به نام خدا

# امنیـــت شبـــکه

بهزاد مولوی  میلاد سلطانی

***انتشارات ارســطو***

***( چاپ و نشــر ایران )***

***۱۳۹۳***

سرشناسه : مولوی ، بهزاد ، ۱۳۶۸
عنوان و نام پدیدآور : امنیت شبکه/ بهزاد مولوی ، میلاد سلطانی.
مشخصات نشر : مشهد : ارسطو ، ۱۳۹۳
مشخصات ظاهری : ۱۴۵ ص : .مصور.
شابک : 9 78-964-91176-7-6
وضعیت فهرست نویسی : فیپا
موضوع : شبکه های کامپیوتری -- تدابیر ایمنی
موضوع : کامپیوترها -- ایمنی اطلاعات
شناسه افزوده : سلطانی، میلاد ، ۱۳۶۴
رده بندی کنگره : TK۵۱۰۵/۸ الف ۸م / ۵۹ :۱۳۹۳
رده بندی دیویی : ۰۰۵۸/
شماره کتابشناسی ملی : ۳۵۳۶۵۲۳

نام کتاب : امنیت شبکه
مولفان : بهزاد مولوی – میلاد سلطانی
ناشر : ارسطو ( چاپ و نشر ایران )
نوبت چاپ : اول ۱۳۹۳
شمارگان : ۱۰۰۰
صفحه آرایی و طرح جلد : پروانه مهاجر
قیمت : ۱۴۵۰۰ تومان
شابک : 9 78-964-91176-7-6
تلفن های مرکز پخش : ۵۰۹۶۱۴۶-۵۰۹۶۱۴۵-۰۵۱۱
www.chaponashr.ir

یارب دل ما را تو به رحمت جان ده، درد همه را به صابری درمان ده

این بنده چه داند که چه می باید جست، دانندهٔ تویی هر آنچه دانی آن ده

تقدیم به مهربان فرشتگانی که:

لحظات نـاب باور بودن، لذت و غرور دانسـتن، جسارت خواستن، عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگیم، مدیون حضور سبز آنهاسـت

# مقدمه

به نام خداوند لوح و قلم. حقیقت نگار وجود و عدم، خدایی که داننده‌ی رازهاست، نخستین سرآغاز آغازهاست. امروزه پیشرفت روزافزون علم کامپیوتر و الکترونیک سبب شده است که بیشتر ارتباطات انسان از طریق دنیای مجازی شبکه‌های کامپیوتری صورت بگیرد. عدم مراجعه حضوری افراد در محیط‌های عمومی، کابرپسندی، سرعت بالای انجام کارها در محیط مجازی سبب شده است که بیشتر کارهای اداری کاربران از طریق دنیای مجازی صورت گیرد. از چالش‌های اصلی ارتباطات مجازی، برقراری و حفظ امنیت کاربران می‌باشد. پیشرفت‌های نرم‌افزاری باعث شده است که افراد با کمترین دانش ارتباطی می‌توانند مخرب‌ترین ابزارها نفوذ به شبکه‌های کامپیوتری را در دسترس داشته باشند. از این رو امروزه حفظ امنیت کاربران در شبکه‌های کامپیوتری به عنوان یکی از نیازهای اساسی مطرح می‌گردد.

کتاب حاضر رویه امن‌سازی پروتکل‌های تجاری را مورد بررسی قرار می‌دهد. بخش عظمی از پروتکل‌های معرفی شده در این کتاب مبتنی بر منحنی بیضوی می‌باشد. در فصل اول و دوم این کتاب اهمیت برقراری امنیت و تعاریف پایه‌ای در بحث امنیت شبکه مطرح می‌شود. در فصل سوم مقدمات ریاضی لازم در جهت منحنی بیضوی مطرح می‌گردد. این فصل باعث می‌شود که خواننده درک بهتری از ابزار پروتکل‌های تجاری مبتنی بر منحنی بیضوی داشته باشد. در فصل چهارم اهیمت و ویژگی امضاء دیجیتال در محیط تجاری، و بررسی چند پروتکل امضاء بیان شده است. فصل پنجم شامل طریقه ایجاد تبادلات مالی امن و کنترل دسترسی در شبکه می‌باشد. در فصل ششم روش‌های تحلیل پروتکل تجاری مورد بحث قرار می‌گیرد.

