate لایه session OSI یا لایه یک TCP/IP میباشد.

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

استفاده از حالت State Full filtering در فایروالهای سخت افزاری (مقیسه هر Packet دریافتی نسبت به در یافتهای قبلی) جزء موارد پیشگیری میباشد.

7 TCP/IP Hijacking

● معمولا به آن جعل نشست (Session Hijacking) نیز گفته می شود. هکر می تواند نشست TCP بین دو ماشین را به دست آورد. یک روش مشهور استفاده از Source-route کردن IP ها می باشد. Source-route کردن یعنی بسته های IP را طوری تغییر دهیم که از مسیری خاص بگذرند. همانند Replay میباشد با این تفاوت که هکر آدرس مقصد را بسمت خود عوض میکند.

روش پیشگیری مانند Replay میباشد.

8 DNS Poisoning (مسمومیت DNS)

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

9 Social Engineering(مهندسی اجتماعی)

● بیشتری زمانی رخ می دهد که هکر به سیستم‌های واقعی قصد نفوذ دارد. راه دیگر هنگامی می باشد که نفوذگر با استفاده از نقاط ضعف کاربر انتهایی (End User) راه نفوذ به شبکه را پیدا می کند. سوءاستفاده از نقاط ضعف افراد با به دست آوردن عادت های شخصیتی افراد برای اغفال آنها و یا تحت فشار قرار دادن آنها تا اطلاعات مورد نیاز برای نفوذ به شبکه را در اختیار فرد هکر قرار دهد.

10 Brute Force

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

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

ادامه حملات (Attacks)

11 Dictionary

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

روش پیشگیری
- برای مقابله با این حمله باید از کلماتی استفاده کرد که در لغتنامه وجود ندارد . البته امروزه راه دیگر مقابله با تهدیدات از نوع Brute Force و Dictionary استفاده از یک فعالیت انسانی است. مثلا یک شکل گرافیکی با اشکالی که توسط سیستمهای الکترونیکی قابل تشخیص نیستند ، شما را مجبور به تایپ می‌کنند.

12 Software Exploitation

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

13 Sniffing

- اطلاعاتی مانند نام عبور (U/Id) و رمز عبور (P/W) توسط هکر بر روی خط شنود شده و یا اینکه با حمله به دیتابیس‌ها و به دست آوردن این اطلاعات، هکر میتواند خود را به جای کاربر مجاز معرفی کرده و سوء استفاده نماید.

روش ها و سیستم های کنترل دسترسی (جلوگیری از دسترسیهای غیر مجاز Unauthorized Access)

(Confidentiality) محرمانگی هدف اصلی آن است که دسترسی به اطلاعات وخواندن آنها بدون مجوز انجام نپذیرد .

(Integrity)تمامیت و صحت داده ها هدف آن است که اجازه ندهیم تغییرات هوشمندانه ای در مجموعه اطلاعات انجام گیرد . یعنی اجازه نوشتن اطلاعات را بدون مجوز ندهیم .

(Availability) در دسترس بودن در بحث در دسترس بودن این انتظار را داریم در زمان های مشخص شده که به کاربر اجازه دسترسی داده می شود ، و با وجود پهنای باندی که باید در اختیارش باشد، همیشه این امکان یعنی دسترسی به منابع و اطلاعات برایش مقدور باشد .

Subject یک موجود فعال است، مانند یک کاربر، یا مثل یک برنامه ، یک پروسس ، یا یک کامپیوتر، و یا حتی یک دیتابیس که تلاش و فعالیت آنها در راستای دسترسی به یک منبع اطلاعاتی می باشد . **(سرویس گیرنده)**

Object منظور همان منبع اطلاعاتی می باشد که می تواند یک برنامه دیگر، یک فایل دیگر، یک کامپیوتر دیگر، و یا اطلاعات مربوط به کاربری دیگر باشد دارند و حالت غیر فعال Passive دارد . **(سرویس دهنده)**

عمل انتقال اطلاعات از سمت Object به سمت Subject میباشد.

تکنیکهای کنترل دسترسی

1 قانون حداقل اجازه (Least Privilage)

-تکنیک این است که در یک شبکه متشکل از تجهیزات و منابع اعم از کامپیوترها ، دیتابیس ها، فایل ها، چاپگرها و . . . کاربر به هیچ عنوان نتواند اجازه دسترسی عمومی داشته باشد . یعنی به هیچ کس اجازه دسترسی عمومی (Global Access) داده نشود به عبارت دیگر به هر subject اجازه دسترسی به object هایی را میدهیم که برای انجام کار مشخصی از قبل تعریف شده است.

-در یک شبکه ابتدا کلیه اجازه های دسترسی لغو میگردد و با توجه به صلاحدید مدیر سیستم (Admin)،objectها برای subjectها فعال میگردد.

2 حسابرسی کاربران (Accountability)

-این لایه باعث میگردد که اطلاعات هر گونه دسترسی یک subject و اقدام بر روی یک object بر روی سیستم ذخیره(Log) گردد.

-فرایند حسابرسی با یک عمل شناسایی (Identification) هویت subject آغاز میگردد. (نام کاربری و رمز عبور ، بهره گیری از کارتهای هوشمند (Smart Card)

ادامه تکنیکهای کنترل دسترسی

3 کنترل Object ها

کنترل دسترسی فیزیکی (Physical Access Control)

-هدف ایجاد حدود دسترسی ها به منابع (عمدتا سخت افزاری) می باشد . این روش مشابه انواع روش های ممانعت فیزیکی ورود و خروج افراد به محیط و سازمان می باشد

کنترل دسترسی اجرایی (Administrative Access Control)

-تکیه بر سیاستهای (Policy) امنیتی سازمان دارد که توسط مدیر سیستم (Admin) سطوح دسترسی هر فرد در سازمان مشخص میشود ،مثلا پیچیدگی رمز عبور و ،آموزشهای امنیتی لازم افراد سازمان ...

کنترل دسترسی منطقی (Logical Access Control)

محدود سازی دسترسی به Objectها (Object Access Restriction)

-یعنی تنها subject هایی که در فرآیند شناسایی (Authentication) احراز هویت گردیده اند و بر اساس رویه های امنیتی سازمان دسترسیشان به منابع تایید گردیده است قادر به دسترسی به object های مختلف را داشته باشند.

رمز نگاری (Encryption)

-هدف محرمانه کردن اطلاعات با بهره گیری از تکنیکهای رمز نگاری میباشد.

معماری دسترسی شبکه ای تفکیک شده (Network Architecture/Segregation)

-جدا سازی حداکثری در شبکه مد نظر میباشد. بعنوان مثال بعضی اطلاعات لزومی ندارد در شبکه باشد یا backupگیری در جایی غیر از سرورهای شبکه ،تفکیک سرورهای مختلف از همدیگر یا توزیع یک سرور خیلی بزرگ بر روی مجموعه سروهای دیگر مانند سرور های yahoo

انواع کنترل ها **Control Types**

۱-پیشگیرانه Preventative

جلوگیری از رخداد یک حمله انجام می گیرد .

از ابتدا اجازه نمیدهیم که یک Subject به یک Object غیر مجاز دسترسی داشته باشد.

۲-نمایان سازی و کشف Detective

استراتژی را به شکلی تعریف می کنیم که پس از وقوع یک حمله موفق، اولا وقوعش اعلام شود و ثانیا اینکه توسط چه کسی حمله انجام پذیرفته مشخص شود .

ممکن است ظاهر حمله به شکلی باشد که حمله اصلی را از چشم افراد امنیتی دور نگاه دارد.

۳-بازدارنده و تنبیه کننده Deterrent

استراتژی را به شکلی تعریف می کنیم که پس از وقوع یک حمله موفق، اولا وقوعش اعلام شود و ثانیا اینکه توسط چه کسی حمله انجام پذیرفته مشخص شود .

چنانچه یک دسترسی به object بدون اجازه انجام پذیرد.subject مهاجم شناسایی شده و بر اساس تصمیمات سازمان که در بخش مدیریت سیستم تعریف میگردد با مهاجم برخورد میگردد.

بطور مثال (این فروشگاه مجهز به دوربین است یا دوربینهای موجود در اتوبان) که جزء موارد administrative access control میباشد .

٤-تصحیح کننده Corrective

هدف آن است به محض بروز یک حمله بلافاصله سیستم را به وضعیت مناسب آن برگردانیم . بطور مثال فرض کنید به سرور پست الکترونیک یک سازمان یک حمله به منظور پر کردن حجم آن انجام گرفته است Restore کردن سیستم به حالت قبل از حمله corrective)

۵-بازگشت و بازیابی Recovery

برگرداندن اطلاعات درست (recover) بعد از عمل corrective تا حداقل آسیب برای کاربران ایجاد شود.

کنترل دسترسی بصیرتی (Discretionary) DAC مطابق میل و اختیار مالک object

–در این روش ایجاد کننده یا مالک (owner) هر Object میتواند بر روی آن object تغییراتی اعمال کند یا به الباقی subject ها ا جازه دسترسی یا عدم دسترسی و انواع اختیارات از قبیل (دیدن ،حذف ،تغییر ،..) را اعمال کند. مالک میتواند یک فرد یا یک گروه باشد.

–این روش مبتنی است بر شناسایی (Identify) هر Subject بنابراین با عنوان **Identify-Based Access Control** نیز شناخته میشود.

–این نوع کنترل دسترسی بیشتر ماهیت غیر متمرکز دارد .یعنی کسی که object را کنترل میکند خودش اقدام به صدور مجوز برای دسترسی subject های دیگر به آن object میکند.

–یک کاربر subject میتواند در یک نقش وظیفه مدیر سیستم admin را داشته باشد و در نقش دیگر وظیفه بررسی و کنترل حقوق کاربران را داشته باشد.

–برای کنترل دسترسی به یک object باید لیست کنترل دسترسی ایجاد شود.

–ازاین روش بیشتر در محیطهای تجاری استفاده میشود. حالت بصیرتی مربوط به گسترش فیزیکی اطلاعات در جاهای مختلف است تا سطح دسترسی به یک object

لیست کنترل دسترسی

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

کنترل دسترسی الزامی MAC (Mandatory Access Control) اجباری بر اساس قوانین سازمان

–این نوع کنترل دسترسی ماهیت متمرکز دارد .و بر اساس قوانین مشخص Rules که توسط مدیریت سازمان مشخص گردیده تعریف میشود .این روش بنام **Rule-Base Access Control** نیز شناخته میشود.

–برای این منظور برای هر کاربر یک برچسب Label امنیتی تولید میشود و در محیطهای تجاری دارای طبقه بندی زیر میباشد. (برای هرکدام از subjectها وobjectها برچسب امنیتی درست میشود)

–عمومی (Public) ، –حساس در سطح دپارتمان (Sensitive) ، – شخصی (Private) ،–دارای مالکیت معنوی (Confidential) ← بالاترین سطح (امکان دسترسی به سطوح پایینتر)

–بطور مثال از این روش در فایروالها Firewall استفاده میشود (–امنیت در لایه IP بر اساس اطلاعاتی از قبیل IPگیرنده ،IP فرستنده ،.....)

کنترل دسترسی غیر بصیرتی NADC (Non-Discretionary Access Control)

کنترل دسترسی بر اساس نقش و وظیفه RAC (Role-Base Access Control)

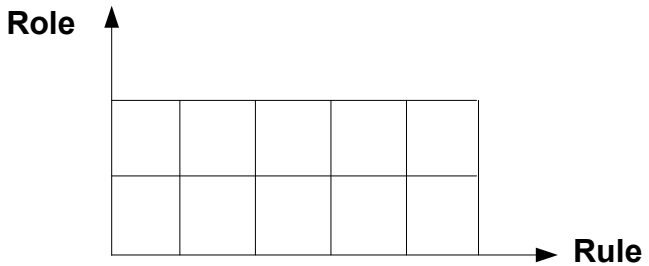
–بر اساس مشخصه کاربر (User ID) اجازه دسترسی صادر نمیشود بلکه بر اساس شرح خدمات هر کاربر این کار انجام میشود.

–در سازمانهایی که موقعیت شغلی افراد به سرعت تغییر می کند، افراد ممکن است دارای چندین مسئولیت گردند . بطور مثال در داخل یک پروژه، چندین زیر پروژه در بخشهای مختلف زمانی تعریف می گردد و وظایف فرد تغییر می کند . پس در این روش اجازه دسترسی بر اساس شرح وظایف کاری یک کاربر انجام می پذیرد .

کنترل دسترسی بر اساس شبکه بندی LAC (Lattice-Based Access Control)

– ازترکیب دوروش بر مبنای نقش و وظیفه و بر مبنای قوانین استفاده میشود. در این روش برای وظیفه افراد برچسب های امنیتی تعریف میگردد.مثلا کسی که مدیر سیستم است برچسب شخصی private میگیرد. لذا علاوه بر اطلاعات سطح private دسترسی با سطوح امنیتی پایینتر امنیتی یعنی sensitive,public را نیز دارا میباشد.

این روش برای محیط های با تغییرات زیاد و دوره ای در پرسنل آن (مانند محیطهای پروژه ای) مناسب می باشد .



تعیین هویت Identification و احراز هویت Authentication

- Authenticationاولین مرحله امنیت و قبل از Authorization میباشد.
-قبل از اینکه یک Subject مجاز یا غیر مجاز شناخته شود باید تعیین هویت **Identify** گردد و سپس این اسم احراز هویت **Authentication** گردد.
-شناسه یک Object برای Identification میتواند شامل (نام کاربری **User ID** ،کارت هوشمند **Smart Card** ، یک نشانه **Token**) باشد.

تکنیکهای احراز هویت

① **What You Know** اطلاع خاص منحصر بفردی است که تنها کاربر میداند.

Password(P/W) : یک رشته از کاراکترها که میتواند صرفا رقم PIN ،یا حروف یا ترکیبی از این دو باشد. از آنجا که اطلاعات مربوط به P/W در داخل یک پایگاه داده نگهداری میشود و همیشه امکان حمله به آن وجود دارد ،این روش احراز هویت جزء روشهای ضعیف محسوب میشود.

② **What You Have** چیز منحصر بفردی که کاربر برای اثبات هویت خودش به همراه می برد .

کارت هوشمند **SmartCard** و نشانه **Token** جزء این موارد میباشد.

③ **What You Have** به معنای ویژگی های منحصر بفرد افراد می باشد (ویژگی های بیومتریک افراد) .

-این تکنیکها(روشهای زیست سنجی) بهترین و در عین حال گرانترین روشها میباشند. (**اثرانگشت ،عنبیه چشم ، الگوی صدا ،الگوی فشردن کیبورد ،الگوی صورت ،الگوی امضاء**)
-در این حالت Subject که معمولا یک عامل انسانی است با توجه به مشخصات منحصر به فرد خود شناسایی میشود.
-از روش بیومتریک هم در مرحله Identification و هم در نوع سوم Authentication میتواند مورد استفاده قرار گیرد.

