دانشگاه علم وصنعت ایران

دانشکده مهندسی کامپیوتر

بررسی و پیشنهاد روشهای ایجاد امنیت در سیستمهای کامپیوتری

عباس خسروبیگی

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته

مهندسی کامپیوتر

اساتید راهنما :

دکتر محمود فتحی و دکتر محسن شریفی

مردادماه ۱۳۷۵

بسم الله الرحمن الرحيم

تقدیم :

به جامعه انفورماتیک

چکیده

یکی از مهمترین لوازم مورد نیا ز سیستمها و شبکه های کـامپیو تـری دردنیـا ی امروز، برقراری امنیت می باشد . در این پایان نامه نشان داده می شـود کـه در ارتبـاط بـا ایجاد امنیت در سیستمهای کا مپیوتری ، موارد بسیا ری بایسـتی مـد نظـر طراحـان ، برنامـه نویسان ،و مسؤلین مراکز کامپیوتری کوچک یا بزرگ باشد. سرمایه های سیستمهای کامپیوتری شامل سخت افزار ، نرم افزار ، داده ها ، ونیروی انسانی میباشد.آفندهایی که متوجه قسـمتهای مختلف سیستمها ی کا مپیوتری می باشد شامل وقفه ، نشت ، تغییر ، و ساخت است . برای جلوگیری از این حملا ت بایستی سیاستها و مکا نیز مهای خاصی بکارگرفته شود .

تاکنون روشهای مختلفی برای برقـراری امنیـت در قسـمتهای مختلـف سیسـتمهای کامپیوتری ابداع و پیاده سازی شده اند، که هر یک دارای مزایا و معایب عدیـده ای میباشـند. دراین پایان نامه پس از بررسی برخی از این روشها ، روشهای جدیـد و سـاده ای از جملـه تلفیق روش RSQ وPRSQ ، فشرده سازی ، تقویت ایمنی توسط برخی نرم افزارها منجملـه ADM ، بکارگیزی سطوح مختلف تصدیق اعتبار کاربر با کلمات عبور، ارائه می شوند .

مقایسه این روشها با روشهای موجود نشان میدهد که روشهای پیشـنهادی مـی تواننـد در بسیاری از کاربردها مؤثر و کـاراً باشـند . روشـهای پیشـنهادی همگـی بنیـادی بـوده و در کاربردهای مختلف می توان از تلفیقی از آنها استفاده کرد . برای انتخاب روشهای مناسب در سیستمهای کاربردی بایستی مراحل تحلیل و طراحی سیستم ، با توجه به ساختار سیسـتمهای اطلاعاتی و استانداردهای موجود در این زمینه طی شوند.

تقدیر و تشکر :

بدینوسیله اززحمات اساتید ارجمند ، آقایان دکترفتحی و دکتر شریفی ، که اینجانب را در انجام این پروژه و تهیه این پایان نامه راهنمائی نموده اند ، سپاسگزاری و قدر دانی مینمایم . همچنین ازاعضای محترم هیئت داوری بخاطر حضور در جلسه د فاعیه صمیمانه تشکر می کنم . در پایان از همسرم نیز بخاطر تحمل رنجها و مشقت های دوره تحصیل کارشناسی ارشد وهمراهی وتشویق او کمال تشکر را دارم .

امیدوارم پایان نامه حاضر مورد توجه علاقمندان واقع گردد.

مرداد ۱۳۷۵

فهرست مطالب

فهرست تصاویر

فهرست جداول

فصل اول

بسمه تعالی

مقدمه

ادامه حیات انسان بعنوان یک موجود اجتماعی مستلزم وجود سه منبع اساسی یعنی غذا، انرژی و اطلاعات است. عصر کنونی قرن تکنولوژی اطلاعات نامیده شده است. تکنولوژی اطلاعات امروزه نقش اساسی در پیشرفت جوامع بشری دارد. در سیستمهای امروزی ایجاد امنیت در نگهداری و جلوگیری از دستیابی غیر مجاز به اطلاعات از اهمیت بالایی برخوردار است. از دیرباز تاکنون روشهای مختلفی برای برقراری امنیت از دیدگاههای مختلف ابداع و پیاده‌سازی شده است. با توجه به اینکه ایران در ابتدای راه بهره‌وری گسترده از سیستمها و شبکه‌های کامپیوتری می‌باشد، توجه به ابعاد مختلف مسائل امنیتی سیستمهای کامپیوتری و خصوصاً سیستمهای رمز نگاری از اهمیت خاصی برخوردار است.

هر کاربر کامپیوتری لازم است که تهدیدات و اقدامات متقابل موجود در سیستم‌های کامپیوتری را بشناسد.

در سال ۱۹۸۷ گروهی از جوانان آلمان غربی با استفاده از ارتباط با کامپیوترهای امریکا به سیستمهای محاسباتی NATO به صورت غیرمجاز دست یافتند. در سال ۱۹۸۶ فردی در آزمایشگاه تحقیقاتی - علمی امنیت آمریکا رخنه کرد. در ۱۹۸۳ نوجوانانی موسوم به گروه ۴۱۴ به داخل تعدادی از سیستمهای کامپیوتری منجمله سیستمهای بیمارستانی و بانک‌های امنیتی نفوذ کردند. تهدیداتی از این قبیل نه تنها غیر عادی نبوده، بلکه به عنوان حملات موفق از طریق

رسانه های خبری منتشر شده اند و در صورتی که در سیستمهای کامپیوتری برای ایمن شدن سیستمها چاره ای اندیشیده نشود ممکن است ضایعات جبران ناپذیری در برخی زمینه ها ایجاد شود .

ایمنی کامپیوتری موضوع بسیار مهمی برای افرادی که پیشهٔ آنها کامپیوتر می باشد ، محسوب می گردد . کاربران و راهبران سیستمهای کامپیوتری بزرگ در دو دهه ۱۹۶۰ و ۱۹۷۰ تکنیک هایی در برقراری امنیت کامپیوتری ایجاد کردند که تاثیرات معقول و مستدلی بر علیه تهدیدات آن دوره بر جای گذاشت .

در سال ۱۹۷۵ الگوریتم DES (Data Encryption Standard) بعنوان یک روش رمز نگاری منتشر شد ، در حالیکه قبل از این تاریخ نیز روشهای زیادی برای برقراری امنیت بکار گرفته شده بود . این کار رقابت شدیدی را برای شکستن آن به راه انداخت . در سال ۱۹۹۳ دو تن از محققان ایرانی [۱] توانستند تراشه ای موسوم به DESB (DES Breaker) طراحی کنند که ارزانتر و مفیدتر از ماشین هلمن در نقض DES می باشد .

در این فصل ابتدا مقوله های مورد بحث و استفاده در پایان نامه فهرست وار تعریف شده اند . سپس سناریوهای مختلفی که عمدتا سیستمهای کامپیوتری را تهدید می کنند فهرست و تعریف شده اند و در نهایت اشاره ای به تئوریهای زمینه شده است .

در فصل دوم لزوم ایجاد امنیت در سیستمهای کامپیوتری بررسی می شود . در فصل سوم روشهای ایجاد امنیت خصوصا رمز نگاری و برخی روشهای پیاده سازی آن بررسی شده و دو روش جدید پیشنهادی ارائه می شود . فصل چهارم مؤلفه های سخت افزاری و نرم افزاری سیستمهای کامپیوتری را مشخص نموده و مسائل مربوط به ایجاد امنیت در بخش های مختلف اعم از کامپیوترهای شخصی ، شبکه های کامپیوتری ، سیستمهای عامل ، پایگاه داده ها ، وامنیت فیزیکی را به اختصار بیان می نماید و همینطور چگونگی پیاده سازی دو روش را در قالب کامپیوترهای شخصی مطرح می نماید . فصل آخر به نتیجه گیری و بحث پیرامون پیشنهادات ارائه شده در پایان نامه می پردازد .

در پیوست ۱ مروری بر استانداردهای موجود و اشاره ای به برخی از استاندارد های ایمنی خواهد شد. در پیوست ۲ منحنی های مقایسه دو روش DES و پیشنهادی برای Encryption آمده است . پیوست ۳ یک دیسکت حاوی ۵ برنامه بهمراه توضیحات مربوط به آنها می باشد.

۱-۱- تعاریف

امنیت (Security) : امنیت ، محافظت از درستی ، صحت و تمامیت اطلاعات میباشد .

رمز نگاری (Cryptography) : مساله ایجاد امنیت در سیستمها و شبکه های کامپیوتری ، که نقش اعصاب دنیای کنونی را دارند ، یک موضوع حیاتی است . برای پیشگیری از فهمیدن اطلاعات توسط افراد غیر مجاز از علم رمز نگاری استفاده می شود .

Plain Text یا Message : به مفهوم پیام ، متن علنی (m) و یا متن ساده استفاده میشود .

کلید (Key) : رشته کوتاهی که برای رمزگذاری و رمز گشائی متون بکار می رود .

Cipher Text : منظور از این اصطلاح ، متن رمز شده (c) و یا سری می باشد که از ترکیب کلید و متن اصلی بدست می آید .

الگوریتم رمز : الگوریتمی است که یک متن ساده را به یک متن رمز شده تبدیل میکند.

معمانگاری(Cryptanalysis) : دانشی است که در رابطه با طراحی و تحلیل سیستمهایی که امنیت را تامین کرده و در مقابل تحلیل مقاومت می کنند ، بحث می کند .

امنیت مطلق (Perfect Security) : شانون می گوید که امنیت کامل هنگامی برقرار شده است که اگر شخصی P متن رمز شده C_p , ... , C_2, C_1 را دریافت کرده باشد ، نتواند با دریافت متن C_{p+1} ، پیام m_{p+1} را بفهمد . فرض بر اینست که دشمن الگوریتم E (رمزنگاری) را نیز دارد . یعنی حدس زدن کلید غیر ممکن باشد ومتن C_{p+1} هیچگونه اطلاعات اضافی را به تحلیلگر ندهد. بنابراین شرط برقرار بودن امنیت مطلق ، برابری تعداد پیامها با تعداد کلیدهایی است که برای رمز کردن آنها بکار رفته است . البته عملا اینکار مقدور نمی باشد و لذا در عمل از " امنیت عملی " استفاده می شود .

امنیت عملی (Practical Security) : در این مورد از فاکتور کاری (work factor) که نسبت پیچیدگی تحلیل یک سیستم به پیچیدگی رمز آن برحسب زمان می باشد ، استفاده میشود. در این سیستمها امکانات لازم برای تحلیل سیستم (مالی ، زمانی و اطلاعاتی) خارج از دسترس تحلیلگر است . یعنی دشمن توانائی دارد ولی امکانات کشف رمز را ندارد .

شنود (Wiretapping) : شنود به معنی استراق سمع کردن می باشد . شنودهای انجام شده یکی از دو حالت غیر فعال (Passive) و یا فعال (Active) را دارند . در حالت اول صرفا اطلاعات دریافت می شوند ولی در حالت دوم تغییر نیز می کنند ویا دشمن ارتباط اصلی را قطع کرده و خود را جایگزین منبع پیام می کند . برای مقابله با خطر اول لازمست پیامها را محرمانه و سری کنیم و در مورد دوم بایستی صحت و اصالت را تست کنیم .

امنیت مطلق سیستم را می توان ثابت کرد ، ولی نمی توان ثابت کرد که یک سیستم بطور عملی امن است . ولی اگر یک قرد ماهر نتواند سیستم رمز را بشکند ، می توانیم تا حدود زیادی مطمئن باشیم که سیستم عملا امن است.

۲-۱- سناریوهای مختلف تهدیدات

حمله به متن رمز شده (Cipher Text only Attack) : در این حالت دشمن تنها میتواند متن های رمز شده را از روی خط بردارد و فقط الگوریتم رمزنگاری را می داند .

حمله به متن علنی شناخته شده (Known Plain Text Attack) : در این حالت استراق سمع کننده علاوه بر دانستن الگوریتم و شنود کردن از متن های رمز شده ، با داشتن تعدادی از متن های اصلی سعی می کند رمز را بشکند .

حمله انتخابی به متن رمز شده (Chosen Cipher Text Attack) : در این حمله دشمن می تواند اطلاعات رمز شده را بدهد و اطلاعات متن اصلی مربوطه را بدست آورد و به این ترتیب سیستم را بشکند.

حمله انتخابی به متن رمز شده/علنی (Chosen Plain/Cipher Text Attack) : در این حمله دشمن می تواند یک سری متن معمولی را انتخاب کرده و وارد سیستم کرده و متن رمز شده را ببیند. همچنین یک سری متن رمز را انتخاب و متن اصلی را مشاهده می کند و با استفاده از اطلاعات بدست آمده سیستم را می شکند .

در سیستمهای کامپیوتری علاوه بر مشکلات سیستمهای مخابراتی ، مشکلات زیر نیز موجود است :

چریدن (Browsing) : در این مورد یک شخص غیر مجاز به فایلهایی که اجازه دسترسی ندارد ، دسترسی پیدا می کند . برای حل این مشکل اطلاعات را محرمانه می کنند و کنترل دستیابی قرار می دهند .

نشت دادن (Leakage) : برنامه ای داریم که قانونا می تواند به اطلاعاتی دستیابی داشته باشد. ممکن است این برنامه اطلاعات محرمانه را به افراد غیر مجاز بفرستد . با رمز کردن اطلاعات ، اعمال کنترل دستیابی و اعمال کنترل جریان اطلاعات ، می توان این مشکل را حل کرد .

استنتاج (Inference) : در این حالت دشمن با توجه به اطلاعاتی که در باره موضوع دارد (معمولا اطلاعات آماری) اطلاعات مورد نظر خود را پیدا می کند .

هر سه مورد فوق در زمره شنود غیر فعال بشمار می روند. نمونه هایی از شنود فعال به شرح زیر هستند:

دستکاری کردن (Tapering) : در این حالت فرد غیر مجاز ، اطلاعات موجود در سیستم را تغییر می دهد.

تغییر قیافه دادن : در این حالت ناخواسته از برنامه ای که غیر مجاز است ولی ظاهر آن مجاز نشان می دهد ، استفاده می کنیم و این برنامه یکسری کارهای غیر مجاز انجام میدهد. بعنوان مثال ، برنامه ای یک صفحه تقلبی را در اختیار کاربر قرار میدهد تا کلمه عبور را بدست آورد . کاربرگول خورده و Login می کند و به این ترتیب کلمه عبور او کشف میشود. برنامه غیر مجاز پس از دریافت کلمه عبور کار خود را تمام می کند و روتین اصلی Login سیستم را فراخوانی می کند .

۳-۱- تئوریهای زمینه

تئوری پیچیدگی: این تئوری راجع به مشکل بودن ذاتی مسائل صحبت می‌کند. اگر شخصی نتواند مسئله‌ای را حل کند دلیل بر مشکل و پیچیده بودن آن مسئله نیست، زیرا ممکن است اطلاعات شخص مذکور کم بوده باشد. از این تئوری در مشخص کردن اینکه یک سیستم رمزنگاری یا یک الگوریتم رمز قابل شکستن و حل شدن می‌باشد یا نه، استفاده می‌شود و اصولاً آیا اگر دشمن بخواهد آن را حل کند با مسئله پیچیده‌ای روبرو است؟ از اینجا نتیجه می‌گیریم که سیستم عملاً امن است یا خیر؟! برای مشخص کردن میزان پیچیدگی یک مسئله از تعداد عملیات اولیه لازم یا تعداد پارامترهای ورودی استفاده می‌شود و بعنوان مثال برای مسئله‌ای که n پارامتر دارد می‌گوییم پیچیدگی $O(n^2)$ می‌باشد. ممکن است یک مسئله را بتوان از چند راه حل کرد. در این صورت انتخاب بهترین راه مهم می‌باشد و برای این انتخاب نیز معیاری لازم است. در تئوری پیچیدگی از معیار بدترین حالت استفاده می‌شود. اگر رمزگذاری پیام را پیچیده کنیم ممکن است رمزگشایی هم غیرممکن شود. لذا از Trap - Door استفاده می‌شود. بدین معنی که نکته‌ای را در مسئله بگذاریم که اگر کسی آن نکته را بداند، بتواند به پاسخ دست یابد.

تئوری اعداد: در این تئوری در مورد حساب مدولار صحبت می‌شود که برای کسانی که بخواهند در زمینه رمزنگاری پیشرفته کار کنند، کار بیشتر در این زمینه الزامی است. در این مورد روی حساب هم نهشتی، مجموعه کامل باقیمانده‌ها، مجموعه کاهش یافتهٔ باقی‌مانده‌ها و موارد دیگری بحث می‌شود.

تئوری اطلاعات: این تئوری راجع به میزان اطلاعات موجود در پیامها صحبت می‌کند. با توجه به اینکه در سیستمهای رمزنگاری با داشتن پیامهای رمز شده اطلاعات ما راجع به پیامهای اصلی زیادتر می‌شود، بنابراین در عمل، سیستمها کاملاً امن نیستند. شانون اثبات کرده است که تنها یک سیستم امن است و آن سیستم One - Time - Pad می‌باشد. تئوری اطلاعات، میزان اطلاعات موجود در یک منبع پیام را اندازه‌گیری کرده و آنرا بر حسب تعداد بیتهای لازم جهت کدکردن آن بیان می‌کند. میزان اطلاعات را آنتروپی منبع پیام مشخص می‌کند. در مورد سیستمهای کاملاً سری، تئوری اطلاعات می‌گوید که کلیدهای مورد استفاده برای رمزنگاری بایستی کاملاً تصادفی انتخاب شوند و حداقل بطول پیامهایی که رمز می‌کنند باشند. یکی دیگر از مواردی که در اینجا بحث می‌شود حداقل طول متن سری که برای شکستن رمز لازم است می‌باشد. هرچه افزونگی زبان بیشتر باشد، سیستم رمز راحتتر شکسته می‌شود و هرچه آنتروپی کلید بیشتر باشد، سیستم رمز مشکلتر شکسته می‌شود.

فصل دوم

لزوم ایجاد امنیت در سیستمهای کامپیوتری

۱-۲- ناامنی سیستمهای کامپیوتری

هدف یک تبهکار کامپیوتری می‌تواند هر یک از قسمتهای سیستم کامپیوتری باشد. یک سیستم کامپیوتری مجموعه‌ای از سخت‌افزار، نرم‌افزار، حافظه‌های جانبی، داده‌ها و اشخاصی می‌باشد که به منظور انجام عملیات محاسباتی و خدمات داده آمائی سازماندهی شده‌اند. همانگونه که در یک سیستم بانکی پول هدف سرقت می‌باشد، در یک سیستم کامپیوتری بعنوان مثال، لیستی از اسامی و آدرسهای افرادی که در بانک پول می‌گذارند، می‌تواند هدف باشد. این لیست ممکن است روی کاغذ، حافظه‌های مغناطیسی و یا حافظه اصلی کامپیوتر ذخیره شده باشد و نیز ممکن است بصورت الکترونیکی از طریق خطوط تلفن در حال انتقال بین کامپیوترها باشد. این کثرت هدفها مسئله ایمنی در سیستمهای کامپیوتری را مشکلتر می‌سازد.

در هر سیستم ایمن، ضعیفترین نقطه، آسیب‌پذیرترین نقطه می‌باشد. مسلم است که اگر پنجره‌ای امکان دسترسی ساده‌تر را ایجاد کرده باشد، یک سارق اقدام به خراب کردن دیواری فلزی با قطر ۱۰ سانتی متر نمی کند . اولین اصل امنیت کامپیوتری (اصل ساده ترین نفوذ) به شکل زیر بیان می شود :

اصل ساده‌ترین نفوذ: از یک فرد مخل امنیت انتظار استفاده از هر راه نفوذی می‌رود.

لزومی ندارد که این نفوذ از طریق آشکارترین راه باشد و همینطور ممکن است که این نفوذ

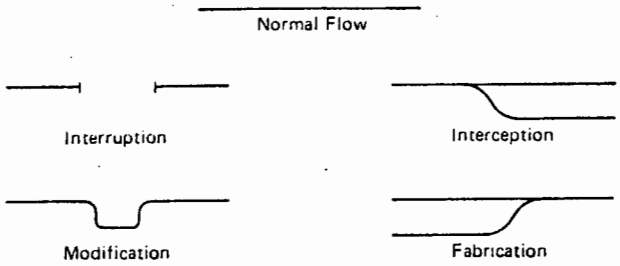
از تاریکترین راه نیز نباشد.

این اصل به ما می‌گوید که مسئول ایجاد امنیت کامپیوتری بایستی همه راههای ممکن برای نفوذ را در نظر داشته باشد. چرا که افزایش ایمنی از یک راه ممکن است باعث کاهش امنیت راههای دیگر برای نفوذ شود. حال ما به بررسی این راههای نفوذ می‌پردازیم.

۲-۲- انواع رخنه در امنیت

از دیدگاه امنیت، یک افشاء (Exposure) شکلی از نابودی یا خسارت احتمالی در یک سیستم کامپیوتری می‌باشد. مثالهایی از افشاء را می‌توان «دسترسی غیرمجاز به داده‌ها، تغییر داده‌ها، یا رد یک دسترسی مشروع و مجاز به سیستمهای محاسباتی» دانست. یک آسیب‌پذیری (Vulnerability) عبارتست از وجود نوعی ضعف در سیستم ایمن بطوریکه موجب از دست رفتن یا صدمه دیدن آن شود. فردی که از آسیب‌پذیری سیستم بهره‌برداری می‌کند یک تک یا حمله (Attack) به سیستم را مرتکب شده است. تهدیدهای متوجه یک سیستم کامپیوتری رویدادهایی هستند که بصورت بالقوه توانایی از بین بردن یا صدمه زدن به سیستم را دارا می‌باشند. بعنوان مثال حملات انسانی یک تهدید به شمار می‌روند. به همین ترتیب بلایای طبیعی، خطاهای غیرعمدی انسانها و عیبهای داخلی سخت‌افزار و نرم‌افزار نیز تهدید به شمار می‌روند. نهایتاً کنترل وسیله ای (ازقبیل یک عمل، یک دستگاه ، یک رویه و یا یک تکنیک) برای حفاظت می باشد که می تواند آسیب پذیری سیستم را کاهش دهد .

ثروتهای اصلی سیستمهای کامپیوتری شامل سخت افزار، نرم افزار و داده ها می باشند. چهار نوع عمده تهدید امنیت سیستمهای کامپیوتری عبارتند از: وقفه (Interruption) ، نشت (Interception) ، تغییر (Modification) و ساخت (Fabrication) . هر چهار نوع تهدید از نقاط آسیب پذیر سیستمهای کامپیوتری سوء استفاده می کنند. تهدیدات مذکور در شکل ۱-۲ نمایش داده شده و تعریف هر یک از آنها در ادامه ارائه می شود:



شکل (۱-۲) چهار گروه از تهدیدات امنیت سیستمهای کامپیوتری

۱- وقفه : در اثر یک وقفه ، یک سرمایه کامپیوتری از دست رفته وبا خارج از دسترس و غیر قابل استفاده می شود . بعنوان مثال یک انهدام دستگاه سخت افزاری از روی عناد ، حذف یک فایل داده یا برنامه ، یا خراب کردن یک مدیر فایل سیستم عامل بطوریکه نتواند قسمتی از یک فایل را پیدا کند ، همگی وقفه محسوب می شوند .

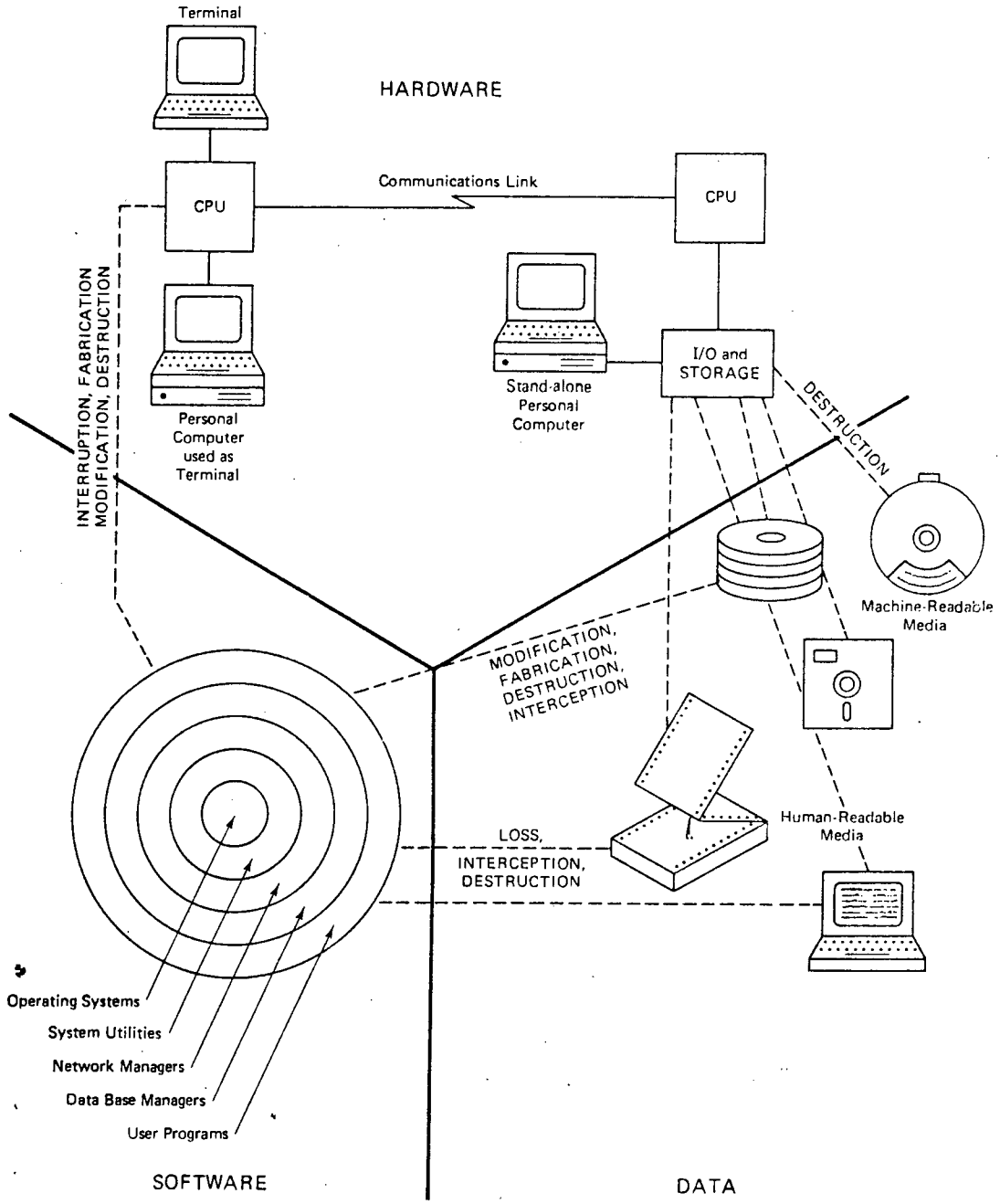
۲- نشت: نشت بدین معنی است که یک بخش غیر مجاز بتواند به یکی از منابع کامپیوتری دسترسی پیدا کند. قسمت خارجی می تواند یک شخص، یک برنامه یا یک سیستم کامپیوتری دیگر باشد. بعنوان مثالهایی از اینگونه تهدید، میتوان از کپی غیر قانونی از برنامه یا فایلهای داده و استراق سمع برای بدست آوردن داده ها در یک شبکه نام برد. از آنجائیکه گم شدن اطلاعات میتواند بخوبی و سریع کشف شود، بنابراین عمل " نشت" بایستی خیلی بی سر و صدا و بدون برجای گذاردن رد پایی انجام شود.

۳- تغییر: اگر قسمتی از اطلاعات نه تنها مورد دسترسی غیر مجاز قرار گیرد بلکه ناخنک نیز بخورد ، اصطلاحا می گوئیم تغییر کرده است . برای مثال ممکن است فردی مقادیر ارزشهای ضبط شده در یک پایگاه داده (Data Base) را تغییر دهد، یا یک برنامه را به گونه ای تغییر دهد که محاسبات اضافی انجام دهد ، یا اطلاعاتی را که بصورت الکترونیکی منتقل می شوند تغییر دهد. همچنین ممکن است که سخت افزار نیز در معرض تغییر قرار بگیرد . بعضی از حالتهای تغییر با اندازه گیریهای ساده ای قابل تشخیص می باشندوبرعکس برخی دیگرغیرقابل تشخیص می باشند.

۴- ساخت : نهایتا ممکن است قسمتی از یک سیستم کامپیوتری به صورت جعلی ساخته شود . فرد مزاحم ممکن است بخواهد اطلاعات نادرستی را به یک سیستم مخابراتی شبکه

اضافه کند ، یا به یک بانک اطلاعاتی رکوردهایی رابیافزاید . گاهی اوقات ، اگر اینکار استادانه انجام شده باشد ، این اضافات بعنوان سند شناخته می شوند و تقریبا از اطلاعات واقعی غیر قابل تشخیص می باشند.

این چهار نوع تهدید و یا بعبارتی دیگر چهار گروه از مداخلات در فعالیتهای کامپیوتری ، انواع ممکن افشاء را بیان می کنند. جلوه هایی از این مداخلات در شکل ۲-۲ به تصویر کشیده شده است.



شکل (۲-۲) انواعی از استفاده غیر مجاز در سیستمهای کامپیوتری

۳-۲- نقاط آسیب پذیر

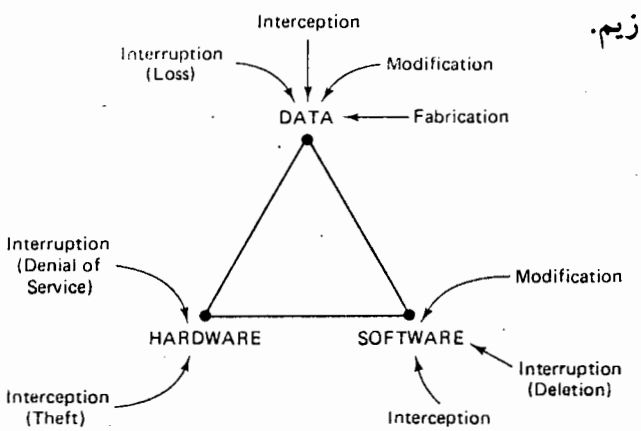
یک سیستم ایمن کامپیوتری دارای سه مشخصه می باشد : سری بودن (Secrecy) ، کامل بودن (Integrity) ، و در دسترس بودن (Availability) .

- سری بودن : سری بودن بدین معناست که سرمایه های سیستم کامپیوتری تنها توسط قسمت های مجاز قابل دسترسی باشند . نوع چنین دسترسی را خواندن (Read) می نامیم که می تواند شامل خواندن ، مشاهده کردن ، چاپ کردن ، و یا حتی اطلاع از وجود یک شیء بشود .

- کامل بودن : کامل بودن بدین معناست که سرمایه های کامپیوتری فقط توسط قسمتهای مجاز قابل تغییر باشند. این تغییر شامل نوشتن، عوض کردن، عوض کردن وضعیت، حذف و یا ایجاد می شود.

- در دسترس بودن : در دسترس بودن بدین معناست که سرمایه ها در دسترس قسمتهای مجاز باشند. کلیه افراد یا بخشهای مجاز نباید از دسترسی به چیزهایی که برای آنها قانونی میباشد، منع شوند. برای مثال یک سیستم ایمن می تواند کاملا سری حفاظت شود به گونه ای که هیچ فردی اجازه خواندن قسمتی از اطلاعات را نداشته باشد . در این صورت این سیستم فاقد شرایط در دسترس بودن برای برخی دسترسی ها می باشد.

شکل شماره ۳-۲ سه ضامن امنیت را در قبال سرمایه های سخت افزاری ، نرم افزاری و اطلاعاتی نشان میدهد. این سه منبع و اتصالات آنها ، می توانند نقاط آسیب پذیر امنیت محسوب شوند . در قسمتهای زیر به بررسی آسیب پذیری یک ثروت معین از سیستمهای کامپیوتری می پردازیم.