در انتها از تمام اساتید و دوستان که ما را در تهیه این اثر یاری نمودند کمال تشکر را دارم. با توجه به اینکه هیچ کتابی بدون اشکال نیست، اگر اشکالی در این کتاب مشاهده فرمودید بر ما بخشیده و نظرات و اطلاحات خود را به آدرس الکترونیکی **behzad_molavi2006@yahoo.com** ارسال نمایید.

بهزاد مولوی قلعه‌نی

میلاد سلطانی

# فهرســت مطالــب

# فصل اول

## مقدمه امنیت شبکه

### ۱–۱ امنیت چیست؟

اگر بخواهیم تعریف کلی از امنیت داشته باشیم، می‌توانیم بگوییم محافظت از آنچه که مورد ارزش است امنیت می‌باشد. در گذشته برقراری امنیت توسط حراست فزیکی صورت می‌گرفت. افزایش تعداد نگهبان‌ها، استفاده از قفل‌های سنگین، استفاده از دیوارهای بلند و ... نمونه‌هایی از حراست فزیکی می‌باشند. توسعه و پیشرفت علوم کامپیوتر باعث گردید که روند نگهداری اسناد از حالت فزیکی به حالت الکترونیکی قرار گیرد. افزایش سرعت دسترسی افراد، عدم خرابی فزیکی اسناد، فضای کم فزیکی نگهداری و ... از مزیت‌های ذخیره‌سازی اسناد به صورت الکترونیکی است. قرارگیری اسناد از حالت فزیکی به حالت الکترونیکی سبب شد تا مسئله امنیت در این محیط به صورت خاصی تعریف شود. در دنیای کامپیوتر، برقراری محرمانگی[۱]، صحت[۲]، دسترسی پذیری[۳]، بروی منابع اطلاعاتی سیستم را امنیت[۴] گوییم.

- محرمانگی: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز است. معمولا این نیاز با ابزارهای رمزنگاری رفع می‌شود.

---

[1] *Confidentiality*
[2] *Integrity*
[3] *Availability*
[4] *Security*

- صحت: صحت یعنی جلوگیری از تغییر داده‌ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات. صحت وقتی نقض می‌شود که اطلاعات در حین انتقال بصورت غیرمجاز تغییر داده می‌شود. سیستم‌های امنیت اطلاعات به طور معمول علاوه بر محرمانه بودن اطلاعات، صحت آنرا نیز تضمین می‌کنند.

- دسترسی پذیری: دسترسی پذیری در سیستم‌های اطلاعاتی یعنی اینکه کاربران مجاز بتوانند به راحتی به اطلاعات دسترسی داشته باشند. برقراری امنیت باید به گونه‌ای باشد که دسترسی کاربران مجاز دشوار نشود، این رویه باید به گونه‌ای باشد که کاربران غیر مجاز نتوانند به منابع اطلاعاتی سیستم دسترسی پیدا کنند.