-برای بالا بردن سطح امنیتی احراز هویت از روش چند فاکتوری **Multiple Factors** استفاده میشود. که از ترکیب همزمان حداقل ۲ فاکتور از سه فاکتور ذکر شده استفاده میشود.
-استفاده از دو عنصر از یک فاکتور بصورت همزمان مثلا دو نوع P/W نیز گاهی استفاده میشود ولی به این حالت Multi Factor نمیگویند.

خطاهای بیومتریک

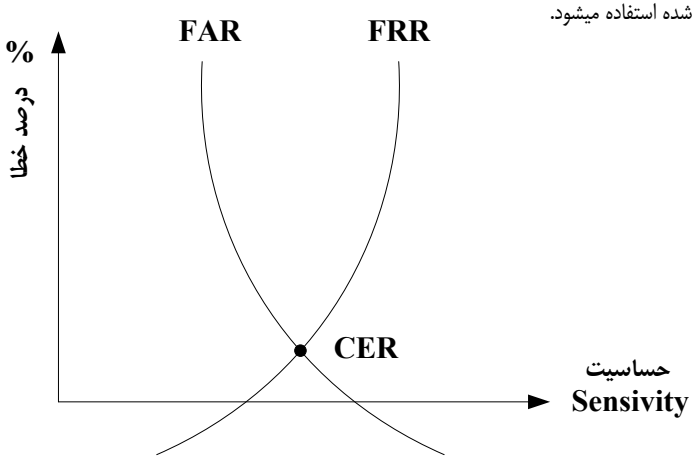
در دستگاههای مبتنی بر بیومتریک به دلیل میزان حساسیت دستگاه ما مواجه با دو نوع خطا می باشیم

① **False Rejection Rate (FRR)**

-یعنی میزان **عدم تشخیص درست فرد دارای اعتبار** برای سیستم . یعنی مثلا اثر انگشت فردی که در سیستم به عنوان فرد معتبر می باشد به دلیل آلودگی محیطی تشخیص داده نشود .
-دراین حالت دسترسی Availability دچار مخاطره میشود.

② **False Acceptance Rate (FAR)**

-یعنی **میزان پذیرفته شدن افراد غیر معتبر** به عنوان فرد معتبر در سیستم می باشد . که عمدتا بدلیل کافی نبودن حساسیت سیستم می باشد .
-در این حالت صحت داده ها Integrity و محرمانگی Confidentialy دچار مخاطره میشود.



-هر چه حساسیت بالا رود FAR پایین می آید ولی در مقابل FRR بالا میرود.
-هرچه حساسیت پایین بیاید FRR پایین می آید و در مقابل FAR بالا میرود.

Crossover Error Rate (CER)

-نقطه تلاقی FRR,FAR که هر دو مولفه بصورت همزمان دارای حداقل حساسیت میباشند و بهترین حالت برای مباحث تجارت الکترونیک میباشد.

روشهای پیاده سازی احراز هویت

① Centralized متمرکز

-عملیات احراز هویت بطور متمرکز بر روی یک سرور انجام می پذیرد.

-حسن آن اینست که چون احراز هویت برای دسترسی به object ها در یک نقطه واحد انجام میپذیرد مدیریت آن براحتی انجام میپذیرد.

-ضعف آن اینست که ۱- اگر امنیت سرور دچار اختلال شود آنگاه امنیت کل سیستم مختل میشود ۲-در صورت پایین آمدن کارایی سرور سرعت کل سیستم مختل میشود ۳-در صورت خرابی سرور کل سیستم از کار می افتد **Single Point Of Failure**

② Decentralized غیر متمرکز

-در واقع عمل احراز هویت از راه دور می باشد . مثلا وقتی از بیرون یک سازمان بخواهند عمل احراز هویت انجام دهند و به سرورهای مختلف آن سازمان دسترسی پیدا کنند، معمولا از این روش استفاده می کنند.

-در این روش مدیریت دسترسی در نزدیکی objectهای مورد کنترل اعمال میشوند نه در مرکز اصلی IT سازمان .مانندا‌حراز هویت برای اعلام نتایج کنکور

-این روش در ذات خودش حالت توزیع شوندگی دارد و بین سرورهایی که بصورت مشترک عملیات احراز هویت را انجام میدهند نیاز به یک هارمونی یا هماهنگی میباشد. و این عاملی است برای افزایش پردازشهای لازم **Overhead**

③ Hybrid ترکیبی

-هدف استفاده از مزاياي دو روش قبلي بطور همزمان مي باشد . براي بعضي از منابع حياتي سيستم مثل فايل هاي مهم و ديتابيس هاي فيزيكي بهتر است از روش متمرکز استفاده شود و برای سایر objectها که دارای حساسیت کمتری است از روش غیر متمرکز استفاده کرد.

تکنیک های کاربردی برای مقابله با حملات علیه سیستم کنترل دسترسی

① Monitoring

-هدف اصلی اینست که تمامی فعالیت های subject قابل حسابرسی باشد.

-هدف امنیتی آن اینست که کلیه فعالیتهای غیر مجاز و تلاش برای نفوذ در سیستم و یا خرابکاری از طریق **ثبت وقایع Log** و **حسابرسی Auditing** مورد شناسایی قرار گیرد.

-ثبت وقایع کلیه فعالیتهای مهم قبل از شروع یک نشست ،مانند فعالیت درخواست شده توسط یک کاربر .ثبت وقایع مربوط به رخدادهای (**سیستم** ، **برنامه کاربردی** و **برنامه های کاربر**)میباشد.

② Intrusion Detection System (IDS)

- در مبحث IDS هدف جستجو و بازرسی در فایلهای ثبت شده و همچنین اتفاقاتی که بصورت زنده در سیستم در حال انجام می باشد بمنظور شناسایی تلاش های نفوذگران به سیستم می باشد.

IDS معمولا به دو شکل معرفی میگردد.
- -بخشی از شبکه را بطور کامل تحت سرویس های امنیتی خود قرار دهد.
- -تنها ماشین و یا Host خاصی را که عملیات با حساسیت بالایی را انجام می دهد، تحت پوشش سیستم کشف نفوذگر قرار دهد

سرویسهای IDS

① Active فعال

-بلافاصله پس از شناسایی یک نفوذ یا تجاوز Violation ،با استفاده از سیاستهای امنیتی **یک اقدام یا واکنش جدی** انجام میدهد مانند کشف حملات DOS در داخل شبکه که بلافاصله آن ارتباط را قطع میکند .

-در این حالت IDS برای انجام یک واکنش **خودش تصمیم میگیرد**.

② Passive غیر فعال

-بلافاصله پس از شناسایی یک نفوذ **واکنش سریعی انجام نمیگیرد** و IDS این **رخداد را در Log File ثبت کرده** تا بعدا توسط مدیر سیستم تصمیمات لازم اتخاذ گردد.

③ Hybrid مرکب

-در اینحالت هر دو کار بصورت همزمان انجام میگیرد ،یعنی **هم اتفاقات ثبت و ضبط** میشود و **هم عکس العمل مناسب** انجام میگردد.

نحوه شناسایی IDS Methods

① Signature Based مبتنی بر نشانه

-در این روش از قبل برای وقوع حملات سناریوهایی در نظر گرفته میشود.مثلا برای دسترسی به فایل رمزهای عبور کاربران توسط هکر نشانه هایی وجود دارد(راه های مشخص) و در درون دیتابیس IDS که حاوی ترتیب رفتاری نامناسب است ذخیره میگردد. و در صورت حمله با تطبیق آن و این دیتا بیس عکس العمل مناسب (فعال ،غیر فعال یا ترکیبی)انجام میشود.

② Behavior Based مبتنی بر رفتار

-رفتارهای کاربران را در طی دورانهای زمانی شناسایی و دسته بندی می کنند . بدین شکل الگوهای رفتاری هر کاربر مجاز به دست آمده و در درون دیتابیس نگه داری می شود. و در صورتی که یک کاربر رفتار متفاوت با الگوهای شناسایی شده رفتاریش انجام دهد، معلوم می گردد که این فرد که خود را به عنوان یک کاربر مجاز معرفی کرده، همان فرد مجاز نمی باشد، بلکه یک نفوذگر می باشد.

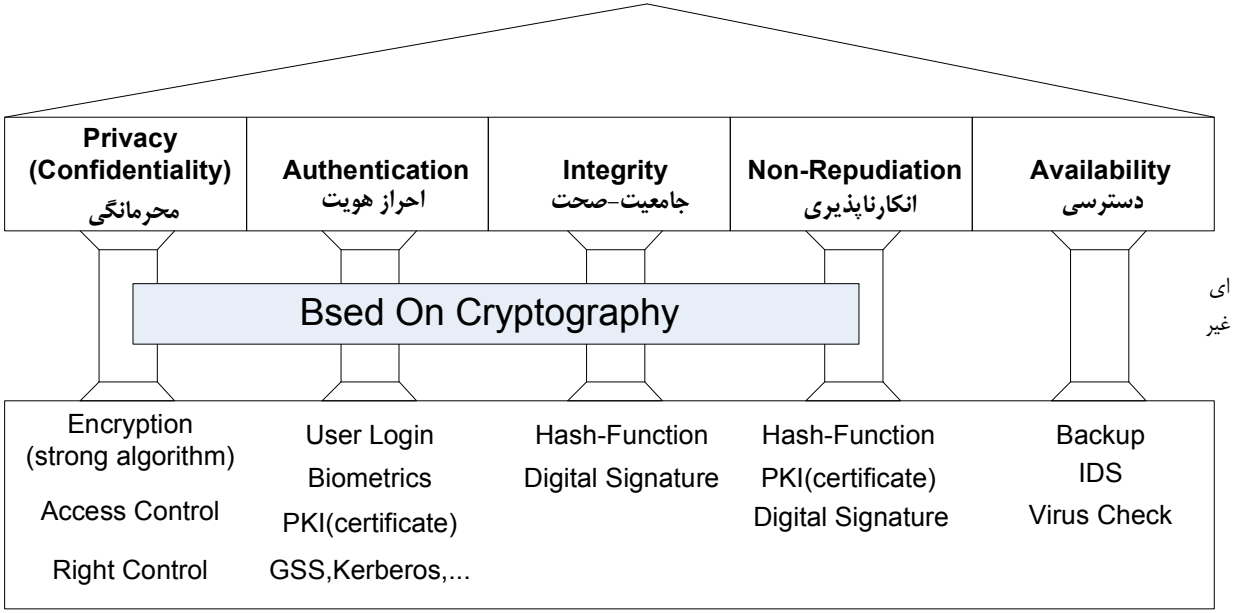
-از این روش گاهی اوقات با نام Expert System معرفی میگردد.

Cryptography

رمزنگاری

اطلاعات حساسی که عموما رمزنگاری میشود.

۱-اطلاعات کارت اعتباری ۲-شماره های عضویت در انجمن ها۳-اطلاعات خصوصی ۴-جزئیات اطلاعات شخصی ۵-اطلاعات حساس در یک سازمان ۶-اطلاعات مربوط به حساب های بانکی



رمزنگاری عبارت است از انجام محاسبات بر روی متن داده ای ورودی به منظور تبدیل کردن آن به یک متن غیر واضح و غیر قابل آشکارسازی توسط افراد غیر مجاز .

شرایط لازم برای امنیت فناوری اطلاعات –بر اساس رمزنگاری

مفاهیم رمزنگاری Cryptography Concept

متن واضح (Plain Text)

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

متن رمز شده (Cipher text)

-بعد از انجام يك عمل رمزنگارانه متن واضح اوليه را به يك متن رمز شده تبديل مي كنيم . اين متن (متن رمز شده) تنها زماني قابل خواندن است كه توسط الگوريتم رمزگشايي از حالت رمز خارج گردد .

رمزنگاری (Cryptography)

–به فرآیندی که در آن متن واضح با اعمالی همچون آرایش مجدد، و یا جایگزین کردن علامت، کاراکتر یا نشانه و یا علامت دیگری، از حالت قابل خواندن به متن غیر قابل خواندن تبدیل می شود، رمز نگاری اطلاق می گردد .

الگوریتم (Algorithm)

–عبارت است از قدم های متوالی و از پیش تعیین شده ای که بر روی متن واضح انجام می شود و در خروجی آن متن رمز شده حاصل می گردد . باید توجه داشت که این تعریف شامل الگوریتم های رمزگشایی (Decryption) هم میشود.

کلید (Key)

–هر الگوریتم به ازای کلید متفاوت خروجی متفاوتی تولید می کند .

–نکته بسیار مهم در بحث رمزنگاری مدیریت کلید است، به نحوی که که اطلاعات به سادگی افشا نگردد .

متن رمز شده	متن اصلی
DEF	ABC
Khoor	Hello
Dwwdfn	Attack

روش رمزنگاری سزار

الفبای رومی را ۳ حرف به سمت راست می چرخاندند .

Exhaustive Search جستجوی فراگیر

مورد جستجو قرار دادن تمام حالات ممکن یک کلید **n** بیتی . 2^n

انواع حملات به سیستم های رمزنگاری

1 فقط رمز شده (Cipher Text Only)

–فرد مهاجم فقط یک متن رمز شده دارد و (با استفاده از جستجوی فراگیر) از روی آن می خواهد کلید استفاده شده برای رمزنگاری را بدست آورد .

2 متن واضح دانسته شده (Known Plain Text)

–فرد مهاجم یک متن واضح و یک متن رمز شده متعارف با آن را دارد . پس در این حالت به نوعی می تواند تشخیص دهد چه کاراکتری از متن واضح به چه کاراکتری از متن رمز شده مبدل گردیده است . در این روش هدف مهاجم مشخص سازی کلید می باشد .

3 متن واضح انتخاب شده (Chosen Plain Text)

–در این روش مهاجم این امکان را دارد که برای تعدادی متن واضح که در اختیار دارد، متن رمز شده آن را تولید کند . در این روش نیز هدف مهاجم مشخص کردن کلید است .