شکل (۳-۲) نقاط ضعف سیستمهای کامپیوتری

۱-۳-۲- حمله به سخت افزار

از آنجائیکه یک دستگاه فیزیکی قابل رؤیت می باشد ، بنابراین می تواند یک نقطه ساده برای حمله باشد. صدمه های فیزیکی شامل موارد زیر است که ممکن است سهوی و یا عمدی باشند:

کامپیوترها خیس شده اند،آتش گرفته اندوبا برق شهری یا منابع تغذیه دیگر آسیب دیده اند. جزئی از گرد و غبار در برخی از قسمتهای دستگاههای کامپیوتری رخنه کرده است. کامپیوترها ضربه خورده اند، لرزه دیده اند و سوراخ نیز شده اند.

ماشینها مورد اصابت تفنگ واقع شده اند . بمبها ، آتش و تصادفاتی محلهای استقرار کامپیوترها را خراب کرده اند . کلید ، قلم و پیچ گوشتی ها برای اتصال کوتاه کردن مسیرهای عبور جریان روی بردها و دیگر قسمتهای کامپیوتر استفاده شده اند و نهایتا کامپیوترها به سرقت نیز رفته اند.

سرقت و تخریب تکنیکهای ابتدائی صدمات محسوب میشوند. مدیران مراکزاصلی کامپیوتری از مدتها پیش متوجه آسیب پذیری ماشینهایشان شده اند و برای حفاظت از آنها سیستمهای ایمنی فیزیکی را نصب کرده‌اند. اما افزایش ریزکامپیوترها در دفاتر سبب شده است که مردم هزاران دلار تجهیزات را روی میزها و خارج از اطاقهای کامپیوتر بی‌توجه رها کنند. گاهی اوقات امنیت اجزاء سخت‌افزاری،با ابزارهای فیزیکی ساده‌ای از قبیل قفل یا نگهبان می‌تواند بسیار افزایش پیدا کند.

۲-۳-۲- حمله به نرم افزار

کامپیوتر بدون نرم‌افزار بی‌فایده می‌باشد. نرم‌افزار می‌تواند از روی عناد خراب شود و یا تغییر کرده، حذف شده یا بطور اتفاقی گم شود. البته صرفنظر از انگیزه، نتیجه در همه موارد یکی است:از دست رفتن نرم‌افزار توسط کسی که می‌خواهد آنرا اجرا کند، آشکار خواهد شد. این حملات همگی مسائلی هستند که در دسترس بودن نرم‌افزار را به مخاطره می‌اندازند.

ماهرانه‌تر اینکه نرم‌افزار اجرا شود اما تغییر یافته باشد. تجهیزات فیزیکی معمولاً مشخص است که آسیب دیده‌اند، اما از دست رفتن یک خط از برنامهٔ اصلی یا Object آن معمولاً اثر مشخصی را در برنامه موجب نمی‌شود. بنابراین ممکن است یک برنامه تغییر کند بطوریکه همه آنچه را قبلاً انجام می‌داده، انجام دهد و سپس کارهای دیگری نیز بکند. در این حالت تشخیص تغییر ایجاد شده در نرم‌افزار بسیار مشکل خواهد بود. سه نوع حمله علیه نرم افزار را می توان برشمرد :

حذف نرم‌افزار: نرم‌افزار به سادگی قابل حذف می‌باشد. ممکن است که حتی برنامه‌نویس اتفاقاً یک فایل را حذف کند یا یک کپی خراب از برنامه را ذخیره کند و کپی سالم قبلی را خراب کند. از آنجاییکه نرم‌افزارها در مراکز تجاری کامپیوتری دارای ارزش بالایی می‌باشند، دسترسی به آنها معمولاً به دقت از طریق عملیات «مدیریت پیکربندی» کنترل می‌شود و بنابراین نرم‌افزارها بصورت اتفاقی حذف، خراب و یا جایگزین نمی‌شوند.

تغییر و تبدیل نرم‌افزار: در این تهاجم یک برنامه کاری تغییر می‌کند، به‌گونه‌ای که یا در

طول اجرا با شکست مواجه شود و یا موجب شود که عمل ناخواسته ای انجام گیرد. نرم افزار نسبتا بسادگی قابل تغییر است : عوض کردن یک یا دو بیت می تواند موجب تغییر آن شود. برحسب اینکه کدام بیت تغییر کند، برنامه ممکن است موقع شروع به اجرا یا پس از گذشت مدتی از اجرا در هم شکسته شود .

با کمی کار کردن می توان تغییرات را ماهرانه تر انجام داد ، بطوریکه برنامه مدت زمان زیادی درست کار کند ولی در یک لحظه زمانی خاص خراب شود. این گونه تغییرات، معمولا توسط ویروسهای کامپیوتری داده می شود و یا یک کارمند ناراضی ممکن است یک برنامه تجاری را به گونه ای تغییر دهد که با دسترسی به تاریخ سیستم ناگهان پس از اول تیر ماه متوقف شود . چه بسا خود کارمند در اول اردیبهشت محل کار را ترک کرده و در محل جدیدی مشغول به کار شده باشد. نوع دیگری از تغییر شامل گسترش دادن به عملیات یک برنامه میباشد، بگونه ای که یک برنامه بی ضرر عوارض جانبی دیگری نیز در پی داشته باشد. برای مثال ، برنامه ای که ظاهرا بنحوی سازماندهی شده است که لیست فایلها را به یک کاربر نشان دهد، ممکن است حفاظت فایلها را تغییر داده و موجب شود که کاربران دیگری به همان فایلها دسترسی پیدا کنند. دسته بندی تغییرات نرم افزار شامل موارد زیر است:

۱- یک اسب تراوا ، برنامه ای که ظاهرا کاری را انجام میدهد در صورتی که باطنا کار دیگری را انجام میدهد.

۲- یک دریچه ، یک نقطه ورود مخفی به یک برنامه .

۳- برنامه ای که اطلاعات را فاش میسازد و این اطلاعات را در دسترس برنامه ها یا افرادی که قصد آنرا ندارند ، می گذارد.

البته ممکن است که یک برنامه جدید ساخته شده و آنرا در یک سیستم کامپیوتری بجای یکی از برنامه‌هانصب کنند. کنترل غیر کافی روی برنامه‌هایی که در یک سیستم کامپیوتری نصب

شده و اجرا می‌شوند، امکان چنین انواعی از رخنه در امنیت نرم‌افزار را فراهم می‌کند.

سرقت نرم‌افزار: این آفند شامل کپی غیرمجاز نرم‌افزار می‌شود. تهیه کنندگان و توزیع کنندگان نرم‌افزار حق این را دارند که در مقابل استفاده از محصولاتشان منصفانه پاداش داده شوند. [۲] کپی غیرمجاز از نرم‌افزار مورد پیگرد قانونی قرار می‌گیرد.

۳-۳-۲- حمله به داده ها

معمولا امنیت سخت افزار بستگی کمتری به کارمندان مراکز کامپیوتری دارد، لیکن امنیت نرم افزار ابعاد وسیعتری داشته و به همه برنامه نویسان و تحلیلگرانی که برنامه ها را ایجاد یا اصلاح می کنند ارتباط دارد.

برنامه‌های کامپیوتری به زبانهای قابل فهمی برای افرادی که حرفه‌شان کامپیوتر می‌باشد، نوشته می‌شوند و بنابراین یک لیست فاش شده متن اصلی برنامه چندان به درد مردم عادی نمی‌خورد. اما داده‌های چاپ شده می‌توانند توسط مردم عادی نیز براحتی تفسیر شوند. بنابراین بخاطر ماهیت عمومی داده‌ها، حمله به آنها از حمله به سخت‌افزار و نرم‌افزار گسترده‌تر می‌باشد. بنابراین مقادیر داده عمومی‌تر از سخت‌افزار و نرم‌افزار می‌باشد، به این خاطر که بیشتر مردم می‌دانند که چگونه اطلاعات را تفسیر و یا استفاده کنند. داده‌ها لزوماً مقادیر مرتبی نباید باشند. به همین دلیل اندازه‌گیری ارزش داده مشکل است. اما داده‌ها ارزشمند بوده و شاید توسط هزینه‌ای که صرف احیای آنها و یا ایجاد و توسعه آنها می‌شود، قابل اندازه‌گیری باشند. اطلاعات محرمانه‌ای که برای یک رقیب فاش شده باشد، می‌تواند حلقه رقابت را تنگتر کند. نهایتاً امنیت ناکافی ممکن است به بدهی مالی منجر شود، اگر اطلاعات شخصی، عمومی شود. بنابراین داده ها مقادیر ارزشمندی به شمار می روند، اگر چه این ارزش معمولا به سختی قابل اندازه گیری است. هم

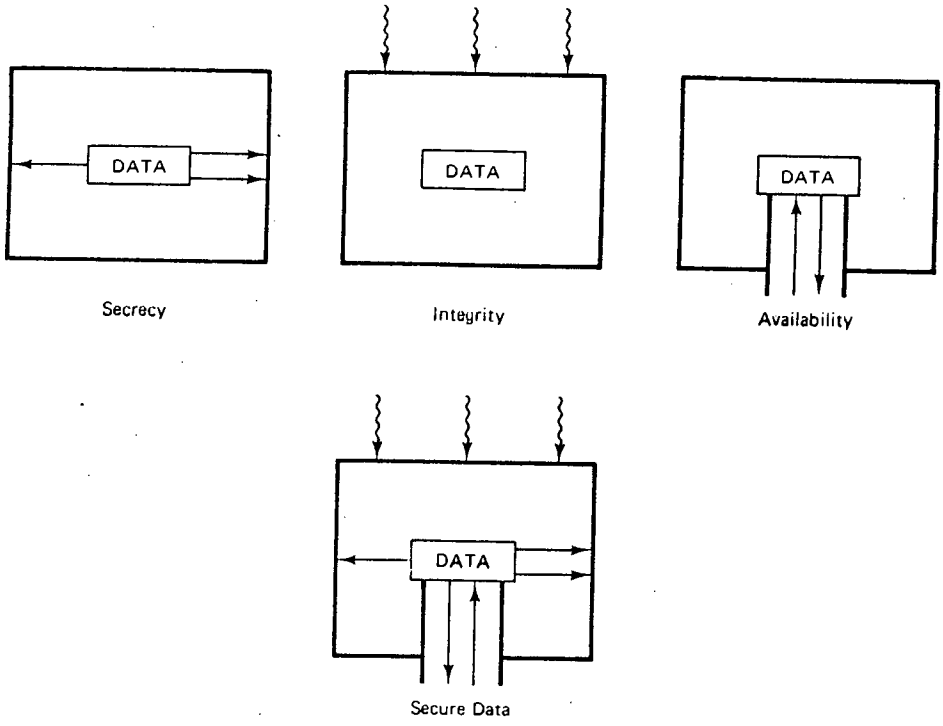
نرم افزار و هم سخت افزار معمولا دارای عمر نسبتا طولانی میباشند. مقـادیر داده هـا ممکـن است خیلی زیاد باشند، اما فقط قسمتی از آنها درمدت کوتاهی جلب توجه خواهد کرد. مثـال زیر را در نظر بگیرید:

متناوباً تحلیلگران دولتی اطلاعاتی در مورد اقتصاد ملی بدست می‌آورند. نتایج در تاریخ و ساعت معین منتشر می‌شوند. قبل از آن زمان، دسترسی به این اطلاعات می‌تواند موجب این شود که فردی در بازار صاحب سود فراوانی شود. فرض کنید که تحلیلگری اطلاعاتی را ۲۴ ساعت قبل از انتشار ایجاد کرده و بخواهد نتایج را با کمک تحلیلگر دیگری قبل از انتشار بازبینی کند. یک روش حفاظتی مورد نیاز است که بتواند این اطلاعات را فقط برا ی ۲۴ ساعت نگهداری کند و مسلم است که پس از ۲۴ ساعت دیگر احتیاجی به حفاظت این اطلاعات نیست. مطالعه امنیت داده ها ، اصل دوم امنیت کامپیوتری را مطرح می سازد که اصل ارزش زمانی است.

اصل ارزش زمانی : اقلام کامپیوتری تا زمانی نیاز به حفاظت دارند که ارزش خـــود را از دست نداده باشند.

این اصل به ما می گوید که چیزهایی که عمر کوتاهی دارند می تواننـــد توسـط ابزارهـای ایمنی که به همان اندازه اثر دارند مورد حفاظت قرار بگیرند. این اصل ترجیحا در مـــورد داده اعمال می شود ، زیرا داده ها عناصری از امنیت کامپیوتری میباشند که معمولا کوتاهترین عمر را دارا میباشند .

شکل ۴-۲ سه عامل حفاظت داده ها را نشان می‌دهد:سری بودن (جلوگیری از افشاءسازی غیرمجاز)، کامل بودن (جلوگیری از تغییر غـیرمجاز) و در دسـترس بـودن (جـلوگیری از رد دسترسی مجاز).



شکل (۴-۲) امنیت داده ها

سری بودن داده‌ها: داده‌ها می‌توانند بوسیله استراق سمع از کابلها، با نصب میکروفون مخفی در دستگاههای خروجی، وارسی سطلهای زباله، گوش دادن به علائم رمزی الکترومغناطیسی، تطمیع کارمندان کلیدی، حدس زدن یک قسمتی از داده با توجه به مقادیر دیگر آن و یا ساده‌تر با درخواست آن جمع‌آوری شوند. از آنجاییکه اغلب داده‌ها به صورتی می‌باشند که انسان می‌تواند بخواند، سری بودن آن مهمترین اهمیت را در ایمنی کامپیوتری دارا می‌باشد.

کامل بودن و درستی داده ها : ربودن ، خریدن ، پیدا کردن یا شنیدن داده ها به امکانات پیشرفته کامپیوتری نیاز ندارد در حالیکه تغییر یا ایجاد داده های جدید نیاز به دانستن تکنولوژی چگونگی انتقال یا ذخیره و نگهداری اطلاعات دارد . بنابراین سطوح پیشرفته تری برای تغییر داده های موجود و یا جعل داده های جدید به جهت جلوگیری از داده های موجود نیاز است . منبع اصلی تکرار چنین مساله ای برنامه ها ی بد اندیش ، سیستم فایل های سرگردان یا امکانات مخابراتی معیوب می باشد . داده ها مخصوصا از جهت تغییر ، آسیب پذیرند .

تغییرات کوچک یا عمده انجام شده ممکن است از راههای موجود قابل تشخیص نباشند. برای مثال، یک تبهکار می‌تواند برنامه‌ای بنویسد که از حساب بانکی هر شخصی یک ریال کاسته و این پولها را به یک حساب ویژه منظور کند. معمولاً مشتریان خیلی دقیق حساب موجودی خود را ندارند و اگر هم داشته باشند کسی پیدا نمی‌شود که به خاطر یک ریال به مسئولین بانک اعتراض کند. چنین حمله‌ای موسوم به حمله سالامی (Salami) می‌باشد که در آن یک کلاهبردار مقدار کمی از هر حساب را برداشته و مجموع این مقادیر کم راکه یک مقدار قابل ملاحظه خواهد شد در حساب خود می‌گذارد.

یکی از عملیات پیچیده‌تر سعی در پردازش مجددی است که از دیتا استفاده می‌کند. در مکالمات بین بانکها،یک جاعل ممکن است پیغامی راکه یک بانک از بانک دیگر تقاضای وام برای حساب فرد مشخصی را می‌کند، دریافت کند و خود مجدداً این پیغام را بفرستد. بانک دریافت کننده پیغام خیال می‌کند که مجدداً از همان حساب تقاضای وام شده است. فرد کلاهبردار می‌تواند با تغییر شماره حساب یا مقدار مورد تقاضا همین عمل را دوباره تکرار کند.

در دسترس بودن : همانطور که قبلا ذکر گردید ایجاد امنیت در سیستم کامپیوتری نباید مانع دسترسی مجاز به داده ها باشد .

۴-۳-۲- سرمایه های بی پناه دیگر

نقاط اصلی آشکار در سیستمهای کامپیوتری سخت افزار ، نرم افزار و داده ها می باشند . اما ممکن است که هر قسمت دیگری از سیستم نیز هدف باشد . در این قسمت ما به برخی دیگر از نقاط مورد حمله اشاره می کنیم .

رسانه های ذخیره سازی : حافظه ها ی ثانویه که اطلاعات را در خود نگه میدارند نقاط آسیب پذیری می توانند باشند.ایمنی مؤثر ایجاب می کند که طراحی به گونه ای

باشد که نسخه های پشتیبان از داده ها و همینطور حفاظت فیزیکی از منـابع پشـتیبان در نظـر گرفته شده باشند .

شبکه‌ها: شبکه‌ها معمولاً کلکسیونی از سخت‌افزار، نرم‌افزار و دیـتا، بـعنوان ۳ سـرمایه اصلی سیستمهای کامپیوتری می‌باشند. هر گره موجود در شبکه، یک سیستم کامپیوتری با همهٔ مسائل معمول امنیت می‌باشد.

در شبکه، به اینها بایستی مسائل مربوط به ارتباطات راکه از طرق مختلفی انجام می‌گیرد و مسائل دسترسی از راه دور و همچنین قابلیت اعتماد به سیستم کامپیوتری را نیز افزود. شبکه‌ها بطور ساده مشکلات امنیت کامپیوتری را چندین برابر می‌کنند. فقدان نزدیکی فیزیکی، استفاده از ناامنی، دستگاههای مشترک و احتیاج به شناسایی کاربران دوردست مسائل امنیتی هستند که کار را در شبکه‌های کامپیوتری مشکلتر کرده‌اند.

دسترسی: نحوهٔ دیگری از افشاء،دسترسی به تجهیزات کامپیوتری است. اولاً فرد مزاحم ممکن است درست زمانی که کامپیوتر بایستی محاسبات انجام دهد، آنرا به سرقت ببرد. سرقت سرویسهای کامپیوتری همسو با سرقت برق یا دیگر چیزهای سودمند می‌باشد. البـته چـه بسـا سرویسی که کامپیوتر می‌دهد بسیار باارزشتر از سرویس دستگاههای بـرقی دیگـر بـاشد. ایـن دسترسی حساب نشده هزینه واقعی نگهداری سیستمهای کـامپیوتری بـرای سـرویس‌دهی بـه کاربران مجاز را افزایش می‌دهد. ثانیاً دسترسی بدخواهانه به یک سیستم کامپیوتری، نرم‌افزار یا داده را نیز می‌تواند در معرض انهدام قرار دهد. و نـهایتاً یک دسـترسی غـیرمجاز مـمکن است سرویس‌دهی به یک کاربر درست و حسابی را نیز مانع شود. برای مثال کاربری که در یک لحظه بحرانی برای انجام کاری نیـاز به سیستم دارد، ممکن است منتظر در دسترس قرار گرفتن مـنابع

محاسباتی بماند . بنابر این بایستی از دسترسی غیر مجاز به سیستمهای کامپیوتری ممانعت بعمل آید .

اشخاص کلیدی: نهایتاً اشخاص می‌توانند نقاط ضعف بزرگی برای ایمنی باشند. اگر تنها یک نفر بداند که چگونه می‌توان از برنامه نگهداری یا استفاده کرد، در این صورت اگر او دچار بیماری شود، اتفاقی برای او بیفتد یا کار را رها کند،اشکالاتی بوجود خواهد آمد. افراد قابل اعتماد بعنوان اپراتورها یا برنامه‌نویسان سیستم بایستی به دقت انتخاب شوند چون توانایی بالقوه‌ای برای اثرگذاری روی همهٔ کاربران سیستم دارا می‌باشند.

۵-۳-۲- اشخاص گرفتار شده

همانطور که دیده اید افراد شرور و بدکار معمولاً لباسهای کهنه‌ای می‌پوشند، نگاههای شیطانی و هدفداری دارند و همراه جنایتکاران در خارج از شهر زندگی می‌کنند. در مقابل مردان شریف بخوبی لباس می‌پوشند، سربلند می‌ایستند و در شهر برای همه شناخته شده می‌باشند و ترسی از حمله جنایتکاران ندارند. برخی از تبهکاران کامپیوتری افراد پستی می‌باشند ولی اکثر آنها لباسهای فاخر می‌پوشند، درجه دانشگاهی دارند، و از ارکان اجتماع خود محسوب می‌شوند. اکثراً نوجوان یا دانشجوی دانشگاه می‌باشند. برخی از آنها مجریان میانسال تجارت می‌باشند. برخی از آنها از نظر روانی دیوانه می‌باشند و یا کاملاً متخاصم می‌باشند یا بشدت به هدف یا جنبشی سرسپرده می‌باشند و به کامپیوترها به عنوان سمبل حمله می‌برند. برخی دیگر مردمی هستند که وسوسه منافع شخصی، انتقام، رقابت، پیشرفت و یا امنیت شغلی آنها را فریفته است. صرفنظر از انگیزه‌های آنها، تبهکاران کامپیوتری دسترسی به مقادیر هنگفتی از سخت‌افزار، نرم‌افزار و داده‌دارند. آنها پتانسیل فلج کردن و از کار انداختن تجارت مؤثر و همچنین دولتها را در

جهان دارا می‌باشند.

اجازه بدهید جرم یا جنایت کامپیوتری را تعریف کنیم. در برخی کشورها پلیس، جرم و جنایت کامپیوتری را از جنایت‌های دیگر جدا نمی‌داند. بنابراین اکثر شرکتها جرمهای کامپیوتری را به دلایل عدیده به پلیس گزارش نمی‌کنند. ضرری که بابت جنایات و جرایم کامپیوتری تخمین زده شده است، سالانه بین سیصدمیلیون دلار تا پانصد میلیارد دلار می‌باشد. بیشتر کارشناسان معتقدند که ایمنی کامپیوتری یک مشکل اساسی می‌باشد. مطالعاتی برای تعیین مشخصات افرادی که جرایم کامپیوتری را مرتکب می‌شوند در حال انجام است. در این مطالعات برآنند که به کشف جرایم و شناسایی مجرمین و جلوگیری از آنها کمک کنند. در ذیل به برخی از افرادی که مرتکب جرایم کامپیوتری می‌شوند اشاره شده است.

مبتدیان: مبتدیان بیشترین جرایم گزارش شده در این زمانه را مرتکب شده‌اند. بیشترین اختلاسها را نه مجرمین حرفه‌ای بلکه مردم عادی که به نقصی در امنیت سیستم پی برده‌اند، که به آنها اجازه می‌دهد به پول یا چیزهای قیمتی دیگر دسترسی یابند،مرتکب می‌شوند. بدین لحاظ بیشتر مجرمین کامپیوتری کاربران عادی کامپیوتر هستند که زمانی متوجه می‌شوند که می‌توانند به چیز باارزشی دسترسی یابند که دارند کارهای خود را انجام می‌دهند. مبتدیان ممکن است استفاده از کامپیوتر را برای نامه‌نگاری یا انجام محاسبات شروع کنند. این وضعیت ممکن است تا وقتی ادامه یابد که کارمندی در حال انجام محاسبات تجاری باشد، یا سهامی را به موجودی بیافزاید، یا با استفاده از امکانات کامپیوتری کارمندان، در حال چاپ اوراق بهادار باشد. در این حال مبتدی ممکن است بخاطر موقعیت شغلی منفی خود ناراحت شود و با خود عهد کند که بوسیله خراب کردن سیستم کامپیوتری انتقام بگیرد. نکته‌ای که دربارهٔ تبهکاران مبتدی وجود دارد اینست که آنها زمینه علمی و فنی خیلی ضعیفی دارند که این مسئله کمتر منجر به مشکوک شدن به آنها می‌شود.

افراد Hacker : این افراد معمولا دانش آموزان دبیرستانها یا دانشجویان دانشگاهها میباشند که مبادرت به دسترسی به امکانات محاسباتی غیر مجاز می کنند . نقطه مشترک اینان گرایش و رفاقت آنان با چند دوست می باشد، که این مسئله مزاحمت آنان را دو چندان میکند . آنها اکثرا با هوش میباشند ولی شفاها قادر به ابراز این هوش به مردم نیستند . آنها بجای مردم به کامپیوترها رو می آورند و می دانند که کامپیوترها آنها را از خود طرد نمیکنند و بنابراین کامپیوترها وسیله سربلندی اجتماعی آنان را فراهم می کنند. شکل دیگری از روابط اجتماعی استفاده از امکانات مخابراتی Bulletin Board میباشد، که دارای دیوار الکترونیکی ایمن و محفوظی میباشد.

رخنه کردن در استحکامات کامپیوتری یکی از جرایم بدون تلفات می باشد . هیچکس زخمی یا کشته نمی شود حتی اگر در حال ایجاد ارتباط با کامپیوتر دیده شود. اکثر رخنه ها می تواند بدون روبرو شدن با شخصی و یا حتی بدون شنیدن صدای انسانی انجام شود . افراد Hacker در صورت عدم وجود هشدارهای آشکار در موقع نفوذ به سیستم ، خیال میکنند که دسترسی به سیستم مجاز می باشد. شبکه ای از افراد Hacker برای عبور موفق از قسمتهای سری به مانند چند قطعه ایزوله کوچک که برای ایجاد یک اثر بزرگ گرد هم جمع شده اند، به همدیگر کمک می کنند.

رخنه به سیستمهای کامپیوتری یک خطر جدی است که ممکن است میلیونها دلار ضرر ببار آورد، لذا رخنه کنندگان بایستی قانونا جریمه های هنگفتی را بپردازند.

مجرمین حرفه ای :در مقابل مبتدیان و افراد Hacker ، جنایتکاران کامپیوتری حرفه ای هدف از جرم کامپیوتری را به خوبی درک کرده اند . تبهکاران حرفه ای، میدان کار خود را از آتش زدن ، نابودی و سرقت به محاسبه تسری داده اند.

همانگونه که قبلاً اشاره شد برخی از شرکتها در پیگیری مجرمین کامپیوتری محتاط هستند. در حقیقت پس از کشف یک جرم کامپیوتری، اگر مجرم بی سر و صدا کناره گیری کند یا استعفا

بدهد، شرکتها ممنون خواهند شد و بنابراین مجرم آزاد خواهد بود که همان کارهای غیرقانونی را در شرکتهای دیگر ادامه دهد.

۴-۲- روشهای دفاع

شکی نیست که جرایم کامپیوتری ادامه می یابند. هدف ایمنی کامپیوتری برقرار نمودن کنترلهایی است که سری بودن ، درستی و در دسترس بودن را حفظ کند. گاهی اوقات این کنترلها قادر به جلوگیری از حملات هستند . روشهای ضعیفتر فقط می توانند یک رخنه را در هنگام وقوع یا پس از وقوع آن تشخیص دهند [۳] .

۱-۴-۲- کنترلها

در این بخش ما به بررسی کنترلهایی می‌پردازیم که قصد جلوگیری از سوء استفاده از نقاط آسیب‌پذیر سیستمهای کامپیوتری را دارند.

رمزنگاری: قویترین ابزار در مهیا نمودن امنیت کامپیوتری، رمزکردن می‌باشد. به این دلیل که در هنگام نقل و انتقال دیتا، برای شاهدان خارجی پیچیده و نامفهوم می‌باشد. همچنین جلوگیری و احتمال تغییر و تحریف دیتا را بی‌تأثیر می‌کند. رمزنگاری برای داده‌ها سری بودن را مهیا می‌کند. بعلاوه از آنجاییکه دیتایی که خوانده نشود، عموماً تغییر نیز نمی‌کند، می‌تواند برای نیل به درستی اطلاعات نیز استفاده شود. از این گذشته، رمزنگاری در پروتکل‌هایی که سری عملیاتی را برای به انجام رساندن کاری ترتیب می‌دهند، دارای اهمیت می‌باشد. برخی پروتکل‌ها دسترسی به منابع را تضمین می‌کنند. بنابراین رمزنگاری در مرکز روشهای تضمین هر سه هدف ایمنی کامپیوتری قرار دارد. رمزنگاری یک ابزار مهم در ایمنی کامپیوتری می‌باشد، اما نباید خیلی به یک چیز اهمیت داده شود. کاربران بایستی بدانند که رمزنگاری همهٔ مسائل و مشکلات ایمنی کامپیوتری را حل نمی‌کند. از این گذشته اگر رمزنگاری به طرز مناسبی استفاده نشود،آنگاه هیچ

تأثیری در امنیت نخواهد داشت و در حقیقت کارآیی کل سیستم را نیز کاهش خواهد داد. بنابراین مهم این است که بدانیم در چه مواقعی رمزنگاری مفید و مؤثر می‌باشد.

کنترلهای نرم‌افزاری: برنامه‌ها خود می‌توانند دومین حلقه زنجیر ایمنی کامپیوتری باشند. برنامه‌ها بایستی در مقابل حملات خارجی به اندازه کافی امن باشند. همچنین بایستی به گونه‌ای توسعه یافته و نگهداری شده باشند که فرد بتواند به قابلیت اطمینان برنامه دلگرم باشد. کنترلهای برنامه شامل انواع زیر است:

۱- کنترلهای پیاده سازی و توسعه،که استانداردهایی هستند که تحت آنها یک برنامه طراحی، کد، تست و نگهداری می شود. مطابق این استانداردها،در موقع پیاده سازی نرم افزاری سیستم های کاربردی بایستی کنترلهایی برای جلوگیری از دسترسی غیر مجاز قرار داده شود[۴].

۲- کنترلهای سیستم عامل،که محدودیتهای ایجاد شده توسط سیستم عامل برای حفاظت هر کاربر از دیگر کاربران میباشد.این دسته از کنترلها در سطح سیستم عامل اعمال میشود و حداقل امنیت لازم بایستی در این سطح قرار بگیرد [۵].

۳- کنترلهای داخلی برنامه،که محدودیتهای امنیتی را، از قبیل محدودیت دسترسی در برنامه های مدیریت پایگاههای داده به اجرا می گذارند.این دسته از کنترلها آخرین سطح کنترل لازم برای برقراری امنیت میباشند که در داخل برنامه ها و زیربرنامه ها بکار گرفته میشوند [۶].

کنترلهای نرم‌افزاری ممکن است بعنوان ابزارهایی مانند اجزاء سخت‌افزاری، رمزنگاری یا گردآوری اطلاعات بکار گرفته شوند. معمولاً کنترلهای نرم‌افزاری مستقیماً کاربران را تحت تأثیر قرار می‌دهند و بنابراین اولین نمود ایمنی کامپیوتری هستند که به نظر می‌رسند. از آنجاییکه کنترلهای نرم‌افزاری راههای محاوره کاربران با سیستمهای کامپیوتری را تحت تأثیر خود قرار می‌دهند، لذا بایستی خیلی دقیق طراحی شوند. معمولاً سادگی کاربرد و توانایی از جمله هدفهایی می‌باشند که در طراحی کنترلهای نرم‌افزاری مدنظر قرار دارند.

کنترلهای سخت‌افزاری: دستگاههای سخت‌افزاری زیادی برای مساعدت در ایمنی کامپیوتری ساخته شده‌اند. این دستگاهها از پیاده‌سازی سخت‌افزاری رمزنگاری تا ممانعت از دسترسی متجاوزان به دستگاهها برای تعیین هویت کاربران را شامل میشوند.

