امنیت شبکه

فصل اول: مقدمه

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

- تعاریف
- اهداف امنیت شبکه
- سایر اهداف و چالشها
- حملات و خطرات
- انواع حملات
- سرویسهای امنیتی
- مکانیزمهای امنیتی

تعاریف اصلی

عبارت "امنیت کامپیوتر" در NIST

حفاظت داده شده به یک سیستم اطلاعاتی مکانیزه بمنظور بدست آوردن اهداف کاربردی شامل حفظ یکپارچگی، دسترس‌پذیری و محرمانگی منابع آن سیستم اطلاعاتی (شامل سخت‌افزار، نرم‌افزار، سفت‌افزار، اطلاعات/داده و ارتباطات) را امنیت کامپیوتر گویند.

اهداف امنیت کامپیوتر

محرمانگی

یکپارچگی

دسترس پذیری

تعاریف اهداف امنیت شبکه

محرمانگی: این عبارت به دو مفهوم بر می‌گردد:

محرمانگی داده: اطمینان از اینکه اطلاعات محرمانه و شخصی برای افراد احراز هویت نشده قابل دسترس نبوده و فاش نمی‌شود.

حریم خصوصی: اطمینان از اینکه افراد بتوانند کنترل کنند که چه اطلاعاتی مربوط به آنها جمع‌آوری شده و ذخیره می‌گردد و همچنین بوسیله چه کسانی و برای چه کسانی این اطلاعات ارسال شده و فاش می‌شود.

یکپارچگی: این عبارت به دو مفهوم برمی‌گردد:

یکپارچگی داده: اطمینان از اینکه اطلاعات تنها در یک وضعیت خاص و تایید شده تغییر می‌یابند.

یکپارچگی سیستم: اطمینان از اینکه یک سیستم توابع انتخابی خود را در وضعیت سالم و بدون عیب و دور از دستکاریهای تایید نشده عمدی یا سهوی اداره می‌نماید.

دسترس پذیری: اطمینان از اینکه سیستمها بدون معطلی کار می‌کنند و سرویسها همواره برای کاربران احراز هویت شده فعال و در دسترس هستند.

مشخصات اهداف امنیت شبکه بر پایه استاندارد NIST

محرمانگی: حفظ محدودیت مجوزها روی دسترسی و فاش نمودن اطلاعات بهمراه معانی حفاظت از استقلال پیامهای شخصی و اطلاعات اختصاصی. در واقع فقدان محرمانگی باعث فاش شدن غیر مجاز اطلاعات خواهد شد.

یکپارچگی: محافظت در برابر دستکاری و خرابی غیرمجاز اطلاعات شامل اطمینان از عدم انکار فعالیت‌ها و اعتبار اطلاعات. در واقع فقدان یکپارچگی باعث دستکاری بدون مجوز یا خرابی اطلاعات خواهد شد.

دسترس پذیری: اطمینان از دسترسی بموقع و قابل اعتماد به اطلاعات و استفاده از آنها. فقدان دسترس پذیری باعث قطع دسترسی و استفاده بموقع از اطلاعات یا یک سیستم اطلاعاتی خواهد شد.

سایر مفاهیم در امنیت شبکه

اعتبار: ویژگی واقعی بودن و توانایی بازبینی شدن و قابل اعتماد بودن، یعنی اطمینان در قابلیت اعتماد به یک انتقال، یک پیغام، یا مولد یک پیغام. این بدین معناست که کاربر همان کسی است که ادعا می‌کند و هر ورودی رسیده به سیستم از منبع قابل اعتمادی ارسال شده است.

پاسخگویی: هدف امنیتی که باعث می‌شود نیاز به ردیابی فعالیتهای یک موجودیت تنها از طریق همان موجودیت انجام گردد را پاسخگویی گویند. این مفهوم عملیاتی چون عدم انکار فعالیت، بازداری از انجام یک عملیات، تشخیص علت و محل ایجاد مشکل، پیشگیری و تشخیص نفوذ، و فعالیتهای بازیابی و منطقی پس از آنها را پشتیبانی می‌نماید.

