امنیت در وب

فصل اول: مبانی امنیت

مهندس بابک حاج عظیم زنجانی

مرجع

- فصل اول کتاب زیر:

Security in computing; fourth edition
By Charles P.Pfleeger et al.

در این فصل:

- **شناسایی ریسک های موجود**
- **هدف برنامه های امنیتی:**

  محرمانگی، یکپارچگی ، دسترس پذیری
- **تهدیدهای امنیتی**

  شنود، وقفه، دستکاری، جعل.
- **کنترل های موجود در مقابل تهدیدات**

  رمزنگاری، کنترل های برنامه نویسی، سیستم های عامل، کنترل های شبکه، کنترل های مدیریت، قوانین و اخلاق

مقدمه

- امروزه به دلیل بالا رفتن و پیشرفته شدن سطوح امنیتی موجود، امکان سرقت ها، از جمله سرقت پول های بانک ازبین رفته یا کاهش یافته است.
- می توان برای محافظت از اطلاعات ارزشمند روش های حفاظتی را که در گذشته برای موارد گوناگون مانند بانک استفاده شده بکار برد.
- جدول زیر مقایسه ای بین حفاظت پول و حفاظت اطلاعات انجام داده است:

مقدمه–ادامه

خصوصیت	بانک نگهدارنده پول	افراد نگهدارنده اطلاعات
اندازه و قابلیت حمل	محل نگهداری پول ساختمان های بزرگ است؛ غیر قابل جابجایی و حمل؛ نیاز به گارد امنیتی؛ وجود سطوح امنیت فیزیکی	محل نگهداری داده کوچک است؛ اجزای محاسباتی فیزیکی بسیار کوچک بوده و تعداد زیادی از آنها قابل جاسازی در کیف و حمل است.
جلوگیری از برخورد فیزیکی	به سختی؛ بخصوص زمانی که مجرمی تقاضای پول می کند	براحتی؛ وقتی اطلاعات به صورت الکترونیکی جابجا می شوند هیچ برخورد فیزیکی وجود ندارد؛ مانند انتقال الکترونیکی پول
ارزش دارایی	بسیار بالا	متغیر، از خیلی زیاد تا خیلی کم؛ داده هایی مانند تراکنش های مالی و اطلاعات دارایی حساسیت زیاد و اطلاعاتی مانند تلفن یا ادرس که در دسترس همه است حساسیت کم دارند

مقدمه–ادامه

خصوصیات نفوذ به کامپیوتر

- هر کدام از قسمت های یک سیستم کامپیوتری می تواند به عنوان هدف حملات شناخته شوند.
- سیستم محاسباتی مجموعه ای از سخت افزار، نرم افزار، ابزارهای چندرسانه ای، داده و افرادی است که یک سازمان برای عملیات محاسباتی اش استفاده می نماید.
- تمام قسمت های یک سیستم می تواند هدف حمله قرار گیرد
- به دلیل تنوع هدف ها و حملات نظیر، امنیت کامپیوتر بسیار مشکل است.

مقدمه–ادامه

خصوصیات نفوذ به کامپیوتر–ادامه

- **اصل آسانی نفوذ:**

یک نفوذگر می تواند از هر راه نفوذی برای ورود به سیستم استفاده کند که این راه نفوذ همواره واضح ترین و مشخص ترین راهی که ما می شناسیم و آن را مقاوم نموده ایم نیست.

با توجه به این اصل، تمام نقاط ضعف سیستم باید شناخته شده و آسیب ها برطرف شوند.

حملات

- در زمان طراحی هر سیستم باید هرگونه نقص را در نظر گرفته و موارد مقابله یا رفع آنها را مشخص نماییم.