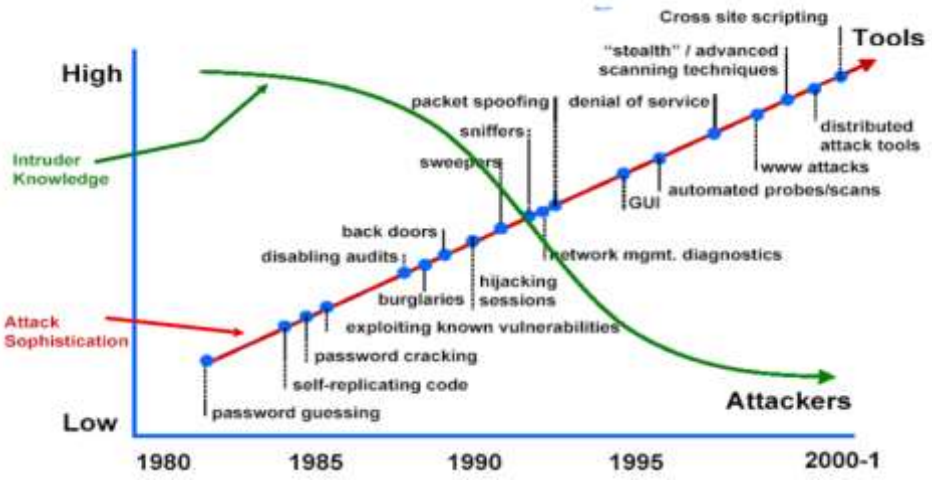
## ۲-۱ بررسی اهمیت امنیت

آمارهای منتشر شده از سازندگان ضد مخرب‌ها نشان می‌دهد که ابزارهای نفوذ به شبکه‌های کامپیوتری روزبه‌روز در حال توسعه می‌باشند، از طرفی این ابزارها به راحتی در دسترس افراد قرار می‌گیرد، این امر باعث می‌شود که افراد با کمترین دانش از علوم امنیت مخرب‌ترین حملات را پیاده‌سازی نمایند.

شکل ۱ دو نمودار دانش و رویه رشد ابزاهای نفوذگران را در سال‌های متفاوت نشان می‌دهند. همانطور که در شکل دیده می‌شود در سال ۱۹۸۰ نفوذگران فقط ابزارهای حدس رمز عبور کاربران را در دسترس داشته‌اند، از این رو برای پیاده‌سازی سایر حملات[1] می‌بایست دانش زیادی از علم امنیت داشته باشند، رشد ابزارهای نفوذ در

[1] *Attacks*

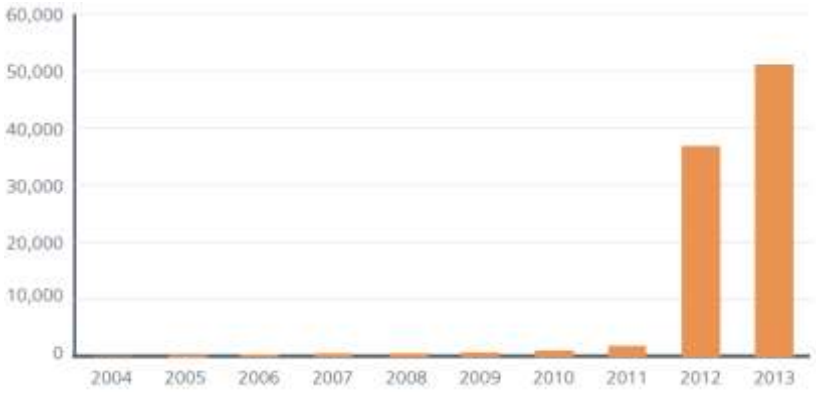
شبکه‌های کامپیوتری سبب شد تا دانش نفوذ به شبکه‌های کامپیوتری کاهش یابد. در شکل ۱ همانطور که مشاهده می‌کنید در سال ۲۰۰۱ نفوذگران با کمترین دانش و بالاترین ابزار می‌توانند خطرناک‌ترین حملات در محیط مجازی را پیاده‌سازی نمایند [1].




شکل ۱ دانش و ابزار نفوذگران

شکل ۲ رویه رشد بدافزارها[1] را در سال‌های متفاوت نشان می‌دهد، همانطور که مشاهده می‌کنیم، رویه رشد در سال‌های اخیر بیشینه می‌باشد. آمارهای ذکر شده نشان می‌دهد که برقراری امنیت در محیط مجازی روزبه‌روز در حال افزایش می‌باشد.