چالشهای امنیت شبکه

- امروزه امنیت به سادگی آن روزهایی که تازه ظاهر شده بود، نیست. بنظر می‌رسد که امروزه نیازمندیها مشخص باشند، اما مکانیزمهای پوشش دادن این نیازمندیها می‌تواند کاملاً پیچیده بوده و درک آنها ممکن است علتهای زیرکانه بیشتری را نیز درگیر نماید.
- در پیاده‌سازی یک الگوریتم یا مکانیزم امنیتی خاص، همواره حملات بالقوه مرتبط به آن خاصیت امنیتی نیز می‌بایست مورد بررسی قرارگیرند.
- بر پایه علت شماره دو، فرآیند مورد استفاده برای مهیا نمودن سرویسهای خاص اغلب درست و قابل اعتماد بنظر نمی‌آیند.
- طراحی مکانیزمهای امنیتی مختلف وابسته به تصمیم‌گیری مربوط به محل استفاده آنهاست.
- مکانیزمهای امنیتی در واقع در بیشتر از یک الگوریتم یا پروتکل خاص درگیر هستند.
- امنیت شبکه و کامپیوتر یک نبرد عقلانی اساسی بین یک مجرم، شخصی که بدنبال یافتن منافذ است و یک طراح یا راهبر که بدنبال بستن آنهاست، می‌باشد. یکی از برتری‌هایی که یک مهاجم دارد آن است که او تنها بدنبال یک ضعف می-گردد درحالی که یک طراح برای دستیابی به امنیت کامل می‌بایست همه نقاط ضعف را یافته و برطرف نماید.
- در اصل همواره یک گرایش طبیعی در بسیاری از کاربران و مدیران سیستمها برای سرمایه‌گذاری اندک روی بخش امنیتی تا زمانی که یک شکست امنیتی رخ ندهد، وجود دارد.
- امنیت نیازمند نظارتی منظم و حتی ثابت، است که این امر امروزه برای زمانهای کوتاه آن هم در محیطهای شلوغ و پرکار بسیار مشکل خواهد بود.
- متاسفانه هنوزهم در اغلب اوقات بجای آنکه امنیت بعنوان بخش جدایی ناپذیر فرآیند طراحی باشد، بصورت یک بخش اضافه شده به یک سیستم بعد از طراحی بعنوان چاره اندیشی موقت گنجانده می‌شود.
- هنوز هم بسیاری از کاربران (و حتی مدیران امنیتی) امنیت بالا را بعنوان یک مانع برای موثربودن و کاربرپسند بودن یک سیستم یا استفاده از اطلاعات یک سیستم می‌دانند.

معماری امنیتی OSI

- **حمله امنیتی**: هر فعالیتی که امنیت اطلاعات متعلق به یک سازمان را بخطر بیاندازد.

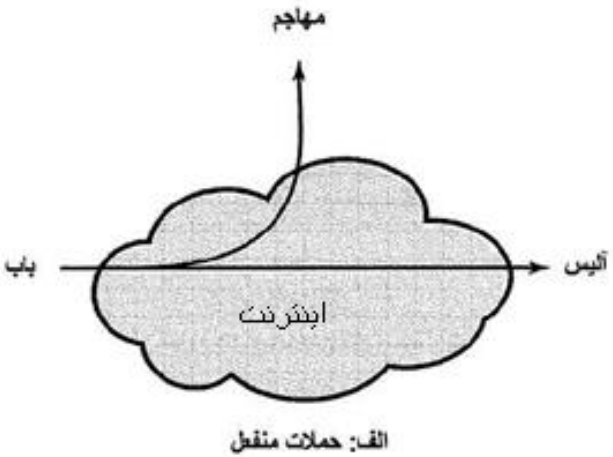
- **مکانیزم امنیتی**: یک پردازش (یا یک تجهیز که چنین پردازشی را داراست) که برای تشخیص، پیشگیری یا بازیابی اطلاعات از یک حمله امنیتی طراحی شده است.