بنابراین

- **نکته اصلی طراحی سیستم امنیتی**: توجه به سوءاستفاده های احتمالی سیستم و تخریب امنیت داده ها

حملات – ادامه

آسیب پذیری، تهدید، حمله و کنترل

- **آسیب پذیری (vulnerability)**: هرگونه ضعف در امنیت سیستم

  مثال: آسیب پذیری در حفاظت از داده ها به علت عدم وارسی اصالت کاربران هنگام دسترسی

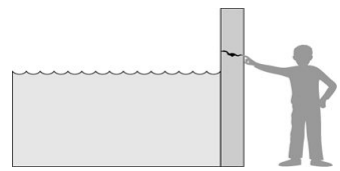
- **تهدید (threat)**: مجموعه عواملی در سیستم که پتانسیل وارد کردن آسیب و ضرر را دارند.

  مثال :
  - خطاهای انسانی
  - مشکلات نرم افزاری
  - وقایع طبیعی همچون آسیب به مرکز داده براثروقوع زلزله

حملات – ادامه

آسیب پذیری، تهدید، حمله و کنترل – ادامه

- تفاوت میان تهدید و آسیب پذیری:
  - آب موجود پشت سد به علت امکان شکستن سد، یک تهدید برای شخص است.
  - تَرک موجود در سد به عنوان یک آسیب پذیری شناخته می شود.



حملات – ادامه

آسیب پذیری، تهدید، حمله و کنترل – ادامه

- حمله **(attack)**: هرگونه آسیب پذیری که از حالت بالقوه به بالفعل تبدیل شود.

- انجام حمله علاوه بر انسان ها می تواند توسط سیستم های دیگر به وقوع بپیوندد.

مثال : وقتی سیستمی مجموعه ای از پیام ها را برای سیستم دیگری می فرستد و بطور مجازی باعث از بین رفتن عملکرد آن می شود. مانند حمله منع سرویس یا denial of service .

حملات – ادامه

آسیب پذیری، تهدید، حمله و کنترل – ادامه

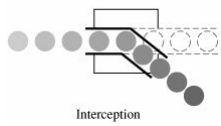
- کنترل به عنوان یک اقدام محافظتی شناخته می شود.
- **کنترل** : هر عمل ، ابزار ، رویه و یا تکنیکی که به منظور حذف یا کاهش آسیب پذیری ها مورد استفاده قرار می گیرد.
- رابطه تهدید، کنترل و آسیب پذیری به صورت زیر است:

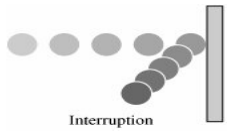
تهدید ها با کنترل آسیب پذیری ها حذف می شوند.

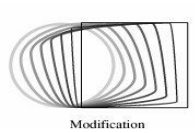
حملات – ادامه

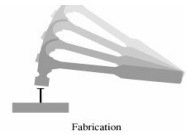
هر تهدید می تواند یکی از انواع زیر باشد:

- شنود(interception)
- وقفه (interruption)
- دستکاری (modification)
- جعل هویت (fabrication)





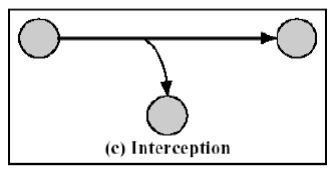


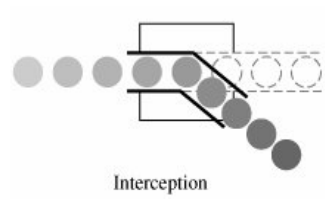


حملات – ادامه

- شنود: دسترسی یک موجودیت غیرمجاز به داده های در حال جریان بین مبدا و مقصد
- موجودیت غیرمجاز می تواند شخص ، سیستم کامپیوتری ، برنامه های کامپیوتری و ... باشد.

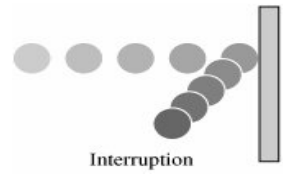
- مثال : کپی غیرقانونی داده ها ، شنود داده های شبکه و ....