مصلحت اندیشیها: برخی کنترلها، حاصل جمع‌بندی روشهای سخت‌افزاری یا امکانات نرم‌افزاری ذکر شده فوق می‌باشند. کنترلهای دیگر ذاتاً سیاسی می‌باشند. در حقیقت برخی از ساده‌ترین کنترلها، از قبیل تعویض مکرر کلمات عبور (Password)، می‌توانند بدون هیچ هزینه‌ای انجام شوند، اما اثرات فاحشی را برجای گذارند. کنترلهای قانونی و اخلاقی بخش مهمی از امنیت کامپیوتری هستند. قانونها خیلی کند تصویب می‌شوند ولی برعکس تکنولوژی کامپیوتر به طور ناگهان پدیدار می‌شود. اگرچه حفاظت قانون مورد نیاز و پسندیده می‌باشد، اما در این زمینه به خوبی اکثر جرایم شناخته شده دیگر قابل اطمینان نمی‌باشد. زمینه اخلاقیات کامپیوتر خیلی واضح و آشکار نیست، نه به این معنی که مردان کامپیوتر ضد اخلاقند، بلکه بدین معنی که مانند اخلاقیات عامه مردم، اخلاق کامپیوتری در فرمهای استانداردی از آداب و رسوم اخلاقی تعریف نشده است. هنوز در اکثر کشورها تعریف واضحی برای جرم و جنایت کامپیوتری وجود ندارد و قوانین مناسبی برای دادن جزای مناسب به جرایم کامپیوتری تصویب نشده است. [۷] این مسئله نیز مهم است که، قبل از قانونی کردن اخلاق، به طور گسترده‌ای آن خلق و خو پذیرفته شده و بنابراین مؤثر می‌باشد، و انجمن کامپیوتر و اجتماع عمومی نیاز به درک این دارد که بداند چه انواعی از آداب و رسوم نامناسب می‌باشند و چرا؟

کنترلهای فیزیکی: یکی از ساده‌ترین، اما مؤثرترین و کم هزینه‌ترین کنترلها، کنترل فیزیکی است. کنترل فیزیکی شامل قفل درب‌ها، نگهبانی در مبادی ورودی، نسخه‌های پشتیبان از

نرم‌افزارها و اطلاعات مهم و طراحی فیزیکی سایت‌ها در جهت کاهش خطرات ناشی از حوادث طبیعی می‌باشد. اغلب کنترلهای فیزیکی ساده، در مواقعی کـه روشـهای پـیچیده‌تری اسـتفاده می‌شوند، به فراموشی سپرده می‌شوند.

۲-۴-۲- بررسی تاثیر کنترلها

برخورداری از روشهای کنترل، در صورتی که بخوبی استفاده نشوند، کفایت نمی کنـد. در این بخش نگاهی اجمالی به برخی عوامل مؤثر بر کنترل خواهیم انداخت.

اطلاع از مسائل و مشکلات: کسانی که از روشهای کنترلی استفاده می‌کنند بـایستی نسبت به نیاز به امنیت متقاعد شده باشند. فقط در صورتی که مردم بدانند در هر موقعیتی به چه علت امنیت مورد نیاز می‌باشد، آنگاه مایل به همکاری با نیازهای امنیتی خواهند بود. اما برخی از کاربران از لزوم نیاز به امنیت آگاه نیستند . مخصوصا در موقعیتهایی که یک گروه جدیدا عهده دار وظائف محاسباتی شده اند که قبلا توسط یک قسمت کامپیوتری مرکزی انجام میشده است.

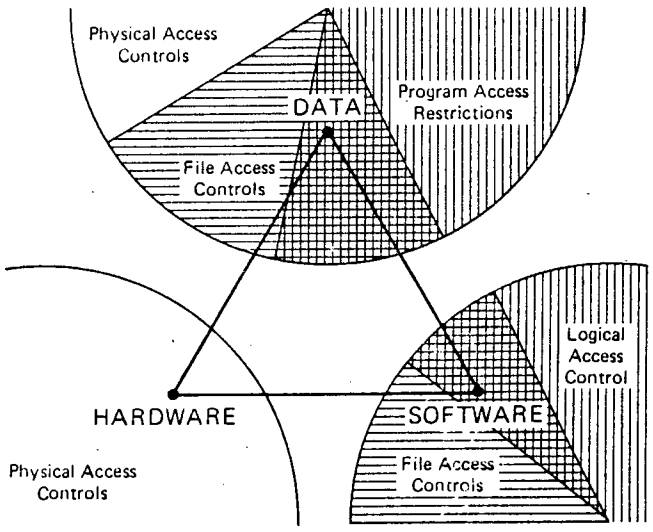
لزوم استفاده: مسلم است که روش کنترلی قبل از استفاده مؤثر نخواهد بـود. قـفل موجود روی درب اطاقهای کامپیوتری، در صورتی که افراد دربها را باز بگذارند، بی‌فایده خواهد بود. در طول جنگ جهانی دوم، منشی‌های رمزکننده اطلاعات از کدهای منسوخ و قدیمی استفاده می‌کردند، آنهم فقط به خاطر اینکه آنها را خوب یادگرفته بودند و می‌توانستند پیغامها را سریع رمز کنند. متاسفانه ، جبهه مخالف برخی از آن رمزها را شکسته بود و بنابراین می توانست براحتی پیغامها را از رمز خارج کند. این موضوع اصل مؤثر بودن را ببار می آورد :

اصل مؤثر بودن: کنترلها بایستی استفاده شوند تا مؤثر افتند. آنها بایستی مؤثر، سـاده

برای استفاده و مناسب باشند.

این قانون به ما می‌گوید که کنترلهای ایمنی کامپیوتری بایستی از نظر زمان، فضای حافظه مورد نیاز، فعالیت انسانی، یا سایر منابع مورد استفاده به اندازه کافی مؤثر باشند. بنابراین کسی که از یک روش کنترلی استفاده می‌کند، نباید کار حفاظت شده‌اش متأثر از روش کنترلی باشد. کنترلها باید به گونه‌ای انتخاب شوند که از دسترسی مجاز و قانونی مانع نشوند.

اشتراک کنترلها: ممکن است چند روش کنترلی مختلف برای جلوگیری از یک افشاء بکار برود. برای مثال امنیت ایجاد شده برای یک برنامهٔ کاربردی در ریزکامپیوتر ممکن است به وسیله ترکیبی از کنترلهای دسترسی برنامه به داده دسترسی فیزیکی به ریزکامپیوتر و حافظه‌های جانبی، و حتی به وسیله قفل کردن فایلها در مقابل دسترسی به برنامه‌های پردازشی، فراهم شده باشد. این مورد در شکل ۵-۲ نمایش داده شده است.



شکل (۵-۲) اشتراک کنترلها

بازدید متناوب: روشهای کنترلی به صورت دائمی مؤثرند. درست وقتی که متخصص ایمنی راهی را برای امنیت منابعی در مقابل انواعی از خطرات پیدا می‌کند، طرف مخالف کوشش خود را در شکست‌دادن مکانیزم امنیت دوبرابر می‌کند. بنابراین تشخیص میزان تأثیر روش کنترلی، یک کار مداوم باشد.[۸]

۵-۲- خلاصه

در این فصل ، جنبه های مهم ایمنی در سیستم های کامپیوتری بیان گردید. ضمن بیان مسائل مهم ایمنی در کامپیوترها ، کنترل هایی که در مقابل آن مسائل مؤثر می باشند ، ذکر گردیدند . ایمنی کامپیوتری بایستی سری‌بودن، کامل بودن و در دسترس بودن مؤلفه‌های سیستم کامپیوتری را بیمه کند. سخت‌افزار، نرم‌افزار و داده سه قسمت مهم از سیستمهای کامپیوتری می‌باشند، که مورد حمله قرار می‌گیرند. این سه قسمت و ارتباطات بین آنها نقاط اساسی آسیب‌پذیر سیستمهای کامپیوتری را تشکیل می‌دهند. در این بخش چهار نوع حمله به سیستمهای کامپیوتری شناسایی شد: وقفه، نشت ، تغییر و ساخت.

سه قاعده در برقراری ایمنی کامپیوتری بایستی مد نظر باشد. اصل ساده‌ترین نفوذ می‌گوید: یک رخنه‌کننده به سیستم کامپیوتری از ساده‌ترین وسیله برای حمله استفاده می‌کند. بنابراین همهٔ جنبه‌های ایمنی سیستمهای کامپیوتری بایستی یکجا در نظر گرفته شوند و نکته‌ای فراموش نشود. اصل ارزش زمانی می‌گوید: سیستم تا زمانی نیاز به حفاظت دارد که نفوذ برای نفوذکننده ارزش داشته باشد. اصل مؤثر بودن می‌گوید: روشهای کنترلی بایستی قابل استفاده باشند و همچنین به کار گرفته شوند تا اثر لازم را داشته باشند.

کنترلها در سطوح مختلفی از داده، برنامه‌ها، سیستم، دستگاههای فیزیکی، ارتباطات مخابراتی، محیط و پرسنل می‌تواند اعمال شود. گاهی اوقات چند روش کنترلی برای پوشش دادن

به یک نقطه آسیب‌پذیر مورد نیاز است و گاهی اوقات نیز یک روش کنترلی چند قسمت را به طور همزمان اداره می‌کند.

فصل سوم

روشهای ایجاد امنیت

این فصل به بررسی برخی از روشهای سرّی کردن اطلاعات[۹]و روشهای تصدیق اعتبار و صحت می‌پرداز د. در مواردی که افراد غیر مجاز امکان دسترسی به اطلاعات را داشته باشند، برای جلوگیری از پی بردن به ماهیت اطلاعات، رمزنگاری بهترین و مؤثرترین روش میباشد. اگر مسئله، قرار دادن کنترل در دسترسی به اطلاعات باشد، و یا دشمن امکان تغییر اطلاعات دستکاری شده را نیز داشته باشد، در این صورت بحث روشهای تصدیق اعتبار و صحت مطرح می شود. در پایان این قصل روشهای پیشنهادی برای رمزنگاری بررسی خواهند شد.

۱-۳- روشهای رمز کردن اطلاعات

۱-۱-۳- رمزهای کلاسیک

۱-۱-۱-۳- رمزهای جایگزینی(۱) تک الفبایی

در سیستمهای جایگزینی تک الفبایی، یک حرف با حرف دیگری عوض می شود . از جمله این روشها می توان سیستمهای زیر را نام برد:

سیستم رمز جمع‌شونده: در این روش به هر حرف شماره‌ای اختصاص می‌یابد و به ازای هر حرف، حرفی را در نظر می‌گیرند که مقداری جلوتر از آن است. به عنوان مثال برای حرف

(1) Substitution

iام حرف j+iام را در نظر می‌گیرند و jدر حقیقت کلید رمز سیستم می‌شود.

سیستم رمز ضرب شونده : این سیستم از ضرب یک عدد که نسبت به تعداد حروف الفبای مورد نظر اول باشد در شماره حروف به رمز دست می یابد. اگر z تعداد حروف الفبا و a ضریب مورد نظر باشد ، برای رمزگذاری:

$$E: i \rightarrow (a*i) \bmod z$$

و برای رمزگشایی:

$$D: i \rightarrow (a^{-1}*i) \bmod z$$

رمز الفبای درهم: این حالت عام سیستمهای تک‌الفبایی است. در این سیستم هر حرف را با حرف متناظری نگاشت می کنیم. کلیدی وجود ندارد ، بلکه کل نگاشت را برای تحلیل باید بدست آوریم.

۲-۱-۱-۳- رمزهای جایگشتی(۱)

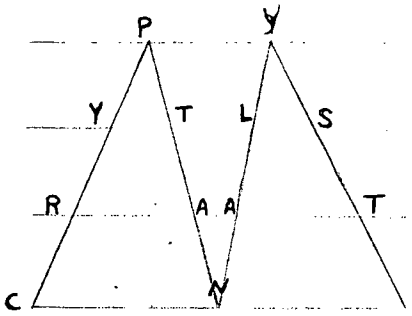
در روشهای جایگشتی ترتیب حروف عوض می‌شود نه خود حروف. از جمله این روشها می‌توان سیستمهای زیر را نام برد:

سیستم جایگشتی تک‌الفبایی: در این رمزها یک پریود تعریف می‌کنیم. به عنوان مثال برای یک دوره تناوب d=4 و یک ترتیب ستونهای f=(2,4,1,3) متن اصلی CRYPTANALYST به متن رمز RPCYAATNYTLS تبدیل می‌شود. در این روش حروف هر مجموعه چهارتایی از متن اصلی طبق f قرار می‌گیرند. با توجه به اینکه فراوانی حروف در متن اصلی و متن رمز یکسان است، از خصوصیت آماری زبان می‌توان برای تحلیل رمز استفاده کرد.

---

(1) Permutation

سیستم رمز مثلثی: در این سیستم عمق پله، کلید رمز سیستم می‌باشد. برای مثال فوق داریم:



Py

YTLS

RAAT

CN

بنابراین رمز شدهٔ کلمهٔ اصلی ، کلمهٔ **PYYTLSRAATCN** خواهد شد .

۳-۱-۱-۳- رمزهای چند الفبایی

در سیستمهای چند الفبایی ، یک حرف به چند حرف دیگر تبدیل می شود . بعبارت دیگر هر حرف ، در هر بار تبدیل ، به حرفی تبدیل میشود که ممکن است در بار قبل تبدیل نشده باشد . بعنوان مثال حرف T یکبار به a و بار دیگر به b تبدیل میشود . از جمله این سیستمها روشهای زیر را می توان نام برد :

رمز ویژنر (vigenere) : در این سیستم رمز، کلید رشته‌ای از حروف است. d پریود سیستم رمز است و تابعی که برای تبدیل هر حرف به کار می‌رود به d بستگی دارد.

$$f_i(a)=(a+K_i) \bmod n$$

رمز بیوفورت: این سیستم مشابه سیستم قبلی است، با این تفاوت که در اینجا از تفاضل استفاده می‌شود.

$f_i(a)=(K_i-a) \mod n$

$f^{-1}{}_i(c)=(K_i-c) \mod n$

نوع دیگری از رمز بیوفورت به شکل زیر است:

$f_i(a)=(a-K_i) \mod n$

در سیستمهای چندالفبایی هر چه d را بیشتر کنیم، شکستن رمز مشکلتر می‌شود. اگر طول کلید به اندازه طول پیام باشد، سیستم امن است. به این سیستمها Running Key می گویند.

به عنوان مثال می‌گوییم این کتاب کلید رمز است. کتاب را باز کرده و از ابتدا هر حرف را با حرف متناظر پیام با یکدیگر جمع می‌کنیم.

سیستمهایی که بررسی نمودیم یک حرف را به حرف دیگری تبدیل می‌کردند. می‌توان از تبدیل دو حرف به دو حرف دیگر نیز استفاده کرد. برای این منظور روشهای زیر وجود دارنـد که به دلیل اختصار تنها به ذکر نام آنها بسنده می کنیم :

۱) Play Fair Cipher

۲) Hill Cipher

۳) ماشینهای الکترومکانیکی

از یک دیدگاه دیگر سیستمهای رمز به دو گروه تقسیم می شوند :

▣ **سیستم رمز قطعه‌ای:** در آنها پیام به چند قسمت شکسته می‌شود و هر قطعه با یک قطعه دیگر جایگزین می‌شود. در این سیستمها کلید برای کلیه قطعات مشترک است.

▣ **سیستم رمز رشته‌ای:** در این سیستمها پیام به صورت دنباله‌ای از حروف مد نظر قرار می‌گیرد و هر یک از حروف با کلید مخصوص خود به حرف دیگری تبدیل می‌شود.

در سیستمهای رمز چندالفبایی اگر d را کوتاه بگیریم، سیستم شبیه سیستم رمز قطعه‌ای خواهد شد و هر چه طول d بزرگتر باشد، شبیه سیستم رمز رشته‌ای خواهد بود.

۲-۱-۳- رمزهای مدرن

این سیستمها به دو دسته متقارن و نامتقارن تقسیم می‌شوند. در ذیل به برخی از روشهای مورد استفاده در این سیستمها اشاره می‌شود.

۱-۲-۱-۳- سیستمهای رمز رشته ای (Stream Cipher)

یکی از سیستمهای رمز مدرن استفاده از XOR است. یک سیستم رمز دنباله‌ای را در نظر بگیرید:

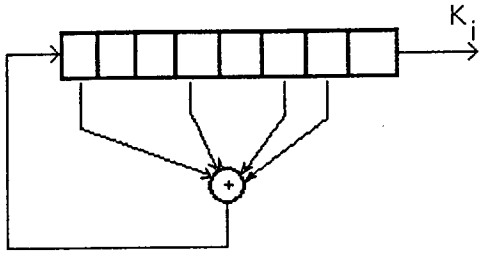
$m_i \oplus k_i = c_i$

که در اینجا k_i ، کلید می باشد.

شکل ۱ - ۳ سیستم رمز دنباله‌ای

اگر دنباله K_i پریودیک باشد، سیستم رمز پریودیک است. و اگر غیرپریودیک باشد، سیستم رمز غیرپریودیک می‌باشد. برای اینکه در اینجا One - time - pad داشته باشیم، باید دنباله کلید را کاملاً Random تولید کنیم. مشکل موجود این است که اگر دنباله اولی کاملاً اتفاقی باشد، مولد دومی نمی‌تواند دقیقاً همان دنباله را تولید کند. برای اینکه دو دنباله مشابه باشند، از دنباله‌های Pseudo Random استفاده می‌کنند [۱۰] که به یک هسته اولیه وابسته است. برای این کار یک هسته (Sead) یا کلید اولیه وارد مولد می‌کنند و مولد شروع به تولید دنباله کلیدها می‌کند. در مولد رمزگشا کافی است همان کلید اولیه را وارد کنیم تا دنباله‌ای مشابه دنباله اول تولید شود.

به عنوان مولد یک LFSR (Linear Feedback Shift Register) را در نظر بگیرید. تعدادی از خانه‌های رجیستر با هم جمع شده و به ورودی فرستاده می‌شود. این سیستم از نظر ویژگیهای آماری بسیار خوب است.

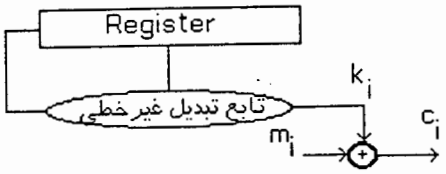


شکل (۲ - ۳) یک LFSR برای تولید دنباله کلیدها

چند جمله ای P(x) که رابطه ایجاد کننده سری کلیدهای شبه اتفاقی است ، باید Primitive باشد تا بتواند 2^n حالت را ایجاد کند .

مثلاً اگر رجیستر را ۵ بیتی در نظر بگیریم و $P(x) = x^4 + x + 1$ باشد، یعنی خانهٔ صفرم، یکم و چهارم را جمع کرده و به ورودی رجیستر بدهیم، به این ترتیب کل ۳۲ حالتی را که رجیستر می‌تواند داشته باشد بوجود آورده‌ایم.

اشکالی که این سیستم دارد این است که فیدبک یک تابع خطی است. برای رفع این اشکال می توان یک تابع تبدیل غیر خطی برای انتخاب بیت های ترکیب شونده رجیستر را مورد استفاده قرار داد .



شکل (۳ - ۳) استفاده از تابع تبدیل غیرخطی برای ایجاد دنباله کلید

۲-۲-۱-۳- سیستمهای رمز بلوکی

سیستم رمز بلوکی (قطعه‌ای) یک بلوک از متن پیام راگرفته و یک بلوک از متن سری تحویل می دهد . شانون به این نتیجه رسید که برای اینکه سیستم رمز خوب باشد ، باید عمل تبدیل را بصورت بی قاعده انجام داد [۱۱] .

برای اینکار تبدیل مخلوط کننده را معرفی کرد. در این سیستم مجموعه‌ای از تبدیلات ساده که در هم ادغام شده‌اند مورد استفاده قرار می‌گیرد. فرم کلی تابع عملی رمز در اینگونه سیستم‌ها به شکل زیر است:

$F = f_1 \circ f_2 \circ \ldots\ldots \circ f_n$

معمولاً سیستم‌های رمزنگاری موجود از شبکه‌ای از این توابع استفاده می‌کنند که یک مرحله عمل جانشینی (جایگزینی) و مرحله دیگر عمل جایگشت را انجام می‌دهد. اینها سیستم‌های رمز با کیفیت خوب و قوی هستند.

مثال: EXAMPLE

پس از جانشینی کلمهٔ فوق به کلمه رمز زیر تبدیل می شود :

FYBNQMF

و نهایتا پس از جایگشت ، کلمهٔ رمز زیر بدست می آید :

BFQYFNM

روشهای مختلفی برای رمزنگاری بصورت مدرن از جمله RSA [1] و DES مطرح شده است . برای آشنایی در اینجا روش DES [۹] مطرح می شود .

۱-۲-۲-۱-۳- معرفی DES

الگوریتم رمزنگاری استفاده شده در اغلب واحدهای رمزنگاری، سیستم رمزنگاری استاندارد NBS[2] یا DES است. این الگوریتم برای مراکز غیرنظامی توصیه شده است. بمنظور

---

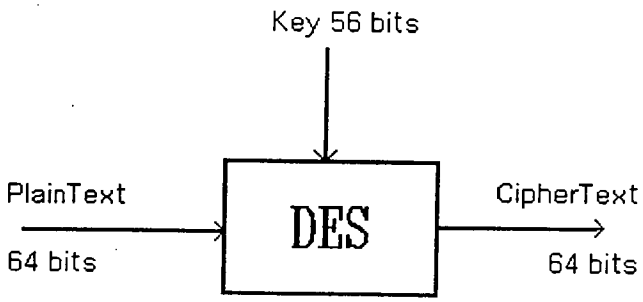
(1)Rivet Shamir Adelman

(2)National Bureau of Standard

تأمین ایمنی در سیستم‌های کامپیوتری نیاز به داشتن سخت‌افزار مناسب در رمزنگاری می‌باشد، که اگر این سخت‌افزار به شکل یک مدار مجتمع در یک تراشه قرار گیرد قابلیت زیادی پیدا می‌کند. از جمله اینکه روی برد سخت‌افزار بعنوان یک بلوک رمزکنندهٔ داده مورد استفاده قرار می‌گیرد.

DES از مهمترین و معروفترین سیستم‌های رمزنگاری قالبی است. در سال ۱۹۷۷ این سیستم توسط ادارهٔ ملی استانداردها(NBS)عرضه شد که با سیستم اصلاحی Lucifer - که بوسیله IBM بسط داده شده بود - تطبیق گردید.

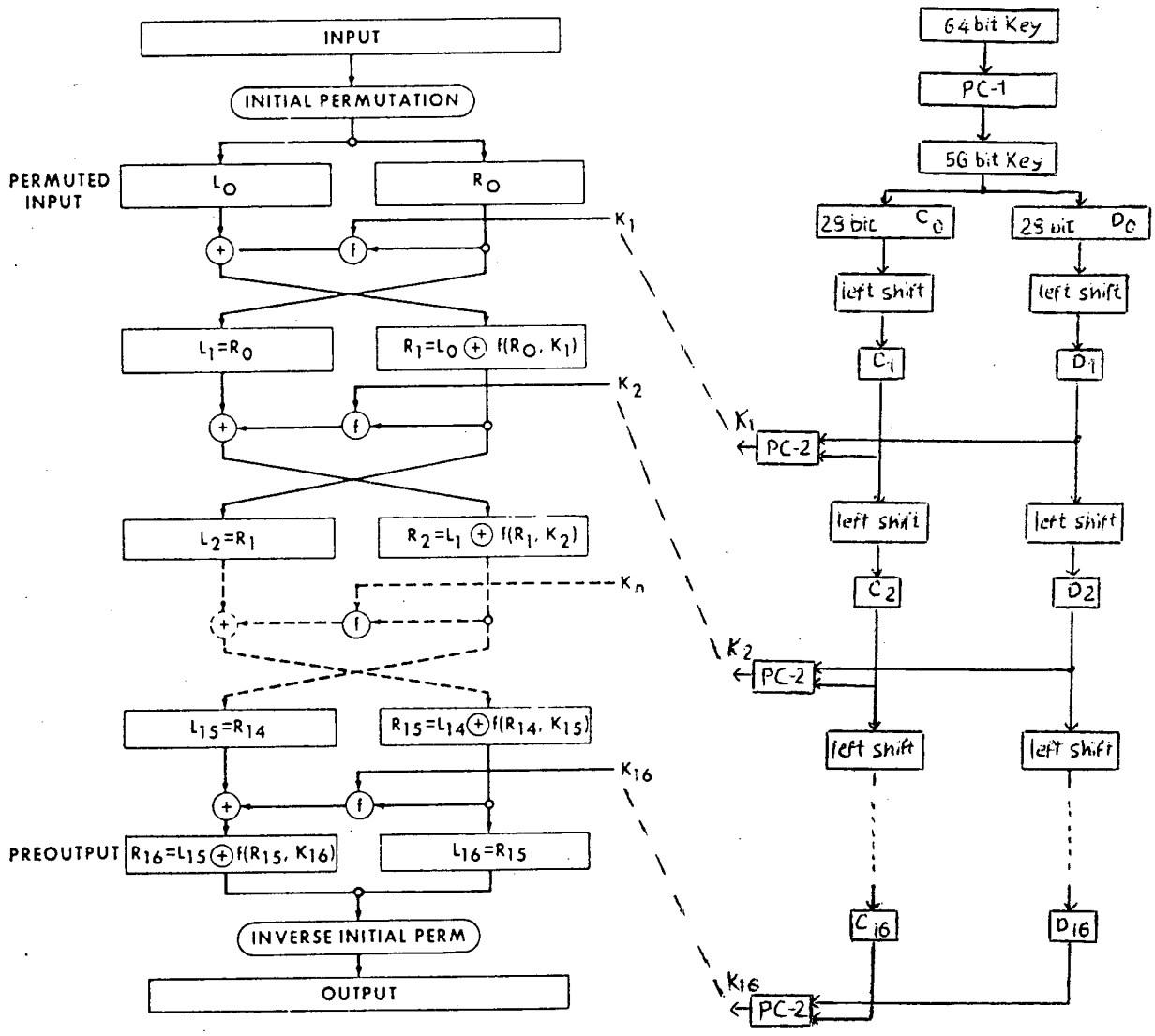
DES برای رمزکردن اطلاعات حساس و غیر طبقه‌بندی شده پیشنهاد گردیده است. اعتبار سیستم حدود ۱۰ تا ۱۵ سال از زمان طراحی تضمین شده بود. لیکن همچنان DES بعنوان یک زمینه تحقیقاتی ارزش خود را حفظ کرده است. DES را می توان بعنوان یک رمزنگار قالبی با سایز الفبای 2^{64} سیمبل تلقی کرد، که بلوک دیاگرام آن در شکل ذیل نشان داده شده است:



شکل (۴ - ۳) بلوک دیاگرام DES

جزئیات مربوط به الگوریتم DES و سیستم تابع بلوک دیاگرام در شکل ۵-۳ نشان داده

شده است. این الگوریتم با یک کلید ۵۶ بیتی پارامتریک می‌شود و دارای ۱۹ طبقه است. اولین طبقه یک Initial Permutation از متن اصلی ۶۴ بیتی می‌باشد.



شکل (۵-۳) جزئیات DES

۵۸	۵۰	۴۲	۳۴	۲۶	۱۸	۱۰	۲
۶۰	۵۲	۴۴	۳۶	۲۸	۲۰	۱۲	۴
۶۲	۵۴	۴۶	۳۸	۳۰	۲۲	۱۴	۶
۶۴	۵۶	۴۸	۴۰	۳۲	۲۴	۱۶	۸
۵۷	۴۹	۴۱	۳۳	۲۵	۱۷	۹	۱
۵۹	۵۱	۴۳	۳۵	۲۷	۱۹	۱۱	۳
۶۱	۵۳	۴۵	۳۷	۲۲	۲۱	۱۳	۵
۶۳	۵۵	۴۷	۳۹	۳۱	۲۳	۱۵	۷

جدول (۳ - ۱) Initial Permutation (IP) در DES

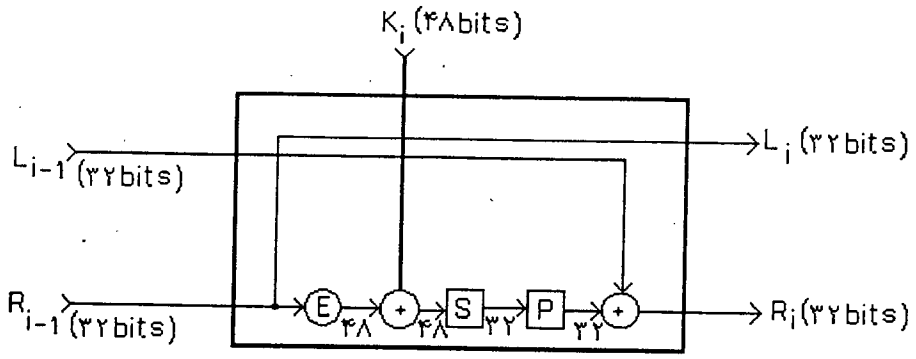
مطابق جدول ۳ - ۱ بیت‌های متن اصلی طبق الگوی موجود در این جدول جابجا می‌شوند یعنی:

متن اصلی IP Initial Permutation

$x_1\ x_2\ x_3 \ldots x_{64} \rightarrow x_{58}\ x_{50}\ x_{42} \ldots x_7$

بعد از این تبدیل قلب الگوریتم رمزنگاری از ۱۶ تکرار با استفاده از SBB (Standard Building Block) شروع می‌شود: SBB، ۴۸ بیت کلید را برای تبدیل ورودی ۶۴ بیتی استفاده می‌کند که ورودی با ۳۲ بیت سمت راست و چپ مشخص شده است.

خروجی هر SBB برای دیگری ورودی است. ۳۲ بیت سمت راست (R_i - 1) عیناً در ۳۲ بیت سمت چپ (L_i) کپی می‌شوند.



شکل (۶-۳) بلوک دیاگرام SBB (Standard Building Block)

سپس $R_i - 1$ به ۴۸ بیت توسعه می‌یابد (با استفاده از جدول ۲-۳) آنگاه با ۴۸ بیت کلید X - OR می‌گردد.

$$R_i - 1 = x_1\ x_2 \ldots\ldots x_{32}$$

$$E(R_i - 1) = x_{32}\ x_1\ x_2 \ldots\ldots x_1$$

دقت کنید بیتهای لیست شده در ستونهای اول و آخر جدول ۲-۳ موقعیت بیتهایی هستند که دوبار برای تبدیل ۳۲ به ۴۸ بیت استفاده می‌شوند.

$$E(R_i - 1) + K_i = B_1\ B_2 \ldots\ldots B_8$$

سپس $E(R_i - 1)$ با i_{th} کلید، که بعداً شرح داده خواهد شد، X - OR شده و نتیجه ۸ بلوک ۶ بیتی می‌باشد.

۳۲	۱	۲	۳	۴	۵
۴	۵	۶	۷	۸	۹
۸	۹	۱۰	۱۱	۱۲	۱۳
۱۲	۱۳	۱۴	۱۵	۱۶	۱۷
۱۶	۱۷	۱۸	۱۹	۲۰	۲۱
۲۰	۲۱	۲۲	۲۳	۲۴	۲۵
۲۴	۲۵	۲۶	۲۷	۲۸	۲۹
۲۸	۲۹	۳۰	۳۱	۳۲	۱

جدول (۳ - ۴) E - Table Bit Selection

هر کدام از این B_j ها بعنوان ورودی به S - box استفاده می‌شوند و تابع S - box یک خروجی ۴ بیتی باز می‌گرداند.

$[S_j(B_j)]$. بنابراین ۴۸ بیت ورودی به ۳۲ بیت خروجی توسط S - box ها تبدیل می‌شوند. جدول ۳ - ۳ توابع نگاشت این S - box ها را نشان می‌دهد. تبدیل $B_j = b_1\ b_2\ b_3\ b_4\ b_5\ b_6$ از این قرار است:

Row	Column 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

جدول (۳ - ۳) توابع انتخاب S - box

عدد صحیح مترادف با b_1 b_6 سطر و عدد صحیح متناظر با b_2 b_3 b_4 b_5 ستون را در جدول S - box (جدول ۴ - ۳) اختیار می‌کند. بطور مثال اگر $B_1 = 110001$،

سطر $11 = b_1\ b_6$ ← 3 و ستون $1000 = b_2\ b_3\ b_4\ b_5$ ← B که نشاندهندهٔ عدد ۵ می‌باشد که به شکل ۰۱۰۱ یعنی خروجی ۶ بیتی S - box می‌باشد. ۳۲ بیت خروجی S - box به یک P - box داده می‌شود که الگوی آن در جدول ۴-۳ داده شده است.

