مفاهیم امنیت اطلاعات

دنیایی که در ان زیست می کنیم سرشار از قطعات ریز و درشت الکترونیکی شده است.مظاهر زیبای طبیعت ارام ارام از زندگی انسان عصر جدید رخت بر بسته و ساختمان های سر به فلک کشیده فولادی و بتونی;شهرنشین را به زندانیان شادمان مدرنیسم تبدیل کرده است.پیرامون زندگی هر بشر امروزی کامپیوتر های شخصی; سیستم های متعدد تلفن ثابت و همراه .دستیاران دیجیتالی (PDA)کامپیوتر های کیفی;خودپرداز بانک;انواع واقسام کارت های اعتباری;کارت های هوشمند;دستگاه های کنترل از راه دور.دزد گیربی سیم.وسائل اشپزخانه تمام دیجیتال.سیستم های ماهواره ای.موقعیت یاب دیجیتال(GPS).ابزار های لیزری و مایکروویو.سیستم های رادیو و تلویزیون و ده ها نوع دیگر از این وسائل و ابزار تلنبار شده است.

وقتی بافت و جوهره زندگی سنتی در حال استحاله به الگو های مدرن باشد بزه کاری های اجتماعی و ناهنجاری های مدنی نیز رنگ و بوی مدرنیته به خود می گیرد!در سال 1988یک دانشجوی کارشناسی داشگاه کورئل به نام((روبرت موریس)) اولین ((کرم کامپیوتری))را به جان کامپیوتر ها انداخت تا با الوده ساختن کامپیوتر ها منجر به خاموشی انها شود.هرچند نیت واقعی او صرفا اثبات برتری هوش و خرد انسان در مقابل ماشین و صرفا یک تفریح بی مزه علمی بود ولی سراغاز ایجاد یک جبهه جدید علیه اعصاب و روان اجتماع شد که بعدا به دلیل تنیده شدن کامپیوتر ها در تار و پود زندگی مردم,خسارت های مالی و معنوی هنگفتی نیز در پی داشت.تا جایی که در سال1994کلاه برداری اینترنتی یک گروه روس منجر به10/4میلیون دلار خسارت بهCitibank شد.

گروه های اخلال گر برای انکه قدرت خود را به رخ جهانیان بکشند در سال 1996به وبسایت های CIAوUSA DOJ (که خود از امنیتی ترین مراکز امریکا به شمار می اید) تعرض کردند وبا نفوذ در انها ,چهره این وب سایت ها را تغییر داد!

پس از سال2000 تقریبا ه سال بیش از یک میلیون حمله علیه اطلاعات موسسات و سازمان های دولتی,خصوصی,مراکز مالی اعتباری,شرکت های خدماتی وتجارت الکترونیکی گزارش شده است.این تعداد از حملات فقط انهایی بوده که رسما اعلام و گزارش شده است,در حالی که بسیاری از اخلال گری ها هرگز درجایی ثبت نمی شوند.