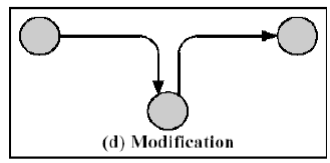
حملات – ادامه

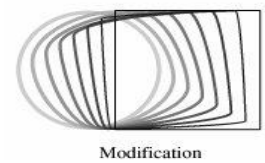
- وقفه : از کار انداختن ، از دسترس خارج کردن ویا غیرقابل استفاده کردن یک دارایی سیستم
- مثال : از کارانداختن یک سخت افزار ، پاک کردن اطلاعات یک فایل داده



حملات – ادامه

- **دستکاری : هرگونه تحریف یا دستکاری در داده ها توسط یک شخص غیرمجاز**
- **مثال: تغییر در مقدار داده های یک پایگاه داده ، تغییر در عملیات اجرایی یک برنامه کامپیوتری**

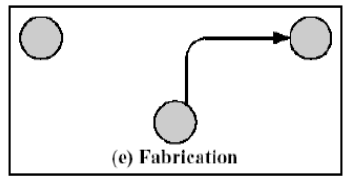


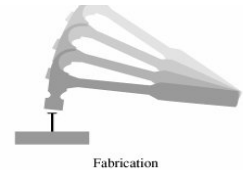


حملات – ادامه

- جعل هویت : ایجاد موجودیت جعلی توسط یک شخص غیرمجاز

- مثال : اضافه کردن یک رکورد در پایگاه داده ، ایجاد تراکنش جعلی در شبکه





حملات– ادامه

نفوذگر

- یک شخص نفوذگر نیازمند سه مورد است :
  - روش : مهارت ، دانش ، ابزار مناسب
  - فرصت : زمان و امکان دسترس
  - انگیزه : دلیل برای انجام حمله

- اطلاعات راجع به سیستم ها در عین کارا بودن به آسانی در دسترس نفوذگرها هستند. بسیاری از تولیدکنندگان اطلاعاتی راجع به طراحی سیستم ها در اختیار قرار میدهند وبه این ترتیب نقاط ضعف سیستم ها آسان تر کشف می شوند.

امنیت سیستم کامپیوتری

- هر سیستم کامپیوتری دارای ضعف های ذاتی و اجرایی است.
- هدف امنیت کامپیوتر پیشنهاد راه هایی برای جلوگیری از سوءاستفاده از ضعف ها می‌باشد.

هدف امنیت :

- امنیت سیستم های کامپیوتری دارای سه وجه است :
  - محرمانگی (confidentiality)
  - صحت اطلاعات (integrity)
  - دسترس پذیری (availability)

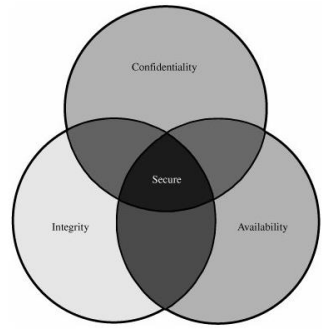
امنیت سیستم کامپیوتری

هدف امنیت – ادامه

- **محرمانگی** : مجموعه مکانیزم هایی که از دسترسی افراد غیرمجاز به اطلاعات کاربران جلوگیری می کند. دسترسی به معنای خواندن، دیدن، پرینت و به طور کلی اطلاع از آنچه وجود دارد می باشد.
- **صحت اطلاعات(integrity)**: مجموعه مکانیزم هایی که از هرگونه تحریف، دستکاری و حذف اطلاعات توسط افراد غیرمجاز جلوگیری می کند.
- **دسترسی پذیری (availabilty)**: افراد مجاز امکان دسترسی به داده ها را در زمان مناسب داشته باشند. گاهی این مفهوم با متضاد آن یعنی منع سرویس (denial of service) شناخته می شود.