[1] *Malware*




شکل ۲ روند رشد بدافزارها به گزارش شرکت کاسپر

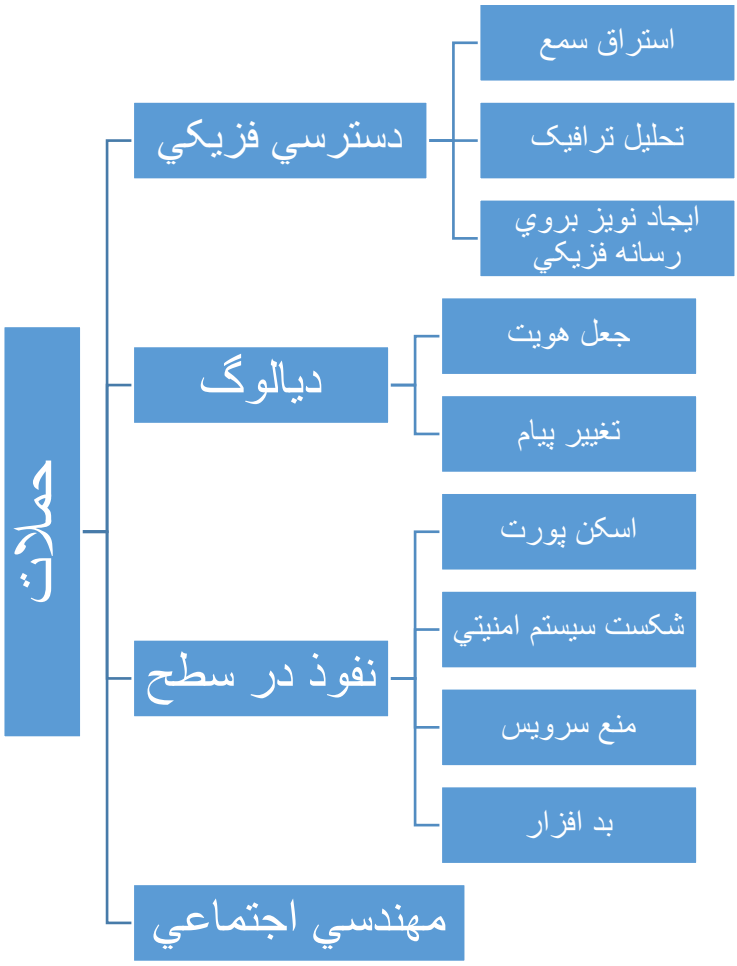
## ۳-۱ دسته‌بندی حملات

حملات موجود در شبکه‌های کامپیوتری از نظر وضعیت ارتباط به دو دسته زیر تقسیم می‌شود [2].

۱- حملات فعال[1]
۲- حملات غیر فعال[2]

در حملات فعال نفوذگر منابع اطلاعاتی سیستم را به صورت غیر قانونی تغییر می‌دهد اما در حملات غیرفعال نفوذگر بدون تغییر منابع اطلاعاتی، حمله را انجام می‌دهد. معمولا حملات فعال مخرب‌تر از حملات غیرفعال می‌باشند.

[1] *Active*
[2] *Passive*




شکل ۳ تقسیم حملات

حملات بر حسب پیاده‌سازی به چهار دسته دسترسی فزیکی[۱]، دیالوگ[۲]، نفوذ در سطح، مهندسی اجتماعی[۲] تقسیم می‌شوند [3].

[1] *Physical Access Attacks*
[2] *Dialog Attacks*

در حملات دسترسی فزیکی، رسانه فزیکی مورد حمله قرار می‌گیرد. شنود کانال فزیکی، تحلیل ترافیک کانال، ایجاد نویز در کانال در جهت قطع ارتباط، نمونه‌هایی از حملات فزیکی می‌باشد. حملات شنود و تحلیل ترافیک جزء حملات غیر فعال می‌باشند و حمله نویز کانال جزء حملات فعال است.