اگر((رخداد های ناخوشایند وخطرناک))را در یکی از رده های دسترسی غیرمجاز به داده ها((نشت اطلاعات محرمانه))((از دسترس خارج شدن خدمات یک سرویس دهنده))((تغییر مخفیانه در داده ها))((سرقت داده ها))((نابود شدن داده ها))((اختلال در عملکرد صحیح ماشین کاربران))وهر نوع تعرض به حریم داده های یک ماشین))تلقی کنیم((امنیت داده ها))عبارت است از مجموعه تمهیدات و روش ها که در یکی از بند های زیر قرار بگیرد:
الف)تمهیداتی که اطمینان میدهند رخداد های ناخوشایند هرگز حادث نمی شوند.
ب)تمهیداتی که احتمال وقوع رخداد های خطرناک را کاهش می دهد.
ج)تمهیداتی که نقاط حساس و خرابی های استراتژیک را در سطح شبکه توزیع کند.
د)تمهیداتی که اجازه می دهند به محض وقوع رخدادهای خطرناک.شرایط در اسرع وقت وبا کمترین هزینه به شکل عادی برگردد و کمترین خسارت را برجا بگذارد.
به عنوان یک مثال خارج از دنیای کامپیوتر.فرض کنید بخواهیم مجموعه ی تمهیدات لازم برای حفظ امنیت منزل شخصی از تعرض سارقان را در چهار رده بالا دسته بندی کنیم!د اینجا ((رخداد ناخوشایند))سرقت مایملک افراد واسیب به صیانت زندگی و حریم خصوصی عموم مردم است:(الف)تعبیه قفل های مستحکم.دربهای غیر قابل نفوذ.دیوار های بلند ودارای حصار.نصب سیستم حفاظتی وبه کار گماشتن نگهبان از تمهیدات رده اول محسوب می شود.(ب)هماهنگی با همسایه ها.اعتماد نکردن به افراد بیگانه.تکثیر نکردن کلید ها.تغییر متناوب قفل ها.مراقبت از کلید.پنهان نگاه داشتن عدم حضور در منزل.از تمهیداتی است که در رده دوم از احتمال وقوع رخداد های ناخوشایند کاست.(ج)عدم نگاه داری پول و اشیا قیمتی در یک نقطه متمرکز تقسیم انها به چند مجموعه و مخفی کردن انها در نقاط مختلف و مطمئن منزل.از تمهیدات رده سوم به شمار می ایدا!(د)با تمهیدات فوق باید وضعیت را به گونه ای تنظیم کنید که در صورت وقوع یک سرقت چیزی باقی بماند تا بتوان روال زندگی را در اسرع وقت به شکل عادی از سر گرفت!
متاسفانه تمهیدات امنیتی یک شمشیر دو لب هستند که هرچه سریع ترومفصل تر به اجرا گذاشته شوند:اولا دسترسی افراد مجازو خودی را به منابع شبکه.دشوارتر و دست وپا گیر ترمیکنند.ثانیا هزینه پیاده سازی و نگهداری سیستم را به شدت بالا می برند.مثلا برای تضمین امنیت منازل شخصی بدیهی است که شما میتوانید از دربهای فولادی چند تنی استفاده کنید.سیم های خاردار اطراف منزلتان را به برق فشار قوی متصل نمایید وپشت دیوار ها را مین گذاری کنید!و به جای سگ نگهبان یک پلنگ گرسنه ی وحشی درمنزل خود رها کنید!!!چنین تمهیداتی امنیت منزل شما را به حد متعالی می رساند ولی زندگی کند!!در چنین وضعیتی اصطلاحا ((قابلیت دسترسی))به مخاطره افتاده است. (Availability) هیچکس حاضر نیست در چنین جهنمی

بزرگترین چالش هایی که پیش روی طراحان مکانیزم های امنیتی قرار دارد عبارت اند از:
1)حفظ امنیت سیستم هایی که ذاتا متفاوت و عموما ناسازگارند چندان ساده نیست.
2)ایجاد اتصال امن بین دو سیستم ناهمگون نیاز به تمهیدات و مراقبتهای ویژه ای دارد.
3)نیاز ها و اهداف امنیتی سیستم ها کاملا متفاوت اند.
4)بخشی از امنیت یک سیستم به هوش فردی و رعایت یک مجموعه از اصول و ضوابط توسط تک تک کاربران وابسته است.
5)تمام راه های ورودی و خروجی یک سیستم باید به دقت تحت نظارت ومراقبت باشند.
6)هزینه پیاده سازی تمهیدات امنیتی باید در سطح معقولی پایین باشد.
7)تمهیدات امنیتی نباید دست و پا گیر بوده وسیستم را از بهره وری ساقط کند.

.آرمانی ترین حالت وقتی حاصل می شود که تمهیدات امنیتی برای کاربران مجاز و افراد خودی اصلا به چشم نیاید و به اصطلاح شفاف باشد درحالی که برای کاربران غیر مجاز یک حصار باریک و غیر قابل نفوذ ایجاد کند.

سنگ بنای تمام تمهیدات و مکانیزم های امنیتی بر بدبینی مفرط و وسواس بی حد گذاشته می شود .همیشه فرض بر ان خواهد بود که دشمن در کمین و منتظر فرصت است و هیچگاه از حالاتی که ممکن است به ندرت اتفاق بیفتد چشمپوشی نخواهد شد.به عنوان مثال همیشه می توان فرض کرد دشمن درکمین داده ها دارای یک ابر رایانه با صد هزار پردازنده و قدرت پردازشی هزار میلیارد دستورالعمل در ثانیه است!هرچند چنین احتمالی در عمل صفر است ولی وقتی مکانیزمی با این فرض طراحی شود جای اما و اگر باقی نخواهد ماند و امید دشمن بدل به یاس می شود.

