سایر آسیب پذیری ها:

به عنوان مثال افراد کلیدی سازمان یا ... می توانند آسیب پذیری را ایجاد کنند.

جریم های کامپیوتری:

۱. هر جرمی که با هدف حمله به کامپیوتر باشد.

۲. هر جرمی که به وسیله کامپیوتر انجام می شود.

مجرمین کامپیوتری:

۱. مجرمین مبتدی: فقط از راه های مشخص نفوذ استفاده می کنند، در زمینه امنیت اطلاعات خاصی ندارند و علم زیادی نیز در این زمینه ندارد، در صورت عدم دسترسی اهداف تخریبی دارند و معمولا با استفاده از نرم افزارها انجام می شود. بیشترین تعداد مجرمین را در این گروه داریم.

۲. هکرها و کرکرها: گروه هایی هستند که معمولا تحصیلات دارند و اگر نقصی وجود داشت که هیچ ولی اگر نقصی نبود راه نفوذ جدیدی ایجاد می کنند. هدفمندتر حمله می کنند. برخی از این افراد در موضوع کرک معمولا برای کسب اعتبار این کار را انجام می دهند.

۳. تروریست ها: معمولا سازمان های دولتی شرکت ها را مورد حمله قرار می دهند، و سه هدف نهایی دارند.

۳,۱. سرویس را کامل از دسترس خارج کنند. (از کار انداختن سایت های دولتی)

۳,۲. حمله به سیستم را جهت ابزار تبلیغاتی استفاده می کنند. به عنوان مثال نمایش یک شعار یا یک پرچم بر روی یکی از سایت های پربازدید.

۳,۳. استفاده پردازشی به سیستم های مورد حمله، به عنوان مثال یک گروهی در چین به آمریکا حمله می کند ولی با این روش می تواند مسیر حمله را دور بزند و مثلا از ترکیه به آمریکا حمله کنند.

در حالت امنیت لایه ای هر یک از مجرمین با توجه به علم و دانش تا یکی از این لایه ها می توانند نفوذ کنند.

روش دفاعی رمزنگاری:

صحت و محرمانگی را فراهم می کند. و جلو شنود، دستکاری و جعل را خواهد گرفت.

رمزنگاری ضعیف: رمزنگاری ضعیف داشته باشیم خیلی بدتر از این است که رمزنگاری نداشته باشیم. به این علت که احساس امنیت داریم و به همین علت با خیال آسوده اطلاعات را رد و بدل می کنیم.

روش دفاعی نرم افزاری:

کنترل هایی که در نرم افزار هست و کنترل هایی که در سیستم عامل وجود دارد.

روش های دفاعی سخت افزاری:

مانند فایروال ها، چک کردن هویت با اثر انگشت و عنبیه چشم و ...

روش های دفاعی قوانین:

یکسری قوانین ارائه می کنیم و همه باید این کار را انجام دهند. به عنوان مثال تغییر رمز سه ماه یکبار و ...