حملات دیالوگ در لایه‌های مختلفی از شبکه می‌توانند پیاده‌سازی شوند، در حمله جعل هویت نفوذگر هویت یک نود مجاز در داخل شبکه را بدست می‌آورد، سپس نفوذگر خودش را به جای نود قانونی در شبکه معرفی می‌کند این نوع حملات به روش های متفاوتی در یک شبکه ایجاد می‌شوند. تغییر یک پیام نیز از جمله از حملاتی است که در گروه حملات دیالوگ قرار می‌گیرد. حملات جعل هویت و تغییر پیام جزء حملات فعال قرار می‌گیرند.

حملات نفوذ در شبکه معمولا با ماژول‌های آماده پیاده‌سازی می‌شوند. در حمله اسکن پورت و یا آدرس، نفوذگر به دنبال یک آدرس شبکه‌ای[۳] فعال به همراه پورت‌های باز آن می‌باشد، این نوع حمله از نوع غیر فعال می‌باشد. اما سایر حملات این گروه مثل منع سرویس، و یا بدافزارها به علت تغییر و دستکاری در منابع اطلاعاتی جزء حملات فعال قرار می‌گیرند.

در حملات مهندسی اجتماعی، متخاصم سعی می‌کند که از نظر روانشناسی اطلاعات خصوصی افراد را به دست بیاورد.

---

[1] *Penetration Attacks*
[2] *Social Engineering*
[3] *Ip*

حملات از دید وضعیت اجرا نیز به دسته‌های زیر تقسیم می‌شوند.

- حملات منفرد[1]
- حملات توزیع شده[2]

در حملات منفرد، نفوذگر از یک سیستم برای نفوذ در شبکه استفاده می‌کند، در این حالت قدرت پردازشی و سرعت ارتباطی نفوذگر باندازه‌ی یک نود معمولی در شبکه می‌باشد. اما در حالت توزیع شده متخاصم عملیات نفوذ در شبکه را با استفاده از چندین کامپیوتر انجام می‌دهد، در این حالت بار پردازشی بین چند کامپیوتر توزیع می‌شود، حملات توزیع شده معمولا مخرب‌تر می‌باشد زیرا در این نوع حملات قدرت پردازشی نود متخاصم چندین برابر می‌باشد.

## ۱-۴ چالش‌های برقراری امنیت

چالش‌های برقراری امنیت در شبکه‌های کامپیوتری به صورت زیر می‌باشد [4].

- برقراری امنیت در شبکه‌های کامپیوتری هزینه‌بر می‌باشد. هزینه صرفا شامل هزینه اقتصادی نمی‌باشد. سربار داده‌ای، زمانی، پردازشی، کدنویسی، و... همگی شامل هزینه می‌باشند.
- همانطور که قبلا اشاره کردیم برقراری امنیت دسترسی‌پذیری افراد به شبکه را کاهش می‌دهد، از این رو کاربران عادی امنیت را نوعی مانع در برابر کارهای عادی می‌دانند.

[1] *Single Attack*
[2] *Distribute Attack*

- فرایندهای نقض امنیت زمانی مفهوم پیدا می‌کنند که تهدیدهای امنیتی اجرا شوند.
- پویایی شبکه‌های کامپیوتری و افزایش مقیاس این شبکه‌ها باعث شده که مدیریت امنیت کاری بسیار دشوار باشد.
- پیاده‌سازی الگوریتم‌های امنیتی معمولا بسیار پیچیده می‌باشند.
- رشد ابزارهای نفوذگران در طی سال‌های گذشته سبب شده است که روزانه راه‌های نفوذ جدیدی در سیستم‌های اطلاعاتی پدیدار شود، از این رو مکانیزم‌های امنیتی باید دائم به‌روزرسانی شوند.
- پیوند دو شبکه ناهمگن با مکانیزم‌های امنیتی متفاوت امری بسیار دشوار می‌باشد.