شاید بزرگترین چالش در دنیای امنیت اطلاعات ان است که نبرد واقعی بین ((الگوریتم های امنیتی))و((هوش و خرد انسان))اتفاق می افتد.وقتی یک طراح مکانیزم های یا تمهیدی را طراحی و ان را در قالب سخت افزار یا نرم افزار پیاده میکند و پی کار خود می رود از ان پس در یک طرف جبهه الگوریتمی اجرا شده بر روی ماشینی بدون شعور قرار دارد و در طرف دیگر دشمنی مجهز به هوش و ذکاوت که با شکیبایی فراوان در تلاش برای شکست دادن حریف است.

قبل از اینکه در بخش بعدی به انواع تهدید ها وحملات علیه منابع و اجرایی شبکه بپردازیم در جدول شکل 1-1سیر تکاملی خدمات کامپیوتری در حلال 20سال اخیر و افزایش مخاطرات امنیتی را در طی این سال ها بررسی کرده ایم

تهدیدات و حملات

در بخش قبل تعریفی ساده از رخدادهای ناخوشایند و خطرناک ارائه دادیم و دانستیم که در تعریفی عام ((امنیت))عبارت است از مکانیزم های پیشگیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین وقوع رخدادهای ناخوشایند(وقتی که رخدادهای خطرناکحادث میشوند).هر عاملی که بطور بالقوه بتواند منجر به وقوع ((رخدادی خطرناک))بشود ((تهدید امنیتی))به شمار می اید.تهدید های امنیتی می توانند از عوامل ذیل ناشی شوند:

الف)تهدید های طبیعی این تهدیدها از عواملی مثل زلزله.سیل.گردباد.رعد وبرق.اتش سوزی.اتشفشان و نظائر آن از قوه ی فعل می رسند و نسل بشر چنین تهدید هایی را به عنوان حقایق زندگی پذیرفته است این تهدید ها همانگونه که زندگی را مورد هدف گرفته اند می توانند در درجات خفیف تر منجر به نابود شدن یا افشای اطلاعات محرمانه و اختلال در سرویس دهی مولفه های اساسی شبکه شوند.از آنجا که خدمات شبکه های کامپیوتری مرز های جغرافیایی را در نور دیده است لذا تهدیدهای طبیعی میتوانند در خارج از محدوده بلا دیده نیز منجر به اختلال در عملیات روزمره افراد و انتشار بحران در سطح وسیع شوند.لذا اگرچه تهدید های طبیعی خارج از قدرت بشرند ولی برای باز گرداندن خدمات شبکه از وضعیت بحران به وضعیت عادی از همان ابتدای طراحی شبکه تمهیداتی برای جلوگیری از گسترش دامنه بحران به مناطق دیگر پیش بینی و اجرا می شود.به عنوان مثال ایجاد مراکز پشتیبان در دیگر مناطق جغرافیایی و بهره گیری از خطوط ماهواره ای در کنار خطوط فیبرنوری در این رده از تمهیدات قرار می گیرد.

ب) تهدیدات غیر عمد تهدیدات غیرعمد از اشتباهات سهوی و ناخوداگاه عوامل انسانی(همانند مدیران شبکه.کارکنان وکاربران)ناشی می شود و می تواند منجر به افشاء ویا نابودی اطلاعات یااختلال در خدمات معمول شبکه و گاه تحمیل خسارت های کلان به جمع کاربران شود از این تحدیدات غیر عمد می توان به موارد ذیل اشاره کرد:

1)طراحی نا صحیح زیر ساخت شبکه یا عدم وجود افزونگی در تجهیزات شبکه.
2)عدم تهیه نسخه های پشتیبان از داده های حیاتی.
3)سهل انگاری در وظائف روزمره(مثل بررسی مستمر سیستم ها از لحاظ الودگی به ویروس).
4)نا اگاهی کاربران از ماهیت عملیات خطرناک.
5)بروز اشکالات پیش بینی نشده در سطح سخت افزار نرم افزار یا سیستم عامل
6)عدم اعمال صحیح سیاستهای انتخاب و تعویض مدام کلمات عبور توسط عوامل درگیر شبکه

ج)تهدیدات عمدی تهدیدات عمدی(که بیشترین خسارت و دشوارترین راه مقابله را دارند)عبارت است از:هرگونه اقدام برنامه ریزی شده جهت افشاء نابودی یا تغییر در داده های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده ها بطورعام هرگونه اقدام برنامه ریزی شده برای تحقق یک رخداد خطرناک(با تعریفی که در بخش قبل از ان ارائه شد)((یک تهدید امنیتی عمدی))تلقی می شود.