ارتباط میان محرمانگی، صحت، دسترس پذیری

- شکل زیر ارتباط بین ۳ مفهوم را بیان می کند که این مفاهیم در عین مستقل بودن با یکدیگر همپوشانی نیز دارند.



آسیب پذیری ها

- همواره در مراحل اولیه طراحی و آماده نمودن یک سیستم باید به موارد آسیب پذیری آن و روش های جلوگیری از آنها توجه داشت.
- آسیب پذیری های سیستم به سه دسته تقسیم می شوند :
  - مرتبط با سخت افزار
  - مرتبط با نرم افزار
  - مرتبط با داده ها
- چهار نوع حمله ذکر شده (شنود، وقفه، دستکاری و جعل هویت) برای هر کدام از سه مورد امکان پذیر است.

آسیب پذیری ها – سخت افزار

- سخت افزار ها به دلیل فیزیکی و قابل دید بودن بسیار آسیب پذیر هستند.
- از جمله مواردی که سخت افزار ها را تهدید می کنند :
  - رطوبت
  - گرد و غبار
  - آسیب به قسمت های متحرک و ماشینی کامپیوتر بوسیله دود (ازجمله دود سیگار)
  - بلایای طبیعی (زلزله ، سیل ، ..)
  - سرقت
  - آسیب فیزیکی به کابلهای شبکه (مثلاً جویده شدن کابل و سیم توسط موش ! یا قطع عمدی کابل)
  - اضافه یا حذف کردن برخی از اجزا
  - از بین رفتن توسط بمب، آتش سوزی و ...

آسیب پذیری ها– نرم افزار

- یک سیستم کامپیوتری بدون وجود نرم افزار هیچ گونه کارایی ندارد.
- نرم افزارها می توانند در معرض جابجایی، تغییر، خراب شدن و یا حذف قرار گیرند.
- گاهی تغییرات و آسیب ها واضح و قابل شناسایی هستند؛ اما گاهی مشخص نشده و به نظر می رسد نرم افزار به خوبی کار می کند.
- انواع تهدید ها:
  - ازکار انداختن نرم افزار
  - تغییر عملکرد نرم افزار به عملکرد مورد نظر
  - اضافه کردن عملیاتی به عملیات اصلی نرم افزار
  - کپی برداری غیرمجاز و ...
- به طور کلی آسیب پذیری های نرم افزار به سه دسته تقسیم می شوند: حذف، دستکاری ، سرقت

آسیب پذیری ها- نرم افزار -حذف

- مشکل اصلی نرم افزارها این است که امکان حذف ، خراب شدن و ناقص کپی شدن آنها به سادگی وجود دارد.

- در مراکز داده ، برای حذف این مشکل از مدیریت پیکربندی استفاده می شود.

- مدیریت پیکربندی تنها زمانی اجازه می دهد یک برنامه با نسخه جدید خود جایگزین شود که از عملکرد صحیح برنامه جدید مطمئن باشد.

آسیب پذیری ها- نرم افزار- دستکاری

دستکاری نرم افزارها:

- نوع اول: تغییر یک یا دو بیت در یک نرم افزار می تواند با عث خراب شدن یا تغییر عملکرد نرم افزار شود.
- نوع دوم : برنامه به صورت عادی کار می کند، اما در زمان های خاص یا در حلقه های خاص دچار مشکل می شود و حتی ممکن است برنامه کاملا از کار بیفتد.
- نوع سوم : یک قابلیت به برنامه اضافه می شود تا برنامه کار اضافه ای را نیز انجام دهد. به عبارت دیگر برنامه دارای جنبه های مخفی خواهد بود.

آسیب پذیری ها- نرم افزار- دستکاری

- نمونه های دیگری از دستکاری عبارتند از :
  - اسب تروجان : برنامه هایی که در ظاهر یک عمل را انجام می دهند ولی در باطن کار دیگری را انجام می دهند.
  - ویروس : نوع خاصی از اسب تروجان، که می تواند خود را از کامپیوتری به کامپیوتر دیگر منتقل کند.
  - Trapdoor: برنامه ای که یه راه ورود مخفی دارد.
  - کد هایی که به افراد یا برنامه های غیرمجاز اجازه دسترسی به اطلاعات را می دهند.