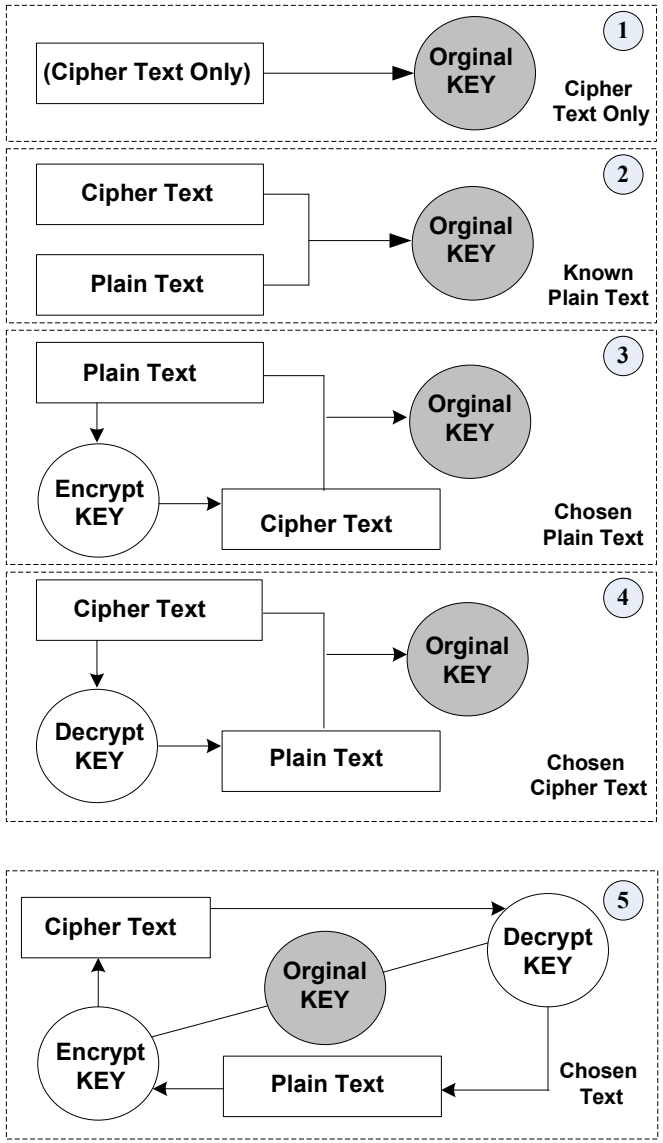
–مثلا فرد مهاجم منشی و یا کارمند یک دفتر است و یا دشمن در این دفتر جاسوس دارد، و از طریق این جاسوس می تواند با دستگاه رمزنگاری این دفتر کار کند ولی نمی تواند کلید را تغییر دهد و یا تنظیم کند و یا بخواند و فقط می تواند به دستگاه رمزنگاری متن واضح را وارد کند و متن رمز شده را بدست آورد ، به این ترتیب در دفعات متوالی اطلاعات مهاجم نسبت به کلید اضافه می شود و فضای جستجو و آنالیز برای بدست آوردن کلید مرتبا برای مهاجم کاهش پیدا می کند .

4 متن رمز شده انتخاب شده (Chosen Cipher Text)

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

5 متن انتخاب شده (Chosen Text)

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



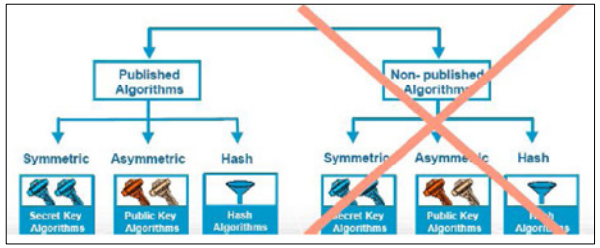
انواع الگوریتمهای رمزنگاری

الگوریتمهای منتشر شده (Published Algorithm)

–الگوریتم هایی هستند که توسط گروه های تحقیقاتی طراحی گردیده و به بازار تجاری ارائه می گردد و توسط گروه های مختلف مورد آزمایش و بررسی قرار گرفته و معایب آن مرتفع می گردد .

الگوریتمهای منتشر نشده (Non-Published Algorithm)

–معمولادر صنایع مخابراتی و نظامی مورد استفاده قرار می گیرند . باید توجه داشت از آنجا که این الگوریتم ها برای مراکز خاصی طراحی می شوند و کاربرد عمومی ندارند،



انواع الگوریتمهای منتشر شده (1) **متقارن (Symmetric) - (Secret Key Algorithm)** (2) **نا متقارن (Asymmetric)** (3) **توابع درهم ریز (Hash)**

الگوریتمهای متقارن (Symmetric) - (Secret Key Algorithm) -الگوریتمی است که در آن کلید رمزنگاری و کلید رمزگشایی در هر دو طرف گیرنده و فرستنده یا با هم برابرند، یا به سهولت توسط توابع ساده ریاضی می توان از روی کلید رمزنگاری کلید رمز گشایی را استحصال کرد .

الگوریتمهای جایگشتی (Transposition Algorithm)

-در این حالت جایگاه حروف تغییر میکند.

I	S	A	A	C
4	5	1	2	3
i 1	□ 2	l 3	i 4	k 5
e 6	□ 7	l 8	e 9	a 10
r 11	n 12	□ 13	k 14	e 15
y 16	×	×	×	×

بصورت ستونی خوانده میشود

i like learn key — Encrypt → ll iekkae niery

i□like□learn□key — Encrypt (□ =Space) → ll□iekkae□□niery

Key=ISAAC **تعداد ستونها=کلید خصوصی**

$\frac{\text{text}}{\text{key}} = \frac{16}{5} = 3.-$ **نیاز به ٤ ردیف برای جایگشت میباشد.**

Table(5*4)-text=20-16=4
در ٤ سلول آخر بصورت ردیفی(×)چیزی درج نمیشود.

I	S	A	A	C
4	5	1	2	3
i 13	□ 10	l 1	i 4	k 7
e 14	□ 11	l 2	e 5	a 8
r 15	n 12	□ 3	k 6	e 9
y 16	×	×	×	×

بصورت سطری خوانده میشود

Plain text to cipher text

Encrypt

i like learn key ⇄ **ll iekkae niery**

Decrypt

Cipher text to plain text

الگوریتمهای جا نشینی (Substitution Algorithm)

-در این حالت خود حروف تغییر میکند.

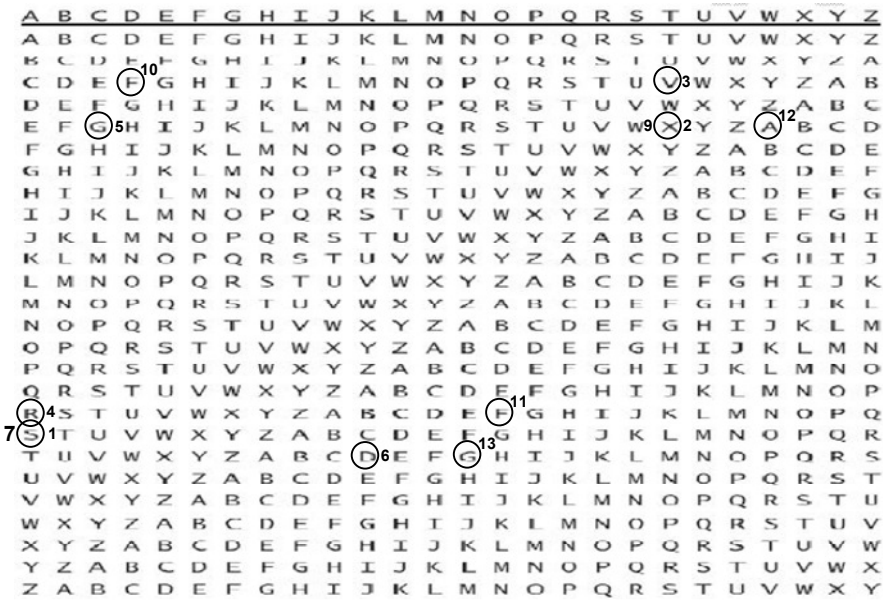
-در الگوریتم جانشینی بطور کلی هر حرف مربوط به متن واضح را با یک مقدار حرف جدید جایگزین می کنیم . در واقع ما به جدولی نیاز داریم که در آن جدول مشخص می شود که بازای هر کاراکتر چه کاراکتری باید جایگزین شود ،مثال ساده آن الگوریتم رمز سزار یا روتیشن ۳ بود

-هم فرستنده و هم گیرنده از یک جدول جانشینی استفاده میکنند

OTP(One-Time_Pad) نوعی ازالگوریتم جانشینی که در ذات خود به صورت تئوریک غیر قابل شکستن میباشد و مبتنی بر حروف تصادفی است.
-درهر بار عمل رمزنگاری یک OTP جدید تولید میکنیم.

(Cipher Vigenere) شکلی رمز چند الفبایی است . بدین معنی که به ازای هر کاراکتر در متن واضح چندین کاراکتر به عنوان کاراکتر رمز شده قرار می دهیم و به این دلیل حمله کننده دیگربا حملاتی مثل حملات تکرار و تعداد کاراکترهای رمز شده در متن رمز شده به اطلاعات متن واضح دسترسی پیدا کند .

جدول جانشینی وایگنر Substitution Table



Encrypt

Clear Text: ATTACKATDOWN (ستون)
Key:SECRET SECRET (سطر)

Cipher text:SXVRGDSXFFAG

Decrypt

Key:SECRET SECRET (سطر)
Cipher text:SXVRGDSXFFAG (سطر)

اولین حرف مطابق با حرف متناظر متن رمز شده و سپس پیدا کردن اولین حرف متناظر در ستون

Clear Text: ATTACKATDOWN

الگوریتم متقارن

معایب

–در این الگوریتم، کلید رمزنگاری و کلید رمزگشایی مشابه هم می باشد، و یا اینکه به سهولت و از طریق محاسبات نسبتا ساده از روی همدیگر قابل محاسبه می باشند . مثلا یک کلید عکس کلید دیگر می باشد .

–توزیع کلید بین طرفین مبادله کلید به خودی خود کاری مشکل و پر مخاطره می باشد و این بدان معنی است که کلید رمز نگاری و یا رمزگشایی باید از کانال امنی انتقال یابد .

–مشکل دیگر این الگوریتم ها این است که سرویس انکارناپذیری را پوشش نمی دهند .

–این نوع از رمز نگاری مقیاس پذیر نمی باشد، یعنی آنکه نمی توان این نوع از رمزنگاری را بصورت بلوکی و بازای طول بلوک های مختلف انجام داد .

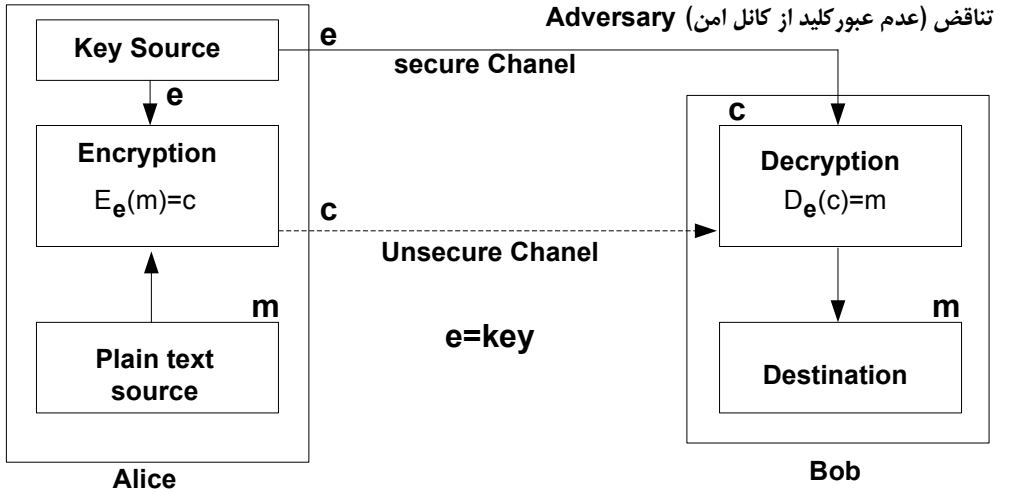
–در این روش رمزنگاری بدلیل امکان لو رفتن کلید رمزنگاری، طرفین رمزنگاری باید به صورت دوره ای کلید رمزنگاری را تغییر دهند .

–مشکل دیگر در این روش رمزنگاری این است که با بالا رفتن طرفین تبادل اطلاعات، تعداد کلید رمزنگاری به صورت نمایی افزایش می یابد

مزایا

–این الگوریتم ها در مقایسه با الگوریتم های نامتقارن، بسیار سریع هستند .

مدل رمزنگاری متقارن
Symmetric Cryptography Model



–در حالتی که کانال نا امن باشد متن کد شده بهمراه کلید در کانال انتقال داده میشود.

–اگر کانال امن وجود کلید از طریق کانال امن فرستاده میشود و متن رمز شده از کانال نا امن

–تعداد کلید از فرمول $n(n-1)/2$ تبعیت میکند که در این فرمول n تعداد نفرات میباشد.

–پس از مدتی مدیریت کلیدها در یک شبکه به یک کار بسیار پیچیده ای تبدیل میشود.

الگوریتم های رمزنگاری متقارن

DES (Data Encryption Standard)

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

Triple DES

–سه بار عملیات الگوریتم DES را انجام میدهد. دارای کلیدی با طول bit ۱۲۸ بیتی میباشد.کاربرد وسیعی دارد .نسبت به DES امن تر است ،اما کند است.

AES (Advances Encryption Standard)

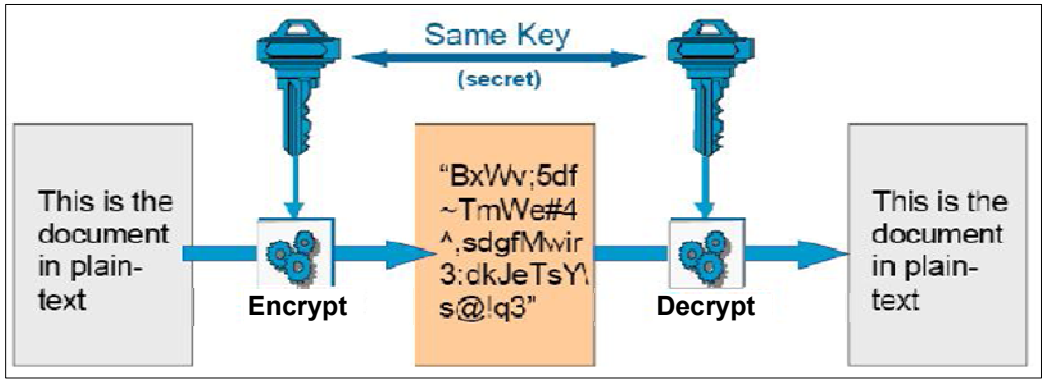
–طول کلید متغییر دارد.آخرین استاندارد دولتی امریکا میباشد . جای الگوریتم DES را گرفته است.

IDEA (International Data Encription Algorithm)

–دارای کلید bit ۱۲۸ بیتی بوده و برای استفاده نیاز به مجوز دارد.

Blowfish

–طول کلید متغییر دارد.الگوریتم آن رایگان است و بسیار سریع است.



الگوریتم های رمزنگاری نامتقارن Public Key Alghorithm - (Asymetric Alghorithm)

Public Key Alghorithm

فرستنده اطلاعات یک زوج کلید را تولید می کند . یکی از کلیدها مخفی و خصوصی است ،(Private Key) و دیگری کلید عمومی است (Public Key)که آن را در اختیار عموم افراد قرار می دهد .