واژه های زیر در دنیای امنیت اطلاعات کاربردبسیار فراوانی دارند:

(حمله) هرگاه تهدیدی از قوه به فعل در آید اصطلاحا یک حمله رخ داده است خواه آن حمله موجب خسارت به منابع بشود و خواه یک تلاش نافرجام بشود.

(Attack)

(اسیب خسارت)حمله ای که در اثر ان منابع شبکه از بین برود یا دستکاری شود.یا اطلاعات و داده های محرمانه افشاء ویا حریم خصوصی افراد مورد تعرض قرار بگیرد یا با توسل به جعل هویت و فریبکاری از خدمات معمول شبکه سوءاستفاده شود اصطلاحا ((حمله))به مرحله((اسیب))رسیده است.

((حاشیه ی امنیت)) میزان تخمین قبلی از تهدید هایی که متوجه یک موجودیت در شبکه است و تعیین تمهیدات لازم برای پیشگیری از این تهدیدات به((حاشیه امنیت))موسوم است. قبل از ارائه هرنوع سرویس ابتدا بایستی حاشیه ی امنیت تمام مولفه های شبکه را تعیین کرد.

((نقطه اسیب پذیر)) هرگونه ضعف یا اشکال یک مولفه از شبکه در مقابل تهیدیدات احتمالی(شامل اشکالات نرم افزاری یا سخت افزاری سیستم های عامل یا اشتباهات انسانی)که بتواند منجر به ((حمله))شود اصطلاحا نقطه آسیب پذیر گفته می شود در تعیین حاشیه ی امنیت بایستی نقاط شبکه به درستی تعیین و مراقبت های لازم را به عمل آید.گاه وجود اشکالات بالقوه در یک مولفه از قبل قابل پیش بینی نیست و به ناگاه بروز میکند لذا همیشه برای تعیین حاشیه امنیت باید با فرض انکه آسیب پذیر نا به هنگام اشکار و موجب خسارت می شوند پیش بینی های لازم را انجام داد.

((میزان خطر)) تخمینی از احتمال وقوع یک حمله و همچنین پیش بینی خساراتی که ااین حمله به بار می اید به((به میزان خطر))شهرت یافته است.یک ((مهندس امنیت))باید بتواند میزان خطری که هرکدام یک از مولفه های شبکه را تهدید می کند((تحلیل))کرده و پیامد های ان را با دقت نیز گفته می شودبراورد کند (به این فرایند نیز گفته می شود به عنوان مثال باید براورد شود که به ازای هر یک ساعت که خدمات شبکه از دسترس خارج می شود چه میزان خسارت مالی وارد خواهد شد.

((استراتژی امنیتی/استراتژی خطر)) تعیین دقیق راهکار های مقابله با تهدیدات احتمالی شامل تعیین حداقل حاشیه ی امنیت و ارائه استدلال هر راهکار(به گونه ای که موفقیت خود را در تئوری و عمل به اثبات رسانده باشد)استراتژی امنیتی خوانده می شود.

طرح امنیتی)) نقشه ای دقیق برای نظارت و کنترل تهدید ها پیاده سازی عملی استراتژی امنیتی و تحت کنترل در اوردن نقاط اسیب پذیر(که به ناکاه خود را نشان می دهد)و به حداقل رساندن اسیب های احتمالی در صورت بروز حمله ای موفق به طرح امنیتی شهرت دارد.

((مکانیزم امنیتی)) هر روش یا الگوریتمی که برای تشخیص یا پیشگیری از وقوع حمله یا برگشت به وضعیت معمولی(پس از وقوع حمله)طرحی می شود مکانیزم امنیتی نامیده می شود هیچ مکانیزم واحدی که بتواند امنیت داده ها را تضمین کند وجود ندارد.