۱۶	۷	۲۰	۲۱
۲۹	۱۲	۲۸	۱۷
۱	۱۵	۳۳	۲۶
۵	۱۸	۳۱	۱۰
۲	۸	۲۴	۱۴
۳۲	۲۷	۳	۹
۱۹	۱۳	۳۰	۶
۲۲	۱۱	۴	۲۵

جدول (۴-۳) P - Table Permutation

خروجی P - box	جدول ۴-۳	خروجی S-box
$x_{16}\ x_7\ x_{20}.....x_{25}$	←	$x_1\ x_2.....x_{32}$

این خروجی ۳۲ بیتی با ۳۲ بیت سمت چپ ورودی $(L_i - 1)$، X - OR می‌شوند که در شکل ۶-۳ نشان داده شده است.

f تابعی است که بر حسب جدول E، S - box و P - box تنظیم می‌شود. پس از ۱۶ تکرار SBB نتیجه Swap می‌شود یعنی ۳۲ بیت سمت چپ و راست با هم عوض می‌گردند. سپس

نتیجه برای محاسبه نهایی برای وارون کردن به بلوک (IP^{-1}) Final Inverse Permutation

داده می‌شود که جدول ۵-۳ برای اینکار استفاده می‌شود.

۴۰	۸	۴۸	۱۶	۵۶	۲۴	۶۴	۳۲
۳۹	۷	۴۷	۱۵	۵۵	۲۳	۶۳	۳۱
۳۸	۶	۴۶	۱۴	۵۴	۲۲	۶۲	۳۰
۳۷	۵	۴۵	۱۳	۵۳	۲۱	۶۱	۲۹
۳۶	۴	۴۴	۱۲	۵۲	۲۰	۶۰	۲۸
۳۵	۳	۴۳	۱۱	۵۱	۱۹	۵۹	۲۷
۳۴	۲	۴۲	۱۰	۵۰	۱۸	۵۸	۲۶
۳۳	۱	۴۱	۹	۴۹	۱۷	۵۷	۲۵

جدول (۵-۳) (IP^{-1}) Final Permutation

برای Decrypt کردن از همین الگوریتم استفاده می‌کنیم، لیکن ترتیب بیت‌های کلید در SBB متفاوت می‌باشد.

انتخاب کلید (Key Selection)

انتخاب کلید در هر یک از ۱۶ تکرار انجام می‌شود. با توجه به شکل ۵-۳ کلید ورودی ۶۴ بیتی است که ۸ بیت آن توازن فرد می‌باشد[1]. که در موقعیت‌های ۸، ۱۶ و... و ۶۴ قرار داده شده‌اند. PC - 1 (permutation Choice 1) (جدول ۶-۳) بیتهای توازن را discard می‌کند و یک کلید ۵۶ بیتی درست می‌کند (بر طبق الگوی جدول ۶-۳).

1- Odd Parity

۵۷	۴۹	۴۱	۳۳	۲۵	۱۷	۹
۱	۵۸	۵۰	۴۲	۳۴	۲۶	۱۸
۱۰	۲	۵۹	۵۱	۴۳	۳۵	۲۷
۱۹	۱۱	۳	۶۰	۵۲	۴۴	۳۶
۶۳	۵۵	۴۷	۳۹	۳۱	۲۳	۱۵
۷	۶۲	۵۴	۴۶	۳۸	۳۰	۲۲
۱۴	۶	۶۱	۵۳	۴۵	۳۷	۲۹
۲۱	۱۳	۵	۲۸	۲۰	۱۲	۴

جدول (۶-۳) PC - 1 (Key Permutation)

خروجی ۵۶ بیتی PC - 1 به دو گروه ۲۸ بیتی تقسیم می‌شود که برای ایجاد کلیدهای ۴۸ بیتی مختلف در هر ۱۶ تکرار می‌باشد.

بلوک‌های C و D به ترتیب شیفت پیدا می‌کنند: $C_i = LS_i(C_i - 1)$

$D_i = LS_i(D_i - 1)$

LS_i ها تعداد شیفت‌ها را در هر کدام از ۱۶ تکرار مطابق جدول ۷-۳ می‌باشد. آنگاه C_i و D_i با PC - 2 (Permutation Choice 2) (طبق جدول ۸-۳) تبدیل می‌شوند و نتیجه خروجی ۴۸ بیتی K_i می‌باشد. DES غالباً بعنوان یک روش Code book تلقی می‌شود.

iteration	Number Of left Shifts
١	١
٢	١
٣	٢
٤	٢
٥	٢
٦	٢
٧	٢
٨	٢
٩	١
١٠	٢
١١	٢
١٢	٢
١٣	٢
١٤	٢
١٥	٢
١٦	١

جدول (٣-٧) Key Schedule Of Left Shifts

١٤	١٧	١١	٢٤	١	٥
٣	٢٨	١٥	٦	٢١	١٠
٢٣	١٩	١٢	٤	٢٦	٨
١٦	٧	٢٧	٢٠	١٣	٢
٤١	٥٢	٣١	٣٧	٤٧	٥٥
٣٠	٤٠	٥١	٤٥	٣٣	٤٨
٤٤	٤٩	٣٩	٥٦	٣٤	٥٣
٤٦	٤٢	٥٠	٣٦	٢٩	٣٢

جدول (٣-٨) Key Permatation Choice 2 (PC - 2)

معایب DES:

چون DES یک رمزنگار قالبی است بین قالب خروجی و ورودی تحت یک کلید ثابت یک تناظر یک به یک وجود دارد. یعنی با استفاده از این روش با داشتن یک بلوک ورودی متن اصلی همیشه یک خروجی رمز شده یکسان تحت کلید ثابت خواهیم داشت.

وجود این تناظر یک به یک از لحاظ رمزنگاری خطرناک است زیرا در صورتیکه قالب متن اصلی به هر دلیلی تکرار شود همان متن رمز شده قبلی را تولید می‌کند. اطلاعاتی که از تکرار متن رمزشده بدست دشمن بیفتد نقش مهمی در تحلیل ترافیک و آسیب‌پذیری سیستم رمزنگاری توسط دشمن ایفا می‌کند. قویترین حمله‌ای که علیه DES انجام شده حمله تفاضلی است و با وجود این حمله DES هنوز در کاربردهایی که مربوط به سطح امنیتی پائین یا متوسط هستند، کاربرد دارد . به همین دلیل NBS روشهای زیر را برای رفع چنین مشکلی پیشنهاد می کند :

۱- روش عملکرد ECB (Electronic Code Book)
۲- روش عملکرد CBC (Cipher Block Chaining)
۳- روش عملکرد CFB (Cipher Feed Back)
۴- روش عملکرد OFB (Output Feed Back)

۲-۳- روشهای تصدیق اعتبار و صحت

در این بخش به ذکر نام روشهای تصدیق اعتبار و صحت بسنده می‌کنیم و فقط یکی دو روش را قدری بازتر مطرح می‌کنیم.

همانطور که قبلاً ذکر شد دو نوع حمله داریم: حملهٔ منفعل و حملهٔ فعال. در بحث گذشته مابه دفاع در برابر حملهٔ منفعل پرداختیم. یعنی کاری کردیم که دشمن پیام را نفهمد. در این بحث ما به دفاع در برابر حملهٔ فعال می‌پردازیم یعنی کاری می‌کنیم که فرد غیرمجاز نتواند به جای منبع اصلی پیام ارسال کند. در اینجا دیگر مهم نیست که دشمن پیام را بفهمد، بلکه فقط باید کاری کنیم که نتواند پیام‌های اصلی را بفرستد. در این بحث به دو موضوع می‌پردازیم:

۱ - تست صحت منبع

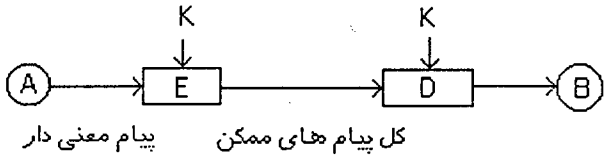
۲ - تست صحت پیام

برای تست اصالت پیام، اطلاعات اضافی تحت عنوان Authenticator به پیام اضافه می‌شود که گیرنده توسط آن می‌تواند صحت پیام را دریابد.

۱-۲-۳- روشهای حفظ اصالت پیام در سیستمهای رمز متقارن

در سیستم رمز متقارن فرستنده و گیرنده هر دو دارای یک سیستم رمز با کلیدهای یکسان هستند. در اینجا فرستنده معمولاً پیامهای معنی‌دار می‌فرستد. سیستم E این پیامها را روی مجموعهٔ تمام پیام‌های ممکن توزیع می‌کند.

به این ترتیب کسی که خط را شنود می‌کند و می‌خواهد حملهٔ فعال کند چاره‌ای ندارد که یک انتخاب اتفاقی روی فضای کل پیام‌ها انجام دهد، گیرنده هنگامی که دریافت می‌کند نگاه می‌کند که آیا پیام ساختار لازم را دارد یا خیر؟!



شکل (۸ - ۳) سیستم رمز متقارن

حال در نظر بگیرید که ساختار مورد نظر افزونگی زبان باشد. در مورد زبان انگلیسی داریم:

پیام N : $26^N = 2^{RN} = 2^{4.7N}$

پیام‌های معنی‌دار: $2^{rN} = 2^{1.5\,N}$

احتمال بدست آوردن یک پیام معنی‌دار: $P_e = \frac{2^{rN}}{2^{RN}} = 2^{(r-R)N} = 2^{-3.2\,N}$

در روابط فوق، N تعداد پیام‌ها، R نرخ مطلق لغات زبان و r افزونگی زبان است. هرچه r کوچکتر باشد، افزونگی زبان بیشتر و در نتیجه احتمال موفقیت دشمن در حملهٔ فعال کمتر خواهد بود. در ذیل به ذکر نام روشهای اولیه حفظ اصالت پیام با استفاده از Authenticator بسنده شده است.

۱ - روش شامیر (Shamir)

۱ - روش انگ - اشنر - شامیر (Ong-Schnorr-Shamir)

۳ - روش طاهرالجمال (El-gamal)

۴ - روش R.S.A

یکی دیگر از راههای تصدیق اصالت پیام، کانال زیر آستانه می‌باشد که به سه روش زیر پیاده‌سازی شده است:

۱ - روش سیمونز

۲ - روش انگ - اشنر - شامیر

۳ - روش طاهرالجمال

۲-۲-۳- امضای رقمی

یکی دیگر از روشهای تصدیق اعتبار و صحت، امضای دیجیتال [۱۲] می‌باشد. در حالت عادی امضاء مستقل از متن است. در حالت دیجیتال امضا در متن گنجانده می‌شود که به متن وابسته باشد و اصالت آنرا نشان دهد.

سیستم غیر مکانیزه (و امضای واقعی) دارای مشخصات زیر است:

۱ - شیئی ملموس، تقاضای انجام کار می‌باشد.

۲ - امضاء، بیانگر تصدیق اصالت می‌باشد.

۳ - در صورت جعلی بودن، قابل عرضه در دادگاه است.

۴ - با یکبار استفاده دیگر قابل استفاده نیست.

۵ - بسیاری از تقلبات قابل تشخیص است.

این مشخصات بایستی در امضای دیجیتال گنجانده شود و بنابراین امضای دیجیتال دارای خواص زیر باید باشد:

۱ - غیر قابل جعل

۲ - اصیل

۳ - غیر قابل تغییر

۴ - غیر قابل استفاده مجدد

ما در این مختصر روشهای امضای رقمی را نام می‌بریم:

روشهای استفاده کننده از سیستم رمز متقارن:

۱ - روش استفاده از Arbitor: در این روش یک قاضی صحت امضاء را بررسی می‌کند.

۲ - روش دیفی - لمپورت (Diffie - Lamport)

۳ - روش رابین (Rabin)

۴ - روش Matyas - Meyer: این طرح بر اساس DES ایجاد شده است.

روشهای استفاده کننده از سیستم رمز نامتقارن:

۱ - روش R.S.A

۲ - روش بهم‌ریزی ساختار ریاضی پیام

۳-۲-۳- کلمه عبور

یکی از روشهای تصدیق اعتبار کاربر روش کلمه عبور[۱۳] میباشد. در این روش سیستم قبل از در اختیارگذاری امکانات مورد تقاضای یوزر، از او یک کلمهٔ شناسایی و عبور می‌پرسد. در صورتی که کاربر اطلاعات خواسته شده را بداند، مجاز به استفاده از سیستم خواهد بود. و در غیر اینصورت سیستم امکانات مورد تقاضای او را در اختیارش نخواهد گذاشت و در عوض، در صورت لزوم اقدامات احتیاطی دیگری را انجام خواهد داد که در طی آنها راهبران و مدیران سیستم به قصد یک Intruder برای نفوذ و رخنه در سیستم پی ببرند. در مورد این روش دقت در حفظ و نگهداری کلمه عبور برای کاربران و مدیران سیستم حیاتی می‌باشد. قسمتی از وظیفه حفاظت از کلمهٔ عبور بعهده راهبر سیستم و سخت‌افزار و نرم‌افزار مورد استفاده برای این منظور و قسمت دیگری از آن بعهده فرد استفاده کننده می‌باشد. در اکثر سیستم‌هایی که از روش کلمات عبور استفاده می‌کنند، کلمات عبور به صورت رمزشده در سیستم نگهداری می‌شوند نه بصورت

آشکار.

لازم به ذکر است که در برخی نرم‌افزارها می‌توان تمهیداتی را فراهم کرد که در طول اجرای برنامه نیز تست‌ها، سؤالات یا اطلاعاتی از کاربر پرسیده شود که در صورت پاسخ منفی یا عدم اطلاع از آنها مشخص شود که کاربر مورد نظر یک کاربر مجاز نمی‌باشد و از آن‌پس جلوی اجرای برنامه توسط کاربر غیرمجاز گرفته شود.

۳-۳- روشهای پیشنهادی برای رمزنگاری

۱-۳-۳- تلفیق روشهای RSQ و PRSQ

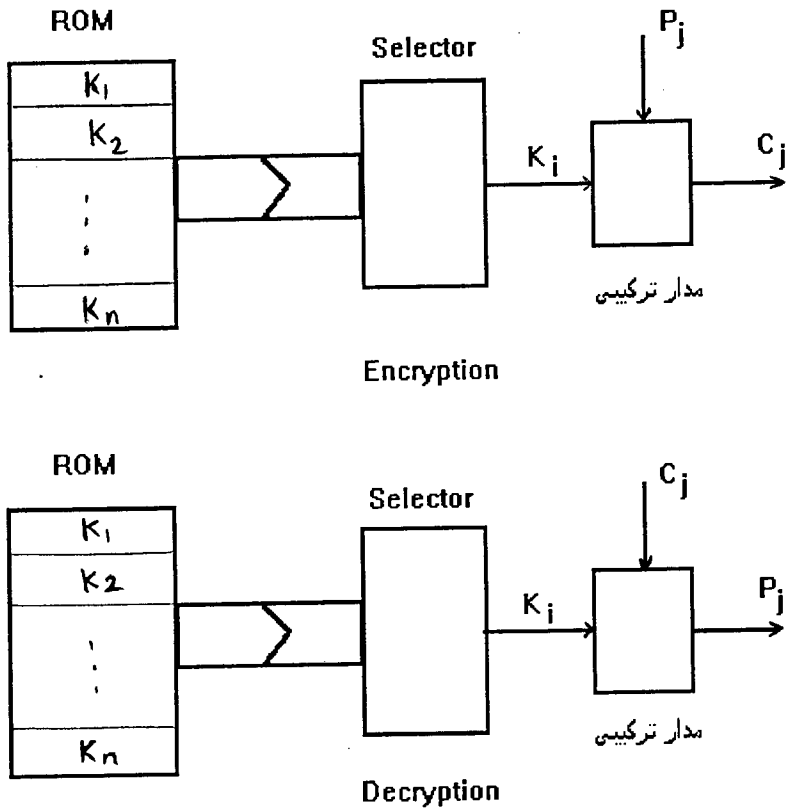
همانطور که در بخش ۱-۲-۱-۳ ذکر گردید ، یکی از روشهای Stream Cipher روش RSQ(Random Sequence) می باشد. برای رفع اشکال این روش (حجم زیاد کلیدهای مورد نیاز برای Encryption) روش PRSQ(Pseudo Random Sequence) پیشنهاد شده است که بکارگیری آن موجب کاهش ضریب ایمنی سیستم می گردد. لازم بذکر است که این روشها می توانند به دو صورت Bit Oriented و یا Character Oriented مورد استفاده قرار گیرند .

روش پیشنهادی Character Oriented می‌باشد و با استفاده از یک مدار پایه سخت‌افزاری که در کاربردهای عملی می‌تواند پیچیده‌تر نیز انتخاب شود قابل پیاده‌سازی است. این روش می‌تواند از روش PRSQ ایمن‌تر باشد.

۱-۱-۳-۳- طرح اولیه

همانطور که قبلاً ذکر گردید، در یک سیستم ارسال و دریافت یا ذخیره و بازیابی اطلاعات، یکی از روشهای تبدیل Plaintext به Ciphertext تعویض کدها با استفاده از یک روش کدگذاری موسوم به Encryption می‌باشد.

برای این منظور می‌توان از روش Random Sequence استفاده کرد. در این روش متن اصلی با یک سری کلیدهای اتفاقی ترکیب شده و متن کدشده بدست می‌آید. این سری کلیدهای اتفاقی برای ایجاد امنیت بالا بایستی یکبار مصرف باشند، در غیر اینصورت با داشتن یک نسخه متن اصلی و رمزشده آن کلیدهای مورد استفاده برای رمزگذاری براحتی بدست می‌آیند. در این صورت موقع دریافت یا بازیابی، نیاز به حجم زیادی کلید جدید خواهیم داشت. برای رفع اشکال فوق روش زیر پیشنهاد می‌شود که شمای کلی آن در شکل ۸-۳ نمایش داده شده است.



شکل (۸-۳) طرح اولیه روش پیشنهادی برای Encryption

در این طرح کلیدها در داخل یک حافظه ROM نگهداری می‌شوند. در مدار سخت‌افزاری ساخته‌شده می‌توان سوکتی برای قرار دادن یا تعویض حافظه کلیدها تعبیه نمود. ROM نیز می‌تواند از نوع Programmable باشد که در مواقع دلخواه کلیدها قابل تغییر باشند. مسلم است که تغییر کلیدها بایستی در فاصله‌های زمانی ثابت یا متغیری الزاماً انجام شود. ضمناً برای حفاظت ROM می‌توان پس از اتمام کار با Encryptor یا Decryptor آنرا از روی مدار برداشت.

مدار Selector طرح فوق که وظیفه انتخاب یکی از n کلید موجود در حافظه را دارد، می‌تواند ترکیبی از انتخاب ۱ تا از n را مورد استفاده قرار دهد. بعنوان ساده‌ترین راه می‌توان انتخاب مرتب از ۱ تا n را مورد استفاده قرار داد. یعنی از یک شمارنده ساده بالا رونده

(Up Counter) برای آدرس‌دهی ROM استفاده نمود. تعداد بیتهای شمارنده باید حداقل برابر m باشند، بطوریکه $2^m >= n$ باشد. ضمناً بایستی شمارنده پس از عدد n مجدداً عدد ۱ را بشمارد.

P_j کاراکتر jام از متن اصلی می‌باشد. دبی ورودی به مدار Encryptor بایستی با فرکانس شمارش شمارنده برابر باشد. بعنوان مثال اگر فرکانس ساعت شمارنده 1 HZ باشد بایستی در هر ثانیه یک کاراکتر از متن اصلی وارد مدار Encryptor شود.

مدار ترکیبی وظیفه ترکیب P_j ها را با K_i ها برای ایجاد C_j دارد، که به آن مانند یک جعبه سیاه نگاه می‌شود. در داخل این جعبه هرگونه عملیاتی می‌تواند بدلخواه انجام شود و بسته به کاربرد می‌تواند از پیچیدگی مناسبی برخوردار باشد.

C_j کدهای خروجی یا بعبارت دیگر کاراکترهای متن رمز شده می‌باشند.

در مدار Decryptor مجموعه کلیدهای ذخیره شده در ROM بایستی همانهایی باشند که در مدار Encryptor استفاده شده‌اند. همچنین مدار Selector رمزگشا دقیقاً بایستی همان Function را داشته باشد که در موقع رمزگذاری داشته است. مسئله فرکانس انتخاب کلید Selector و دبی ورودی C_j نیز مانند حالت رمزگذاری بایستی مدنظر قرار بگیرد. اگر تابع عملیاتی انجام شونده در جعبه مدار ترکیبی در موقع Encryption را F در نظر بگیریم، تابع مورد استفاده در مدار ترکیبی Decryptor بایستی F^{-1} باشد. یعنی عکس عملیات رمزگذاری را برای رمزگشایی انجام دهد. بعنوان ساده‌ترین مثال می‌توان از مدار XOR در هر دو طرف استفاده کرد.

۲-۱-۳-۳- روشهای افزایش ایمنی در طرح اولیه

برای افزایش امنیت طرح اولیه می‌توان با اضافه کردن یک مدول دیگر به آن، بصورت زیر

عمل کرد:

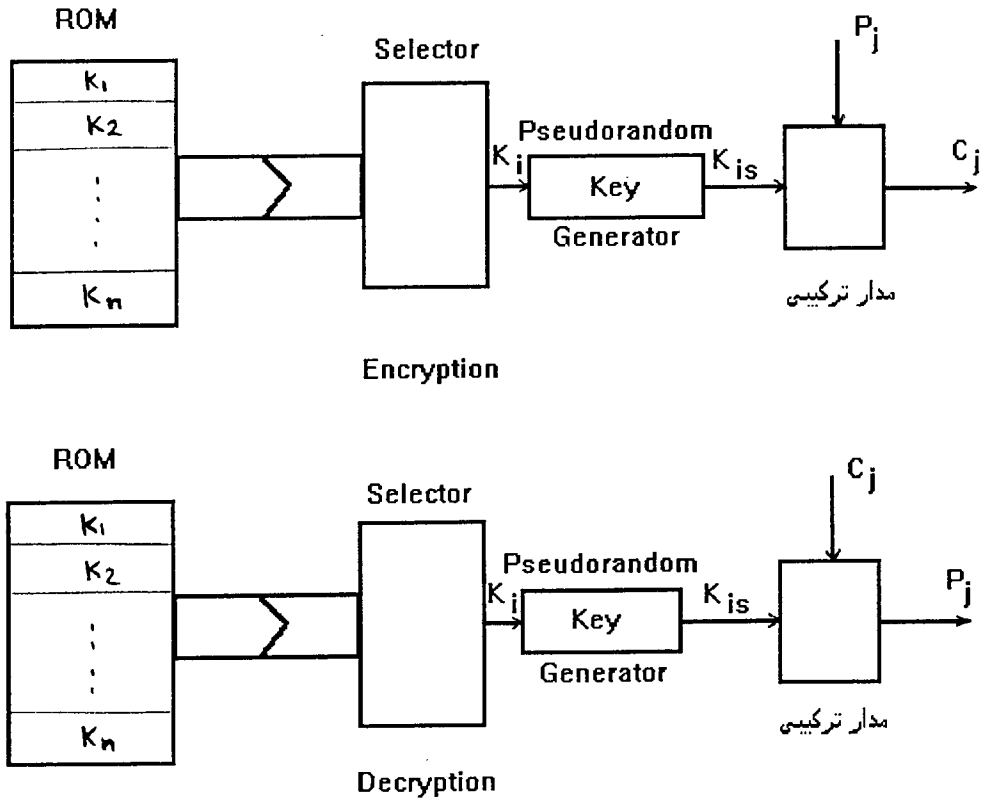
۱ - کلیدی را از میان سری کلیدهای اتفاقی (اولیه) انتخاب می‌کنیم.

۲ - تعدادی دلخواه سری کلیدهای شبه اتفاقی (Pseudorandom) را با استفاده از کلید انتخابی در مرحله اول می‌سازیم.

۳ - تک تک کلیدهای بدست آمده در مرحله دوم را به ترتیب برای کدکردن کاراکترهای متن اصلی استفاده می‌کنیم.

۴ - به مرحله اول باز می‌گردیم و این عمل را تا پایان متن اصلی دنبال می‌کنیم.

لازم به ذکر است که مدار سخت‌افزاری مورد استفاده برای انجام عمل Encryption بایستی مجهز به خط کنترل EncrEn برای فعال یا غیرفعال ساختن مدار کدگذار باشد. در شکل ۹-۳ مدار این طرح نمایش داده شده است.



شکل (۹-۳) طرح توسعه یافته پیشنهادی

همهٔ موارد ذکر شده در رابطه با طرح اولیه در این طرح نیز صادق است. علاوه بر این، در این طرح تعداد کاراکترهای P_j ورودی به مدار در واحد زمان بایستی برابر تعداد کلیدهای K_{is} ورودی به مدار ترکیبی در واحد زمان باشند. تعداد کلیدهای خروجی مدار Selector یعنی K_i بستگی به تعداد کلیدهای Pseudorandom تولید شده در جعبه Pseudorandom Key Generator دارد. مثلاً اگر ما به ازای هر کلید اتفاقی ۱۶ کلید شبه اتفاقی تولید کنیم، در اینصورت تعداد کلیدهای K_i لازم برابر $\frac{1}{16}$ کلیدهای K_{is} مورد نیاز می‌باشد. اینجا این نکته را نیز اضافه کنیم که اگر بخواهیم روش را به صورت Bit Oriented پیاده‌سازی کنیم، می‌توانیم در Pseudorandom Key Generator از بلوکهای FSR, LFSR و امثالهم استفاده کنیم.

همانطور که می‌بینید با اضافه کردن یک قسمت ساده به طرح اولیه، پیچیدگی عمل کدگذاری و کدگشایی چندین برابر شده و احتمال شکسته شدن الگوریتم را کاهش داده است.

تذکر این نکته ضروری به نظر می‌رسد که الگوریتم‌های مورد استفاده برای ایجاد سری کلیدهای Pseudorandom در مرحله Encryption و Decrption بایستی کاملاً یکسان باشند.

با توجه به اینکه یکی از راههای ممکن برای افزایش امنیت، ایجاد اختلاف ظاهری بین روش رمزنگاری و رمزگشایی در مبدأ و مقصد یا در موقع ذخیره و بازیابی می‌باشد - مسلم است که در صورت وجود اختلاف در روش Encryption و Decryption با کشف یکی از این روشهای نمی‌توان به ماهیت روش عکس آن پی برد - می‌توان این روش را نیز در طرحهای فوق به شرح ذیل اعمال کرد.

در طرحهای فوق لزومی ندارد که کلیدهای قرار گرفته در حافظه‌های مورد استفاده در Encryptor و Decryptor و روش Select آنها دقیقاً مشابه هم باشند، بلکه می‌توان ترکیب‌های مختلفی را مورد استفاده قرار داد. (برای ذخیره کلیدها در حافظه و انتخاب یک کلید از

مجموع nکلید) به گونه‌ای که خروجی K_i برای هر دو یکسان باشد. بعنوان مثال اگر در مبدأ کلیدها به ترتیب از اول تا آخر Select می‌شوند، در مقصد کلیدها را از آخر بـه اول بـچینیم و روش انتخاب نیز از آخر به اول باشد. هـمینطور مـی‌توان کـلیدها K_i، روش انـتخاب و روش ایـجاد کلیدهای K_{is} را طوری ترکیب کرد که در مبدأ و مقصد در هر سه قسمت اختلاف موجود باشد، ولی نهایتاً K_{is} های ایجاد شده در هر دو طرف یکسان باشند.

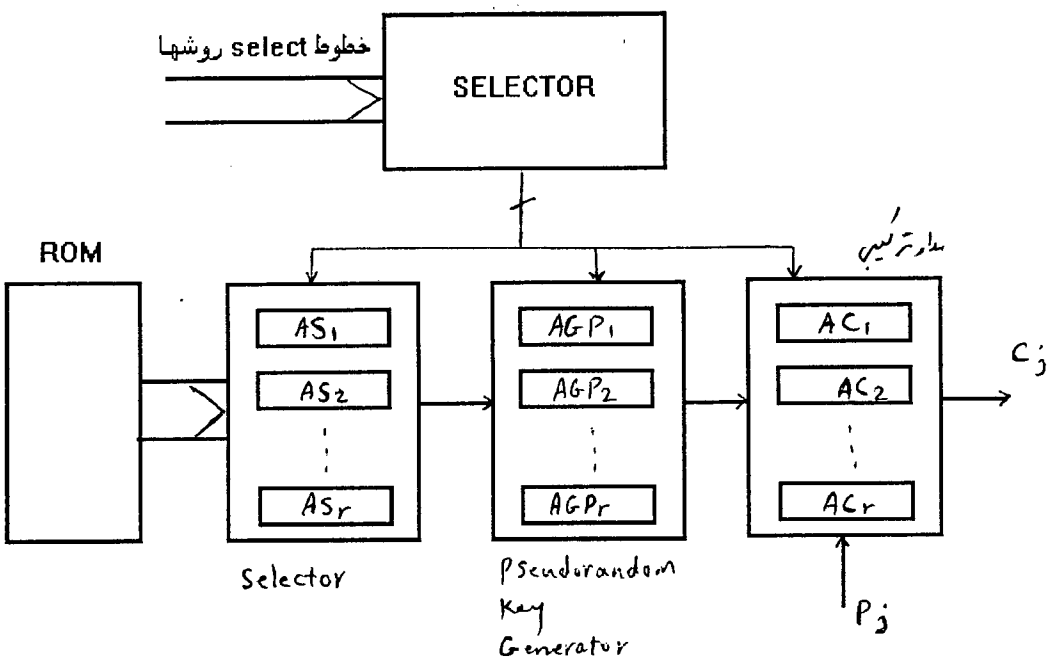
البته این مسئله در افزایش امنیت کلی سیستم چندان تأثیری ندارد، ولی با استفاده از این ترفند می‌توان در مواقع زمانی مشخصی در الگوریتم تغییراتی داد (که لزوماً ایجاد این تغییرات در مبدأ و مقصد همزمان نیست) و بدینوسیله بر پیچیدگی سیستم افزود.

راه دیگر افزایش امنیت، متغیر نمودن الگوریتم‌های انتخاب کلید از میان nکلید اولیه و یا تولید کلیدهای K_{is} از K_i ورودی به قسمت Pseudorandom Key Generator می‌باشد. بعنوان مثال می‌توان روش انتخاب یک کلید از میان nکلید موجود در حافظه را برای nکلید اول به ترتیب (از اول تا آخر) و برای nکلید دوم یک در میان و برای nکلید سوم دو در میان و همینطور برای مابقی در نظر گرفت. همچنین می‌توان این کار را طوری انجام داد که در nکلید انتخاب شده یک کلید از بین کلیدهای موجود در ROM چندبار استفاده شود یا اصلاً استفاده نشود. با توجه به اینکه عملیات رمزنگاری و رمزگشایی در طرحهای فوق در چند سطح انجام می‌شود استفاده از چنین ترفندهایی باعث چندین برابر شدن پیچیدگی کلی سیستم خواهد شد.

در جای دیگری از طرح فوق نیز که می‌توان پیچیدگی سیستم را افزایش داد، مدار ترکیبی می‌باشد که P_j و K_{is} را گرفته و C_j ها را تولید می‌کند. این مدار ترکیبی نیز می‌تواند به صورت متغیر عمل کند.

تعداد الگوریتم‌های متغیر در هر قسمت سیستم می‌تواند نامحدود باشد، ولی اگر محدود باشد می‌توان از یک Selector دیگر برای انتخاب روش مورد استفاده در هر قسمت جهت انجام

عملیات محوله بهره جست. این روش در شکل ۱۰-۳ نمایش داده شده است.