آسیب پذیری ها- نرم افزار- سرقت

- **سرقت نرم افزار** شامل هر گونه کپی برداری غیرمجاز از نرم افزار ها است.
- تولیدکنندگان و صاحبان نرم افزار نیز مانند نوازنده ها و یا نویسندگان کتاب لازم است محصولاتشان به درستی و با رعایت حقوق آنها استفاده شود.

آسیب پذیری ها- داده ها

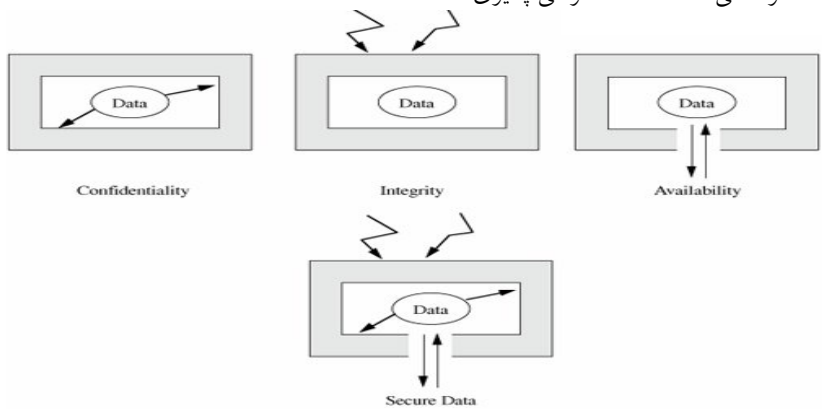
- آسیب پذیری داده ها از آسیب پذیری نرم افزار و سخت افزارها مهم تر می باشد، زیرا :
  - داده ها را افراد بیشتری می توانند درک کنند و مورد استفاده قرار دهند.
  - ارزش نرم افزار و سخت افزار ها به مرور زمان کاهش می یابد، این در حالی است که با گذشت زمان ارزش داده معمولا افزایش می یابد.

اصل کافی بودن محافظت: موجودیت های کامپیوتری تا زمانی که دارای ارزش هستند باید محافظت شوند.

بنابر این اصل موجودیت هایی با عمر مفید کوتاه نیاز به محافظت کمتر دارند و برعکس.

آسیب پذیری ها- داده ها

- محرمانگی ، صحت ، دسترسی پذیری داده ها :



آسیب پذیری ها- داده ها

محرمانگی داده ها :

داده ها معمولا در قالبی ذخیره می شوند که افراد عادی نیز توانایی درک و استخراج اطلاعات کافی از آنها را دارند. به همین دلیل محرمانگی داده اهمیت زیادی دارد.

از جمله راه های شکستن محرمانگی داده ها:

- انشعاب گرفتن از اتصالات شبکه و کامپیوتر
- کاوش در اطلاعات دور ریخته
- نفوذ از طریق یکی از کارمندان اصلی
- و .....

آسیب پذیری ها- داده ها

- داده های کامپیوتری تنها اطلاعات چاپ شده بر روی کاغذ نمی باشند ، انواعی همچون:
  - اطلاعات دیجیتالی ذخیره شده روی سی دی و دی وی دی ها
  - اطلاعات ترافیک شبکه ها و خطوط تلفن
  - اطلاعات منتقل شده از طریق ماهواره ها
  - .....
- این دسته از داده ها مشکلات بیشتری در زمینه تامین امنیت دارند.