- برای انجام رمزنگاری، فرستنده اطلاعات ، متن مورد نظر خود را با کلید عمومی گیرنده متن به رمز در آورده و این متن رمز شده را از طریق کانال ناامنی برای گیرنده ارسال می دارد . گیرنده هم با استفاده از کلید خصوصی خود این متن را رمزگشایی کرده و به متن اصلی و واضح دست پیدا می کند .

-با انتشار کلید عمومی، هکرها و کاربران غیر مجاز هم قادر به آن می باشند که اطلاعاتی را رمزگذاری کرده و به سمت گیرنده ارسال دارند، و با اینکه هکر به کلید عمومی و هم به الگوریتم رمزگذاری دسترسی دارند، اما نمی توانند کلید خصوصی دریافت کننده پیام را کشف و شناسایی کنند.

-این الگوریتم ها برای انجام سرویس های امنیتی **محرمانگی، احراز هویت**، و **انکار ناپذیری**، استفاده می گردد. این الگوریتم ها در دنیای امنیت به عنوان **الگوریتمهای کلید عمومی** نیز نامیده می شود.

انجام سرویس محرمانگی با بهره گیری از الگوریتم های نامتقارن (Confidentiality)

(Confidentiality)

-هدف محرمانه نگه داشتن اطلاعات انتقالی بین طرفین مبادله پیغام می باشد

-فرد دریافت کننده پیام از قبل زوج کلید رمزنگاری را برای خود تدارک دیده است(یک کلید به عنوان کلید خصوصی و یک کلید به عنوان کلید عمومی) . و این گیرنده پیام کلید عمومی خود را برای اطلاع دیگران منتشر کرده است، مثلا آن را برای اطلاع دیگران بر روی وب سایت خود قرار داده و یا آن را طریق نشریات تبلیغاتی به اطلاع دیگران رسانده است . البته لازم به توجه است که کلید دوم یعنی کلید خصوصی را تنها پیش خود بصورت محرمانه نگه داشته است . حال فرستنده پیام با آگاهی از کلید عمومی فرستنده، متن مورد نظر را با کلید عمومی گیرنده رمز کرده و از طریق کانال ناامنی برای گیرنده ارسال می کند . گیرنده هم با دریافت متن رمز شده با بهره گیری از کلید خصوصی خود، این متن رمز شده را از رمز خارج کرده و به یک متن واضح تبدیل می کند.

-از جمله **نقاط قوت** این روش این می باشد که **سرویس انکارناپذیری** را پشتیبانی می کند، **مدیریت کلیدها** راحت می باشد، چرا که تعداد کلیدها به تعداد کاربران می باشد . و همچنین **توزیع کلید راحت** می باشد . اما **نقطه ضعف** آن هم **پایین بودن سرعت** آن می باشد، چرا که میزان محاسبات در الگوریتم های نامتقارن بیشتر از الگوریتم های متقارن می باشد.

انجام سرویس احراز هویت با بهره گیری از الگوریتم های نامتقارن (Authentication)

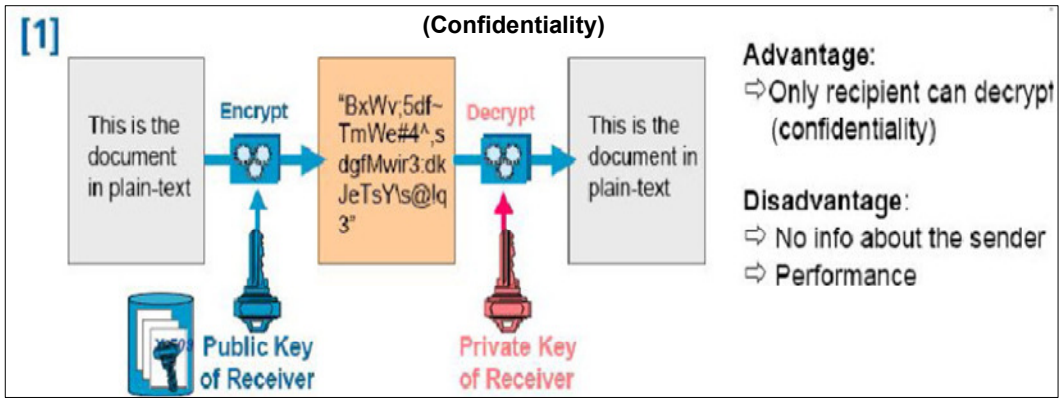
A

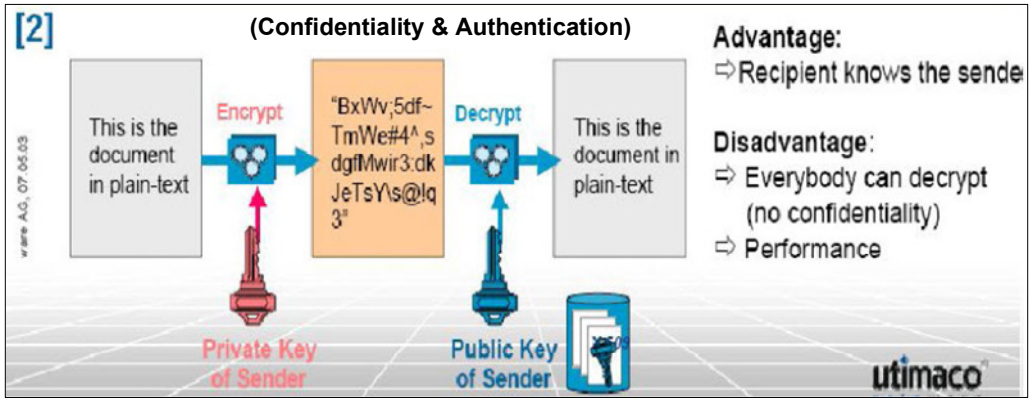
-فرستنده با کلید خصوصی خودش یک متن معنی دار را به یک متن رمز شده تبدیل کرده و آن را منتشر می نماید . در اینجا تمام کسانی که به کلید عمومی او دسترسی دارند می توانند روی متن رمز شده عمل رمزگشایی را انجام داده و متن واضح را شناسایی کنند . باید توجه داشت در این سرویس هدف محرمانگی این اطلاعات نمی باشد، بلکه احراز هویت فرستنده پیام می باشد.

انجام سرویس احراز هویت و محرمانگی با بهره گیری از الگوریتم های نامتقارن (Confidentiality & Authentication)

CA

-یعنی با استفاده از کلید منتشر شده یک گیرنده می توانیم برایش متن رمز شده و محرمانه ارسال کنیم، و همچنین فرد فرستنده می تواند با رمز کردن این متن رمز شده با کلید خصوصی خودش و ارسال آن به گیرنده، گیرنده در ابتدا با کلید عمومی فرستنده مرحله اول رمزگشایی را انجام دهد و در نتیجه می تواند به صحت فرستنده و آنگاه با رمزگشایی مجدد با کلید خصوصی ، (Authenticate)پی ببرد خودش به متن واضح اصلی دست پیدا کند.





تفاوت رمزنگاری متقارن با نامتقارن

-در روش سیمتریک کلید منحصر بفرد بین دو طرف به اشتراک گذاشته می شود . ولی در الگوریتم آسیمتریک از دو کلید عمومی و خصوصی استفاده می شود.

-عمل جابجایی کلید در سیمتریک باید در کانال جدا از کانال ارسال پیام ها انجام گیرد، و این در حالی است که در آسیمتریک عمل انتقال کلید در همان کانال در نظر گرفته شده برای انتقال متن، منتقل می گردد.

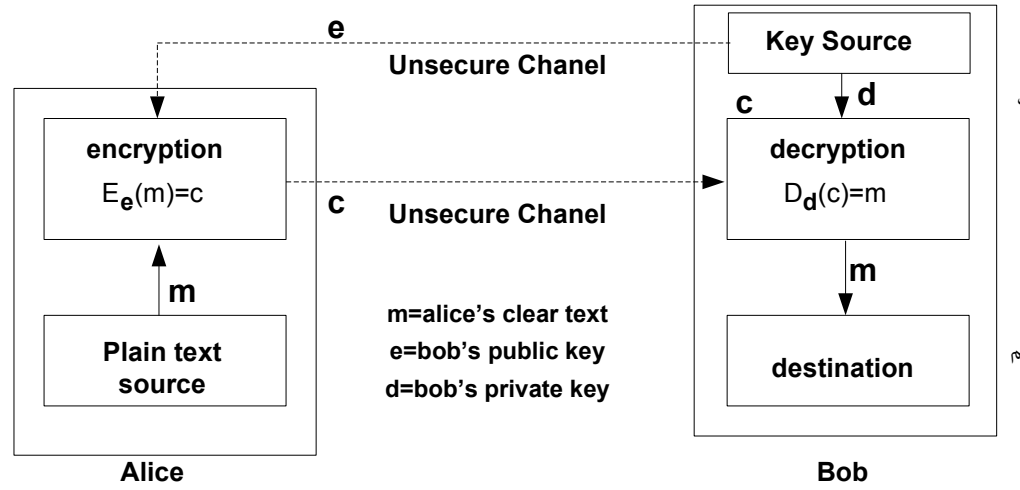
-الگوریتم های رمزگذاری سیمتریک مقیاس پذیر نیستند، یعنی آنکه قابلیت اعمال بر روی بلوک های مختلف داد ه ای با اندازه های مختلف را ندارند . ولی در آسیمتریک این کار امکان پذیر است.

-سیمتریک ها دارای سرعت بالاتر اجرایی نسبت به آسیمتریک ها هستند.

-سیمتریک ها برای اجراء بر روی حجم بالای داده مناسب می باشند. در حالیکه آسیمتریک ها بیشتر برای اعمال بر روی حجم کوچکتر داده بکار می روند . و برای تولید امضای الکترونیکی، گواهی دیجیتالی، پاکت دیجیتالی استفاده می شوند.

-سیمتریک صرفا برای سرویس محرمانگی بکار می رود، در حالیکه آسیمتریک علاوه بر سرویس محرمانگی، سرویس های احراز هویت، و انکارناپذیری را هم پشتیبانی می کند.

روش توزیع کلید درمدل رمزنگاری نامتقارن
Asymmetric Cryptography Model



توابع در هم ریزی Hash Alghorithms

-الگوریتم درهم ریزی با هدف تامین سرویس امنیتی **صحت و جامعیت داده** بکار گرفته می شود . درهم ریزی یک تابع یک طرفه میباشد که سایزی ثابت از مقادیر مبتنی بر اندازه های مختلف از حجم داده ورودی را تولید می کند . یک تابع درهم ریزی در هر بار اجراء بر روی دیتای مشخصی، خروجی ثابت دارد، و این بدان معنی می باشد که با اجراء مختلف بر روی داده مشخصی خروجی متفاوتی نمی دهد. بعضی از الگوریتم های درهم ریزی معروف **SHA-۱,MD-۵,MD-۴** میباشند.

-تابع درهم ریزی را می توان با اثر انگشت مقایسه کرد . همانطور که اثر انگشت هرکس انحصاری است و دارای اندازه ثابتی است. نتیجه تابع درهم ریزی هم انحصاری است و نمی توان مقادیر یکسان از داده های متفاوت بدست آورد.

MD-4 خروجی آن یک مقدار ۱۲۸ بیتی است . خیلی سریع می باشد، برای اهداف امنیتی سطح متوسط مناسب می باشد.

MD-5 خروجی آن یک مقدار ۱۲۸ بیتی است . سریع می باشد(اما نه به اندازهMD-۴)از MD-۴ امن تر است . در بسیاری از مکان ها استفاده می شود.

SH-1 خروجی آن یک مقدار ۱۶۰ بیتی است . استاندارد دولتی آمریکا میباشد.اما ازMD-۵ کندتر میباشد.

معرفی اجزاء زیرساخت کلید عمومی

PKI=Public Key Infrastructure

- PKIاز زوج کلید آسیمتریک، نرم افزارهای ترکیبی، و تکنولوژی های رمزنگاری، برای ایجاد امنیت ارتباطات و تراکنشهای تجاری استفاده میکنند.

-استاندارد PKI که در محیطهای اینترنتی مورد استفاده قرار میگیرد استانداردX.۵۰۹ میباشد. که شامل تاییدیه، تایید کننده تاییدیه، ابزار مدیریتی تاییدیه ها، و برنامه های کاربردی که تاییدیه ها را بکار می گیرند، می باشد.

اجزاء PKI

تاییدیه دیجیتالی Digital Certificate

-یک اعتبار نامه الکترونیکی برای احراز هویت کاربران میباشد.

مرکز قانونی صدور تاییدیه Certification Authority (CA)

-یک کامپیوتر که تاییدیه دیجیتالی را صادر می کند، یک لیست تاییدیه های معتبر را نگه داری می کند، و همچنین یک لیست از تاییدیه هایی که به دلایلی اعتبار آن باطل شده را هم نگه داری می کند.

مرکز قانونی ثبت نام Registration Authority (RA)

-مرکزی که برای رسیدگی به شرایط ثبت نامی و ثبت نام از متقاضیان در خواست تاییدیه های دیجیتالی، و ارسال درخواست ها به CA، فعالیت می کنند.

ابزار مدیریت تاییدیه ها و کلیدها Key & Certification Management Tools

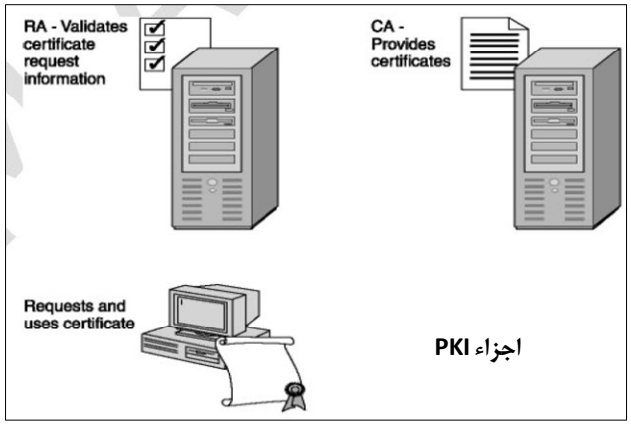
-ابزار برای حسابرسی و مدیریت تاییدیه های دیجیتالی.

نقطه انتشار تاییدیه ها Certification Publication Point

-مکانی که تاییدیه ها ذخیره و منتشر می شوند.

سرویسها و برنامه های فعال ساز کلید عمومی Public Key-Enabled Applications and Service

-برنامه های کاربردی و سرویسهایی که استفاده از تاییدیه را پشتیبانی میکنند.



اجزاء PKI

تاییدیه Certificate چه میباشد.

-تاییدیه یک معرف دیجیتالی می باشد که شما را معرفی کرده و توسط CA صادر می گردد . این CA معمولابه عنوان سوم شخص قابل اعتمادیا Trusted Third Party (TTP) . هم شناخته می شود، در هر تاییدیه مشخصات سوم شخص معتمد صادر کننده آن، تاریخ اعتبار تاییدیه، و امضاء تاییدیه سوم شخص معتمد برای تایید صدور آن، وجود دارد.