شکل (۱۰-۳) طرح نهایی

۳-۱-۳-۳- تحلیل آماری:

اگر فرض کنیم که دشمن، کلیه اطلاعات مربوط به سیستم رمز، غیر از خود کلیدها را داشته باشد، در روش PRSQ ، اگر تعداد بیتهای کلید اولیه m تا باشد ، با توجه به اینکه یک کلید m بیتی ، 2^m حالت می تواند داشته باشد، برای دستیابی به متن اصلی نیاز به 2^m آزمایش می باشد [۱۴] .

در روش RSQ ، با فرض فوق ، اگر طول پیام رمز شونده یا بعبارت دیگر تعداد کلیدها برابر l و تعداد بیتهای هر کلید برابر m باشد، حداکثر تعداد آزمایشات لازم برای دستیابی به متن اصلی 2^{m*l} می باشد .

در روش پیشنهادی با فرض فوق، اگر تعداد بیتهای هر کلید، m و تعداد کلیدها n باشد، تعداد آزمایشات لازم برابر 2^{n*m} خواهد بود. مقایسهٔ این نتیجه با نتیجه مربوط به روش PRSQ خود گویای کارآیی این روش می‌باشد زیرا تعداد آزمایشات لازم برای کشف رمز در این روش $2^{m*(n-1)}$ برابر تعداد آزمایشات لازم در روش PRSQ می‌باشد.

بعنوان مثال اگر n = 10 و m = 8 باشد، تعداد آزمایشات لازم 2^{72} برابر تعداد آزمایشات لازم برای روش PRSQ خواهد بود. تعداد کل آزمایشات لازم در این حالت 2^{80} خواهد شد.

در نتیجه روش پیشنهادی کارآتر از روش PRSQ یا DES می باشد . مقایسه این روشها در جدول ۹-۳ آمده است و منحنی های مربوط به این مقایسات در پیوست ۲ پایان نامه میباشد.

روش	اطلاعاتی که بایستی تحلیل‌گر داشته باشد	حداکثر تعداد آزمایشات لازم	مثال:l=1024 m=8 n=32
RSQ	۱ - روش کار مدار ترتیبی	متغیر 2^{l*m}	2^{8192}
PRSQ	۱ - روش کار مدار ترتیبی ۲ - روش تولید سری کلیدهای شبه‌اتفاقی	ثابت 2^{m}	2^{8}
DES	۱- الگوریتم DES	ثابت 2^{56}	2^{56}
پیشنهادی	۱ - تعداد کلیدهای اولیه موجود در ROM ۲ - کلیه الگوریتمهای انتخاب کلیدهای اولیه ۳ - کلیه الگوریتم‌های تولید سری کلیدهای شبه‌اتفاقی ۴ - کلیه الگوریتم‌های مدار ترکیبی ۵ - روش انتخاب یکی از الگوریتمهای متغیر ۶ - روش کلی کار سیستم	ثابت 2^{n*m}	2^{256}

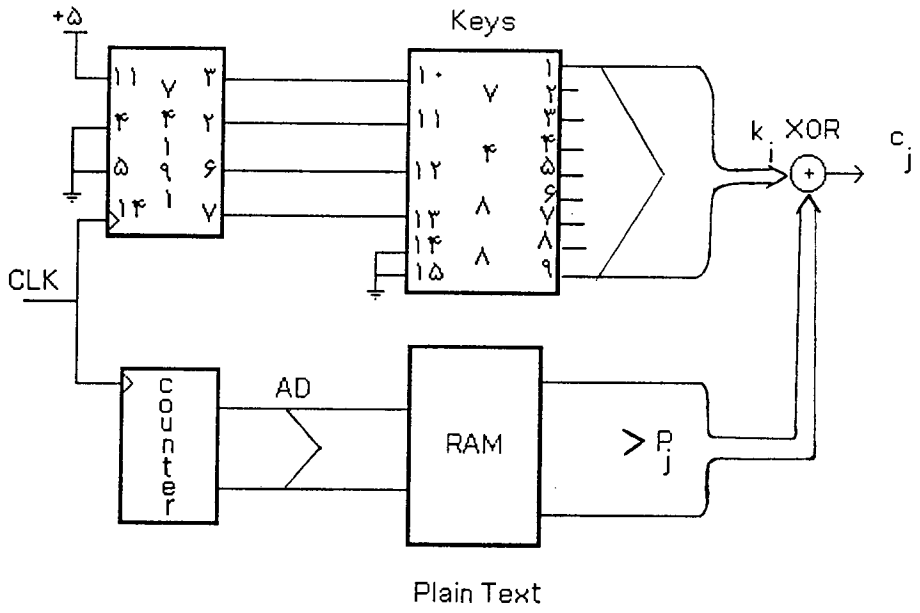
جدول (۹-۳) مقایسهٔ روشهای DES,PRSQ,RSQ و پیشنهادی

۴-۱-۳-۳- پیاده سازی

پیاده‌سازی هر یک از روشهای رمزنگاری می‌تواند به صورت سخت‌افزاری یا نرم‌افزاری باشد. مزایا و معایب هر یک از روشهای سخت‌افزاری و نرم‌افزاری به هیچکس پوشیده نیست. عمده‌ترین مزیت سخت‌افزار سرعت، و عیب آن، قیمت می‌باشد. در عوض نرم‌افزار کند، ارزان و انعطاف پذیر است . انتخاب روش پیاده سازی بستگی به هزینه و زمان اجرا دارد.

پیاده‌سازی سخت‌افزاری: برای پیاده‌سازی سخت‌افزاری می‌توان از IC های موجود استفاده کرد و یا پیاده سازی بصورت VLSI باشد . پیاده سازی سخت افزاری این روش محدودیت خاصی ندارد. با توجه به عدم امکان پیاده سازی VLSI در ایران ، می توان با استفاده از IC های موجود طرح فوق را پیاده سازی کرد . مسلم است که مدار ساخته شده با استفاده از VLSI سریعتر از مداری که از چندین IC استفاده کند، خواهد بود .

قسمتی از طرح عملی به شکل زیر است که بدلیل ساده بودن و بنیادی بودن مدار عملی ساخته شده، لزومی به رسم کامل آن احساس نشد.



شکل (۱۱-۳) قسمتی از طرح عملی اولیه

هزینه ساخت این مدار با توجه به قیمت‌های موجود بازار قطعات الکترونیکی و کامپیوتری در ایران در حدود ۱۵۰۰۰ ریال خواهد شد که از قیمت بسیاری از سخت‌افزارهای آماده برای رمزنگاری کمتر می‌باشد.

پیاده‌سازی نرم‌افزاری: برای شبیه‌سازی طرح فوق در نرم‌افزار می‌توان از زبانهای برنامه‌سازی پیشرفته از قبیل C و Pascal استفاده کرد.در سیستم نرم‌افزاری تهیه شده برای این منظور به زبان Pascal ، که در دیسکت ضمیمه گزارش ذخیره شده است ، متن اصلی از طریق یک فایل ورودی (P.DAT) به برنامه داده می شود و متن رمز شده در فایل خروجی (C.DAT) ذخیره می شود. کلیدهای مورد نیاز سیستم رمزگذاری در فایل دیگری(K.DAT) ذخیره شده اند . لازم بذکر است که در عمل ، حفظ و حراست از فایل کلید بسیار حیاتی میباشد .

زمان اجرا بستگی به سخت افزار مورد استفاده و حجم فایل رمز شونده دارد. در صورت وجود محدودیت زمان اجرا ، می توان روش را بصورت سخت افزاری پیاده سازی نمود .

۲-۳-۳- فشرده سازی

یکی دیگر از روشهای رمزگذاری، فشرده‌سازی می‌باشد. اساس این روش بر این امر استوار است که در سیستم‌های کدگذاری مورد استفاده در سیستم‌های کامپیوتری اعم از ASCII و EBCDIC اولاً کلیهٔ کدهای قابل استفاده در سیستم برای کاراکترهای با معنی و مورد نیاز اختصاص داده نشده‌اند و برخی کدها بدون استفاده‌اند و ثانیاً با توجه به وضعیت آماری متون موجود از برخی کدها بیشتر از کدهای دیگر استفاده شده است. لذا می‌توان با اختصاص تعداد بیتهای کمتری (از ۸ بیت) برای کدکردن اطلاعات موجود، به فشرده‌سازی متون و کاهش حجم مورد نیاز برای ذخیره فایلها یا زمان مورد نیاز برای ارسال اطلاعات، اقدام نمود.

بدیهی است در نهایت نتیجه‌ای که عاید می‌شود تغییر کدهای متن اصلی به کدهای غیر استاندارد می‌باشد. این روش نتیجه‌ای از تئوری اطلاعات می‌باشد.

برای این منظور روشهای مختلفی از دیرباز تاکنون ابداع و پیاده‌سازی شده است که در اکثر آنها تعداد بیتهای لازم برای کدکردن حروف متغیر می‌باشد. بعبارت دیگر برای حروفی که تکرار بیشتری در متون دارند تعداد بیتهای کمتری اختصاص داده می‌شود و بالعکس . اما یکی از مشکلات این روش جداسازی بیتهای مورد استفاده برای کدکردن هر کاراکتر می‌باشد. برای رفع اشکال فوق روش زیر پیشنهاد می‌شود:

۱-۲-۳-۳- روش پیشنهادی و تحلیل آماری

۱ - فایل ورودی (متن اصلی) را یکبار از ابتدا تا انتها مرور کرده و کدهای استفاده شده در متن را می‌شماریم (n). ضمناً در جدولی کدهای استفاده شده را به ترتیب وارد می‌کنیم.

۲ - تعداد بیتهای لازم برای کدکردن n حالت را بدست می‌آوریم. $m = \lceil \log_2^n \rceil$

۳ - حال با استفاده از تعداد بیتهای لازم برای کدگذاری اطلاعات (m)، کاراکترهای مورد استفاده در متن اصلی را کدگذاری می‌کنیم و متن کدشده را در یک فایل خروجی می‌نویسیم.

در موقع کدگذاری لازمست جدول کدهای مورد استفاده را در جایی (مثلاً در یک فایل) ذخیره کنیم تا در موقع کدگشایی با استفاده از این جدول، متن رمزشده را به متن اصلی برگردانیم. برنامهٔ کامپیوتری لازم برای این منظور بنام COMPR در دیسکت ضمیمه ذخیره شده است.

در سیستم عامل MS - DOS برای کامپیوترهای شخصی فایلها به دو دسته اجرایی و غیراجرایی تقسیم می‌شوند. فایلهای اجرایی حاوی کد (دستورالعمل‌های زبان ماشین) و فایلهای غیراجرایی عموماً متن‌هایی با کدهای استاندارد ASCII می‌باشند.

نرم افزارهای مختلفی از قبیل PKZIP , LHARC , ARJ برای فشرده سازی فایلها وجود دارند که درصد فشرده سازی آنها برای فایلهای مختلف متفاوت است . مثلا ممکن است که ARJ یک فایل متن را بیشتر از PKZIP فشرده کند. البته عکس این حالت نیز ممکن میباشد. یعنی ممکن است فایل متن دیگری را PKZIP بیشتر از ARJ فشرده کند. این مسئله ناشی از تعداد تکرارهای مختلف کدها در فایلهای متفاوت می باشد .

روش پیشنهادی ، برای فشرده سازی فایلهای متن ، با توجه به تعداد حروف مورد استفاده در انواع متون زیر ، می تواند برای متون معمولی لاتین حدود ۶۴٪ ، برای متون معمولی فارسی حدود۵۷٪ ، و برای متون فارسی - لاتین حدود ۳۰٪ فشردگی (کاهش حجم) را ایجاد کند.

۴-۳- نتیجه گیری

در این فصل ابتدا اشاره مختصری به روشهای رمز کـردن اطلاعـات و روشـهای تصدیـق اعتبار و صحت شد. سپس دوروش پیشنهادی برای رمزنگاری مطـرح گردیـد. بـا توجـه بـه تحلیلهای آماری و مقایسه این روشها با روشهای مشابه ، روشن گردید که روشهای پیشنهادی اشکالات روشهای مشابه را ندارند و می توانند از آنها ایمن تر باشند.

فصل چهارم

بررسی امنیت در بخش‌های مختلف سیستم‌های کامپیوتری

۱-۴- ایمنی در کامپیوتر های شخصی

ابتدا لازم است این نکته را تذکر دهیم که اگر از یک کامپیوتر شخصی به معنای واقعی آن استفاده شود، آنگاه شاید نیازی به مطرح شدن این بحث نباشد و برای ایجاد امنیت در آن، برقراری امنیت فیزیکی کافی باشد. بحث ما در این قسمت در مورد سیستمهایی خواهد بود که در آنها از کامپیوترهای شخصی، استفاده عمومی می‌شود و بنابراین پیاده‌سازی امنیت در اینگونه مراکز (از قبیل مراکز آموزشی) لازم می‌باشد. نکته دوم اینکه، یکی دیگر از عواملی که موجب اتخاذ تدابیر امنیتی در کامپیوترهای شخصی می‌شود، میزان توانایی سیستم عامل مورد استفاده می‌باشد. بعبارت دیگر اگر سیستم عامل مورد استفاده درکامپیوتر شخصی به قدرکافی توانا باشد، شاید دیگر نیازی به استفاده از امکانات و ابزار جانبی برای برقراری امنیت نباشد. با عنایت به این امر، ما در این قسمت به بررسی نیازهای امنیتی کامپیوترهای شخصی که سیستم عامل مورد استفادهٔ آنها MS - DOS می‌باشد، می‌پردازیم. علت این انتخاب نیز گستردگی استفاده از چنین امکاناتی در سطح کشور ایران می‌باشد.

۱-۱-۴- ایجاد امنیت در سیستم عاملهایی از قبیل MS-DOS

سیستم عامل MS - DOS [۱۵] یک سیستم عامل باز می‌باشد، به این مفهوم که کلیه اطلاعات در مورد جزئیات عملکرد آنرا اکثر کاربران ماهر سیستم می‌دانند. در چنین سیستمی در مقایسه با (بعنوان مثال) سیستم عامل VMS برای کامپیوترهای VAX، که از درون آن چندان اطلاعی در دست نبوده و امکانات امنیتی آن کافی به نظر می‌رسد، ایجاد امنیت توسط ابزارهای کمکی دیگری ضرورت پیدا می‌کند. برای این منظور نرم‌افزارهای مختلفی مانند ADM [۱۶] ADMPLUS [۱۷]، Armor و Diskreet [۱۸] توسط شرکتهای مختلف تهیه شده که هر یک امکاناتی برای حفاظت اطلاعات موجود در یک Partition، Directory و یا File را دارند. اکثر نرم‌افزارهای موجود از بعد ایجاد امنیت ضعیف هستند، بدین معنی که ایمنی ایجاد شده توسط آنها قابل شکست می‌باشد.

بررسی چگونگی ایجاد امنیت توسط نرم‌افزارها روی سیستم عاملهای باز موجب اطلاع از اشکالات آنها و تلاش در جهت رفع این اشکالات و افزایش ایمنی در سیستمهای کامپیوتری خواهد شد.

چرا برخی نرم‌افزارها چنین اشکالاتی را دارند؟ شاید عدم اطلاع کاربران و محققان در زمان تهیه نرم‌افزار از چگونگی ایجاد امنیت و یا نفوذ به آن وجود چنین اشکالاتی را توجیه کند و نیز شاید بتوان گفت عدم توجه و دقت لازم طراحان و برنامه‌نویسان چنین سیستمهایی به نقاط ضعف موجود در آنها عامل وجود چنین اشکالاتی در آنها می‌باشد. در اینجا ما صرفاً به بررسی پیرامون نرم‌افزار ADMمی‌پردازیم.

۴ - ۱ - ۱ - ۱ - نیازهای ایمنی در کامپیوترهای شخصی:

در سازماندهی و پیکربندی کامپیوترهای شخصی مستقر در محیطهایی که ایمنی مورد نیاز باشد، موارد ذیل بایستی رعایت شوند:

۱ - امنیت (Security): تصمیم‌گیری در مورد برقرار نمودن حفاظت داده‌ها یا برنامه‌ها از دسترسی غیرمجاز را می‌توان یکی از مقوله‌های امنیت در کامپیوترهای شخصی در نظر گرفت.

در برخی مواقع ممکن است بخواهیم گروهی از کاربران سیستم به قسمتهایی از دیسک سخت PC بنا به دلایلی دسترسی نداشته باشند.

۲ - حفاظت (Protection): یکی دیگر از مواردی که بایستی در سازماندهی سیستم بدان توجه شود نحوهٔ برقراری حفاظت داده‌ها و برنامه‌ها می‌باشد. منظور از این حفاظت، حفاظت از دسترسی غیرمجاز نیست. بلکه منظور این است که آیا حال که کاربری اجازهٔ دسترسی به یک Partitio از دیسک سخت را دارد اجازهٔ عمل Write را نیز داشته باشد یا فقط بتواند عمل Read را انجام دهد؟ در برخی سیستمها حفاظت می‌تواند حتی تبعات مهمتری از ایمنی داشته باشد. زیرا اگر ما اجازه Write را به همهٔ کاربران بدهیم عملیات PM (نگهداری نرم‌افزاری) برای راهبر سیستم بسیار مشکل خواهد شد. چرا که برخی کاربران عمداً یا سهواً دست به حذف و یا تغییر و دستکاری برخی داده‌ها و برنامه‌ها می‌کنند که این عمل چه‌بسا موجب عدم اجرای یک برنامه شود. اگر کاربری مبتدی در یک Session کاری ناشیانه دستور *.* Del را روی یک مسیر اجرا کند آنگاه راهبر سیستم بایستی احتمالاً وقت زیادی را صرف نصب مجدد نرم‌افزار روی کامپیوتر کند.

۳ – مقابله با ویروسها: ویروسها[۱۹] برنامه‌های کامپیوتری معمولاً مخربی هستند که از طریق دیسک‌های آلوده به حافظهٔ اصلی کامپیوتر نفوذ کرده و از آنجا به سیستم حمله می‌برند. نقاطی که مورد حمله ویروسها قرار می‌گیرند عبارتند از:

۱ - Partition Table

۲ - Boot Sector

۳ - Executable Files

علت حمله ویروسها به این نقاط، امکان راه‌یابی آنها از آنجا به حافظه اصلی می‌باشد.

برای مقابله با ویروسها روشهای زیر بایستی در کامپیوترهای شخصی بکار گرفته شود. ضمناً بایستی نسخه پشتیبان از اطلاعات و برنامه‌های سیستم برای مواقع ضروری همواره در دسترس باشد.

▣ تجسس: در این روش ضد ویروس مورد استفاده با کمک امضاء ویروس به جستجوی او می‌پردازد و در صورت یافتن ویروس کاربر را مطلع می‌سازد.

▣ سرجمع فایلها: روش قبلی قادر به شناسایی ویروسهای شناخته شده می‌باشد. اما ضد ویروس در این روش با کمک سرجمع فایلها، که در موقع سالم بودن آنها ایجاد شده است می‌تواند ویروسهای جدید را نیز شناسایی کند. زیرا در صورت حملهٔ ویروس به فایل و در نتیجه تغییر محتویات آن، سرجمع فایل نیز تغییر خواهد کرد.

هر دو روش فوق در اکثر ضد ویروسهای موجود که به صورت دستی اجرا می‌شوند، بکار گرفته شده‌اند.

▣ جلوگیری از حرکات مشکوک: در این روش، ضد ویروس که معمولاً بصورت یک برنامه رزیدنت (Resident) در حافظه مقیم شده است، به طور اتوماتیک حرکات مشکوک در سیستم

(از قبیل تغییر فایلهای اجرایی، تغییر Partition Table و...) را زیر نظر گرفته و در صورت مشاهده کاربر را مطلع می‌سازد. کاربر می‌تواند با اقدام مناسب جلوی آسیب و یا افزایش آسیب را بگیرد.

۴ – Partitioning: نحوهٔ تقسیم‌بندی دیسک سخت سیستم بایستی کاملاً حساب شده باشد. حداقل تعداد قسمتها برای سادگی عملیات PM باید ۳ قسمت باشد (یکی برای راه‌اندازی سیستم، دیگری برای نرم‌افزارها و سومی برای انجام تمرینات کاربران). پیشنهاد می‌شود برای اکثر کاربران دسترسی به درایوهای :D و :C به صورت Read Only باشد.

۴ – ۱ – ۱ – ۲ – نرم‌افزار ADM:

نرم افزار ADM (Advanced Disk Management System) محصول شرکت MITAC می‌باشد که برای تقسیم‌بندی (Partition) دیسک سخت کامپیوترهای شخصی تحت سیستم عامل MS - DOS و ایجاد امنیت طراحی شده است.

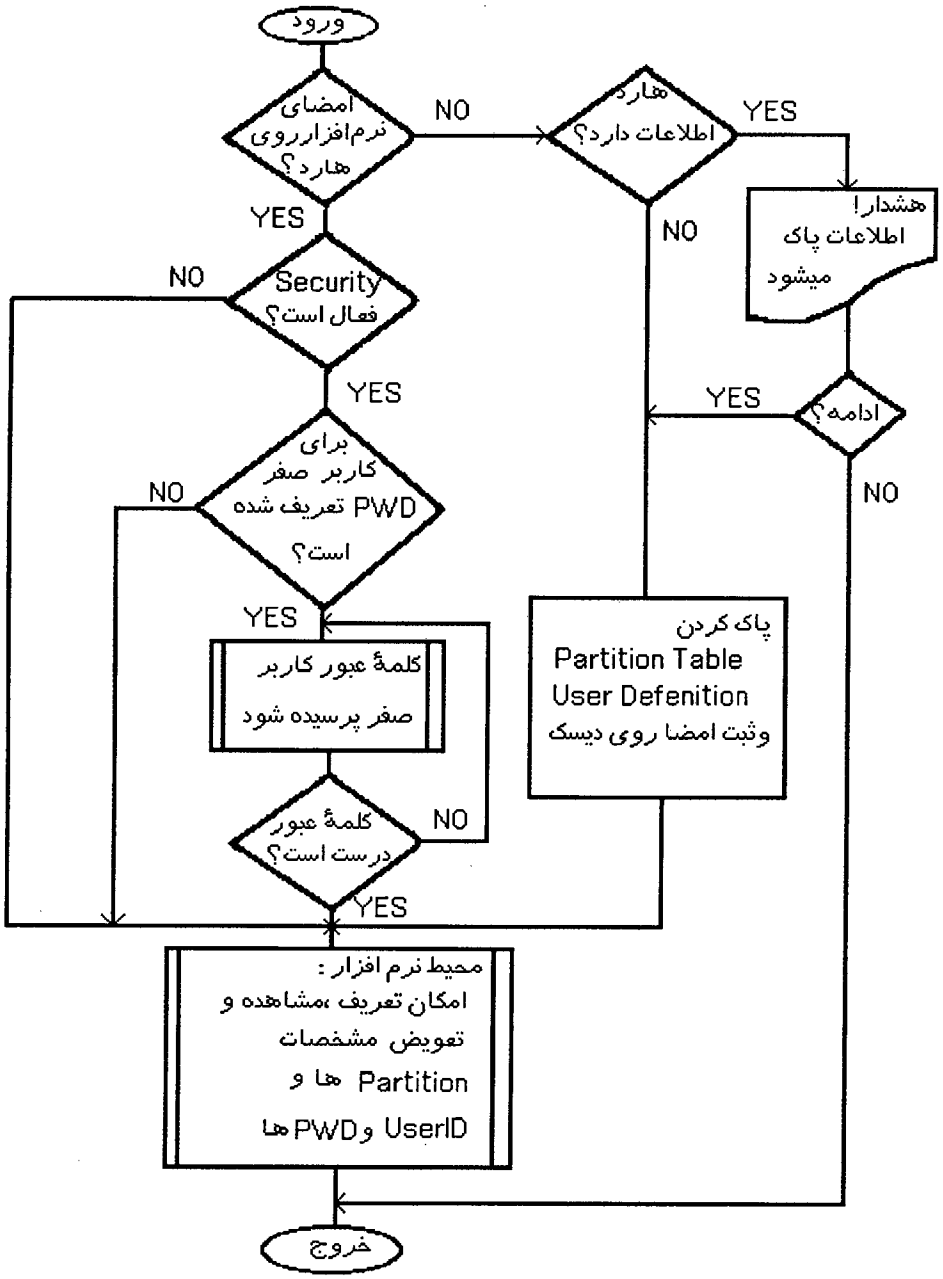
در اکثر مراکز کامپیوتر شخصی در ایران برای ایجاد امنیت لازم از نرم‌افزار ADM استفاده شده است. با کمک این نرم‌افزار در ابتدا دیسک سخت را تقسیم‌بندی، سپس هر قسمت را Initialize کرده و نهایتاً امکان Security را فعال و UserID و Access right و در صورت لزوم Password تعریف می‌کنند. نکات حائز اهمیت در اینجا عبارتند از:

۱ – Type (نوع) Partition ها می‌تواند DOS و یا ADM باشد. البته فقط نوع یک Partition می‌تواند DOS باشد. Partition هایی از نوع ADM را سیستم عامل DOS به خودی خود نمی‌شناسد. برای اینکه کاربر بتواند به Partition های ایجاد شده توسط ADM (با نوع ADM) دسترسی پیدا کند، لازم است که در موقع راه‌اندازی (Boot Up) سیستم

عامل DOS و از طریق فایل Config.sys درایور Adm.sys اجرا شود.

۲ - دسترسی کاربران به Partition ها در قسمت Set User's Access Right تعریف می‌شود که می‌تواند (no access)، یا R (read only)، و یا W (read & write) باشد. اگر برای کاربری دسترسی R به قسمتی از دیسک سخت را انتخاب کرده باشیم در Session کاری او اجازه عمل Write نخواهد داشت.

در مورد نحوهٔ عملکرد نرم‌افزار ADM باید گفت که این نرم‌افزار در طول اجرا ابتدا به دنبال امضای خود روی Hard Disk کامپیوتر می‌گردد. (MITAC - ADM) اگر آنرا یافت و Security، ON بود آنگاه با احضار یک روتین Password کاربر اصلی (Superuser)، که کاربری با شماره شناسایی صفر می‌باشد، را می‌پرسد. اگر فردی که این نرم‌افزار را اجرا کرده اطلاعات خواسته شده را بداند مجاز به ورود به محیط نرم‌افزار و انجام کارهای بعدی می‌باشد. مراحل اجرای نرم‌افزار در شکل ۱ - ۴ نمایش داده شده است. اگر کسی وارد محیط نرم‌افزار شود، اطلاعات مربوط به Partitioning و UserID و pwd ها در اختیارش می‌باشد.



شکل ۱ - ۴ مراحل اجرای نرم‌افزار ADM

۴-۱-۱-۳- راههای نفوذ در ADM و روشهای جلوگیری از آن :

یکی از راههای نفوذ به ADM ، تغییر سه بایت از فایل ADM.EXE بـــه کـد 90 (NOP) میباشد . این تغییر می تواند به کمک نرم افزار Pctools [۲۰] صورت گیرد . با ایجاد ایـــن تغییر عمل احضار روتین پرسش کلمه عبور کاربر اصلی انجام نمی شود که این مسئله بـــاعث بهم خوردن امنیت سیستم می شود .

برای جلوگیری از چنین نفوذی می‌توان امضای ADM را قبل از اولین اجرا تغییر داد. برای این منظور بایستی امضای نرم‌افزار را در فـایل ADM.EXE پـیدا کـرده و بـا کـمک PCtools یانرم‌افزار مشابه آنرا تغییر داده و تغییرات را ذخیره کرد. در اینصورت یک اجرای غـیرمجاز بـا شکست مواجه می‌شود. چرا که در صورتی که ADM اجرا شـود امـضای خـود را روی دیسک سخت پیدا نمی‌کند و بنابراین دیگر ادامه دادن بی‌فایده است و منجر به پاک شـدن Partition Table و User Definition می‌شود. البته عملکرد ADMPLUS در این مورد فرق مـی‌کند. یعنی دیگر Partition Table پاک نمی‌شود، بلکه فقط User Defintion پاک می‌شود.

یکی دیگر از نقاط نفوذپذیر این نرم‌افزار حافظه اصلی می‌باشد. پس از راه‌اندازی سیستم و قرارگرفتن درایور Adm.sys در حافظه اصلی، نحوه دسترسی کاربر به Partition ها در قسمتی از حافظه اصلی نگهداری می‌شود. با عوض کردن محتویات این قسمت از حافظه اصلی می‌توان دسترسی به Partition ها را تغییر داده و به این ترتیب به قسمتی از دیسک سخت که دسترسی وجود نداشت، دسترسی پیدا کرد. و یا اگر دسترسی به صورت Read بوده است آنرا به Write تبدیل کرد. این ایجاد تغییر در محتویات حافظه بعنوان مثال می‌تواند توسط دستورات داخـلی Debug انجام شود.

برای جلوگیری از چنین نفوذی نیز روتینی تهیه شده که به صورت ماندگار (resident) در

حافظه نصب می‌شود و با استفاده از سرویس وقفه صفحه کلید (Keyboard Interrupt Routione) مانع از تغییر Access Right می‌شود. این کار با تست تغییر ایجاد شده در نحوهٔ دسترسی پس از فشار هر کلید و در صورت تغییر، برگرداندن نحوهٔ دسترسی به وضعیت اولیه انجام می‌شود. این برنامه محافظ می‌تواند در موقع راه‌اندازی مشابه درایور adm.sys در حافظه بارگذاری شود.

برنامهٔ کامپیوتری نوشته شده برای این منظور در دیسکت ضمیمه موجود می‌باشد.

۴-۱-۲- روشهای حفاظت فایلها و برنامه ها

یکی از مسائل ایمنی در کامپیوترهای شخصی، حفاظت از فایلها و برنامه‌ها در مقابل کپی غیرمجاز می‌باشد. برای این منظور روشهای زیر موجود است:

۱ – **قانون**: در این روش حق Copyright قانوناً به نویسندگان و توزیع‌کنندگان برنامه داده می‌شود. در صورتی که فردی بصورت غیرمجاز نرم‌افزار را کپی‌برداری کرده باشد،تحت پیگرد قانونی قرار می‌گیرد.

۲ – **قفل**: در این روش به همراه نرم‌افزار یک قفل سخت‌افزاری یا نرم‌افزاری ارائه می‌شود که در صورت عدم وجود آن قفل برنامه اجرا نخواهد شد.

۳ – **رمزگذاری**: در این روش نرم‌افزار یا اطلاعات مورد نظر را می‌توان با یک کلید، Code کرد و به این ترتیب عمل کپی‌برداری غیرمجاز عقیم خواهد ماند. زیرا اطلاعات یا برنامهٔ

کد شده دیگر به درد کسی نمی‌خورد.

ما یک برنامه کامپیوتری (بنام Code) برای این منظور نوشته‌ایم که در دیسکت ضمیمه می‌باشد. این برنامه یک فایل را، اعم از فایل دیتا یا برنامه، خوانده و با یک کلید آنرا رمز می‌کند. محدوده کلیدها از ۹۹۹۹۹۹۹۹۹- تا ۹۹۹۹۹۹۹۹۹+ می باشد . روش رمز کردن بر اساس عملیات دستکاری بیت ها استوار می باشد و پس از رمز کردن ، اطلاعات اولیه تغییر یافته و برای تحلیل کننده غیر قابل استفاده خواهند شد .

۴-کلمه عبور : در این روش در قسمت های مختلف نرم افزار و خصوصا در ابتدای اجرای برنامه کلمه عبور از کاربر پرسیده می شود . در صورتی که کاربر اطلاعات خواسته شده را نداند ، سیستم متوقف می شود . ویژگی این روش همانگونه که در بخش ۳-۲-۳ گفته شد ، تصدیق اعتبار کاربر می باشد . بدیهی است در صورت عدم اطلاع کاربر از کلمه عبور ، اطلاعات در معرض دسترسی غیر مجاز قرار نخواهند گرفت .