((خدمات امنیتی)) پیاده سازی هر نوع مکانیزم امنیتی و ارائه ان ها به کاربران به نحوی که ((میزان خطر)) را به حداقل برساند ((خدمات امنیتی))نام دارد.عمده ترین خدمات امنیتی مورد نیاز در شبکه های کامپیوتری عبارت اند از:

1)محرمانه ماندن اطلاعات به مجموعه مکانیزم هایی که تضمین می کند داده ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگاه داشته می شود ((سرویس محرمانگی اطلاق می شود این سرویس ها که عموما با روش های رمزنگاری تحقق میابند موضوع دروس بعدی خواهند بود روش های مختلف رمز نگاری اطلاعات زیر بنای مابقی سرویس های امنیتی هستند.

2)احراز هویت مجموعه مکانیزم هایی که این امکان را فراهم میکنند که بتوان مبدا(صاحب)یک پیام یا سند یا تراکنش را بدون ذره ای تردید یا ابهام مشخص کرد.سرویس احراز هویت نامیده می شود.

3)تضمین صحت اطلاعات مجموعه مکانیزم هایی که از هرگونه تحریف دستکاری تکرار.حذف یا آلوده سازی داده ها پیشگیری میکنند یا حداقل باعث کشف چنین اقداماتی می شوند.سرویس تضمین صحت اطلاعات نامیده می شوند.

4)غیر قابل انکار ساختن پیام ها مجموعه مکانیزم هایی که به پیام ها و تراکنش ها پشتوانه حقوقی می بخشند و اجازه نمی دهند که فرستنده به هر طریق ارسال پیام خود را انکار کند ویا گیرنده منکر دریافت ان شود به((سرویس غیر قابل انکار ساختن پیام ها))شهرت دارد.

5)کنترل دسترسی مکانیزم هایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترل در اورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه ها در اختیار انها قرار می دهد ((کنترل دسترسی))خوانده می شود.

حملات مختلف علیه منابع یک شبکه یا ماشین بسیار متنوع و از شمار خارج اند.تمام خدمات امنیتی از شامل محرمانگی احراز هویت غیر قابل انکار بودن و صحت پیام ها با این فرض طرلحی و پیاده سازی می شوند که تهدیدهای چهار گانه ذیل همیشه علیه انها وجود دارند و هر لحظه ممکن است اتفاق بیفتد.

الف)استراق سمع هرگاه یک شخص غیرمجاز به هر نحو بتواند نسخه ای از داده های در حال جریان بین مبدا و مقصد را به نفع خود شنود کند حمله استراق سمع به وقوع پیوسته است.

ب)دستکاری هر گاه داده های در حال جریان بین مبدا و مقصد توسط شخص غیرمجاز به هر نحو دستکاری یا تحریف شود حمله دستکاری داده ها رخ داده است.

ج)جعل هر گاه یک شخص غیر مجاز اقدام به تولید پیام های ساختگی کرده و ارسال انها را به شخص مجاز دیگری نسبت بدهد حمله ی جعل و ارسال داده های ساختگی به وقوع پیوسته است.

د)وقفه هرگاه کسی بتواند سیستم یا سرویسی را در شبکه از کار بیندازد حمله ی وقفه رخ داده است.

(استراق سمع)تهدیدی علیه سرویس ((محرمانگی داده ها))((دستکاری))تهدیدی علیه سرویس((صحت اطلاعات))((جعل))تهدیدی علیه سرویس ((احراز هویت))و((وقفه))تهدیدی علیه ((قابلیت دسترسی دائم))به حساب می اید.هرگاه سرویس های امنیتی به هر نحو تضمین کنند که هر تهدیدی در تبادل پیام های بین طرفین مجاز یک ارتباط ناکام خواهد ماند ((کانالی امن))پدید امده است.شکل1-2مفاهیم فوق را به تصویر کشیده است.

حملات چهار گانه ذکر شده احتمال وقوع بالایی دارند و بسادگی اتفاق می افتند.به عنوان استراق سمع داده در محیط شبکه های محلی اغلب به سادگی نصب یک برنامه کوچک به نام است همچنین عناصر میانی شبکه ها مثل مسیر یاب ها می توانند داده های عبوری را به هر دلیل در اختیار یک شخص ثالث قرار بدهند.برای تهدیداتی مثل دستکاری یا جعل داده ها انواع و اقسام نرم افزار تهیه شده و به وفور در اختیار همگان قرار دارد.لذا برای تبدیل شدن تهدید به حمله کافی است یک اختلال گر فقط اراده کند!سهل ترین شرایط برای اختلال گر زمانی است که او به هر طریق به عناصر میانی مثل سوئیچ ها یا مسیر یاب ها دسترسی داشته باشد.