-تاییدیه می تواند توسط برنامه های کاربردی و سرویس های امنیتی مختلف برای انجام مواردی همچون احراز هویت، صحت و یکپارچگی داده ها، و امنیت بکار رود . کاربردهای تاییدیه شامل موارد زیر است

کاربردهای تاییدیه

امن سازی ایمیل: -از پرتکل S/MIME برای اطمینان از **صحت و جامعیت مبداء (فرستنده) و محرمانگی** در**ایمیل** استفاده میشود.

امن سازی ارتباطات وب: -استفاده از تاییدیه در پرتکل SSL/TLS برای **احراز هویت و رمزنگاری** ارتباطات میان **سرور و کلاینت**

راه حلهای امنیت مشتریان: -استفاده از تاییدیه برای **اجرای محرمانگی، صحت، احراز هویت، و انکار ناپذیری** در **برنامه های کاربردی** مشتریان.

امن سازی زیر ساختهای شبکه

کانال های ارتباطی | **تجهیزات ارتباطی** | **منابع شبکه**

انواع حملات ممکن فرا روی زیر ساختهای شبکه

- تخریب فیزیکی تجهیزات
- شنود بسته های اطلاعاتی
- اسکن پورت های شبکه و نقشه شبکه برای شناسایی اهداف جهت تدارک حمله
- چیدمان مجدد و یا غیر فعال کردن ارتباطات تجهیزات امنیتی
- استفاده از تجهیزات شبکه برای تدارک حمله به شبکه ای دیگر
- استفاده از شبکه شما برای میزبانی سرویس های غیرقانونی، مخریف و ناشناخته
- پاک کردن و تخریب داده ها

راه کارهای امن نمودن تجهیزات فیزیکی

- استخدام گارد حفاظتی
- نصب سنسور، و تلویزیون های مدار بسته برای نظارت بر تجهیزات
- استفاده از کارت های امن برای دسترسی قیزیکی
- نصب سیستم برق اضطراری
- پوشش کابل های شبکه و یا قرار دادن آنها درون دیوارها
- قفل نمودن دری اطاق سرور
- قرار دادن تجهیزات در پوششهای مناسب و مهر و موم کردن آنها
- نصب فنس و گیت های ورود و خروج
- نصب سیستم ضد حریق
- اطمینان از استانداردهای نصب و پیاده سازی تجهیزات

کابل های کواکسیال (Coaxial Cable)

-هر کابل کواکسیال شامل : رشته سیم رسانای مرکزی، یک رشته سیم رسانای بیرونی، و یک پوشش بیرونی است. انتقال الکترونیکی (داده های در حال انتقال) از میان رشته سیم رسانای مرکزی عبور می کند. ودر توپولوژی BUS استفاده میشود.

حملات

-معمولا از دو جنبه **تخریب** و یا **استراق سمع** اطلاعات مورد تهاجم قرار می گیرند. و قطع شدن بخشی از کابل باعث قطعی کل شبکه میشود.

-یکی از تخریب هایی که علیه این کابلها انجام می گیرد **برش آنها** بوسیله قیچی های فلزبر(علی رغم محکم بودن این کابل ها) می باشد.

-همچنین **منبع گرمایی شدید** در مجاورت کابل ها عامل دیگری برای تخریب کابل می باشد.

-کابل ها در مقابل **امواج رادیویی** و **امواج مغناطیس** دچار آشفتگی اطلاعاتی می شوند.

-جدا سازی Terminatorتمام کننده در قسمت انتهایی خطوط در این کابل ها باعث قطعی شبکه می شود.

-در این توپولوژی سیگنال های اطلاعاتی در کل شبکه به انتقال در می آیند، پس هر نود متصل به این شبکه در صورت **لحاظ نشدن موارد امنیتی** در شبکه، **امکان استراق سمع** اطلاعات را دارا می باشد.

-هر بخش از کابل شبکه مکان مناسبی برای **یک اتصال جدید** به شبکه توسط مهاجمین می باشد.

ایمن سازی

-قرار دادن این کابل ها در زیر سطح زمین، قرار دادن آن ها در دیوارها، و پوشش گذاری حداکثری آنها برای جلوگیری از استراق سمع.

-مستندسازی کابل کشی ها

-وارسی کردن تمامی را ه های خروجی شبکه کابل کواکسیال.

-بازرسی فیزیکی به صورت دوره ای از تمامی زیر ساخت های کابل.

-وارسی کردن تمامی تجهیزات میزبان و اتصالات مستند نشده.

زوج سیم مسی (Twisted Pair Cable)

-هر کابل زوج سیم مسی دارای یک یا بیشتر زوج سیم تابیده شده بهم قرار گرفته در یک غلاف پلاستیکی می باشند. . هر سیم از جنس مسی می باشد که توسط لایه پلاستیکی به عنوان پوشش در دور آن جهت عدم اتصال الکتریکی سیم ها به یکدیگر محافظت می شود . هر زوج تک سیم بدور یکدیگر جهت جلوگیری از هرز رفتن سیگنال های الکتریکی درونشان، بهم تابیده شده اند.

حملات

-این سیم ها به دلیل جنس نازکشان براحتی قابل **تخریب و بریده شدن** می باشند . همچنین **حرارت گرمایی** نیز بر روی آنها تاثیر مخربی دارد.

-بعلت توپولوژی Starقطع شدن یکی از این سیم ها باعث قطعی کل شبکه نمی شود.

-اتصال فیزیکی یک **پروتکل آنالیزر** به یک نقطه اتصال از این زوج سیم های مسی . پروتکل آنالیزر یک دستگاه و یایک برنامه نرم افزاری کامپیوتری می باشدکه به مهاجم اجازه تصرف و ورمزگشایی ترافیک موجود بر روی شبکه را می دهد.

-بهم **تابیدن به داخل** کابل زوج سیم مسی.

-استفاده از **سیگنال های الکترومغناطیسی** برای استراق سیگنال های عبوری از میان زوج سیم مسی.

به سه مورد آخر حملات بعد از استراق سمع گفته میشود.

امنیت در کانال های ارتباطی شبکه

ایمن سازی
-محافظت فیزیکی کابل بالاخص در مراکز حساس آن مثل محل اتصالات به هاب و سوییچ و . . .
-استفاده از سوییچ به جای هاب، چرا که سوییچ ترافیک مورد نظر را مستقیما به میزبان مورد نظر اصلی می فرستد، در حالی که هاب ترافیک را به سمت تمامی میزبان های موجود در شبکه گسیل می دارد.
-مدیریت سوییچ ها، هاب ها، و روترها به شکلی که در صورت صدمه دیدن بخشی از شبکه و یا ورود یک اتصال جدید به شبکه، به مدیر شبکه پیغام دهد.

فیبر نوری (Fiber Optic Cable)
-کابل فیبر نوری از یک رشته و تار شیشه ای یا پلاستیکی برای انتقال پالس های نوری تشکیل شده است.
-توسط امواج رادیویی و مغناطیس تحت تاثیر قرار نمی گیرند . این کابل ها گران تر و نصب آنها نیز سخت تر می باشد.

حملات
-خرابی بر روی این کابل ها بسیار راحت تر می باشد . این کابل ها براحتی می توانند آسیب دیده، مچاله شده، و یا شکسته شوند. اما شنود بر روی کابل فیبر نوری غیر ممکن است، مگر آنکه فرد مهاجم بخشی از فیبر نوری را بریده و یک کارت قرائتگر فیبر نوری وارد مسیر شبکه نماید.

ایمن سازی
-مهمترین عاملی که جهت امن سازی این کابل ها ذکر می شود محافظت فیزیکی ازآنها و همینطور پیکر بندی شبکه به شکلی که در صورت قطعی در شبکه، بدلیل تلاش مهاجم برای وارد کردن یک کارت قرائتگر فیبر نوری در بخشی از شبکه، فورا هشدارهای لازم به مدیران شبکه داده شود.

امنیت در تجهیزات ارتباطی شبکه

HUBs-هاب یک وسیله ارتباط و اتصال در شبکه های از نوع اترنت می باشد . که دارای دو نوع فعال و غیرفعال می باشد . در نوع فعال ان سیگنال های شبکه تکرار و تقویت می گردد . و چون هاب محل ارتباط اصلی در شبکه می باشد لذا مورد توجه مهاجمین برای تدارک حمله می باشد.

تخریب هاب
-اگر مهاجم به آن دسترسی فیزیکی داشته باشد به راحتی قابل تخریب است . هاب به راحتی میتواند از اتصال خارج و یا خراب شود، و یا اگر از نوع فعال آن باشد، به راحتی خاموش شود.
-شنود بر روی هاب نیز امکان پذیر می باشد . اگر یک پورت بر روی هاب آزاد باشد حمله کننده می تواند از آن پورت برای دستیابی به اطلاعات و یا تخریب بر روی دیگر تجهیزات متصل در شبکه سود برد.

ایمن سازی
-تلاش گردد هاب درون محفظه ای امن قرار داده شود. حداقل به صورت دوره ای هاب مورد بازدید قرار گیرد تا از امن بودن اتصالات آن و عدم اتصال یک فرد غیر مجاز به آن مطمئن شویم.
-هاب های قابل مدیریت اطلاعات آماری و اطلاعات اتصالیشان را برای مدیریت نرم افزار ارسال می کنند . لذا شما می توانید هاب را برای اعلام خطر به هنگام تغییر در بهم بندیش مجهز کنید . اما از آنجا که این روش مدیریت موقعیت و بهم بندی به شکل نرم افزاری انجام میگیرد، فرد مهاجم می تواند چیدمان نرم افزاری را تخریب و یا تدارک حمله ای دیگر از این ناحیه را ببیند.

Switches & Bridges
-سوییچ و بریج در لایه دوم OSI کار میکنند و بر مبنای آدرس کنترل دسترسی کانالهای ارتباطی(MAC Address) هر یک از اتصالات شبکه را انجام میدهند.
-سوییچ و بریج جدولی را برای کمک به ارسال بسته های اطلاعاتی به بخش های مناسب شبکه، ایجاد می کنند . پل یا باصطلاح بریج نوعا یک شبکه را به دو بخش تقسیم میسازند ولی سوییچ ها نوعا هر بخش از شبکه را به چندین قسمت کوچکترتقسیم می کنند، و هر قسمت برای هر پورت سوییچ می باشد.
-این تجهیزات بیشتر برای ارسال اطلاعات بصورت تک مقصده(Unicast) استفاده میشوند ولی بصورت چند مقصده (Multicast) نیز استفاده میشوند.
-سوییچها و پل ها از جدولی از MACها برای نشان دادن اتصالات به هر نقطه از شبکه استفاده میکنند.

تخریب سوییچ
-تخریب جدول MAC در سوییچ و پل و هدف گذاری برا تخریب سوییچ مرکزی
-تملیک دسترسی مدیریت شبکه (user name ,pass) به سوییچ و تخریب مسیر های سوییچ
-دسترسی مهاجم به معکوس سازی پورت (Mirroring Port) که این فرایند مدیر شبکه را قادر میسازد نگاشت ورودی و خروجی از یک یا چند پورت سیستم به یک پورت خاص منتج گردد و از این روش برای عیب یابی استفاده میشود.
-مسموم سازی حافظه ARP (ARP cache Poisoning) . ابتدا دسترسی فیزیککی برقرار میشود و سپس جدول ARP دستکاری میشود.

ایمن سازی
-امن کردن کلیه اتصالات فیزیکی در شبکه و محدودسازی دسترسی به مکان این تجهیزات و نظارت بر تجهیزات از جهت اطمینان از امن بودن اتصالات.
-استفاده از کلمات عبور مرکب و پیچیده برای کنسول های مدیریتی.
-ورود دستی نگاشتهای ARP در تجهیزات بحرانی ،همچون سرورها ،سوییچها و پلهای مرکزی
-سوییچها و پلها را توسط آخرین نسخه های وصله های امنیتی طراحی شده توسط سازندگان آنها مجهز نماییم.
-مستندسازی نحوه بهم بندی دستگاه برای یادآوری ارتباطات نرمال و مجاز در آینده.
-مانیتور کردن شبکه با ابزارهای مدیریتی برای آگاهی از اتصالات غیر مجاز مانند APPWATCH,Solarwindsکه میتواند یک نسخه از جدول MAC به IP را در خود نگاه داشته و تغییرات شبکه را به مدیر شبکه اعلام نماید.

Routers –مسیر یابها در لایه سوم OSI که لایه شبکه میباشدکار میکنند .ضمنا از ARP Cache و جدول مسیر دهی (Routing table) برای انجام وظیفه مسیر دهی در شبکه بهره میگیرند.

تخریب مسیریابها

–ARP Cache و Routing Table خود نقطه ای برای تدارک حمله می تواند باشد. روتر مرکزی همچنین می تواند مکان مناسبی برای تخریب باشد . خراب کردن روتر مرکزی، قطع کردن برق، و یا قطع کردن اتصالات کابل های روتر می تواند عاملی برای جلوگیری از گذر اطلاعات در بین دستگاه در شبکه باشد.

–ARP Cache میتواند مستعد مسموم سازی باشد. تغییر Routing Table نیز میتواند مسیر یابی را دچار اختلال کند

–اگر یک حمله کننده بتواند دسترسی مدیریتی به روتر پیدا کند، او می تواند مسیردهی مجدد در شبکه را انجام دهد . این ارتباطات می تواند به سمت یک میزبان تحت کنترل مهاجم در شبکه مسیردهی مجدد شود.

–تغییر پرتکل اطلاعات مسیر دهی RIP با جدول مسیر یابی اطلاعات نادرست راRIP Spoofing میگویند نوعی حمله میباشد.

–دستگاه های ارتباطی ممکن است مشکلات بهم بندی نرم افزاری و یا نقاط آسیب پذیری امنیتی داشته باشند . بطور مثال، ممکن است شخصی دریابد که یک روتر می تواند بروز و یا غیرفعال شود بدون مجوز مدیریت (به این معنی که در صورت دسترسی به شبکه می تواند آن روتر را تخریب نماید) فروشنگان این تجهیزات در صورت اطلاع از این ضعفها غالبا قادر به حل آن می باشند، لذا برای محافظت از تجهیزات ارتباطی حتما پی گیری از فروشندگان آنها را برای دریافت وصله های مرتفع کننده مشکل، فراموش نکنید.

ایمن سازی

–یک روتر مرکزی هدف مناسبی برای مهاجمین می باشد . تخریب یک روتر مرکزی، قطع برق آن و یا قطع نمودن کلیه کابل های ارتباطی آن ممکن است کلیه ارتباطات متصل به این دستگاه را مختل سازد.

–اطمینان از نگه داری روتر در اطاق قفل دار یا در پوشش مناسب.

–امتحان امنیت تمامی اتصالات ورودی و خروجی.