ما این روش را در برنامهٔ کاربردی PwdiApp پیاده سازی کرده ایم . لیست برنامه در دیسکت ضمیمه موجود می باشد .

۲-۴- امنیت در شبکه های کامپیوتری

در اینجا به مسئله امنیت در شبکه‌های کامپیوتری [۳] پرداخته می‌شود که یکی از مهمترین مسائل مطرح شده در مبحث شبکه‌های کامپیوتری می‌باشد. اصولاً هر سیستم بدون فرض مسائل ایمنی فاقد اعتبار است. اهمیت اطلاعات در امور سیاسی، نظامی، اقتصادی و... سبب می‌شوند که سازمانهای مرتبط با این امور که از شبکه‌های کامپیوتری استفاده می‌کنند، به فکر حفاظت اطلاعات خود باشند.

بهترین مدلی که برای امنیت شبکه استفاده شده است مدل (Open System Interconection) OSI است که به شکل یک استاندارد بین‌المللی مورد استفاده قرار می‌گیرد. در این مدل یک سری سرویس‌های ایمنی و مکانیزم پیاده‌سازی آنها معرفی شده است. از جمله

این مکانیزم‌ها از رمزنگاری می‌توان نام برد. رمزنگاری (Encryption) از مهمترین و قویترین ابزاری است که در بحث ایمنی شبکه‌ها مطرح می‌شود.

یک شبکه کامپیوتری بطور خلاصه مجموعه‌ای است از کامپیوترها و اجزاء سوئیچ کننده و خط ارتباطی که برای مقاصد نظامی، سیاسی، اقتصادی و علمی مورد استفاده قرار می‌گیرند. بطور کلی هدف عمده در ایجاد شبکه‌ها، کاهش قیمت، استفاده مشترک ازم منابع موجود، افزایش توانایی کامپیوترها و سهولت در ارتباط می‌باشد. همانطور که می‌دانید برای ایجاد هماهنگی و ارتباط بین شبکه‌ها در کشورهای مختلف و نیز سازمانهای گوناگون، استانداردهایی وضع شده است که بهترین مدل آن OSI می‌باشد که در آن یک ساختار ۷ لایه‌ای برای شبکه پیش‌بینی شده که وظایف هر لایه کاملاً در آن مشخص شده است.

امنیت عبارتست از حداقل کردن آسیب‌پذیری منابع و سرمایه‌ها. در این استاندارد موارد ذیل به چشم می‌خورند:

- فهرستی از جنبه‌های مهم امنیت که باید بررسی شوند.
- کمک به ایجاد امنیت
- راهنما برای مجریان و خریداران
- وسیله‌ای برای استاندارد ساختن مسائل پیاده‌سازی امنیت

دو هدف اساسی که توسط استاندارد (International Standard Organization) ISO دنبال می‌شوند عبارتند از:

۱ - فراهم کردن یک روش علمی برای تخصیص‌دهی جنبه‌های امنیت به لایه‌های مختلف مدل OSI.

۲ - فراهم کردن یک شاخص / معیار که بر اساس آن بتوان امنیت را ارزیابی کرد.

۱-۲-۴- سرویسهای ایمنی OSI

۱ – محرمانه بودن داده‌ها Data Confidentiatily:

این گروه از سرویس‌ها وظیفه حفاظت داده‌ها را از افشای غیرمجاز یا حفاظت ترافیک در یک زیرسیستم مخابراتی بر عهده دارند. مثال:محرمانه کردن پیامهای موجود در سیستم مخابرات یا داده‌های موجود در بانک اطلاعات شبکه.

۲ – اعتبار Authentication:

باید اطمینان باشد که تبادل داده‌ها با شخص مخاطب است و نه با هر کسی که سعی می‌کند چهرهٔ جعلی از خود نشان دهد. شبکه باید از صحت هویت منبع پیام مطمئن باشد. سه نوع اعتبار وجود دارد:

۱ - ۲ - اعتبار جزء همتا Pear Entity Authentication که اعتبار جزء بالاتر را تأمین می‌کند.

۲ - ۲ - اعتبار منبع پیام Data Origin Authentication

۳ - ۲ - اعتبار طرفین مقابل Pear - to - Pear Authentication

۳ – درستی داده‌ها Data Integtity:

سرویس درستی داده‌ها را اطمینان می‌دهد، داده‌ها به شکل غیرمجاز تعویض یا خراب نمی‌شوند. مفهوم اعتبار و درستی داده‌ها بسیار به هم نزدیک می‌باشند.

۴ – عدم انکار Non - Repudiation:

هنگامی که یکی از طرفین از شرکت در ارتباط خودداری می‌کند مسأله انکار پیش می‌آید.

در این‌جا یک گروه از سرویس‌های ایمنی در OSI پیش‌بینی شده است که عدم انکار نام دارد:

۱ - ۴ - اثبات هویت مبدأ پیام: گیرنده پیام می‌تواند هویت فرستنده را اثبات کند و فرستنده نمی‌تواند آن را انکار کند.

۲ - ۴ - اثبات هویت گیرنده پیام: فرستنده در صورت لزوم می‌تواند هویت گیرنده را اثبات کند و گیرنده نمی‌تواند آن را انکار کند.

۵ - کنترل دسترسی Access Control:

این گروه از سرویس‌های مجاز بودن یک جزء را برای دسترسی به منابع خاصی از شبکه تعیین می‌کند و هیچ جزئی نمی‌تواند اطلاعات طبقه‌بندی شده را به جزئی که اجازه استفاده ندارد ارسال کند. این کنترل عموماً در لایهٔ هفتم قرار دارد ولی در لایه‌های Transport و Network نیز استفاده می‌گردد.

در جدول ۱ - ۴ رابطه بین سرویس‌های ایمنی و لایه‌های OSI نشان داده شده است.

لایه‌های OSI	سرویسهای ایمنی				
	محرمانه‌بودن	اعتبار	درستی داده‌ها	عدم انکار	کنترل دسترسی
کاربردی	✓	✓	✓	✓	✓
نمایش	✓	✓	—	—	—
جلسه	—	—	—	—	—
انتقال	✓	✓	✓	—	✓
شبکه	✓	✓	✓	—	✓
ارتباط داده	✓	—	—	—	—
فیزیکی	✓	—	—	—	—

جدول (۱ - ۴) رابطه بین سرویسهای ایمنی و لایه‌های OSI

۲-۲-۴- مکانیزمهای ایمنی

مکانیزمهای ایمنی روشهای پیاده‌سازی سرویس‌های ایمنی می‌باشند که در جدول ۲ - ۴ نشان داده شده‌اند:

سرویسها	مکانیزمها							
	رمزنگاری	امضاء	کنترل	درستی	اعتبار	پوشش	کنترل	سندسازی
محرمانه بودن	✓	—	—	—	—	✓	✓	—
درستی داده‌ها	✓	✓	—	✓	—	—	—	—
اعتبار	✓	✓	—	—	✓	—	—	—
عدم انکار	—	✓	—	✓	—	—	—	✓
کنترل دسترسی	—	—	✓	—	—	—	—	—

جدول (۲ - ۴) سرویس‌ها و مکانیزمهای ایمنی

مناسب نیست = — مناسب است = ✓

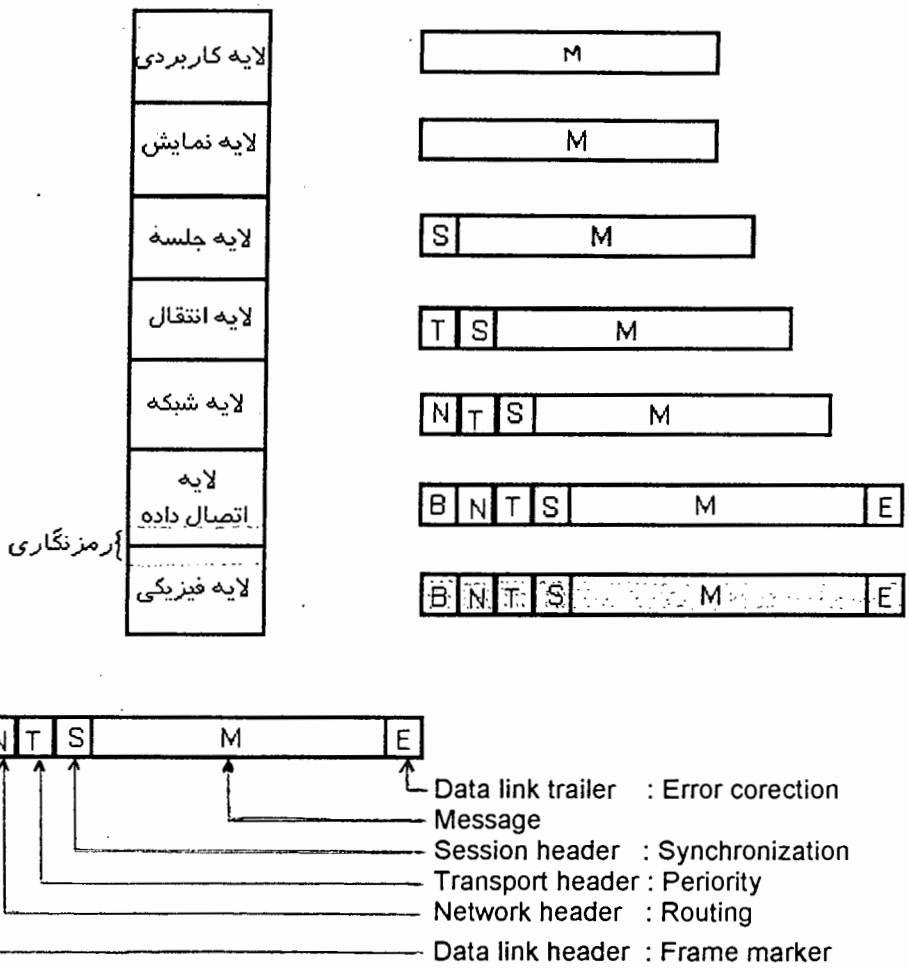
همانطور که می‌بینید در میان تمام مکانیزمهای ایمنی، رمزنگاری از مهمترین آنها به شمار می‌رود.

۳-۲-۴- رمزنگاری در شبکه های کامپیوتری

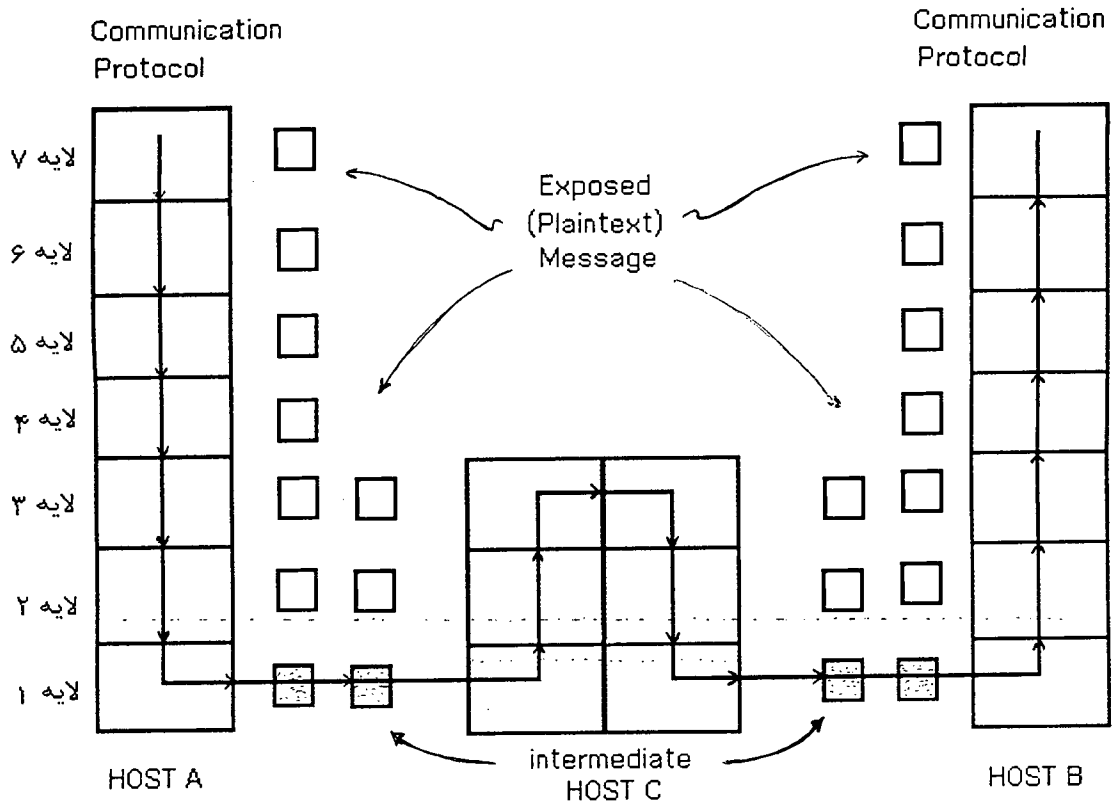
۱ - رمزنگاری شاخه‌ای Link Encryption:

در رمزنگاری شاخه‌ای داده‌ها درست قبل از آنکه روی خط مخابراتی قرار بگیرند رمز می‌شوند. این نوع رمزنگاری در لایهٔ فیزیکی، یا لایهٔ ارتباط داده انجام می‌گیرد. فرایند رمزگشایی

نیز عیناً بطور مشابه در طرف مقابل انجام می‌گیرد:شکل ۲ - ۴ رمزنگاری شاخه‌ای را نشان می‌دهد. مشکلی که در این نوع رمزنگاری وجود دارد در شکل ۳ - ۴ نشان داده شده است. فرض کنیم دو کامپیوتر A و B فقط از طریق C امکان ارتباط داشته باشند و هیچ مسیر مستقیم دیگری بین A و B وجود نداشته باشد. اگر A یک پیام را رمز کند و بفرستد باید در کامپیوتر C این پیام آشکار شود و در واقع کامپیوتر C نقطه آسیب‌پذیری این نوع رمزنگاری است. زیرا اگر کامپیوتر C مورد سوء قصد قرار گیرد، کلیه پیامهایی که از C عبور می‌کنند فاش خواهند شد. پس در واقع در این نوع رمزنگاری هنگامیکه نقاط میانی در ارتباط بین دو Host دخیل شوند، آسیب‌پذیر خواهد شد. هنگامیکه خطوط ارتباط آسیب‌پذیر باشند این نوع رمزنگاری مناسب است.



شکل (۲ - ۴) رمزنگاری شاخه‌ای

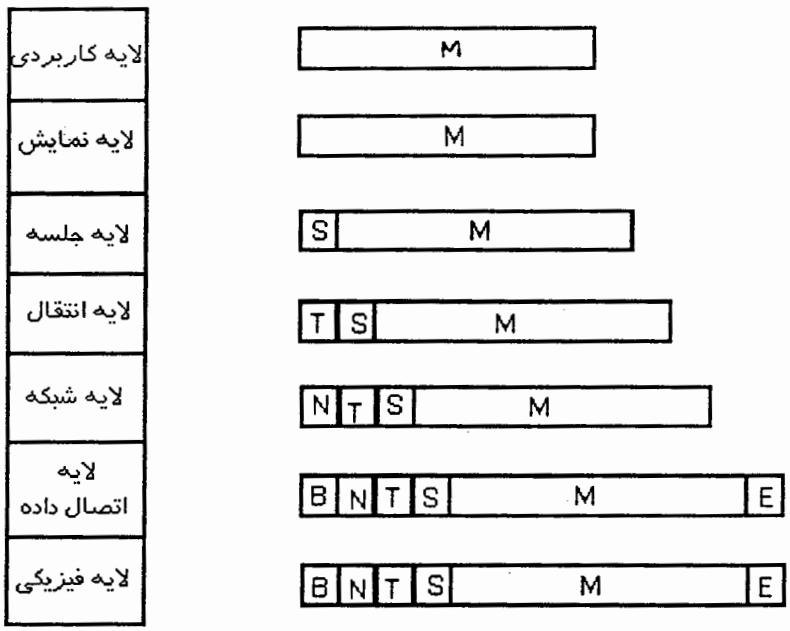


شکل (۳ - ۴) رمزنگاری شاخه‌ای با وجود نقاط میانی

۲ – رمزنگاری انتها به انتها End - to - End Encryption

همانطورکه از اسم این رمزنگاری مشخص است برای ایجاد امنیت بین دو نقطه پایانی یک ارتباط استفاده می‌شود. با دقت در شکل ۴ – ۴ مشخص می‌شودکه در این نوع رمزنگاری پیام‌ها یا بخش‌های داده‌های بسته شبکه از همان ابتدا رمز شده‌اند. پس می‌توان قبل از ورود اطلاعات به کامپیوتر یا شبکه آنها را از طریق سخت‌افزار رمزکرده، البته ممکن است رمزنگار در خود کامپیوتر باشد. پس رمزنگاری از بالاترین لایه یعنی لایه ۷ انجام می‌گیرد.

چون رمزنگاری از ابتدا و قبل از هرگونه ارسال و مسیریابی انجام می‌گیرد بنابراین در کل شبکه پیام به شکل رمزشده انتقال می‌یابد. یعنی اگر امنیت در لایه‌های پایین به خوبی برآورده نشود، در لایه‌های دیگر این امر به خوبی انجام شده است. در این رمزنگاری بسته‌ها حتی اگر از گرهٔ میانی یا چندکامپیوتر واسطه ارسال گردند همچنان رمز شده باقی می‌مانند و امنیت آنها حفظ می‌گردد.



شکل (۴ – ۴) روش رمزنگاری انتها به انتها

۴-۲-۴- مقایسه روشهای رمزنگاری

در روش رمزنگاری شاخه‌ای دستگاه رمزنگار تمام داده‌هایی راکه روی خط خاصی ارسال می‌شوند رمز می‌کند. مشکل اینجاست که هنگامیکه ارتباط کامپیوتر با شبکه فقط از طریق همین شاخه باشد (که معمولاً چنین است) تمام پیامهایی که توسط این کامپیوتر رمز می‌شوند و توسط کامپیوترهای دیگر دریافت می‌گردند، نیاز به دستگاههای رمزنگاری جهت رمزگشایی پیام دارند که یک Overhead در سیستم می‌باشد. بعلاوه تمام این کامپیوترهای میانی باید کلید را در اختیار داشته باشند. بنابراین مشکل مدیریت و توزیع کلید در این شبکه‌ها بسیار مهم می‌باشد.

در رمزنگاری انتها به انتها، رمزنگاری به شاخه‌های منطقی (Logical Link) اعمال می‌شود که شاخه‌های منطقی، کانالهایی بین دو پروسهٔ کامپیوتری در شبکه می‌باشند و در یک ارتباط بین دو کامپیوتر نیازی به کامپیوتر میانی و رمزگشایی و رمزگذاری نیست. بعلاوه رمزنگاری به شکل نرم‌افزاری و در داخل کامپیوتر انجام می‌شود و کاربر می‌تواند به شکل انتخابی کاربرد خاصی یا حتی پیغامی را رمز کند. اما عیب این کار مشکل کلیدهای رمزنگاری است. با استفاده از رمزنگاری انتها به انتها بین هر دو کامپیوتر و کاربر یک کانال رمزنگاری مجازی[۱] به وجود می‌آید. برای رسیدن به امنیت، هر دو کاربر یک کلید منحصر به فرد باید داشته باشند. بنابراین برای n کاربر $\frac{n}{2}(n-1)$ کلید لازم خواهد بود که با افزایش تعداد کاربران تعداد کلیدها افزایش قابل ملاحظه‌ای می‌یابد. در محاسبه فوق فرض شده است که رمزنگاری با کلید یگانه[۲] استفاده می‌شود و اگر از کلید عمومی استفاده شود سیستم رمزنگاری با کلید عمومی فاقد اعتباری است که سیستم رمزنگاری با کلید خصوصی دارد. اگر A و B از کلید خاصی استفاده کنند هر پیغامی که به B برسد و با آن کلید رمز شده باشد، از جانب A ارسال شده و بخودی خود اعتبار A

1- Uirtual Crypto graphic Channel

2- Single Key Encryption

را ثابت می‌کند. اگر از کلید عمومی B (E_B) A استفاده کند، B نمی‌تواند مطمئن باشد پیام رمزشده فقط از جانب A است زیرا هر کس دیگری می‌تواند از کلید عمومی B استفاده کند. بنابراین برای ایجاد و تأمین امنیت و اعتبار، A و B لازم است به طور مداوم یک پروتکل امضاء برقرار کنند.

رمزنگاری شاخه‌ای به گره اعتبار می‌دهد و نه کاربر. پیامی که از جانب A رسیده است فقط می‌تواند از جانب A ارسال شده باشد و هر کاربری که این پیام را توسط A ارسال کرده است در رمزنگاری انتها به انتها کاربر نتایج رمزگذاری را می‌بیند، لیکن در رمزنگاری شاخه‌ای غیرقابل رؤیت است. پس مزیت رمزنگاری انتها به انتها اطمینان به کاربر است. بطور کلی رمزنگاری شاخه‌ای سریعتر و ساده‌تر است، کلیدهای کمتری مصرف می‌کند ولی رمزنگاری انتها به انتها منعطف است و انتخابی و نیز به کاربر نزدیک‌تر می‌باشد.

جدول ۳ - ۴ مقایسه رمزنگاری انتها به انتها و شاخه‌ای را نشان می‌دهد:

	رمزنگاری شاخه‌ای	رمزنگاری انتها به انتها
امنیت در داخل کامپیوترها	پیام در کامپیوتر فرستنده فاش است پیام در گره‌های میانی فاش است	پیام در کامپیوتر فرستنده رمز شده است پیام در گره‌های میانی رمز شده است
نقش کاربر	توسط کامپیوتر فرستنده اعمال می‌شود غیر قابل رؤیت برای کاربر یک وسیله رمزنگاری برای همهٔ کاربران می‌تواند در سخت‌افزار انجام گیرد یا تمام پیامها رمز می‌شوند یا هیچکدام	توسط پروسهٔ فرستنده اعمال می‌شود کاربر رمزنگاری را اعمال می‌کند کاربر رمزنگاری را انتخاب می‌کند پیاده‌سازی نرم‌افزاری کاربر در مورد رمزنگاری هر پیام تصمیم می‌گیرد
مسائل پیاده‌سازی	به ازاء هر زوج کامپیوتر یک کلید مورد نیاز است برای گره اعتبار به وجود می‌آورد	به ازاء هر زوج کاربر، به یک کلید احتیاج است برای کاربر اعتبار به وجود می‌آورد

جدول (۳ - ۴) مقایسه روشهای رمزنگاری در شبکه‌های کامپیوتری

۳-۴- امنیت سیستم عامل

مواردی که در سیستم عامل ممکن است اتفاق بیفتد:

۱ - کاربر مجاز از حقوق خود تخطی کند.

۲ - یک فرد غیرمجاز ظاهر یک کاربر مجاز را به خود بگیرد و از حقوق او استفاده کند.

در این ارتباط چهار نوع حفاظت اهمیت پیدا می‌کند:

۱ - حفاظت حافظه

۲ - حفاظت فایلها

۳ - مراقبت روی دستیابی به منابع کامپیوتری

۴ - اعتبار کاربر

غیر از مورد سوم در رابطه با بقیه موارد تاکنون صحبت‌هایی کرده‌ایم و لذا به بررسی مورد سوم می‌پردازیم:

۱-۳-۴- روشهای حفاظتی سیستم عامل

۱ - **جدایی فیزیکی**: در این روش کاربران را از نظر فیزیکی و با اختصاص امکانات مخصوص به خودشان از هم جدا می‌کنیم.

۲ - **جدایی زمانی**: در این روش پروسه‌ها از نظر زمان با یکدیگر تفاوت دارند و در زمانهای متفاوتی اجرا می‌شوند.

۳ - **جدایی منطقی**: در این روش هر پروسه‌ای در حال اجرا از نظر منطقی پروسه‌های دیگر را نمی‌بیند و کل سیستم را متعلق به خود می‌بیند. بعبارت دیگر از حضور پروسه‌های دیگر

بی‌اطلاع است.

۴ - جدایی رمزنگارانه: فایلها و اطلاعات هر پروسه رمز می‌شوند و بنابراین برای دیگر پروسه‌ها قابل استفاده نیستند.

همانطور که می‌بینید روشهای فوق از بالا به پایین امنیت کمتری دارند و پیاده‌سازی آنها هم مشکل‌تر است.

اما روشهای پایین استفاده بهینه از امکانات را ممکن می‌سازند و خرج کمتری نسبت به جدایی فیزیکی دارند. بنابراین ما هم نیاز به اشتراک منابع و اطلاعات داریم و هم بایستی امنیت اطلاعات در نظر بگیریم. در ذیل اشاره‌ای به سطوح اشتراک اطلاعات می‌کنیم.

۲-۳-۴- سطوح مختلف اشتراک

۱ - اشتراکی وجود نداشته باشد و پروسه‌ها در زمانهای مختلفی اجرا شوند.

۲ - ایزولاسیون:پروسه‌ها در حال اجرا از یکدیگر بی‌خبر باشند.

۳ - کاربر منابع خود را به دو قسمت تقسیم می‌کند:منابع منحصر به فرد و منابع در دسترس همه.

۴ - اشتراک منابع کاربر با اعمال محدودیت روی دستیابی، مثلاً دیگران بتوانند فقط بخوانند.

۵ - اشتراک منابع کاربر با اعمال محدودیت دستیابی و با استفاده از قابلیت‌های کاربران دیگر.

۶ - محدودیت روی استفاده از منابعی که در اختیار دارند. مثلاً اجازه خواندن داشته باشند ولی اجازه کپی‌برداری نداشته باشند.

پیچیدگی پیاده‌سازی از بالا به پایین افزایش می‌یابد. در زمینه امنیت دو موضوع مطرح است: یکی سیاستهای امنیتی و دیگری مکانیزمها.

۳-۳-۴- سیاست های امنیتی

در ذیل به برخی سیاستها در مورد حفظ امنیت سیستم عامل می‌پردازیم:

۱ - مدل ماتریس دستیابی: در این مدل مجموعهٔ (S,O,A) در نظر گرفته می‌شود که در آن، S مجموعه منابع فعال کامپیوتر، O مجموعه منابع مورد دستیابی و A ماتریس دستیابی می‌باشد. این ماتریس رابطهٔ بین هر جفت Subject و Object را نشان می‌دهد و در واقع وضعیت حفاظتی سیستم را بیان می‌کند.

هر Subject از یک زوج (Process,Domain) تشکیل می‌شود. Domain دامنهٔ دستیابی یک پروسه به یک Subject است.

مثال:

Domain

Subject	M_1	M_2	F_1	F_2	P_1	P_2
P_1	R W	R	OWN R W			
P_2		R W	R	OWN RW EXE		

در مثال فوق برای P_2 دامنه (M_2,F_1,F_2) می‌باشد.

۲ – مدل ماتریس دستیابی پویا: این مدل مشابه مدل قبلی است، با این تفاوت که با استفاده از دستورات می‌توان روی آن تغییرات اعمال کرد. هر دستور خود از تعدادی Operation های اولیه تشکیل شده است و کلیه دستورات تحت نظارت یک برنامهٔ Monitor هستند که به آن Access Matrix Monitor گفته می‌شود. Operation های موجود در این مدل به شرح زیر است:

Transfer: وقتی است که یک پروسه، اجازه دستیابی قابل انتقال داشته باشد و آن اجازه را به پروسه دیگری منتقل کند. در اینجا پروسهٔ واگذارنده لزوماً مالک منبعی که مجاز به دستیابی به آن است، نمی‌باشد. علامت Transferable یک * است.

Grant: وقتی یک پروسه یک منبع Own داشته باشد یا یک زیربرنامه تحت کنترل داشته باشد، می‌تواند آن را منتقل کند. در اینجا پروسه مالک چیزی است که واگذار می‌کند.

Delete: مالک یک منبع می‌تواند روی اجازه دستیابی به هر یک از منابع که مالک آن است، هر تغییری که می‌خواهد اعمال کند و مثلاً اجازه دستیابی پروسهٔ دیگری را حذف کند.

Read: اگر یک پروسهٔ Owner چیزی باشد، اجازهٔ خواندن و اطلاع پیدا کردن از تمام دستیابی‌ها به آن منبع را دارد.

Create Object: یک پروسه می‌تواند یک پروسه‌ای ایجاد کند و مالک آن شود و به این ترتیب یک ستون به ماتریس اضافه کند.

Destroy Object: یک پروسه می‌تواند یک پروسه متعلق به خود را حذف کند.

Create Subject: یک پروسه می‌تواند یک پروسه و اجازه دستیابی‌های آن را ایجاد کند.

Destroy Subject: یک پروسه می‌تواند یک پروسه و اجازه دستیابی‌های آن را نابود کند.

دقت کنید که حق Own یا کنترل قابل واگذاری نیست.

روش دایرکتوری:

این روش یکی از مکانیزمهای امنیتی یا بعبارت دیگر روشهای پیاده‌سازی سیاستهای امنیتی است. در این روش هر Subject دارای یک Table است که دستیابی به Object ها را مشخص می‌کند. در این روش برای هر کاربر یک جدول ایجاد می‌شود که شامل نام تمام پروسه‌های مورد دستیابی او می‌شود و این فضای زیادی را برای کاربران زیاد اشغال می‌کند.

حال که به اختصار نگاهی به مسائل ایمنی در سیستم عامل انداختیم می‌توانیم به بحث زیر تحت عنوان امکانات امنیتی سیستم عامل VMS بپردازیم.

۴-۳-۴-امکانات امنیتی سیستم عامل VMS برای کامپیوترهای VAX

با توجه به اینکه بکارگیری مجموعه کامپیوترهای VAX در ایران رو به گسترش نهاده و سیستم عامل VMS بعنوان یک سیستم عامل امن برای مراکز نظامی و اطلاعاتی مطرح می‌باشد. ما قسمتی از توجه خود را به بررسی، شناسایی و بکارگیری امکانات ایمنی در این سیستم عامل معطوف نمودیم. در ذیل نتیجه این کار و کاوش به اختصار شرح داده می‌شود.

۴ - ۳ - ۴ - ۱ - راه‌اندازی سیستم عامل VMS و ایجاد ارتباط کاربران با آن:

در کامپیوترهای VAX [۲۱] پس از روشن نمودن، سخت‌افزار سیستم تست شده و برنامهٔ VMB.EXE توسط برنامهٔ Console به حافظه کامپیوتر Load می‌شود. این‌کار پس از دادن دستور Boot در مد کنسول انجام می‌شود.

سپس فایل SysBoot.exe توسط VMB در حافظه Load و اجرا می‌شود. در مرحله سوم SysBoot فایل Sys.exe و تعدادی دیگر از برنامه‌های اجرایی را Load می‌کند و آنگاه برنامهٔ Sysinit.exe اجرا می‌شود. برنامهٔ اخیر فایل Startup.com را پیدا کرده و پس از اجرای آن کنترل را به Systartup.com رد می‌کند که این دیگر پایان کار و متن راه‌اندازی سیستم است. از این پس کنسول اپراتور یا ترمینالهای دیگر آماده استفاده کاربران می‌باشند. لازم به ذکر است که فایلهای سیستم عامل VMS دارای نام، پسوند و شماره نسخه می‌باشند [۲۲]

پسوندهای EXE و COM اجرایی می‌باشند. فایلهای COM حاوی دسته‌ای از دستورات قابل اجرای سیستم عامل می‌توانند باشند که تقریباً مشابه Bat فایلها در سیستم عامل MS - DOS برای کامپیوترهای شخصی یا EXEC فایلها در سیستم عامل VM/SP برای کامپیوترهای مادر IBM می‌باشند [۲۳]

در موقع راه‌اندازی سیستم عامل VMS یک پروسس به نام Audit Server در حافظه فعال می‌شود. این پروسس قسمت اعظم کنترلهای امنیتی در سیستم را بعهده دارد. در سیستم عامل VMS از Username و در صورت وجود Password برای شناسایی کاربران مجاز استفاده می‌شود. پس از نصب سیستم عامل روی دستگاه راه‌انداز کامپیوتر، چهار کاربر بنامهای FIELD، System، Systest، DEFAULT در سیستم تعریف شده می‌باشند که مهمترین آنها System می‌باشد. این یوزر برای راهبر سیستم (System Manager) تعریف شده است. راهبر سیستم می‌تواند با این یوزر به سیستم Login (خود را معرفی) خود کند و به ادارهٔ سیستم بپردازد. یکی از وظایف راهبر سیستم، ادارهٔ یوزرهای سیستم است. این‌کار توسط نرم‌افزاری به نام Authorize انجام می‌شود که اطلاعات کاربران را در فایل SysUAF.DAT ذخیره می‌کند. برای هر کاربر یک رکورد متشکل از چندین فیلد در UAF ایجاد می‌شود.