## ۵–۱ سرویس امنیتی

هر سرویس امنیتی از یک یا چند مکانیزم امنیتی تشکیل شده است. مکانیزم‌های امنیتی در واقع فرایندهایی هستند که در جهت تشخیص حمله، جلوگیری از حمله، بازسازی سیستم پس از حمله مورد استفاده قرار می‌گیرند. در حالت کلی سرویس‌های امنیتی به سه دسته‌ی جدول ۱ تقسیم می‌شوند [5].

جدول ۱ گروه‌بندی سرویس‌های امنیتی

| | |
|---|---|
| **سرویس‌های مدیریتی** | وظیفه اصلی این سرویس‌ها مدیریت برنامه‌های امنیتی سیستم‌های اطلاعاتی می‌باشند. مدیریت بروزرسانی برنامه‌های امنیتی جزء سرویس‌های مدیریتی می‌باشند. |
| **سرویس‌های عملیاتی** | این نوع سرویس‌ها پیاده‌سازی برنامه‌ها و اجرای آن‌ها توسط کاربران را کنترل و نظارت می‌کنند. |
| **سرویس‌های تکنیکی** | این نوع سرویس‌ها رفتار و عملکرد سیستم را مورد بررسی قرار می‌دهند. |

جدول ۲ نمونه‌هایی از سرویس‌های امنیتی را با همراه گروه بیان می‌کند.

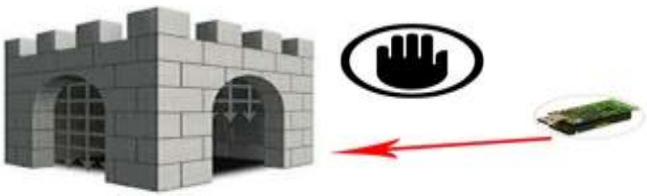
جدول ۲ نمونه سرویس‌های امنیتی

| سرویس | گروه |
|---|---|
| *Security Program* | ***Management*** |
| *Security Policy* | ***Management*** |
| *Risk Management* | ***Management*** |
| *Security Architecture* | ***Management*** |
| *Contingency Planning* | ***Operational*** |
| *Incident Handling* | ***Operational*** |
| *Testing* | ***Operational*** |
| *Training* | ***Operational*** |
| *Firewalls* | ***Technical*** |
| *Intrusion Detection* | ***Technical*** |

## ۶-۱ کنترل دسترسی

کنترل دسترسی[1] یک مکانیزم امنیتی در سیستم‌ها می‌باشد. وظیفه اصلی کنترل دسترسی، جلوگیری از دسترسی غیرمجاز به منابع شبکه است (Stallings, 2011). وجود یک کنترل دسترسی جامع و کامل در سیستم، می‌تواند از وقوع بسیاری از حملات جلوگیری کند. کنترل دسترسی در شبکه‌های کامپیوتری سه وظیفه زیر را انجام می‌دهد [6].

- جلوگیری از ورود نودهای غیر مجاز
- توزیع کلید بین افراد شبکه
- ایجاد ارتباط امن در داخل شبکه



شکل ۴ مدل کنترل دسترسی

شکل ۴ یک نمونه ساده از کنترل دسترسی در شبکه‌ی کامپیوتری را نشان می‌دهد. در این شکل گره‌های مجاز در یک قلعه‌ی امن قرار گرفته‌اند، هر گره جدید ورودی، پس از

[1] *Access control*

احراز اصالت می‌تواند وارد این قلعه‌ی امن شود. احراز اصالت گره در شبکه‌ی کامپیوتری می‌تواند به صورت‌های متفاوتی پیاده‌سازی شود.

## ۱-۷ حفاظت

تعیین سطح دسترسی افراد به منابع اطلاعاتی را حفاظت[1] گوییم. به عبارت دیگر حفاظت، میزان دسترسی افراد و نوع عملیات‌های مجاز یک کاربر را تعریف می‌کند. باید این نکته را در نظر بگیریم که کنترل دسترسی و حفاظت دو جزء کاملا مستقل می‌باشند. در کنترل دسترسی فقط مجوز دسترسی افراد به منابع اطلاعاتی مورد بررسی قرار می‌گیرد اما بحث حفاظت شامل بررسی میزان دسترسی به منابع اطلاعاتی است. در جهت درک بیشتر به مثال زیر توجه کنید.