–محدودسازی دسترسی فیزیکی به تجهیزات زیربنایی شبکه کابل، و اطاق های سرور.

–مانیتورینگ تجهیزات برای حفاظت از نقاط اتصال و تجهیزات.

–بکارگیری کلمات عبور ترکیبی برای کنسول های مدیریتی.

–بهنگام نگه داری روترها با آخرین نسخه وصله های (Patches)امنیتی ارائه شده توسط فروشندگان.

-اطمینان از مستندسازی و نظارت مجدد بر چیدمان و بهم بندی شبکه.

-استفاده از RIP V۲ بجای RIPV۱که شامل رمز نگاری (کلمه عبور) میباشد توصیه میگردد

Firewalls

-بصورت عمومی برای توضیح تجهیزاتی بکار می رود که برای محافظت از یک شبکه داخلی (یا یک میزبان) در مقابل مهاجمین یا کدهای مخرب از شبکه خارجی (یا شبکه ای که آن میزبان به آن متصل است) بکار می رود.

-دیواره های آتش معمولا از اعمال متفاوتی برای فیلتر کردن ترافیک های ورودی و یا خروجی مضر و مخرب، استفاده می کنند.

-اغلب برای پیاده سازی بین ارتباط شبکه داخلی سازمان و اینترنت بکار می روند . البته گاها بعضی از دیواره های آتش برای جداسازی شبکه داخلی و یا حتی محافظت از یک کامپیوتر تنها نیز بکار می رود.

-این دیواره ها هستند که بر اساس مقررات امنیتی موجود تصمیم می گیرند کدام داده ها وارد شبکه شوند یا ازشبکه خارج شوند.

-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.

وظایف اصلی فایروالها

Filtering

Network Address Translation (NAT)

Transparent

وظایف اصلی فایروالها

Filtering

–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 فیلترینگ بر اساس header یک بسته انجام میگردد که به آن Packet filtering میگویند.

–در بیشتر مواقع فیلترینگ در لایه ۲ وبر اساس MAC میباشد ولی در حالت پیشرفته علاوه بر header بسته به ارتباط بسته ها با یکدیگر نیز توجه میشود و بر اساس آن تصمیم گیری میشود به این نوع فیلترینگ stateful inspection گفته میشود که در آن state هر connection نگهداری و برای فیلترینگ استفاده میشود. در برخی دیگر نیز بر اساس محتوی بسته فیلترینگ انجام میشود که به آن content filtering گفته میشود.

Network Address Translation (NAT)

–این حالت استفاده از فایروال بعنوان Gateway میباشد. این کار در اغلب موارد با استفاده از تخصیص IP های Invalid (غیر قابل route در اینترنت) به ماشینهای شبکه داخلی و ترجمه این IP ها به IP قابل rote انجام میگیرد.

Transparent

–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 پیکره بندی خاص (معرفی فایروال بعنوان default Gateway,Proxy,.....) ندارند.

فوائد دیواره آتش

–توانایی کنترل ترافیک در هر دو جهت ورودی و خروجی .

–قابلیت اعمال کنترل متمرکز و یکپارچه به جای کنترل توزیع شده .

–قابلیت محدود کردن دسترسی به سرویسهای غیر امن .

–توانایی انجام فیلترینگ در لایه های مختلف (Data Link-Application)

–هزینه کمتر جهت امن کردن شبکه، در مقایسه با امن کردن مستقل هر یک از Hostها

–پیچیدگی کمتر در مقایسه با امن کردن Host ها ،بخاطر نداشتن سیستم عامل و برنامه های کاربردی پیچیده

معایب دیواره آتش

–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 .

–دیواره آتش، خواه نا خواه برای کاربران قانونی هم محدودیت های دسترسی ایجاد می کند .

–دیواره آتش، حملات Back Door را نمیتواند تشخیص دهد.

–دیواره آتش در برابر بسیاری از نقاط ضعف امنیتی در سطح Application راه حلی ندارد.

–به خاطر اینکه تمام ترافیک از دیواره آتش می گذرد، این مسئله میتواند به معضل throughput در سیستم تبدیل شود.

–نفوذهایی که از درون شبکه داخلی و به قصد ماشینی در همان شبکه انجام می شود، از دید دیواره آتش پنهان می ماند، چرا که اصولا بسته های مربوطه از دیواره آتش عبور نمی کنند . یکی از دلایل لزوم استفاده از سیستم های مهاجم یاب (IDS) نیز همین است .

تخریب فایروالها

پیاده سازی و نصب ضعیف دیواره های آتش

قوانین اجازه به صورت پیش فرض

–به تمام بسته های اطلاعاتی ورودی به شبکه به جزء آنهایی که ممنوع شده اند اجازه ورود می دهند. مدیران شبکه اصولا این مدل را ترجیح میدهند.

قوانین عدم اجازه به صورت پیش فرض

–به هیچ بسته اطلاعاتی ورودی به شبکه به جزءآنهایی که اجازه داده شده اجازه ورود نمی دهد .

نقص و عیب در بخش نرم افزاری دیواره آتش

–معمولا فروشندگان دیواره های آتش پس از پی بردن به این نقائص برای رفع آنها ،بالاخص برای خریداران قبلی، وصله هایی را برای نصب بر روی آنها و رفع عیب طراحی می کنند .

امنیت در تجهیزات ارتباطی شبکه

تخریب فایروالها

دسترسی مهاجم به رمز عبور کنسول مدیریت دیواره آتش

–این کنسول ها در یکی از دو شکل ارتباط نزدیک و از طریق کابل و یا ارتباط از راه دور بوسیله ارتباطات بیسیم بوسیله مدیران شبکه قابلیت دسترسی به سیستم فایروال را ایجاد می کنند .

دسترسی مستقل دیگر برای شبکه می باشد .

–بطور مثال تماس از طریق شماره گیری Dialup Connection برای سرور به خارج از شبکه که این امکان تحت نظارت فایر وال نباشد.

امکان دسترسی فیزیکی به فایروال توسط مهاجمین

ایمن سازی

–زیر نظر داشتن و پی گیری از فروشندگان فایروال برای دریافت وصله های رفع خطای بروز ازآنها.

–بروزسازی فایل های شناسایی ویروس ها

–حفاظت فیزیکی از فایروال ها .

–استفاده از رمزهای عبور ترکیبی برای دسترسی به فایروال ها .

–مستندسازی نحوه بهم بندی سیستم های فایروال و بررسی مجدد آن بصورت دوره ای .

–محدودسازی روش های مدیریت فایروال ها تا حد ممکن .

–اطمینان از عدم وجود راه های دسترسی به شبکه که تحت مدیریت فایروال نباشد .

–استفاده از چند فایروال بصورت پشت سرهم بخصوص از شرکتهای مختلف

Modems –مکان اتصال کامپیوترها به اینترنت و یا شبکه داخلی را فراهم می سازند .

محافظت از مودم

–جداسازی همه مودمهای غیرضروری از کامپیوترهای داخل شبکه

–بررسی بروز بودن همه نرم افزارهای موجود بر روی کامپیوترهای شبکه که نیاز به مودم دارند . بطور مثال آنتی ویروسها یا وصله های امنیتی

–پیگیری از فروشندگان مودم ها برای دریافت وصله های برطرف کننده نقائص مودم ها و بروزسازی آنها .

–نظارت دوره ای بر کامپیوترهای دارای مودم برای آنکه مورد تخریب قرار نگرفته باشند .

Wireless –ارتباطات مابین نقاط دسترسی و کارت های شبکه از طریف سیگنال های رادیویی و سیگنال های مادون قرمز در فضا انجام می گیرد .

–مهاجم نیازی به اتصال فیزیکی و یا برش بر روی سیم ها جهت اتصال به شبکه وجود ندارد . این نقاط دسترسی همچنین می توانند مانند هاب ها، سوییچ ها، و یا روترها عمل نمایند . بنابراین تمام حملاتی که در گذشته بر روی این تجهیزات مطرح گردیده بر روی نقاط دسترسی هم متصور می باشد .

–با توجه به استفاده عموم از اینترنت استفاده از روش های احراز هویت و همچنین رمز گذاری اطلاعات مهم، راه مناسبی برای جلوگیری بسیاری از تخریب ها در این شبکه ها می باشد .

–بروز نگه داشتن تجهیزات امنیتی با استفاده از آخرین وصله های بر طرف کننده عیوب این تجهیزات

–پیاده سازی این تجهیزات در بخش های زیرین زمین و استفاده ازدیوارهای ضخیم می باشد .

–امواج تجهیزات بیسیم ممکن است در مقابل امواج رادیویی و مغناطیس دیگر آسیب پذیر باشند، لذا بالا بردن توان سیگنالینگ این تجهیزات راه حل مناسبی برای این مشکل می باشد .

–در حین نصب تجهیزات بیسیم باید مطمئن گردید که نقاط دسترسی آنها در کنار منابع امواج رادیویی و مغناطیسی دیگر مانند آسانسور، ماشین های کپی، فرستنده های رادیویی، و یا تجهیزات صنعتی نمی باشد .

امنیت در منابع شبکه

امن سازی و مانیتورینگ ایستگاه های کاری Workstation Security

–تخریب ایستگاه های کاری در شبکه باعث اتلاف وقت کاربران آنها و همچنین از دست رفتن اطلاعات ذی قیمت می شوند . اگر یک مهاجم بتواند به یک ایستگاه کاری در شبکه شما وارد شود و اخلالی را ایجاد نماید، احتمالا می تواند به دیگر تجهیزات در شبکه نیز دست اندازی کند .

محافظت ازایستگاه

–نصب آنتی ویروس ها و بروز نگه داشتن

–مانیتورینگ فایل های ثبت وقایع Log File برای ایرادات بوجود آمده

–نصب سیستم ثبت اطلاعات و حسابرسی برای سیستم ها و منابع داده ای حساس در شبکه

–محدود سازی دسترسی به هر ایستگاه کاری توسط یک کاربر یا گروه مشخصی از کاربران

–کنترل دسترسی به منابع داخلی و یا منابع به اشتراک گذاشته شده در شبکه

–برداشتن برنامه ها و سرویس ها غیر ضروری بر روی آنها

–نصب سیستم های اتوماتیک یا مرکزی تهیه نسخه پشتیبان

–اطمینان از نصب بروزترین تعمیرکنندگان امنیتی (وصله) بر روی سیستم های عامل، و برنامه های کاربردی

–اجرای سیستم های مانیتورینگ و سیستم های کشف نفوذ

امنیت در منابع شبکه

مانیتورینگ

-**سیستم ثبت وقایع** : نظارت بر پیغام های خطا در باره تغییرات در سیستم فایلها، تغییر اجازه های دسترسی، سرویس هایی که دیگر امکان شروع و انجام آنها وجود ندارد، و یا دیگر تغییرات در سیستم

-**فضای هارد دیسک** : ایستگاه های کاری ممکن است از انجام ثبت وقایع، ثبت خطاها، کشف حملات و دیگر موارد به شکل صحیح، بدلیل پر شدن فضای هارد دیسکشان باز بمانند . پس مانیتورینگ میزان فضای خالی هارد دیسک ضروری است .

محافظت تجهیزات سیار Mobile Device -لپ تاپ، نوت بوک، دستیار دیجیتالی شخصی PDA و دیگر تجهیزات سیار تمامی مواردی که برای امن سازی ایستگاه های کاری مطرح گردید برای امنیت تجهیزات سیار نیز در صورت امکان ضروری است .

دیگر موارد

-**تجهیزات ضد سرقت** : کاربرد تجهیزات هشداردهی و آلارم های تغییر جا برای این تجهیزات، کابل های قفل شده

-**استفاده از علائم و رنگ های شناسایی اضافی** : اگر این تجهیزات دارای رنگ های خاصی باشند و یا بر روی آنها علائم شناسایی و حتی نام سازمان حک شده باشد، پیگیری آنها را در بیرون سازمان هم مقدورتر می سازد . از طرفی بکار گیری این روش سارقان را در سرقت آنها بی میل تر می سازد .

-**رمزگذاری داده ها** : اگر تجهیزات موبایل شما برای نگهداری و یا انتقال داده های سری و مهم بکار گرفته می شود، حتما این گونه داده ها توسط الگوریتم های پیشرفته رمزنگاری بصورت رمز شده در آورده شود، تا در صورت دستیابی توسط مهاجمین به این تجهیزات، اطلاعات درون آنها قابلیت استفاده برای مهاجم را نداشته باشد .

امن سازی و مانیتورینگ سرورها Server Security

-باید همان عملکردها که برای امن سازی ایستگاه های کاری انجام داده اید، برای سرورها هم انجام دهید . البته سرورها نیاز به مراقبت بیشتری نسبت به یک ایستگاه کاری دارند، چرا که تخریب یک سرور افراد بیشتری را تحت شعاع خود قرار می دهد .

محافظت از سرور

-امن سازی فیزیکی سرورها از طریق قرار دادن آنها در اطاق های قفل دار

-جلوگیری از ورود کاربران بوسیله کنسول ها به آنها

-کنترل دقیق و مانیتورینگ دسترسی به منابع، از جمله سیستم فایل ها، داده های به اشتراک گذاشته شده، و چاپگرها

-کنترل دقیق و مانیتورینگ دسترسی به کلیه سرویس ها . سرویس های اضافی همچون دیتابیس کاربران، سرویس وب، و دیگر سرویس های ارائه شده توسط سرور . همچنین شما باید خطاهای ایجاد شده در دسترسی به سرویس ها، خطا در اجرای سرویس ها، و هر تغییری در اجرای سرویس ها را ره گیری کنید .

-ایجاد نسخه های پشتیبان بصورت دوره ای از بهم بندی سرورها، داده های به اشتراک گذاشته شده، و دیگر داده ها که نیاز به حفاظت از آنها وجود دارد . همچنین باید از حفاظت فیزیکی از این نسخه های پشتیبان مطمئن گردید . قرار دادن رمز عبور بر روی آنها و رمزگذاری آنها و قرار دادن آنها در گاوصندوق های ضد حریق از دیگر موارد مهم امنیتی می باشد .

-باید از مانیتورینگ دسترسی ها و و در دسترس بودن منابع بر روی سرورها مطمئن گردید . بطور مثال شما باید از امکان پذیر بودن سرویس HTTP برای دسترسی به وب سایتها بر روی سرور مطمئن بود.

مانیتورینگ تجهیزات اتصال

-امروزه سیستم های مدیریت شبکه ارائه شده توسط بسیاری از فروشندگان که اطلاعات از تجهیزات اتصال را جمع آوری می کنند، در دسترس می باشند . بطور مثال، اگر یک روتر یا سوییچ بعضی ازفریم های اطلاعاتی را بدلیل حجم بالای دیتاهای ورودی از دست بدهد، یک هشدار می تواند به سمت کنسول مدیریت شبکه و یا دیگر مکان های بالقوه مثل پیجر مدیر شبکه ارسال گردد . مانند پرتکل SNMP-simple network managment

امن سازی برنامه های کاربردی

امنیت بر روی پست الکترونیکی

امن سازی پیغام های الکترونیکی

-ایمیل ها می توانند توسط تجهیزاتی مانند پروتکل آنالایزر در طول مسیر انتقالشان مورد شنود قرار گیرند.