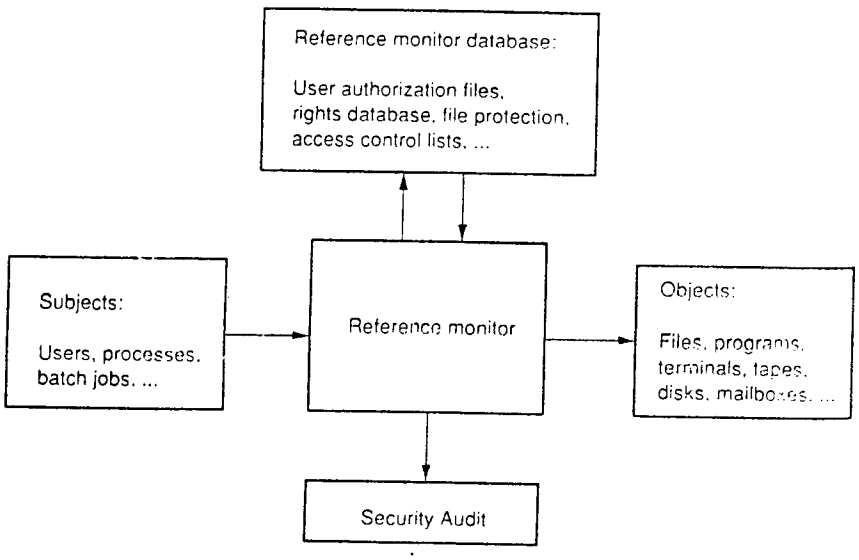
برخی از فیلدهای مهم امنیتی عبارتند از:

Username - Password - UIC(User Identification Code) - Login Flags - LGICMD - Primary & Secondary days -Account - Expiration Pwdlifetime - Authorized Privileges

می‌توان با nopassword یک Open Account داشت. لازم به ذکر است که قبل از اینکه مدیر سیستم بخواهد رکوردی برای یک کاربر ایجاد کند، باید پاسخی برای سؤالهای زیر بیابد:

- چه کسی نیاز به سیستم دارد؟
- چه کاری می‌خواهد انجام دهد؟
- چه منابعی از سیستم را نیاز دارد؟
- چه اطلاعاتی را نیاز دارد؟

برقراری امنیت کاربران در سیستم عامل VMS با مفهوم Reference Monitor در شکل ۵ - ۴ نمایش داده شده است.



شکل (۵-۴) مفهوم Monitor Reference در سیستم عامل VMS

دسترسی و Login به سیستم عامل VMS به روشهای زیر ممکن است:

Local	Detached
Dial - UP	Subprocess
Remote	
Network	
Batch	

البته مدیر سیستم می‌تواند روشهای دسترسی یوزر به سیستم را مشخص و محدود کند.

۴ – ۳ – ۴ – ۲ – محدود کردن دسترسی:

در این مورد به ذکر چند نکته اشاره می‌شود:

۱ – یکی از وسایل مربوط به ایجاد محدودیت در دسترسی به سیستم قراردادن کلمهٔ عبور برای کاربران تعریف شده می‌باشد. در ابتدای تعریف یوزر توسط مدیر سیستم، او می‌تواند برای یوزر، کلمه عبور تعریف کند. کاربر مجاز می‌تواند در طول مدت مجاز کار خود با سیستم، یعنی در مدت زمانی که Username او در سیستم تعریف شده و فعال است، با دستور Set Password کلمهٔ عبور خود را عوض کند. البته این امکان را مدیر سیستم می‌تواند از کاربر بگیرد. ضمناً کاربر یا مدیر سیستم می‌تواند برای یوزر، کلمهٔ عبور دومی نیز تعریف کند که این امکان به درجه امنیت سیستم می‌افزاید.

۲ – مدیر سیستم می‌تواند با کمک دستورات و امکانات نرم‌افزار Authorize، زمان دسترسی کاربران به سیستم را مشخص و محدود کند.

۳ – مدیر سیستم می‌تواند برای کلمات عبور، عمر مفید (Life Time) تعریف کند. این امکان می‌تواند در مورد کلمهٔ عبور اول و دوم بکار گرفته شود. پس از اتمام مهلت فوق در اولین بار

Login کاربر به سیستم، سیستم از او خواهد خواست که کلمهٔ عبور خود را عوض کند.

۴ - برای حفاظت از کلمهٔ عبور، کاربران اولاً بایستی از گفتن آن به افراد دیگر خودداری کنند و ثانیاً پس از اتمام کار خود با سیستم، Logout کنند.

۵ - برای هر کاربری یک UIC یکتا در سیستم تعریف می‌شود. این کد از دو عدد تشکیل شده که اولی شمارهٔ گروهی که کاربر بدان تعلق دارد و دومی شمارهٔ فرد در گروه می‌باشد.

کاربرانی که در یک گروه قرار می‌گیرند تا حدودی می‌توانند به فایلها و اطلاعات یکدیگر دستیابی داشته باشند. با توجه به UIC، کاربر در یکی از ۴ دسته زیر قرار می‌گیرد (در رابطه با فایلها و منابع مورد دستیابی)

System

Owner

Group

World

نحوهٔ دسترسی هر یک از اعضای گروههای فوق به اطلاعات به صورتهای زیر می‌تواند باشد:

Read

Write

Execute

Delete

Control

۶ - بعضی از امتیازات (Privileges) در زمان ایجاد (تعریف) کاربر به او داده می‌شود. با دارا بودن یا عدم دارایی این امتیازات است که کاربر می‌تواند دستوراتی را اجرا کند و یا از

انجام برخی کارها منع می‌شود. لیست مرتب الفبایی این امتیازات در ذیل آمده است. بدلیل اختصار از شرح آنها خودداری شده است. علاقمندان می‌توانند برای کسب اطلاعات بیشتر به مراجع مذکور در این رابطه مراجعه نمایند.

ACNT - Allspool - ALTPRI - BUGCHK - BYPASS CMEXEC - CMKRNL - DETACH - DIAGNOSE - EXQUOTA - GROUP - GRPNAM GRPPRV - MOUNT - NETMBX - OPER - PFNAM - PHY - IO PRMCEB PRMMBX - PWDAPM - READALL - SECURITY - SETPRV - SHARE SHMEM - SYSLCK - SYSNAM - SYSPRV - TMPMBX - VOLPRO WORLD

۷ – بسته به امتیازات داده شده به کاربر، او در یکی از هفت دستهٔ کلی زیر قرار می‌گیرد.

توانایی‌های هر دسته به اختصار ذکر شده‌اند:

- none: بدون امتیاز
- normal: حداقل امتیازات برای استفاده مؤثر از سیستم
- group: توانایی مداخله در کار اعضای همان گروه
- devour: توانایی مصرف کردن منابع سیستمی غیربحرانی
- system: توانایی مداخله کردن در عملیات معمولی سیستم
- files: توانایی به مخاطره انداختن امنیت فایلها
- All: توانایی کنترل سیستم

۸ – هر یک از منابع سیستم (بعنوان مثال دیسک‌ها یا نوارهای مغناطیسی و زیر شاخه‌ها) دارای Owner (مالک) می‌باشند. هر کاربری تنها می‌تواند به منابعی که مالک آن می‌باشد یا اجازهٔ

دستیابی به آنها به او داده شده است، دسترسی داشته باشد. مالک هر Object بر اساس UIC شناخته می‌شود.

۹ - توسط ACL (Access Control List) می‌توان سطح دیگری از حفاظت برای فایلها و زیرشاخه‌ها ایجاد کرد. در اینحالت با استفاده از Security Alarm می‌توان دسترسی غیرمجاز به سیستم را، به اپراتوران امنیت کامپیوتر خبر داد.

۱۰ - اطلاعات مربوط به کاربران مجاز شبکه و نحوهٔ دسترسی آنها به منابع و اطلاعات، در فایلهای NETPROXY.DAT و RIGHTSLIST.DAT نوشته می‌شود.

۱۱ - توسط برخی Flag ها تحت عنوان Login Flag محدودیت دسترسی و کنترلهای امنیتی اعمال می‌شود. اسامی Flag ها در ذیل آمده است:

Audit - Autologin - Captive - DefCL1 - Disctly - Disforce - PwdChange - Dismail - Disnewmail - DisReport - Disuser - Diswelcome - Genpwd - Lockpwd - Pwd - expired - PWD2 - expired - Restricted

۱۲ - امکاناتی برای سهمیه‌بندی فضای دیسک اختصاص داده شده به یوزر وجود دارد. در صورتی که Quxota فعال شده باشد، محدودیت مشخص شده برای استفاده از فضای دیسک اعمال می‌شود. برای دسترسی به سایر منابع از قبیل حافظه و بافرها نیز می‌توان محدودیت‌هایی اعمال کرد.

۱۳ - در صورتی که اشکالاتی در سیستم پیش بیاید (در روتین‌های راه‌اندازی) و منجر به این شود که دیگر سیستم صحیح و کامل بالا نیاید، در اینصورت می‌توان طی یک روال مشخص، سیستم را به صورت اضطراری راه انداخته و با تغییر یکی از پارامترها فایل SYSUAF را نادیده گرفت. در اینصورت کاربر می‌تواند به هر نام و کلمهٔ عبوری که بخواهد به سیستم Login کند.

این یوزر کلیهٔ اختیارات و امتیازات کنترل سیستم (مدیر سیستم با [001,004] UIC)را دارا خواهد بود و به این ترتیب می‌تواند به رفع اشکال به وجود آمده اقدام کند.

۱۴ - برای کاربران، بسته به نوع استفاده از سیستم می‌توان Periority های متفاوتی مشخص کرد.

۱۵ - می‌توان یک Captive Login داشت. در اینصورت یوزر تنها می‌تواند به اجرای برنامهٔ مشخص شده خود بپردازد و هیچگونه دسترسی دیگری به سیستم نخواهد داشت. حتی دستور dir را برای مشاهده لیست فایلها نمی‌تواند اجرا کند. در اینصورت پایان کار یوزر (خروج از برنامه) مصادف با Logout او خواهد بود.

۱۶ - برای ایجاد امنیت در سیستم، راهبر سیستم بایستی کارهای زیر را انجام دهد:

- حفاظت از فایلهای SYSUAF, DAT , NETPROXY.DAT

RIGHTSLIST.DAT

- استفاده از Flag های محدود کننده یوزر و محدودیت‌های ساعتی
- حفاظت از کلمه عبورهای مهم
- شماره‌های Dail - Up را عمومی نکند.
- در خارج از ساعات کار کاربران مجاز، مودم را خاموش یا قطع کند.
- دسترسی World به SYSUAF ندهد.
- تشویق کردن و فراهم کردن وسایل استفاده از ACL و حفاظت فایل
- تشویق کاربران به استفاده از کلمهٔ عبور دوم
- محدود کردن امتیازات کاربر
- ایجاد گزارشات Accounting برای چک کردن استفاده از سیستم
- برچسب زدن به دیسک‌ها و نوارها

- Erase - on - delete و Erase - on - allocate برای فایلها

- امنیت Login

- تشخیص Break - in: در این مورد تعداد دفعات واردکردن کلمهٔ عبور اشتباه در سیستم ثبت و روی کنسول اپراتور نمایش داده می‌شود.

- Security Auditing: در این مورد با Setکردن Audit Flag، مدیر سیستم می‌تواند کلیه فعالیت‌های کاربر را زیر نظر بگیرد (به او گزارش می‌شود). این موارد شامل:تلاش برای دسترسی به فایلها و منابع، مشخص کردن تقاضای کاربر (Read, Execute,...) نتیجه کار (موفق، ناموفق) و... می‌باشد که در Log سیستم نیز ثبت می‌شود.

۴-۴- امنیت پایگاه داده ها

در این قسمت نیز نیم‌نگاهی مختصر به امنیت پایگاه داده می‌کنیم. دستیابی غیرمجاز ممکن است از طریق دو کانال صورت گیرد:

۱ - کاربر مجازی از حقوق خود تخطی نماید.

۲ - کاربر غیرمجازی، با رو کردن هستهٔ امنیتی دستیابی غیرمجاز پیداکند.

امنیت پایگاه داده‌ها به مکانیزمهای امنیتی سیستم عامل پایه‌گذاری شده است.

۱-۴-۴- نیازهای امنیتی D.B.

۱ - امنیت فیزیکی

۲ - صحت منطقی:کسی نتواند در ساختار منطقی D.B. دستکاری کند.

۳ - صحت عناصر و اجزاء

۴ - قابلیت بازرسی و پیگیری:بدانیم که چه افرادی در چه زمانهایی دسترسی داشته‌اند و به

چه اجزاء و مواردی دست یافته‌اند.

۵ - کنترل دستیابی

۶ - شناسایی کاربران

۷ - در دسترس بودن سیستم: قابلیت انعطاف در سیستم باقی بماند و سیستم برای استفاده کاربران راحت باشد .D.B از دو نظر مورد توجه قرار می‌گیرد:

- مخزن فیزیکی
- سیستم منطقی

در مورد ساختار .D.B موارد زیر را در نظر بگیرید:

یک عنصر اطلاعاتی — d: data item

مجموعه‌ای از دنباله‌های مرتب‌شده از item ها — PR: physical Record

$$PR = (d_1, d_2, ..., d_n)$$

مجموعه‌ای از d ها که دارای یک Attribute هستند. — F: Field

زیرمجموعه‌ای از فیلدهای ممکن — LR: Logical Record

$$LR^{(i)}: I(F_1, F_2, ..., F_k)$$

LDB: Logical Data Base

$$LDB^{(i)} = \{LR_2^{(i)}, LR_2^{(i)}, ..., LR_m^{(i)}\}$$

برای برقراری امنیت در .D.B می‌توان از روشهای رمزنگاری استفاده کرد. به عنوان مثال جایگشت data item ها، تبدیل آنها، کاهش آنها، بسط دادن آنها، کد کردن آدرس دستیابی را می‌توان نام برد. برخی از کاربردهای رمزنگاری در حفاظت از اطلاعات در حین پردازش و جلوگیری از استنتاج مطرح می‌شود.

۵-۴- امنیت فیزیکی

یکی از مهمترین لوازم سیستمهای کامپیوتری برقراری امنیت فیزیکی می‌باشد. در این رابطه طراحی سایتها باید به گونه‌ای باشد که کاملاً امن باشند و نقاط نفوذ نداشته باشند. مصالح ساختمانی بکار گرفته شده بایستی مستحکم و مناسب باشند و از طرفی اثرات جانبی از قبیل: میدان مغناطیسی روی کامپیوتر و جریان اطلاعات نداشته باشند. همچنین مسائل مربوط به جلوگیری از حوادث طبیعی از قبیل: سیل، زلزله، آتش‌سوزی و حملات انسانی (جنگها) بایستی در طراحی فیزیکی مد نظر باشد.

یکی دیگر از مواردی که در این ارتباط می‌توان مطرح کرد، چگونگی ادامهٔ کار سیستم پس از وقوع یک حادثه می‌باشد. برای این منظور بایستی نسخهٔ پشتیبان از نرم‌افزارها و اطلاعات موجود در سیستم کامپیوتری در محل امنی (به عنوان مثال در یک گاوصندوق ضد انفجار) نگهداری شوند. اقدامات امنیتی برای جلوگیری از سرقت از قبیل قراردادن نگهبان و سیستمهای الکترونیکی دزدگیر باید به کار گرفته شود. حفاظت از Port های ارتباطی فیزیکی از مقوله‌های امنیت فیزیکی است. دستگاههایی برای شناسایی و تصدیق اعتبار کاربران از قبیل دستگاههای تشخیص هویت با استفاده از اثر انگشت و سیستمهای مدار بسته تلویزیونی قابل Monitor نیز در صورت لزوم بایستی بکار گرفته شوند. و خلاصه همانطور که قبلاً تذکر داده شده است از هیچ کوششی در برقراری امنیت نباید دریغ کرد و هیچ نکته‌ای را نیز نباید فراموش کرد.

فصل پنجم

نتیجه‌گیری

همانطور که در فصل اول بیان شد، برقراری امنیت مطلق در سیستمها بعید به نظر میرسد. لذا در عمل سیستمهای "عملی امن" پیاده سازی می شوند. در این سیستمها امکان نفوذ و برهم زدن امنیت سیستم وجود دارد، ولی از نظر زمانی و مالی این کار در مقطعی که سیستم امن اعلام می شود، با توجه به ابزارهای موجود ، ناممکن است . به عنوان مثال الگوریتم DES برای ۱۰ الی ۱۵ سال بعد از انتشار امن اعلام شد .

فصل دوم گونه های مختلف تهدیدات سیستمهای کامپیوتری را برشمرد. هیچیک از این تهدیدات نباید نادیده گرفته شده یا کم اهمیت پنداشته شوند.

روشهای ایجاد امنیت در فصل سوم بررسی شدند. مشخص گردید که پیاده سازی روش RSQ با مشکلات عدیده ای مواجه بوده و از طرفی بکارگیری PRSQ نیز باعث کاهش زیادی در امنیت سیستم ، نسبت به روش RSQ ، می شود. لذا جهت رفع مشکل ، روش جدیدی پیشنهاد گردید که بکارگیری آن ، با توجه به امکانات سخت افزاری کنونی و تکنولوژی ساخت حافظه های کوچک و کم هزینه ، اگر نگوئیم سیستم مطلقا امنی را به وجود خواهد آورد، لااقل سیستم عملا امنی را خواهد ساخت. این روش پیشنهادی بر حسب میزان پیچیدگی مورد نیاز کاربردهای عملی ، به انحاء مختلف قابل پیاده سازی خواهد بود . یکی دیگر از روشهای پیشنهادی ، رمز کردن به همراه فشرده سازی بود که پیاده سازی این روش ، نسبت به روشهای مشابه ساده تر میباشد.

فصل چهارم مسائل امنیتی را در بخشهای مختلف سیستمهای کامپیوتری اعم از کامپیوترهای شخصی ، شبکه ها ، سیستمهای عامل و پایگاه داده ها مطرح نمود. همچنین

امکانات امنیتی در کامپیوترهای شخصی و شبکه ای از کامپیوترهای VAX بررسی شده و نقاط قوت وضعف هر یک تا حدودی ارائه گردیدند.

امید است که این پایان نامه بتواند در زمینه ایجاد امنیت در سیستمهای کامپیوتری مفید فایده واقع شده و در جهت رفع معایب و نواقص موجود و بکارگیری و تقویت روشهای خوب و موفق ایمن سازی ، به بالا بردن سطح امنیت در سیستمهای کامپیوتری و حرکت به سوی سیستمهای امن مطلق کمک کند.

پیشنهاد می شود که دیگر محققان و علاقمندان به ارتقاء سطح علوم انفورماتیک در کشور، به تحقیق و بررسی بیشتر پیرامون امکانات سخت افزاری و نرم افزاری موجود بپردازند و با کمک تجربیات گذشته و هوش سرشار ایرانی ، سیستمهای جدیدتر و امن تر را طراحی و به دنیای کامپیوتر عرضه کنند. کشور ما در این مقطع حساس تغییر از ساخت سنتی به ساخت صنعتی و تکنولوژیکی ، نیازمند تلاشهای بیشتر در این راه می باشد و اطمینان داریم که مغزهای کامل و متعهد متخصصان ایرانی از عهده این بزرگ برخواهند آمد. به امید بهره وری بیشتر از کامپیوتر و آینده ای بلند وروشن.

پیوست ۱

استانداردها

امروزه سخن از استاندارد بسیار سر زبانهاست. تولیدکنندگان کالاها در هنگام تبلیغ برای محصولات خود و در صورت تطابق محصولاتشان با استاندارد، بر این ویژگی تأکید می‌کنند. برای استاندارد تعاریف مختلفی شده است، از جمله:

چیزی که به وسیله یک مقام مسئول با توافق عمومی مبنای مقایسه باشد. یک مدل تصویب شده.

مؤسسات مختلفی در سطح جهان به تدوین استانداردهای متفاوتی در زمینه‌های مهندسی نرم‌افزار و سخت‌افزار پرداخته‌اند. به عبارت بهتر در برخی زمینه‌ها، برخی مؤسسات استانداردهایی را تدوین کرده‌اند. گروه تدوین مقررات پیمانهای نرم‌افزاری ایران وابسته به شورای عالی انفورماتیک کشور، استانداردهای موجود را جمع‌آوری کرده است. البته متن اصلی بیشتر استانداردها در دسترس نمی‌باشد، ولی برای اکثر آنها اطلاعات مختلف و پراکنده‌ای موجود است. حدود ۱۷۵ عنوان استاندارد در دسترس گروه فوق می‌باشد. در ذیل اسامی برخی استانداردهای مرتبط با موضوع امنیت آمده است.

لازم به ذکر است که این استانداردها را وزارت دفاع آمریکا و انگلیس تدوین کرده‌اند.

- بخش نرم‌افزار نظام دفاعی:

فصل ۱ - ۵ - تحلیل نیازها

فصل ۲ - ۵ - و ۳ - ۵ - طراحی

فصل ۴ - ۵ - رمزسازی

فصل ۵ - ۵ - و ۶ - ۵ - مجتمع‌سازی و آزمایش

فصل ۷ - ۵ - مدیریت پیکربندی

فصل ۸ - ۵ - برآورد کیفیت - نصب و بررس

فصل ۹ - ۵ - مدیریت پروژه

- استاندارد وزارت دفاع انگلستان برای تولید نرم‌افزارهای حساس در مأموریت، نکته‌ای را در اینجا لازم به ذکر می‌دانم و آن اینکه در اکثر موارد مربوط به کامپیوتر و خصوصاً سخت‌افزار به دلیل پیشرفت بسیار سریع تکنولوژی و روشهای به کار گرفته شده، استانداردهای مشخص و مدونی وجود ندارد.

تقسیم‌بندی استانداردها:

تقسیم‌بندی استانداردها بر اساس نوع آنها به شکل زیر است:

۱ - استانداردهای فرآیند (Process)

- روش

- فن

- اندازه‌گیری

۲ - استانداردهای فرآورده (Product)

- نیازها و الزامات

- طرح ساخت

- جزء یا اجزاء

- شرح

- برنامه

- گزارش

۳ - استانداردهای حرفه‌ای

- عناوین شغلی

- مبانی اخلاقی

- گواهی

- صدور مجوز

- مباحث درسی

۴ - استانداردهای علائم

- واژگان

- نمایش

- زبان

بر مبنای موضوع نیز استانداردها را به ۲۴ دسته تقسیم کرده‌اند. اسامی این تقسیمات در ذیل ذکر گردیده است:

۱) آزمایش، صحت‌سنجی و اعتبارسنجی

۲) آموزش

۳) ارزیابی، سنجش، سنجیده‌ها

۴) برنامه‌ریزی

۵) پروژه و کنترل آن

۶) پیاده‌سازی، برنامه‌سازی و زبان

۷) پیکربندی

۸) تدارک

۹) تضمین کیفیت

۱۰) روش و فرار دستی

۱۱) طراحی

۱۲) علائم قراردادی برای مستندسازی

۱۳) کیفیت

۱۴) متفرقه (از جمله استانداردهای طبقه‌بندی استاندارد)

۱۵) مجتمع‌سازی

۱۶) مدیریت

۱۷) مستندسازی (بیشترین تعداد استانداردهای موجود در این زمینه است)

۱۸) مستندات کاربر

۱۹) مشخصات نیازها

۲۰) ممیزی

۲۱) نصب، راه‌اندازی، راهبری

۲۲) نظام کیفیت

۲۳) نگهداشت

۲۴) واژگان

ما از میان این استانداردها، استاندارد نظام دفاعی آمریکا را در ذیل به اختصار بررسی می‌کنیم:

استاندارد نرم‌افزار نظام دفاعی:

با توجه به اینکه نظام دفاعی آمریکا از مدتها قبل متکی بر تمامیت و صحت نظامهای نرم‌افزاری وزارت دفاع و ارتش آن کشور است، بنابراین وزارت دفاع این کشور یکسری استاندارد موسوم به استانداردهای نظام دفاعی را فراهم کرده است که طراحی و پیاده‌سازی اجزاء نرم‌افزاری به وسیله مقاطعه‌کاران خارج از وزارت دفاع و یا به وسیله سازمانهای تولیدکننده نرم‌افزار نظامی داخلی، را اداره می‌کند.

هدف از این استاندارد ارائه یک فراروش برای کلیه دست‌اندرکاران تولید نرم‌افزارهای دفاعی است. استفاده از این استاندارد، با توجه به اینکه کلیه نظامهای دفاعی حساس در مأموریت هستند و اجزاء آنها باید از قابلیت اعتماد بالایی برخوردار باشد، بسیار مهم است. نظامهای حساس در مأموریت حداقل شامل یکی از موارد زیر است:

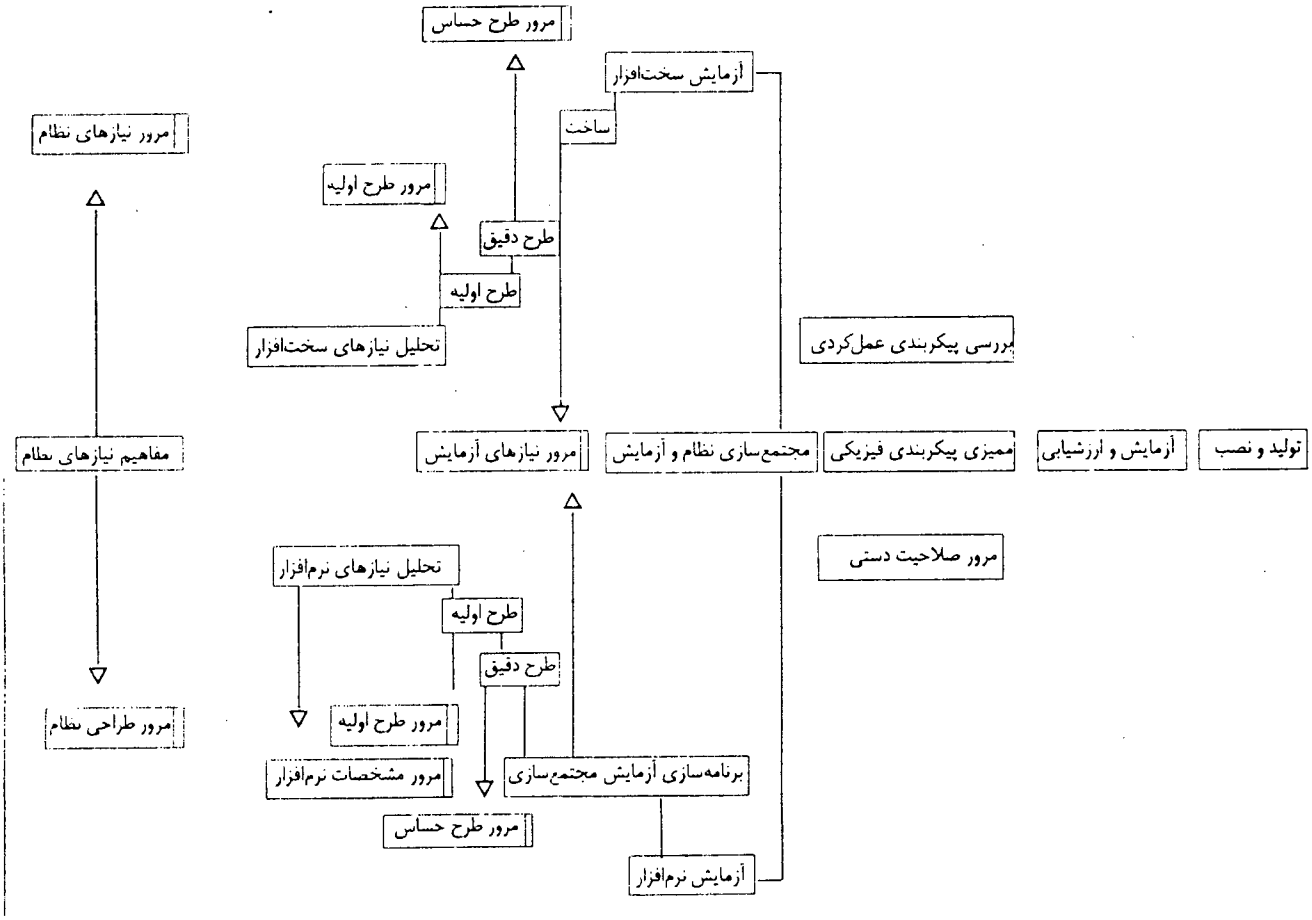
- انجام فعالیتهای جاسوسی
- فرماندهی و کنترل نیروهای نظامی
- تشکیل نظامهای رمزسازی مربوط به امنیت ملی
- تجهیزات یا نرم‌افزاری که بخش مشخصی از یک جنگ‌افزار باشد.

این استاندارد دارای یک رویکرد از بالا به پایین یا چندلایه‌ای به دورهٔ حیات و فرآیند تولید نرم‌افزار است. این فرآیند از بررسی نیازها شروع می‌شود.

بر اساس دستورالعملهای این استاندارد، باید بتوان از پایین‌ترین سطوح تا بالاترین سطوح نیازها را دنبال کرد. این استاندارد برای رسیدن به هدفهای خود بر قابل دنبال بودن نیازها در کل

سطوح و مراحل تأکید فراوان می‌کند. دستیابی به این ویژگی البته کار ساده‌ای نیست. به همین دلیل استفاده از ابزارهای اتوماتیک در میان کارگزاران نرم‌افزارهای دفاعی آمریکا رواج فراوان یافته است.

شکل زیر مدل فرآیند تولید نرم‌افزار و سخت‌افزار استاندارد مذکور را نشان می‌دهد.



شکل ۱ - ۵: مدل فرآیند تولید نرم‌افزار و سخت‌افزار

دورهٔ حیات این استاندارد شبیه به مدل آبشاری است. عمده‌ترین تفاوت در درجهٔ جزئیات و گزارشات و مستندسازیهای فراوان این استاندارد است. هر مرحله از دورهٔ حیات با تکمیل موفقیت‌آمیز نیازها، طراحی و یا بازنگری آزمون به اتمام می‌رسد. در هر نقطه‌ای که باید بررسی صورت پذیرد، مستندات مختلف مطابق با قالب استاندارد تهیه می‌شود. بسیاری معتقدند که این

حجم از جزئیات، کار و مستندسازی غیر ضروری است.

اما از طرف دیگر وجود چنین امری باعث می‌شود تا تولیدکنندگان نرم‌افزار در هر مرحله از کار خود طرح‌ها و مستندات را با دقت بررسی و از بروز ناسازگاری در آنها جلوگیری کنند. این امر باعث کاهش خطر بروز خطا می‌شود و قابلیت اعتماد نظام نرم‌افزاری را بالا می‌برد. البته جنبه منفی این نوع برخورد مدت زمان طولانی تولید نرم‌افزار است.

در این استاندارد بیشترین تأکید بر تحلیل نیازها و تبیین مشخصات طرح است.