مثال: فرض کنید در یک دانشگاه، نگهبان درب ورودی با چک کردن کارت دانشجویان، اساتید، کارکنان، اجازه ورود افراد به محیط دانشگاه را می‌دهد، این نوع نظارت همانند عمل یک سیستم کنترل دسترسی می‌باشد. در محیط دانشگاه هر کس وظیفه‌ی خاص خودش را دارد، به عنوان مثال وظیفه استاد، تدریس درس و اعلام ارزیابی تحصیلی دانشجو می‌باشد. بر همین اساس هر کس بر حسب وظیفه، می‌تواند به منابع اطلاعاتی دسترسی پیدا کند. مثلا استاد می‌تواند تمامی شرح حال تحصیلی یک دانشجو را مشاهده کند، اما هر دانشجو فقط می‌تواند اطلاعات تحصیلی خود را ببیند، رعایت و ایجاد چنین قوانینی به بحث حفاظت مربوط می‌شود.

[1] *Protection*

**اصل حداقل مجوز:**

هر کاربر بر حسب نقشی که در سیستم ایفا می‌کند باید با حداقل مجوز بتواند فعالیتش را در سیستم انجام دهد.

رعایت این اصل سبب می‌شود که هر کس بر حسب نیاز قانونی خود به منابع اطلاعاتی دسترسی پیدا کند. به عبارتی، تا زمانی که نیاز فرد برای دسترسی به اطلاعات آشکار نشود اجازه دسترسی به فرد داده نمی‌شود.

## ۸–۱ بررسی چند تعریف پایه‌ای

در این قسمت چند نعریف پایه‌ای در بحث امنیت را مطرح می‌نماییم.

عامل[1]: موجودیتی است که برای انجام فعالیت خودش می‌بایست به منابع اطلاعاتی دسترسی پیدا نماید.

شی[2]: منابع اطلاعاتی را شامل می‌شود، عامل‌ها برای انجام کارهای خود، باید به اشیا دسترسی پیدا نمایند.

احراز اصالت[3]: احراز اصالت در دو دیدگاه پیام و هویت مورد بررسی قرار می‌گیرد. هدف از احراز اصالت درستی پیام و هویت فرد در شبکه می‌باشد. معمولا رویه احراز اصالت افراد در پروتکل‌های تجاری یک بار در هر ارتباط صورت می‌گیرد.

تایید عملیات[1]: تایید انجام کار یک عامل بروی یک شی را تایید عملیات گوییم. معمولا رویه تایید عملیات در پروتکل‌های تجاری چندین بار صورت می‌گیرد.

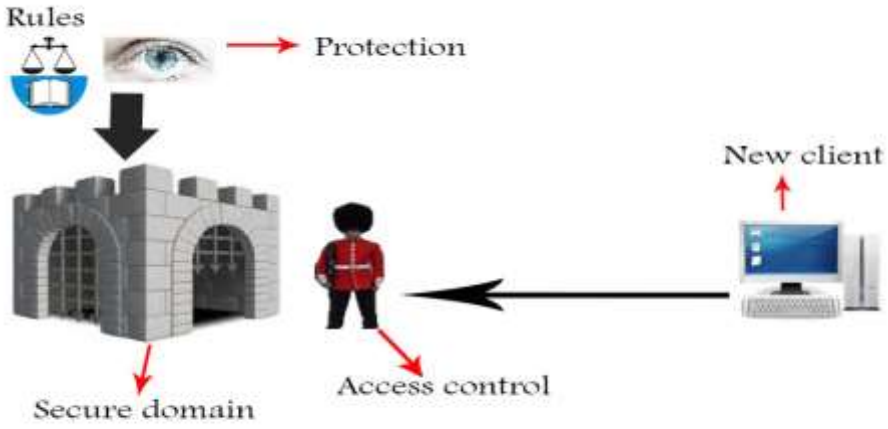
---

[1] *Subject*
[2] *Object*
[3] *Authentication*

اعتماد[۲]: وجود اعتماد به یک عامل خارجی (عامل خارجی، عاملی است که برای سیستم شناخته شده نمی‌باشد) سبب می‌شود که این عامل بتواند به یک شی خاص دسترسی پیدا نماید.