-به دلیل فقدان محرمانگی، ایمیل ها براحتی قابل جعل می باشند . یک فرد حمله کننده می تواند با تغییر فیلد ارسال کننده در ایمیل ها، آنها را به شکلی که از طرف فرد مطمئن و معتبری ارسال شده اند جلوه دهد .

-رمزگذاری ایمیلها این امکان را می دهد که تنها توسط افراد مورد نظر شما قابل فهم باشد . همچنین امن سازی پیغام های الکترونیکی می تواند شامل امضاء الکترونیکی ایمیل ها هم شود . با این کار گیرنده نامه هم مطمئن می گردد که این ایمیل از جانب شخص شما می باشد .

Pretty Good Privacy (PGP)

-مجموعه ای از ابزارهای نرم افزاری است که به شما امکان رمز گذاری، رمزگشایی، و امضاء الکترونیکی بر روی اطلاعات ذاخل کامپیوترتان و همچنین ایمیل ها را می دهد . رمزگذلری و رمز گشایی بصورت نامتقارن میباشد.

تولید کلیدها: زوج کلید عمومی و خصوصی را تولید میکند.

مدیریت کلیدها: امکان نگهداری کلید عمومی دیگران را بصورت محلی برای شما امکان پذیر می سازد .

رمزگذاری و رمزگشایی ایمیل ها : دوستان شما می توانند باکلید عمومی شما پیغام ها را رمزگذاری کنند، و شما هم می توانید با کلید خصوصی خودتان این پیغام ها را از رمز در آورید .

امضاء ایمیل ها : شما می توانید با استفاده از کلید خصوصی خودتان پیغام های ارسالی به دوستانتان را امضاء کنید . و دوستانتان هم با داشتن کلید عمومی شما می توانند این امضاء را رمزگشایی کنند

-کلید عمومی جهت استفاده های آتی برای دیگران ارسال میگردد . کلید خصوصی را میتوان در تجهیزات قابل حمل مانند فلاپی دیسک قرار داد . کلید خصوصی با قرار دادن رمز عبور که در هنگام نصب PGP مشخص میگردد محافظت می گردد.این رمز عبور هر زمان که از کلید خصوصی برای رمزنگاری یا امضاء استفاده میشود خواسته میشود.

PGP میتواند با برنامه های کاربردی زیر مجتمع گردد.Qualcomm Eudora, Microsoft Exchange, Microsoft Outlook, Microsoft express & lotus notes

S/MIME

-این نرم افزار شبیه PGP میباشد با این تفاوت که کاربران به تاییدیه های ایجاد شده توسط PKI اعتماد میکنند. برای استفاده از این تکنیک باید از برنامه هایی که آن را ساپورت میکنند و همچنین دسترسی به یک تاییدیه PKI استفاده شود. این تاییدیه میتواند توسط یک PKI داخل سازمان یا زیر ساختهای تولید کلید خارجی (PKI عمومی)در اختیار افراد قرار گیرد. دونوع از این PKI های عمومی ،شرکت verisign وشرکت Thwate میباشد.

-معروفترین برنامه های کاربردی که S/MIME را قادر به استفاده میکنند عبارتند از Microsoft outlook & express ,Netscape

نقاط آسیب پذیر پست الکترونیک

-ایمیل دارای نقاط آسیب پذیری یرای تخریب خودش می باشد،مهاجمین از این نقاط آسیب برای تخریب دیگر امکانات سیستم مثل پاک کردن اطلاعات بر روی کامپیوتر شما، سوء اسفاده می کنند .

-برای محافظت از شبکه و سازمان تان در مقابل نقاط آسیب پذیری پست الکترونیکی، شما باید در مقابل هشدارهای امنیتی سیستم هشیار بوده و همچنین از ویروس یابهای بروز شده استفاده نمایید .

- سرور درگاه ایمیل می تواند با اسکن ایمیل های ورودی این درگاه را ایزوله کرده و یا ویروس های متصل به ایمیل ها را اجازه ورود به شبکه ندهد .

-تک تک کامپیوترهای موجود در شبکه شما هم می توانند از ویروس یابها برای دفاع محکم تر استفاده کنند . این کار علاوه بر جلوگیری از ورود ویروس های بیرون از شبکه به کامپیوتر شما، از ویروس های ایجاد شده توسط کاربران داخل شبکه شما نیز برای ورود به کامپیوتر شما جلوگیری می نماید .

-باید کاربران شبکه تان را در خصوص نقاط احتمالی حمله به وسیله ایمیل ها آموزش دهید . بطور مثال بسیاری از کدهای مخرب بصورت فایل های متصی به ایمیل ها برای شما می اید، لذا کاربران باید آموزش های لازم برای باز نکردن این ایمیل های مزاحم را دیده باشند .

-هر زمانی که تخریبی بر روی یک نرم افزار ایمیل اتفاق می افتد، فروشندگان این نرم افزارها نسبت به رفع نقاط آسیب آ□ا از طریق وصله های امنیتی مبادرت می کنند،

انواع ایمیل های مخرب Spam,Scam,Hoaxes

SPAM

-این عنوان برای آندسته از ایمیل های ناخواسته (مانند تبلیغات تجاری) که به آدرس های زیادی ارسال می گردند اطلاق میشود.

-برای محافظت سازمان تان در مقابل این نوع از ایمیل های مزاحم، شما باید از نرم افزارهای فیلتر کننده در درگاه سرور ایمیلتان و همچنین تک تک کاپیوترهای شبکه تان استفاده نمایید . spamassassin,brightmail,cloudmark,digiportal's

-عدم پاسخگویی به Spam ها توسط کاربران

-آدرس ایمیلتان را در داخل صفحات وب سایتها پست نکنید

-برای استفاده از گروه های خبری از آدرس ایمیل دومی استفاده کنید .

-هیچگاه چیزی را که در یک Spam تبلیغ شده نخرید.

-هرگز آدرس ایمیل خود را، بدون دانست دلیل اصلی برای خواستن آن، در جایی عرضه نکنید .

-حتما قبل از ورود آدرس ایمیلتان از " عبارات رعایت حریم ایمیل "درخواستی توسط آن سایت مطمئن گردید .

-از فیلترهای Spam استفاده شود.

Scam

-شبیه مورد قبلی این ایمیل ها هم ناخواسته می باشند . تفاوت ایندو در آن است کهScam ها محصولات و کالایی را برای فروش ارائه نمی دهند، بلکه بطور خاص هدفشان سرقت پول، کالاها، و سرویس ها می باشد . اغلب آ□ا از قربانی تقاضای ارسال پول، یا ارائه مشخصات حساب بانکی، و یا اطلاعات کارت اعتباری می کنند . یکی از معروفترین این ایمیل ها، با نام ایمیل پولشویی نیجریه ای معروف می باشد .

-تنظیم سیاستنامه امنیتی و قرار دادن مطالبی در خصوص رعایت محرمانگی اطلاعات ویژه مانند شماره حساب بانکی و یا شماره بیمه نامه و . . . در آن امری لازم می باشد .

-باید در این سیاستنامه کانال های امن ارسال داده و کانال های ناامن مشخص گردند . همچنین آموزش این نکات امنیتی به کاربران شبکه تان لازم می باشد .

چه ایمیلهایی میتواند Scam باشد.

-فرصت های تجاری Business Opportunity Scams
-پول سازی از طریق ارسال ایمیلهای عمده Make Money by sending bulk E-mail
-نامه های زنجیره ای Chain Email
-برنامه کار در خانه Work –at-home scheme
-سلامتی و رژیم Health and Diet scams
-درآمد بدون تلاش Effortless income
-کالای مجانی Free Goods
-فرصتهای سرمایه گذاری investment opportunities
-وامها و یا اعتبارهای تضمین شده Guaranteed Loans or Credit
-اصلاح اعتبار Credit Repair

Hoaxes

-یک ایمیل از نوع Hoaxes مانند یک نامه زنجیره ای در شبکه پخش می گردند .آنها حاوی اطلاعات غلط ولی قابل باوری می باشند . این ایمیلها معمولا از سوی یک شخص به تعداد زیادی از افراد برای اینکه ایده یا دیدگاهی را در افراد به باور برسانند ارسال می گردد . معمولا در این ایمیل ها از گیرنده درخواست می شود که آن را برای دوستانش هم ارسال کند . مانند ایمیل Good time که باعث تخریب هارد میگردید.

-بعضی از این ایمیلها به شما اعلام می کنند که مثلا کامپیوتر شما توسط یک نامه که از طرف دوستتان ارسال گردیده ویروسی شده و نام فایل ویروس را هم اعلام می کنند . درحالیکه فایل اعلام شده یکی از فایلهای سیستمی میباشد و با پاک کردن آن سیستم دچار اشکال میشود.

-در مقابل این نوع از ایمیل ها باید سیاستنامه امنیتی مبنی بر شناسایی این نامه ها و نحوه برخورد با آنها را در سازمانتان تنظیم کرده و آن را به کاربران شبکه تان هم آموزش دهید .

شناسایی ایمیلهای Hoaxes

(Urgent)-فوری کلماتی مانند فوری، مهم، خطر، هشدار ویروس معمولا در عنوان این ایمیل ها وجود دارند

(Tell all Your Friens)به دوستان خود بگویید معمولا این درخواست در داخل ایمیل می تواند وجود داشته باشد .

(This isn't a Hoax)این یک Hoax نیست . این پیغام معمولا شامل معرفی افرادی به عنوان تایید کننده آن هست که افراد قابل اعتمادی می باشند . بطور مثال فرستنده اصلی آن می تواند عبارتی مانند "این هشدار توسط فلان مقام قانونی و یا فلان ایستگاه خبری تایید شده "را برای فریب افراد در آن قرار دهد .

(Dire Consequence) پیامد ناگوار این ایمیلها میتواند حاوی اخطارهای بسیار فوری مبنی بر اینکه مثلا اطلاعات در کامپیوتر شما در حال تخریب میباشد، باشند .

(History) تاریخچه.راگر یک پیغام حاوی "FW" در قسمت موضوع خود باشد و یا تعداد زیادی پرانتز حاشیه دار شبیه (<<<<<<) در عنوان خود باشد این پیغام احتمالا چندین بار فوروارد Forward شده است و احتمال Hoax وجود دارد.

امنیت بر روی وب

-معمولا این حملات متکی بر ضعف های برنامه های کاربردی است که ناشی از ضعف در مرحله طراحی و برنامه نویس آنها می باشد .

-در این بخش هدف بیان مخاطرات و نحوه مقابله با این مخاطرات در محیط وب می باشد .

SSL/TLS-HTTPS-Buffer Overfelow-Active Content-Java Applets-Javascripts-Active X-Signing Active Content-Cookies-CGI-Instant Messaging

Secure Sockets Layer (SSL)
Transport Layer Security (TLS)

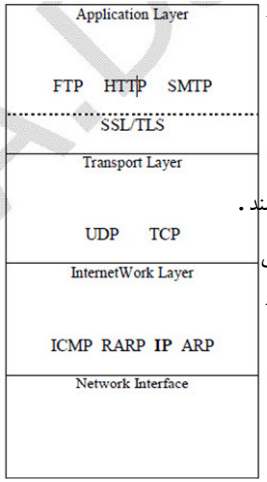
-برای پیاده سازی امنیت در تبادلات کلاینت/سرور در اینترنت بکار برده میشود. SSL در سال ۱۹۹۴ توسط netscape ارائه گردید و بر اساس رمز گذاری کلیدهای نامتقارن توسط RSA ارائه شد.

-در سال ۱۹۹۹ سازمان IETF پرتکل جدیدی را که مبتنی بر SSL بود با نام TLS پایه گذاری نمود. این دو پرتکل در اکثر مواقع در غالب مشترک SSL/TLS یاد میشود.

-SSL/TLS ارتباطات اینترنتی را در مقابل استراق سمع، مداخله، و جعل محافظت می کنند . کلاینت و سرور می توانند با استفاده از آن همدیگر را احراز هویت کرده و پیغام ها را به شکل رمزگذاری شده در اینترنت انتقال دهند.

-SSL/TLS پرتکل غیر وابسته به لایه ای در شبکه میباشد. و مابین دو لایه کاربردی و انتقال قرار میگیرد. و لازمه اجرای آن استفاده برنامه های کاربردی از پرتکل IP وSSL/TLS میباشد.

SSL/TLS در TCP/IP



مزایای SSL/TLS

احراز هویت سرور برای کلاینت: مطمئن بودن سرویس فروش و تعلق آن به فروشنده واقعی آن محصول مطمئن گردد (و اینکه این سایت فروش از جانب یک سارق برای به سرقت بردن اطلاعات کارت فروش مشتری تدارک دیده نشده است) برای این منظور این سرور باید گواهینامه CA را تهیه کند.

مبادله الگوریتم رمزگذاری مشترک:کلاینت و سرور می توانند الگوریتم رمزگذاری مورد استفاده شان را مبادله کنند . این کار طرفین کلاینت و سرور را برای پشتیبانی از تکنیک رمزگذاری قلدر می سازد.

احراز هویت کلاینت برای سرور(اختیاری): وقتی که محدودسازی دسترسی به سرور توسط کلاینت ها مورد نظر باشد، کامپیوترهای کلاینت بایستی گواهینامه معتبری از یک CA را بر روی خود نصب کرده باشند.

استفاده از رمزگذاری غیرمتقارن برای ارسال رمزهای اشتراکی: رمزگذاری غیرمتقارن (یا کلید عمومی) برای شکسته شدن سخت می باشد . و رمزگذاری متقارن برای انتقال داده های حجیم بسیار کارآ می باشد SSL/TLS از رمزگذاری غیر متقارن برای ارسال رمزهای اشتراکی(کلید متقارن) استفاده می کند، بنابراین رمزگذاری داده واقعی بسیار سریعتر می شود، و در عین حال روش برقراری ارتباطات رمزگذاری شده نیز بسیار امن می باشد.

برقراری یک اتصال رمزگذاری شده: تمام ارتباطات میان کلاینت و سرور رمزگذاری شده می باشد.

HTTPS

-ارتباط وبی که بوسیله SSL/TLS امن شده است با عنوان HTTPS نامیده میشود.

-اگرچه HTTPS ارتباط بین کلاینت و سرور را رمزگذاری می کنند، اما قابل اعتماد بودن فروشنده یا امن بودن سرور فروشنده را تضمین نمی کند.