میزان مستنداتی که کارگزاران بایستی به کارفرمایان خود ارائه دهند، بسیار زیاد است. برای هر پروژه نرم‌افزاری بدون در نظر گرفتن متن اصلی برنامه و داده‌های آزمایشی، هر کارگزار باید ۲۷ مستند را به کارفرما ارائه دهد.

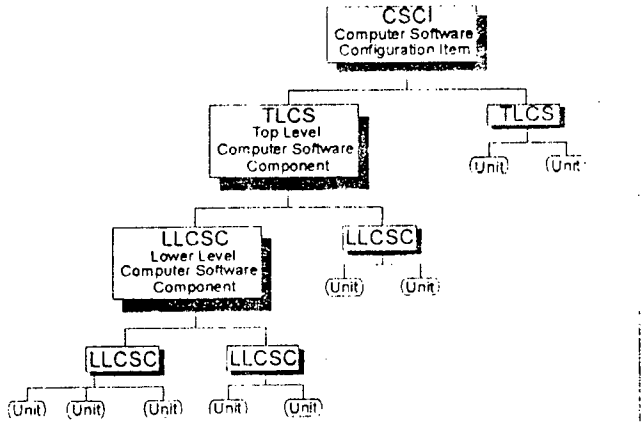
مرحله طراحی به دو زیر مرحله مجزای طراحی اولیه و طراحی دقیق و جزء به جزء تقسیم می‌شود.

طراحی اولیه مربوط است به مؤلفه‌های نرم‌افزاری سطح بالا، مانند کل برنامه‌ها یا اجزاء مهم و بزرگ آنها. پس از تصویب طرح مقدماتی، کارگزار وارد مرحله طراحی جزء به جزء می‌شود و طرح دقیق و کامل را تهیه می‌کند. البته این استانداردها تنها فرآیند توسعهٔ نرم‌افزار را شرح می‌دهد و از چگونگی تولید آن و اینکه از چه ابزاری باید استفاده کرد، سخنی به میان نمی‌آورد.

بسیاری از فعالیتهای توسعه و بازبینی در استاندارد نظام دفاعی آمریکا بر محور اجزاء پیکر نرم‌افزار کامپیوتر (CSCI) متمرکز شده است. نرم‌افزاری که بر اساس این استاندارد فراهم شده باشد از تعدادی مؤلفه موسوم به CSCI تشکیل می‌شود. یک CSCI عبارت است از یک برنامه یا یک پیمانهٔ نرم‌افزار که جدا از دیگران قابل تعریف، شناسایی و کاربرد است. در این استاندارد CSCI به صورت زیر تعریف شده است:

نرم‌افزاری که به وسیله آژانس مقاطعه‌کار جهت مدیریت پیکربندی درنظر گرفته شده است

کارگزار طرح اولیه هر CSCI را با تخصیص نیازمندیهای قید شده در اسناد کارفرما تهیه می‌کند. تصویر زیر نمودارهای ساختار زمانی CSCI ها را نشان می‌دهد:



شکل ۲ - ۵: نمودار ساختار زمانی CSCI

بررسی این استاندارد بخصوص برای دست‌اندرکاران تولید نرم‌افزارهای دفاعی کشورمان می‌تواند جالب توجه باشد، اگر چه وزارت دفاع آمریکا در صدد اصلاح کلی استانداردهای فوق است.

در پایان ذکر این نکته ضروری است که گرچه استانداردسازی وسیله‌ای برای ایجاد هماهنگی در سیستمهای مختلف می‌باشد، لیکن ممکن است در همه‌جا و خصوصاً در رابطه با ایجاد امنیت در سیستمهای کامپیوتری کارساز و کارآمد نباشد و چه بسا لازم باشد که در برخی مواقع سیستم را از حالت استاندارد خارج ساخته و یا برای ایجاد امنیت از روشهای غیر استاندارد استفاده کنیم.

پیوست ۲

در این قسمت منحنی های مقایسه دو روش DES و پیشنهادی (تلفیق RSQ و PRSQ) آمده است .

تعداد آزمایشات لازم برای شکستن روش رمزنگاری DES برابر 2^{56} و تعداد آزمایشات لازم برای شکستن روش پیشنهادی با توجه به اینکه m=8 فرض شده است، برابر 2^{8n} میباشد.

منحنی ۱ تعداد آزمایشات لازم برای شکستن روشهای مذکور به ازای $1 \leq n \leq 8$ را نشان می دهد. منحنی ۲ به ازای $1 \leq n \leq 16$ رسم شده است . منحنی ۳ زمان مورد نیاز برای شکستن الگوریتم رمز بر حسب n را نشان می دهد . این زمانها با فرض اینکه برای انجام هر آزمایش و بررسی نتیجه ، تنها یک ثانیه وقت تلف شود ، محاسبه شده اند.

منحنی های ۴ و۵ و۶ همان منحنی های ۱ و ۲ و ۳ می باشند که در آنها محور Y به صورت لگاریتمی تقسیم بندی شده است .

Chart 1

X Data	Series 1	Series 2
1	7.21E+16	256
2		65536
3		16777220
4		4.29E+09
5		1.10E+12
6		2.81E+14
7		7.21E+16
8	7.21E+16	1.84E+19

Chart 2

X Data	Series 1	Series 2
1	2.56E-18	7.21E-04
2	6.55E-16	
3	1.68E-13	
4	4.29E-11	
5	1.10E-08	
6	2.81E-06	
7	7.21E-04	
8	0.184	
9	47.2	
10	12100	
11	3090000	
12	7.92E+08	
13	2.03E+11	
14	5.19E+13	
15	1.33E+16	
16	3.40E+18	7.21E-04

Chart 3

X Data	Series 1	Series 2
1	8.12E-09	2280000
2	2.08E-06	
3	5.32E-04	
4	0.136	
5	34.9	
6	8930	
7	2280000	
8	5.85E+08	
9	1.50E+11	
10	3.83E+13	
11	9.81E+15	
12	2.51E+18	2280000

Chart 4

X Data	Series 1	Series 2
1	7.21E+16	256
2		65536
3		16777220
4		4.29E+09
5		1.10E+12
6		2.81E+14
7		7.21E+16
8	7.21E+16	1.84E+19

Chart 5

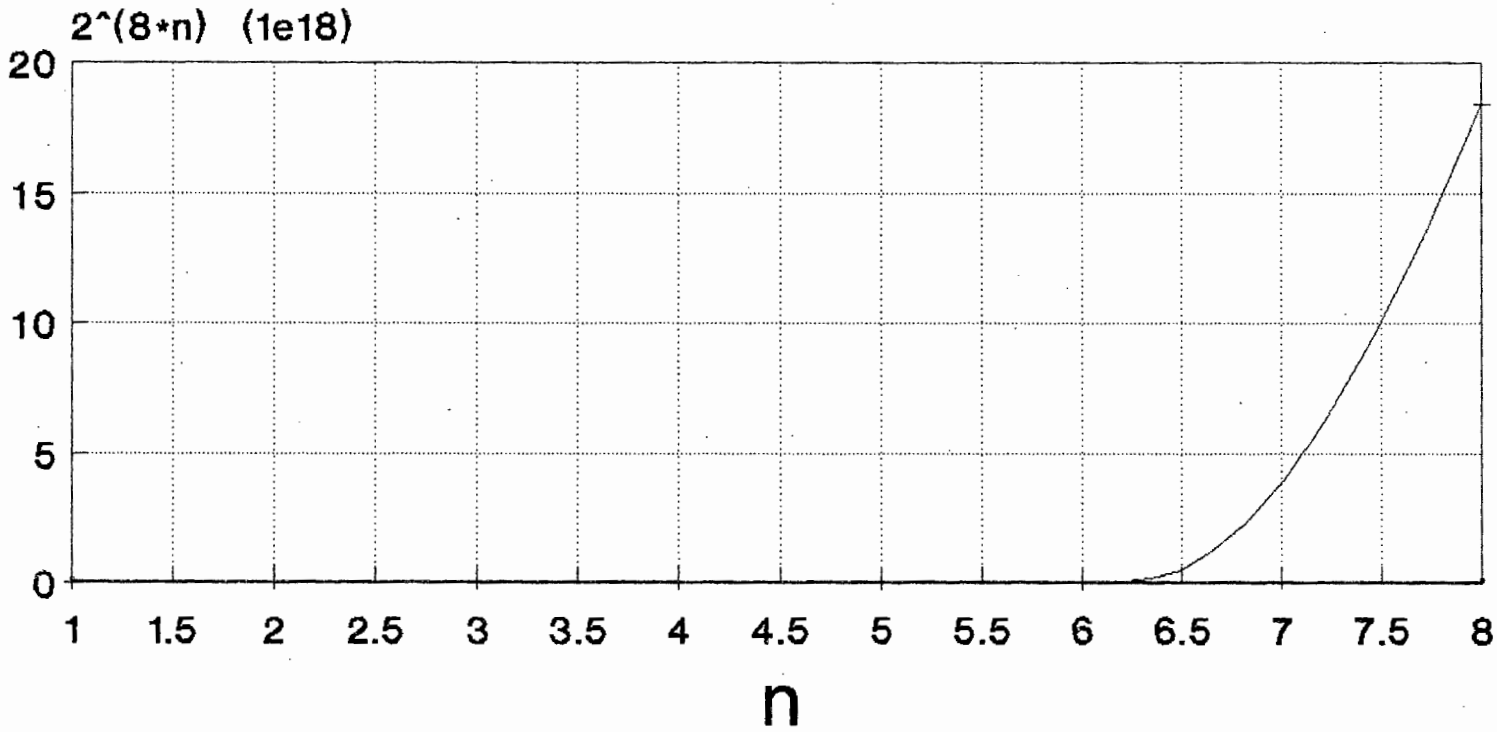
X Data	Series 1	Series 2
1	2.56E-18	7.21E-04
2	6.55E-16	
3	1.68E-13	
4	4.29E-11	
5	1.10E-08	
6	2.81E-06	
7	7.21E-04	
8	0.184	
9	47.2	
10	12100	
11	3090000	
12	7.92E+08	
13	2.03E+11	
14	5.19E+13	
15	1.33E+16	
16	3.40E+18	7.21E-04

Chart 6

X Data	Series 1	Series 2
1	8.12E-09	2280000
2	2.08E-06	
3	5.32E-04	
4	0.136	
5	34.9	
6	8930	
7	2280000	
8	5.85E+08	
9	1.50E+11	
10	3.83E+13	
11	9.81E+15	
12	2.51E+18	2280000

No. of Examinations

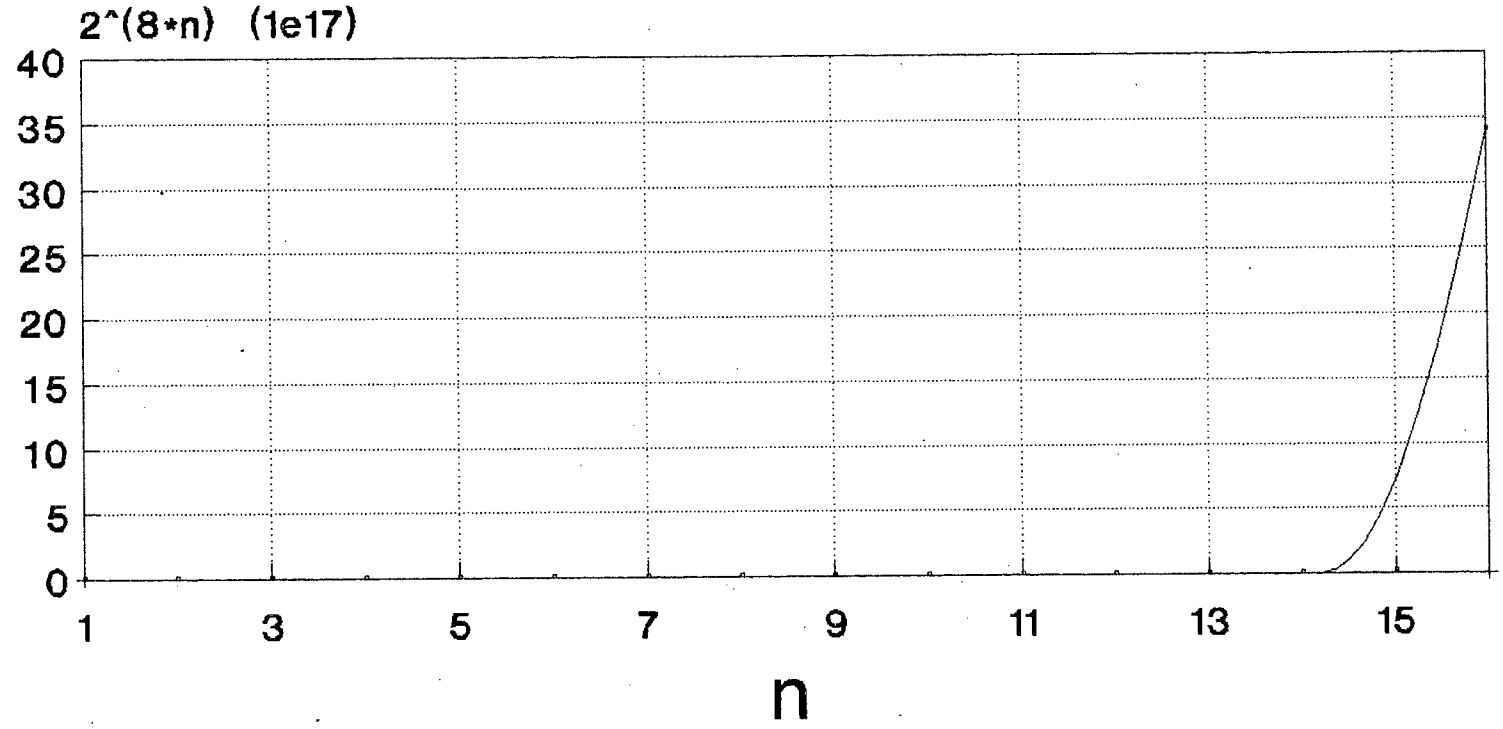
Chart 1



DES Purposed

No. of Examinations

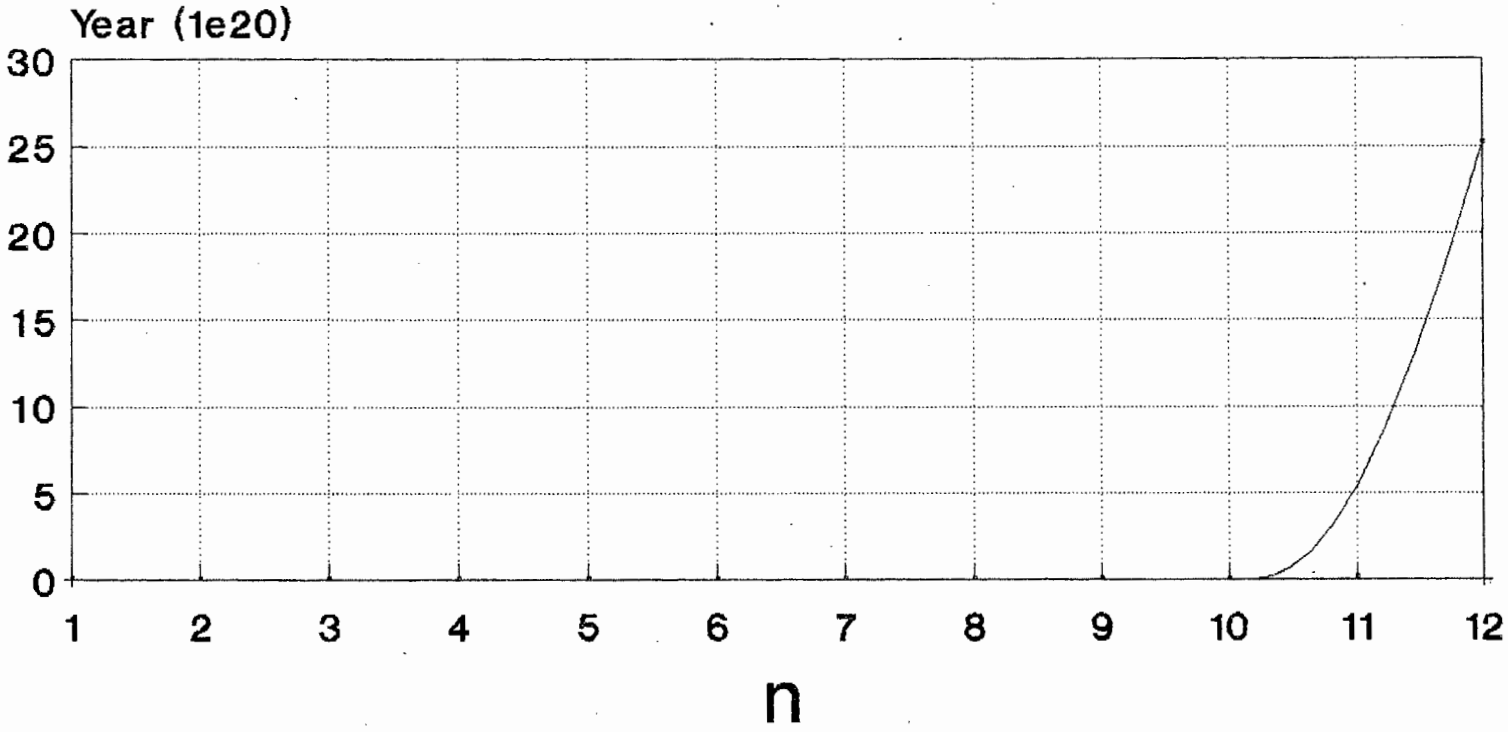
Chart 2



Purposed DES

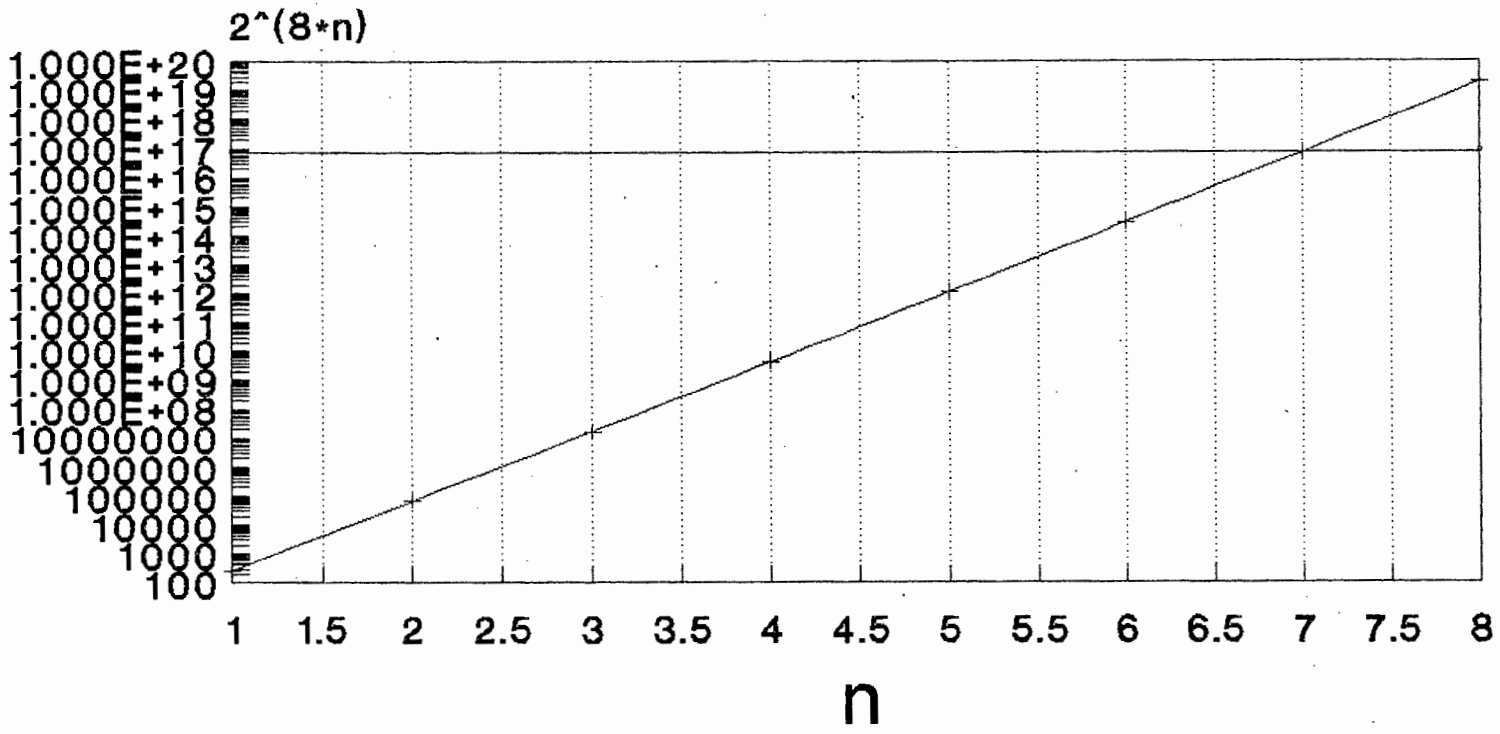
Time Requirement

Chart 3



No. of Examinations

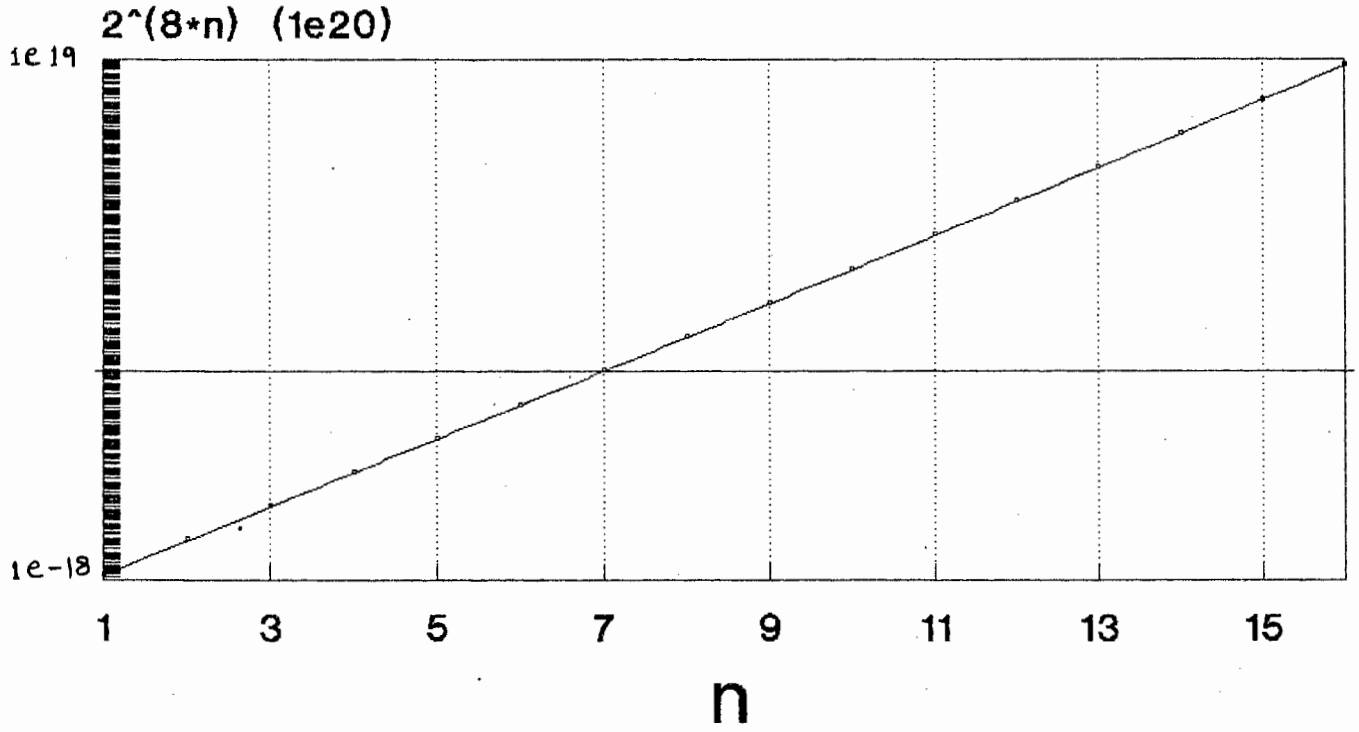
Chart 4



DES Purposed

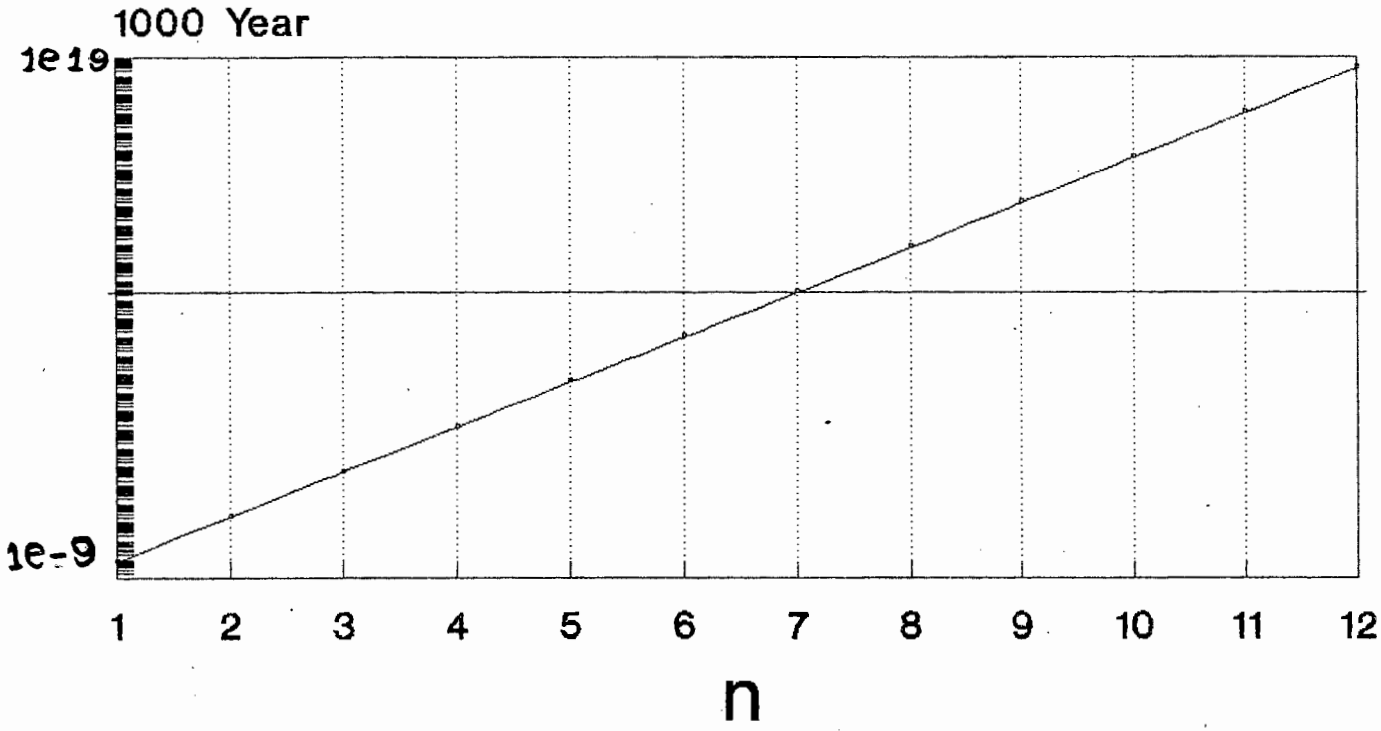
No. of Examinations

Chart 5



Time Requirement

Chart 6



Purposed DES

مراجع

1- F. Hendessi , M.R. Aref , "New Exhaustive Search Attack to the DES" , International Journal of Engineering , IUST, Vol. 4 No. 2 ,Fall 1993 , pp. 53 - 65

2- Chrisreed , "Computer Law" , Blackstone , 1993

3- F. Halsall , "Data Communication , Computer Network and Open Systems" , Addison Wesley , 1994

٤- پرویز ناصری ، " استانداردهای مهندسی نرم افزار" ، خبرنامهٔ انفورماتیك ، شماره مسلسل ٥٩ ، اردیبهشت و تیر ماه ١٣٧٤ ، صفحات ٨٨-٥٤

5- D. Elizabeth , R. Denning , "Cryptography and Data Security" , Addison - Wesley , 1983

6- J. Seberry , J. Pieprzyk , "Cryptography : an introduction to computer security" , Prentice Hall , 1988

٧- محمد حسن دزیانی ، " ابعاد جزایی کاربرد کامپیوتر وجرائم کامپیوتری " ، خبرنامهٔ انفورماتیك ، شماره مسلسل ٥٩ ، اردیبهشت وتیر ماه ١٣٧٤ ، صفحات ١٠١- ٩٤

8- J. E. Ettinger , "Information Security" , Chapman & Hall , 1993

9- Charles P. Pfleeger , "Security in Computing" , Printec Hall , 1989

10- William L. Schweber , "Data Communication",
Mc Graw - Hill ,1988

11- K.C. Zeng , C.H. Yang , D.Y. Wei , and T.R.N. Rao ,
"Pseudorandom bit generators in stream-cipher cryptography ",
IEEE Computer , February 1991 , pp. 8-17

12- C. Chan , J. M. Eng , "Global Corporate Communications with Integrated Services Digital Networks" , International Journal of Satellite Communications , Vol. 9 No. 5 , Sep - Oct 1991 , pp. 267 - 277

13- U. D. Black , "Data Communication and Distributed Networks" , Reston Book , 1992

۱٤- دکتر سید مقتدی هاشمی پرست ، "آمارواحتمال در مهندسی و علوم" ، دانشگاه فنی و مهندسی ، ۱۳۷۱

15- Peter Norton , R. Ashley , J. Fernandez , "Advanced DOS 6" ,
Prentice Hall , 1993

16- MITAC , "Technical Refrence of ADM" , 1987

17- MITAC , "Technical Refrence of ADMPLUS" , 1991

18- Joseph Wikert , "The first book of the NORTON UTILITY 7",
Prentice Hall , 1991

19- Jonathan L. Mayo , "Computer Viruses", Windcrest Books ,1989

20- From the makers of Pctools , "PCTOOLS 8.0 User's Manual" ,
Central Point Software Inc. , 1983 - 90

21- C. Sandler , T. Badgett , L. lefkowitz , "VAX Security , Protecting the System and the Data" , J. Wiley & Sons , 1990

۲۲- جزوات آموزشی شرکت Digital و Help سیستم عامل VMS

۲۳- جزوات آموزشی شرکت IBM و Help سیستم عامل VM/SP

Abstract :

One of the most important requirement for computer systems and networks is Security. In this project it is shown that for establishing security in computer systems, many points must be bear by designers, programmers, and administrators of computer centers. The resources of computer systems are Hardware, Software, Data, and Personnel. The threats for different parts of computer are Interruption, Interception, Modification, and Fabrication. To protect against these attacks, many politics and special mechanisms must be used.

Different techniques had been used for establishment of Security, each of which has many advantages and disadvantages. In this project, after investigation of a few techniques, new and simpler methods, including Composition of RSQ & PRSQ and Compression, are proposed. By comparing these methods with available methods, it has been shown that the proposed methods could be efficeint in most applications. The proposed methods are basic and could be combined and used in different applications. For selecting a suitable method for use in an application system, the sequence and proper phases of analysis, design, and implementation of systems in general, must be followed.

Iran

University of Science and Technology

(I.U.S.T)

College of Computer Engineering

A SURVEY & PROPOSAL FOR ESTABLISHING SECURITY IN COMPUTER SYSTEMS

BY

A. KHOSROBEIGI

A thesis submitted in partial fulfilment of the requirement for the degree of Master of Science in computer Engineering

Adviser:

Dr. M. Fathi & Dr . M. Sharifi

Sep. 1996