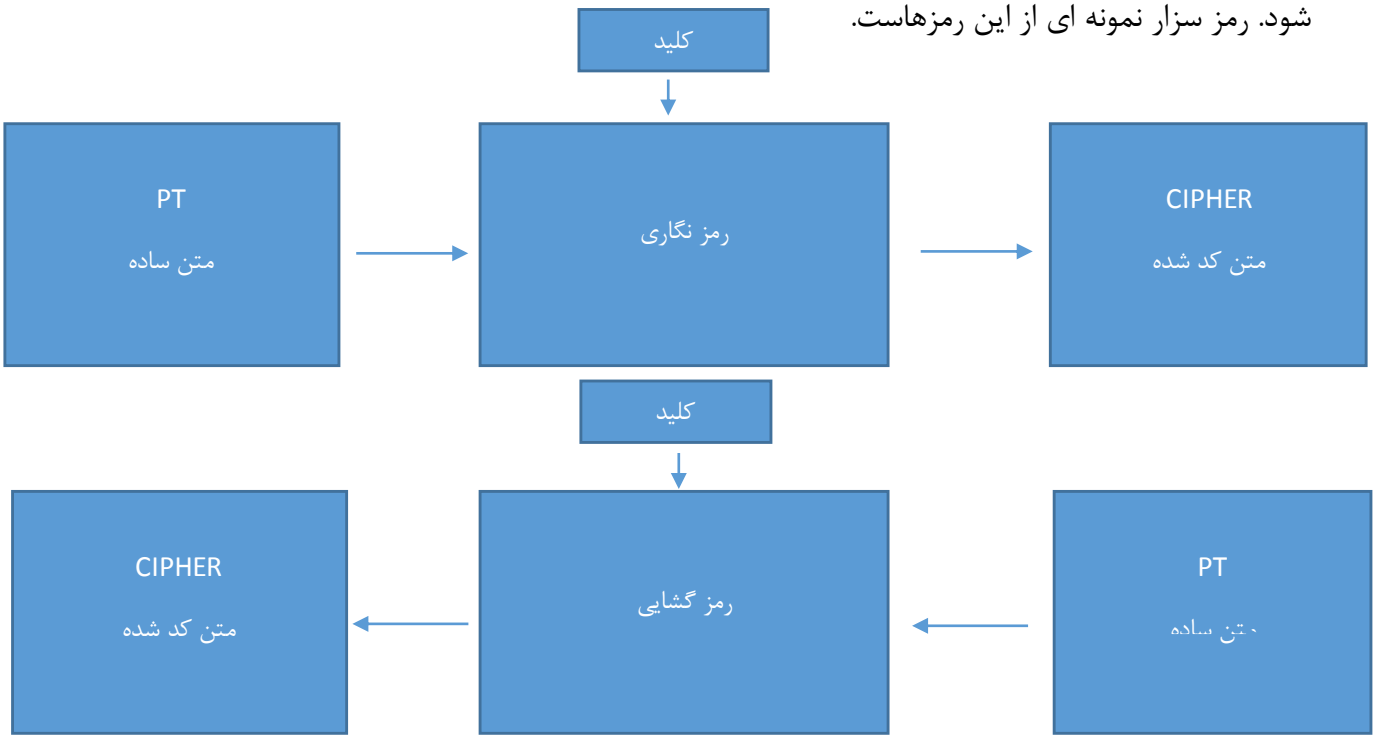
مزیت این روش ها این است که خیلی کم هزینه هستند. نیازی به سخت افزار و نرم افزار خاصی ندارد. عیب این روش این است که همیشه از تکنولوژی ها عقب تر هستند. (در واقع ابتدا باید مشکلات مطرح شوند و بعد رفع شوند) مانند پروتکل های مختلف مثل تورنت و peer to peer که در جاهای مختلف دنیا جرم هستند.

روش های دفاعی فیزیکی:

قفل ضدسرقت، اتفای حریق، توجیه کاربران، بازبینی دوره ای سیستم ها، تاکید این ها در لایه های مختلف امنیت

فصل دوم – رمزنگاری متقارن

رمزهای کلاسیک: رمزهایی که قدمت آن ها به قبل از کامپیوتر بر می گردد. بیشتر در جنگ ها استفاده می شود. رمز سزار نمونه ای از این رمزهاست.



دو الگوریتم داریم که یکی جهت رمزنگاری و دیگری جهت رمزگشایی می باشد. در ضمن در این روش ها فقط **کلید** محرمانه می باشد.

الگوریتم باید در دسترس همه قرار بگیرد تا امنیت آن سنجیده شود و افراد مختلف هم به آن اعتماد کنند.

شاخه های مطالعاتی در رمزنگاری و رمزگشایی

اصول و روش های رمزنگاری

رمزگشایی بدون داشتن کلید Cryptoanalyses

Cryptology

رمزنگاری های متقارن:

رمزنگاری های متقارن، کلید عمومی، سیمیتریک و رمزنگاری تک کلیده، رمزنگاری کلید خصوصی

شرایط رمزنگاری متقارن:

رمزنگاری که یک کلید خصوصی و محرمانه دارد. در واقع باید یک کانال امن وجود داشته باشد جهت رمزنگاری و رمزگشایی بین مبداء و مقصد (کانال امن کانالی است که فرض می کنیم شنود ندارد)

چون حجم کلید کم هست پهنای باند را کم در نظر می گیریم. در ضمن بیشترین حالت امنیت در جایی هست که پهنای باند کمتر باشد چون هر چقدر پهنای باند زیاد باشد موجب نا امنی بیشتری خواهد شد.

نمایش رابطه ای رمزنگاری ها:

$CT = E_k(PT)$

$PT = D_k(CT)$