آسیب پذیری ها- داده ها

صحت داده ها :

- سرقت اطلاعات، فقط نیازمند توانایی درک اطلاعات است. درحالیکه برای تغییر داده ها یا جعل داده ها، نیاز به داشتن اطلاعاتی همچون نوع تکنولوژی مورد استفاده ، فرمت ذخیره داده ها است.
- نوع دیگری از حمله **پردازش مجدد داده های پردازش شده** است.
  - مثال : ارسال مجدد پیغام بانکی جهت انتقال مجدد پول به حساب خود
  - تغییر در پیغام بانکی ارسال شده ، جهت تغییر در مبلغ

انواع دیگرآسیب پذیری ها

- **شبکه ها :** به علت امکان دسترسی از راه دور افراد احراز اصالت نشده به منابع
- **دسترسی ها:** دسترسی به سیستم ها سه نوع آسیب پذیری به همراه دارد:
  - تلف کردن وقت کامپیوتر ها با انجام کارهای غیرمرتبط
  - تخریب و آسیب رساندن به داده ها و برنامه ها
  - جلوگیری از دسترسی افراد مجاز
- **افراد کلیدی:** اگر به تنهایی به اطلاعاتی دسترسی داشته باشند، به عنوان یک گلوگاه در امنیت سیستم تلقی می شوند.

جرم کامپیوتری

- **جرم کامپیوتری** : هر گونه جرمی که به کمک کامپیوتر و یا با هدف حمله به یک کامپیوتر انجام می شوند.

- برای جلوگیری از جرایم رایانه ای لازم است بدانیم چه افرادی و با چه هدفی دست به این جرایم می زنند.

انواع مجرمان کامپیوتری

افراد آماتور و غیرحرفه ای :

- بیشتر جرایم کامپیوتری توسط این افراد صورت می گیرد.
- این افرادی ، معمولا مجرمان حرفه ای نیستند، بلکه افرادی هستند که متوجه یک نقص در امنیت سیستم می شوند.
- در صورت عدم شناسایی نقص هایی درسیستم، سعی در اقداماتی همچون اتلاف وقت کامپیوتر ها می نمایند.

مجرمان کامپیوتری – ادامه

هکر ها و کرکر ها :

- معمولا دارای تحصیلات دانشگاهی در زمینه کامپیوتر هستند.
- کرکر ها معمولا تمایل دارند اثبات کنند توانایی نفوذ به سیستم ها را دارند حتی اگر از این نفوذ خود استفاده دیگری نکنند.

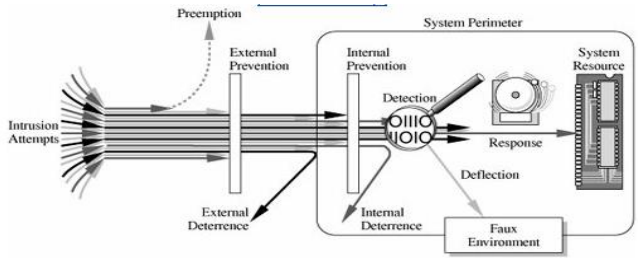
مجرمان کامپیوتری– ادامه

تروریست :

- این افراد به سه روش از کامپیوتر بهره مند می شوند :
  - سیستم کامپیوتری به عنوان **هدف حمله** قرار می گیرد. به عنوان مثال حمله منع سرویس(DOS)
  - **ابزار تبلیغ** : وب سایت ، وبلاگ و ایمیل ها ، آسان ترین ، ارزانترین و سریع ترین راه انتقال پیام ها هستند.
  - **ابزار حمله** : سیستم کامپیوتری به عنوان ابزاری در مسیر حمله استفاده می شوند.

روشهای دفاع

- شکل زیر راه های مختلف محافظت در برابر حملات را نشان می دهد.



- بسته به درجه اهمیت اطلاعات و یا نسبت هزینه مصرفی به ریسک وقوع حملات می توان از یک یا چند روش ذکر شده استفاده شد.