-SSL/TLS قادر به جلوگیری از اعمال غیر اخلاقی بر روی اطلاعات جمع آوری شده از کارت های اعتباری توسط فروشنده ، نمی باشد . همچنین SSL/TLS قادر به محافظت از اطلاعات ذخیره شده بر روی کامپیوتر سرور فروشنده نمی باشد. متاسفانه بسیاری از کامپیوترهای سرور سمت فروشنده مورد تعرض قرار می گیرند (و مشخصات کارت اعتباری خریداران سرقت می شود) به این دلیل بسیاری از فروشندگان اطلاعات کارت اعتباری خریدارانشان را یر روی سرور خود ذخیره نمی کنند.

Buffer Overflows

-بافر به فضای داده ای اطلاق می شود که بوسیله هر دو عنصر تجهیزات سخت افزاری و پروسس های نرم افزاری به اشتراک گذاشته می شود . در این بخش تمرکز ما بر روی بافرهای برنامه ای، که اجازه اجرای برنامه های مختلف با اولویت های مختلف را می دهند، می باشد . هر بافر دارای سطح مشخص و یک مرز می باشد.

-سرریزی بافر زمانی اتفاق می افتد که یک برنامه تلاش می کند داده های بیشتر از ظرفیت بافر را وارد آن کند . این کار گاها باعث آن می شود که حجم داده اضافی بر روی بافرهای کناری ریزش کرده و باعث خرابی داده های موجود در آنها شود.

-سرریزی بافر ممکن است بدلیل ضعف در ساختار برنامه و یا ناشی از یک حمله تخریب آمیز باشد . یک مهاجم از این روش برای در اختیار گرفتن کامپیوتر قربانی استفاده می کند . در یک حمله، سرریز بافر ممکن است باعث خراب شدن فایل ها، تغییرات داده ها، استحصال اطلاعات محرمانه، و یا اجرای کد بر روی ماشین هدف گردد.

-بهترین راه در برخورد با این مشکل این است که پیاده کنندگان نرم افزار از روش های برنامه نویسی امن طبعیت کنند . اجرای عملیات امن برنامه نویسی به معنای طراحی برنامه نویسی به طرق امن آن در ذهن برنامه نویس می باشد.

-بسیاری از پیشنهادات مربوط به طراحی امن یک برنامه را در کیت پیاده سازی برنامه (SDKs) می توان یافت . این کیت یک راهنمای برنامه نویسی است که در آن موضوعاتی از قبیل ساختار یک برنامه، فانکشن ها، و روش های پیاده سازی یک برنامه بر روی پلت فرمی خاص بیان گردیده است.

-یکی دیگر از راه های برخورد صحیح با این پدیده، ره گیری از فروشندگان برنامه ها برای بهره برداری از وصله هایی است که در مرور زمان برای حل مشکلات این نرم افزارها توسط فروشندگان آن به بازار عرضه می گردد.

Active Content

-مواد محتوی فعال برنامه اجرایی کوچک و یا کدهای اسکریپت می باشند که به داخل مرورگرهای وب ارائه می گردند تا صفحات وب مهیج ،کاربردی و مفید گردند. دو نوع مرسوم محتواهای فعال جاوا اسکریپت JavaScript و اکتیو ایکس ActiveX میباشند. محتواهای فعال برای اجرای یک اسکریپت در داخل سیستم کلاینت طراحی شده اند. متاسفانه، این امکان باعث ایجاد ریسک های امنیتی در سیستم ها هم می شود : بعضی از این اسکریپتها باعث ایجاد عملکردهای مخرب در ماشین کلاینت هم می شوند . در این فصل تمرکز اصلی ما بر روی این محتواهای فعال در سمت کلاینت و امکانات تخریب آمیز ممکنه آنها می باشد.

Java Applets

-جاوا زبان برنامه نویسی ارائه شده توسط Sun Microsystems میباشد . برنامه های کوچک کامل در این زبان Java Applets نامیده می شود، که بر روی بیشتر مرورگرهای سمت کلاینت اجرا می گردد . بطور مثال نت اسکیپ و اینترنت اکسپلورر این برنامه های کوچک را پشتیبانی می کنند .

-این برنامه های کوچک از داخل یک صفحه وب توسط برچسب های اپلت (APPLET tag) آدرس دهی می شوند . این برچسب ها برای بارگذاری فایل های مربوط به متن کد جاوا استفاده می شوند . کد متن جاوا توسط موتوری بر روی کلاینت به نام ماشین مجازی جاوا *(Java Virtual Machine)*اجراء می شوند. این VM ها بر روی بسیاری از سیستم های عامل مانند یونیکس، مکینتاش، و ویندوز اجراء می شوند .

-جهت مقابله با حملات JavaScript میتوان امکان پشتیبانی جاوا را بر روی ماشین تان غیر فعال کنید . بسیاری از مرورگرها (مثل نت اسکیپ و اینترنت اکسپلورر)امکان غیر فعال کردن جاوا را به شما می دهند .

-سیستم عامل Windows XP به خودی خود Javaapplet را ندارد و باید بر روی آن نصب گردد.

Java Script

-جاوا و جاوا اسکریپت به صورت مستقل از هم پیاده سازی شده اند و دو زبان مستقل از هم تلقی می شوند .

-جاوا اسکریپت نوعا داخل صفحات HTML قرار داده میشود و توسط مرورگر سمت کلاینت خوانده میشود.یک برچسب اسکریپت Script Tag در داخل کدهای HTML برای نشانه گذاری جاوا اسکریپت قرار داده میشود.

-جاوا اسکریپت معمولا برای ارتباط با دیگر اجزاء (مانند برنامه های CGI) مورد استفاده قرار میگیرد.

-جاوا اسکریپت می تواند برای باز کردن جاوا اپلت ها هم مورد استفاده قرار گیرد . بطور مثال، جاوا اسکریپت و جاوا اپلت ممکن است به همراه هم برای ایجاد یک محاسب میزان رهن ، نقشه های تعاملی، و بسیاری از موارد دیگر استفاده شوند .

-برای محافظت از خودتان و سازمان تان در مقابل جاوا اسکریپت های مخرب، شما می توانید جاوا اسکریپت را بر روی کامپیوترتان غیر فعال کنید .

-در صورتیکه وب سایتی بخواهد به روی کامپیوتر شما محتوای فعالی بفرستد، شما بر روی صفحه کامپیوتر خود جملات زیر را مشاهده خواهید کرد که در صورت کلیک بر روی این جملات راه فعال سازی مرورگر وب شما برای دریافت محتوای فعال را به شما نشان می دهد . "To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options..."

Active X

-این تکنولوژی هم برای فراهم سازی محتوای فعال بوجود آمده است . لازم به توجه است که این تکنولوژی توسط شرکت مایکروسافت تنها برای استفاده در مرورگرهای اینترنت اکسپلورر طراحی گردیده و در حال حاضر در هیچ مرورگر دیگری پشتیبانی نمیشود.

-برای کمک به حفاظت سیستم ها از تخریب های ناشی از سوء استفاده از اکتیوکس، اینترنت اکسپلورر به شما امکان انتخاب دریافت و اجرای کنترل های اکتیوکس را میدهد. می توانید اینترنت اکسپلورر را به شکلی تنظیم نمایید که به صورت اتوماتیک کنترل اکتیوکس را دریافت نماید، یا قبل از دریافت به شما پیغامی مبنی بر دریافت یا عدم دریافت دهد، و یا بطور کلی دریافت هر گونه کنترل اکتیوکس را غیر فعال نماید .

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

Signinig Active Content

-در تلاش برای افزایش امنیت محتواهای فعال، بعضی از فروشندگان فرآیندی را برای انجام امضای دیجیتالی قبل از نصب محتواهای فعال، پیاده سازی کرده اند . تولید کنندگان محتواهای فعال قبل از ارسال این محتواهای فعال آنها را امضای دیجیتالی می نمایند این ارائه دهندگان تاییدیه امضاء برای امضا نمودن محصولاتشان را از یک CA قابل اعتماد مانند Versign دریافت میکنند.

-مایکروسافت از یک تکنولوژی در اینترنت اکسپلورر به نام *Authenticode* برای یررسی صحت امضاء قبل از دریافت محتوای فعال از یک فروشنده، استفاده می کند .

-در مورد حفره های امنیتی که ممکن است در نرم افزاری در آینده مشخص شود، قادر به عملکرد پیشگیرایانه نمی باشد . لذا همیشه توجه داشته باشید که آخرین وصله های امنیتی را هم از فروشندگان برای رفع عیوب دریافت دارید .

Cookies

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

-بسیاری ار وب سرورها قادر به انجام فعالیت صحیح خود بدون آنها نمی باشند . کوکی ها بسته به مرورگر وب مورد استفاده در مکان های مختلفی ذخیره می شوند .

-نت اسکیپ کوکی ها را در فایلی بنام Cookies.txt ودر اینترنت اکسپلورر در فایلهای جداگانه در %windir% internet files\temprory ثبت مینماید.

-بعضی از کوکی ها برای ثبت علایق کاربران وقتی به وب سایتی متصل می شوند، بکار می روند . دیگر کوکی ها برای پشتیبانی از وضعیت اطلاعات بکار می روند(وضعیت اتصال بین کلاینت و سرور) بعضی از سرورها هم از کوکی ها برای مقاصد احراز هویت کلاینت ها استفاده می کنند .

سوء استفاده از کوکی ها

-کوکی ها می توانند اداره شوند و یا دزدیده شوند. حمله کننده می تواند کوکی ها را برای بدست آوردن اطلاعات مهم در مورد کاربران شبکه، سازمان، و مسائل امنیتی در شبکه داخلی شما به سرقت ببرد .

-مهاجم می تواند با قرار دادن یک اسکریپت به داخل کامپیوتر کلاینت، کوکی ها داخل سیستم کلاینت را به طرف سیستم خودش انتقال دهد . حتی احتمال استراق سمع کوکی توسط مهاجمین در حین انتقال وجود دارد .

محافظت سازمانها در برابر تخریب کوکی ها

-وب سرور خود را با اتکا و اعتماد بر اطلاعات ذخیره شده در کوکی های سمت کلاینت جهت کنترل دسترسی به منابع یا ارائه هر سرویس اضافه، پیکربندی نکنید . چرا که ممکن است از این طریق توسط مهاجمی که بر روی کوکی ها دسترسی داشته، تخریبی بر روی وب سرور شما انجام گیرد .

-از کوکی ها برای نگهداری اطلاعات محرمانه و مهم مانند کد شماره حساب بانکی، و گواهینامه های احراز هویت (مانند کلمه عبور)، استفاده نکنید .

-اگر لازم است که اطلاعات مهمی در کوکی ها نگه داری شود، حتما از SSL/TLS برای محافظت از اطلاعات داخل کوکی ها استفاده شود .

CGI

-برنامه های CGI معمولا برای تولید محتوی فعال در وب سرورها استفاده میشود و برای ارسال اطلاعات میان برنامه [کاربردی و وب سرورها می باشند . بطور مثال،آنها معمولا برای انجام کارهایی مانند وارد کردن داده، جستجو، فانکشن های بازیابی در دیتابیس ها، مورد استفاده قرار می گیرند . و توسط زبانهایی همچون C,C++,VISUAL Basic,fortran,Perl ایجاد میگردند.

-برخلاف JAVASCRIPT و ActiveX اجرا می شوند، بر روی کامپیوتر وب سرور اجراء می گردد . البته شبیه دیگر برنامه ها ، این برنامه هم می تواند دارای حفره های امنیتی باشد که توسط مخربین سوء استفاده شود . در زیر برخی از تخریب های ممکنه بر اساس این برنامه ها آورده شده است .

موارد سوء استفاده و تخریب

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

-این برنامه ها ممکن است دارای حفره های امنیتی باشند، و بدین شکل مخربین از آن سوء استفاده نمایند .

-تهدید ممکن است از طریق برنامه های مجانی CGI که دارای حفره امنیتی میباشد انجام پذیرد.

-ارسال داده جعلی به سمت برنامه های CGI ممکن است باعث تخریب گردد.

جهت حفاظت از سرورها از تخریب با CGI

-ایجاد محدودیت در کاربرد برنامه های CGI به این طریق از ایجاد بار زیاد بر روی وب سرور و نتیجتا کاهش سرعت آن، می کاهید .

-نصب برنامه های CGI به شکلی که در شرایط قانون حداقل اجازه Least Privilage User اجراء گردد.

-پاک کردن تمام برنامه های CGI بصورت پیش فرض موجود درون وب سرور

-بررسی برنامه های CGI در جهت پیدا کردن حفره های امنیتی آنان

Instant Messaging

- پیغام گذاری لحظه ای یا IM روشی است که امروزه برای انتقال ، صحبت، فایل، صدا بین کاربران مختلف بصورت مستقیم بر روی وب، مورد استفاده قرار می گیرد .

مشکلات IM

-انتقال داده های رمز نشده: مردم اغلب داده های مهم مثل کلمه عبور و رمز عبور را از این طریق برای افراد مورد اعتمادشان ارسال می کنند .

-فایل های ارسالی ممکن است ویروس یاب ها را دور بزنند :IM به کاربران اجازه انتقال فایل، جدا از سیستم ایمیل که دارای ویروس یاب می باشد را می دهد .

-هکر می تواند نقاط ضعف این سیستم را شناسایی کند، مواردی همچون سرریز بافر . شبیه دیگر برنامه های کاربردی، IM ها هم می توانند دارای حفره های امنیتی باشند، اما این حفره های امنیتی بطور بالقوه خطرناکتر می باشد، چرا که اتصال بصورت مستقیم بین کاربران می باشد . همچنین اشکال برنامه ای در یک طرف ارتباط می تواند عاملی گرد که طرف مقابل ارتباطی، کنترل کامپیوتر دیگری را در اختیار گیرد .

-هکر می تواند طرف مقابل ارتباطی خود را با استفاده از اطلاعات دروغ فریب داده، و اورا مجاب به افشای اطلاعات محرمانه کند(حملاتی از نوع مهندسی اجتماعی)

موارد امنیتی در صورت استفاده از IM در سازمان

-انحصار در استفاده از IMهایی که برای استفاده مجاز میباشند .این عمل شما را از پشتیبانی ،امن سازی و مشکلات چندگانه ناشی از IM های مختلف خلاص میکند.

-اگر اطلاعات انتقالی بین کلاینت ها باید امن باشد، از برنامه IM ای استفاده کنید که قابلیت رمزگذاری داشته باشد .

-تنظیم نظامنامه امنیتی برای استفاده از IM مثلا اینکه از طریق IM انتقال فایل صورت نگیرد.

-آموزش کاربران برای آگاهی آنان از خطرات ممکن IM . به آنها توضیح دهید که انتقال فایل از این طریق چقدر خطرناک می باشد، و اینکه یک هکر ممکن است برای فاش شدن اطلاعات محرمانه او تلاش کند .

-اطمینان از اینکه تمامی استفاده کنندگان ازIM از ویروس یابهای بروز شده استفاده می کنند .

-پی گیری از فروشندگان نرم افزارهای IM برای دریافت آخرین وصله های امنیتی