	1965تا1395	1976تا1989	1990تا1999	3000تا کنون
بستر های موجود	کامپیوترهای چند کاربرهاز نوع یا سیستم عامل واحد واشتراک زمانی	سیستم های توزیع شده مبتنی بر شبکه های کوچک محلی با مخابرات با ماموریت های مشخص و سازمانی	اینترنت جهانی ارایه خدمات گسترده و متنوع همگانی	اینترنت جهان بهمراه سرسام اور دستگاهای همراه وخدمات گسترده روی این ابزار ها .
منابع مشترک	حافظه اصلی حافظه جانبی فایل های داده	خدمات محلی یا سازمانی (مثل صدوربلیط هواپیما صدورقبوض خدمات شهری پست الکترونیکی اداری بولنتهای سازمانی یا دانشگاهی.	پست الکترونیکی فراگیروجهانی .خدمات وب سایت تلفیق رسانه های ارتباط در اینترنت خرید وفروش وسفارش الکترونیکی سیستمهای اتوماسیون اداری.اشتراک گذاری جهانی منابع اطلاعات اخبار(مثل بورس وخبرها	دولت الکترونیک منابع واشیا مشترک و قابل انتقال شامل داده وکد اجرایی .خدمات همراه وهمیشه دردسترس درکنار خدات مرسوم و سنتی اینترنت ارایه سرویس به ابزار های همراه و درحال حرکت
نیاز های امنیتی	شناسایی کاربران واحزار هوییت انان حراست فیزیکی از منابع موجود	جلوگیری از اختلال درخدمات نظارت ساده برعملکرد کاربران	مراقبت ویژه و داهم از تراکنش های یکایک کاربران حفظ حریم خصوصی افراد پیشگیری ازایجاد اختلال درخدمات نظارت سخت گیرانه بر دسترسی افراد به منابع داده احزار هوییت دقیق کاربران از راه دور .حفظ حریم سرویس دهنده وجلوگیری ازنفوذ درانها	کنترل ونظارت شدید بر مجوز افراد در دسترسی به یکایک اجزا اشیا مشترک صیانت ازکدهای اجرایی متحرک امنیت درسطح کوچک ترین سرویس های ارایه شده در معماری مبتنی بر سرویس کنترل ابزار همراه و متحرک
چگونگی پیاده سازی مکانیزم های امنیتی	یک پروسه واحد درسطح سیستمط عامل برایط بررسی هوییت افراد صدور مجوز ورود به سیستم وتعیین سطوح دسترسی	ایجاد مراکز منفرد برای احزار هویت و تعیین دقیق مجوز هرکاربر از طریق یک بانک اطلاعاتی واحد ثبت عملیات کابران	پیاده سازی عوامل چند گانه امنیت درسطح سخت افرار نرم افزار وسیستم عامل تبعیت از سیستم های جهانی حفظ امنیت ایجاد سیستمهای مدیریتی توزیع شده اراهه خدمات بصورت توزیع شده درسطح شبکه و درارایی پشتیبانیهای متعدد ایجاد ارایشهای چند لایه ای امنیتی در بدوپیاده پیاده سازی زیر ساخت شبکه نظارت دقیق بر تراکنشهای افراد	بررسی احراز هوییت هر تراکنش بجای هر کاربر احراز هویت مبتنی بر روش های هوشمند و سیستم های خبره ایجاد گروه و حوضه و تعریف نواحی دسترسی.تعیین سطح دسترسی به یکایک اشیا سیستمی کنترل و بررسی کد های اجرایی ومتحرک . ایجاد پشتوانه های حقوقی برای پیگرد اخلال گران.ثبت دقیق وجزی هر عمل انجام شده از طرف کاربران.رویکرد به کارت های هوشمند وعوامل غیر قابل جعل مثل قرنیه.اثر انگشت و سیسنم های مدیریت چندعاملی .....
سهولت پیاده سازی	بسیار ساده	متوسط	پیچیده	بسیار پیچیده و مستلزم هزینه