روشهای دفاع – رمزنگاری

- مشکل اصلی امنیت داده ها، قابل فهم بودن آنها برای اکثر کاربران است.
- برای تامین امنیت داده ها، باید آنها را به صورت کد شده تبدیل کنیم.
- از جمله اصطلاحات راجع در رمز نگاری می توان به موارد زیر اشاره کرد:
  - Cleartext: متن واضح و بدون هیچ رمزنگاری
  - Ciphertext : متن رمزشده به صورت غیرقابل فهم برای افراد غیرمجاز
- رمزنگاری امکان جلوگیری از جعل اطلاعات یا دستکاری غیرمجاز را فراهم می آورد.

روشهای دفاع- رمزنگاری

- رمزنگاری با وجود فواید خود ، به تنهایی نمی تواند به عنوان یک مکانیزم دفاعی استفاده شود.

- رمزنگاری ضعیف می تواند آسیب بیشتری را نسبت به عدم وجود رمز به همراه داشته باشد، زیرا به سادگی شکسته می شود در حالی که برای کاربران احساس وجود امنیت کافی را به همراه دارد.

روشهای دفاع – نرم افزاری

- در کنار رمزنگاری داده ها ، برنامه ها نیز خود باید از روش هایی برای تامین امنیت بهره مند شوند.
  - **کنترل های داخلی برنامه ها** : قسمت هایی از برنامه که دسترسی کاربران را محدود می کنند.
  - **کنترل های سیستم عامل وشبکه ها** : کنترل محدوده کاربران از یکدیگر توسط سیستم عامل و شبکه ها
  - **برنامه های کنترلی مستقل** : برنامه هایی همچون چک کننده پسورد کاربران ، سیستم تشخیص نفوذ و ...
  - **توسعه دهندگان کنترل** : استاندارد های کنترل کیفیت

روشهای دفاع – سخت افزاری

- سخت افزارهای گوناگونی جهت کمک به تامین امنیت سیستم های کامپیوتری تهیه شده است:
  - سخت افزارهای پیاده سازی رمزنگاری
  - دیواره آتش
  - ابزارهای تشخیص هویت کاربران
  - سیستم های تشخیص نفوذ
  - و .....

روشهای دفاع– قوانین

- این دسته از روش ها ساده ترین و کم هزینه ترین متدهای دفاعی هستند. مثال : مجبور کردن کاربران به تعویض گاه گاه کلمه عبور خود.
- از جمله مشکلات این روش عدم تطابق سرعت استاندارد ها با سرعت پیشرفت تکنولوژی کامپیوتر است.
- از جمله مشکلات دیگر آن عدم وجود قوانین کافی و مشخصی در مورد رفتارهای صحیح و ناصحیح در ارتباطات کامپیوتری است.

روشهای دفاعی- فیزیکی

- از جمله اقداماتی که در این زمینه می توان به آنها اشاره کرد:
  - حفاظت های امنیتی از محل نگهداری اطلاعات مثل سیستم ضدسرقت و ...
  - کپی برداری منظم و مداوم از داده ها
  - برنامه ریزی مناسب جهت ساختن مکان مناسب برای نگهداری اطلاعات به طوری که از آسیب های طبیعی مثل سیل، زلزله به دور باشند.

راه هایی جهت افزایش کارایی روشهای دفاعی

- **افزایش آگاهی کاربران** : درصورتی که کاربران آگاهی کافی در مورد مشکلات امنیتی و کارایی روش های امنیتی داشته باشند، بیشتر به استفاده آنها متمایل می شوند.
- متدهای دفاعی تنها در صورتی مفید واقع می شوند که مورد استفاده قرار گیرند.(قفل درب در صورتی که درب باز باشد ، فایده ای ندارد.)
- **بازنگری دوره ای** : راه های دفاعی تنها برای بازه زمانی مشخصی کارایی دارند. به همین دلیل بررسی کارایی یک روش باید به صورت دوره ای و مداوم صورت گیرد.
- استفاده از چندین روش دفاعی به صورت همزمان