## ۹–۱ رویه ارتباط امن بین یک عامل و شی

با فرض اینکه شی مورد نظر یک شی امن می‌باشد، ابتدا احراز اصالت عامل توسط مکانیزم‌های کنترل دسترسی مورد بررسی قرار می‌گیرد. پس از احراز شدن هویت عامل، با انجام هر عملیات عامل رویه تایید عملیات صورت می‌گیرد. دقت کنید که رویه احراز اصالت در شبکه‌های کامپیوتری معمولا با امضاء دیجیتال صورت می‌گیرد. در فصل‌های بعدی روش‌های امضاء دیجیتال را بررسی می‌نماییم.



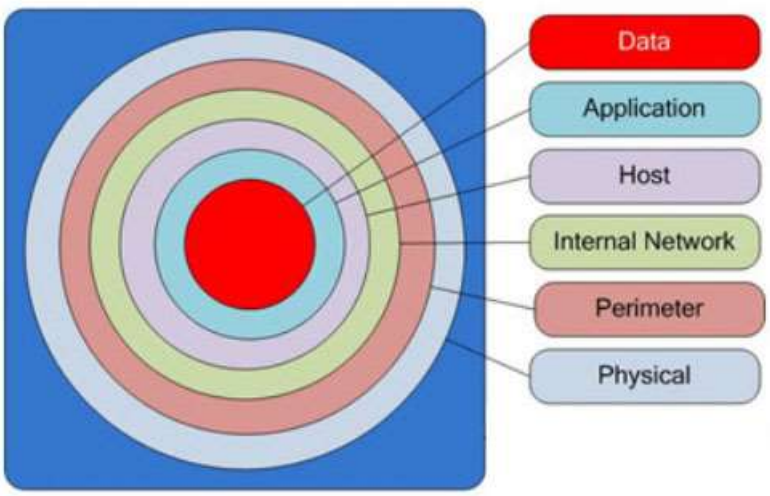

شکل ۵ رویه دسترسی یک عامل به یک شی امن

[1] *Authorization*
[2] *Trust*

در شکل ۵ یک سیستم می‌خواهد به منابع اطلاعاتی یک شی امن دسترسی پیدا نماید، در این حالت در قدم اول کنترل دسترسی اجازه ورود عامل را به حوزه شی مورد نظر می‌دهد. در قدم بعدی هر نوع عملیاتی که عامل بخواهد انجام دهد این عملیات باید مطابق قواعد امنیتی باشد. رویه حفاظت عملیات‌های عامل را بر حسب قواعد امنیتی مورد بررسی قرار می‌دهد.

## ۱۰–۱ دید لایه‌ای به امنیت سیستم

در دید لایه‌ای، امنیت سیستم‌های‌کامپیوتری باید در هر لایه به صورت مجزا حفظ شود. برای انجام این کار، امنیت اطلاعات کامپیوترها را از چند دید مورد بررسی قرار می‌دهند.




شکل ۶ دید لایه‌ای برای برقراری امنیت شبکه

در شکل ۶ برقراری امنیت و حفظ داده خامی که با هیچ کاربردی در ارتباط نیست می‌تواند به راحتی صورت بگیرد، اما زمانی که این داده‌های خام با کاربردهای متفاوت ارتباط برقرار می‌نمایند برقراری امنیت و احراز کاربردهای متفاوت کمی مشکل می‌شود،