- **سرویس امنیتی**: یک پردازش یا سرویس ارتباطی که امنیت سیستمهای پردازش داده و انتقال اطلاعات یک سازمان را بهبود دهد. سرویسها حملات امنیتی را تشخیص داده و از یک یا چند مکانیزم امنیتی برای مهیا نمودن سرویس استفاده می‌نمایند.

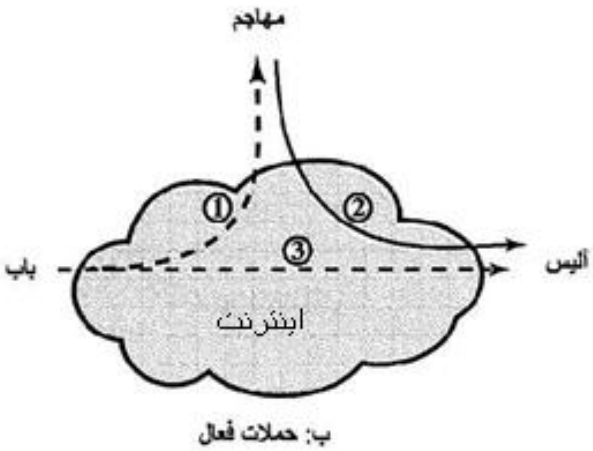
خطرات و حملات

- خطر یا **Threat**: یک پتانسیل برای نقض امنیت که همواره وجود داشته و زمانی که شرایط، توانایی، فعالیت، یا اتفاق خاصی بوجود آید می‌تواند امنیت را نقض کرده و ایجاد آسیب نماید. در واقع **Threat**، یک خطر احتمالی است که از یک نقطه ضعف استفاده می‌نماید.
- حمله یا **Attack**: یک تهاجم به سیستم امنیتی که از یک خطر هوشمندانه حاصل شده است. در واقع حمله یا **Attack**، یک فعالیت هوشمندانه‌ای است که بصورت تلاشی عمدی برای گریز از سرویسهای امنیتی و ایجاد نقص در سیاست امنیتی یک سیستم انجام می‌گیرد.
  - حملات منفعل (تصویر 1. 1الف) بطور ذاتی درحال استراق سمع یا بازبینی انتقالها هستند. هدف طرف مهاجم بدست آوردن اطلاعاتی است که منتقل می‌شوند. (مانند آنالیز ترافیک)
  - حملات فعال (تصویر 1. 1ب) در ایجاد تغییراتی در جریان داده یا تولید یک رشته کاذب شرکت نموده و می‌توانند به چهار دسته تقسیم شوند: ناشناس، بازپخش، دستکاری پیامها، و محرومیت – از - خدمات.

خطرات و حملات (ادامه)



الف: حملات منفعل



ب: حملات فعال

تعریف سرویسهای امنیتی

در استاندارد X.800 :

یک سرویس امنیتی عبارت است از سرویسی است که توسط یک پروتکل لایه-ای در سیستم‌های باز ارتباطی مهیاگردیده و از امنیت کافی سیستمها و یا انتقال داده‌ها درآن اطمینان حاصل شده باشد.

در سند RFC4949 :

یک پردازش یا سرویس ارتباطی که توسط یک سیستم برای دادن یک نوع خاص حفاظت به منابع سیستم مهیاگردیده است؛ سرویسهای امنیتی در واقع سیاستهای امنیتی را پیاده‌سازی نموده و توسط مکانیزمهای امنیتی پیاده‌سازی می‌شوند.

انواع سرویسهای امنیتی

- احراز هویت
- کنترل دسترسی
- محرمانگی داده
- یکپارچگی داده
- عدم انکار

سرویسهای امنیتی (X.800)

یکپارچگی داده اطمینان از اینکه داده رسیده همانی باشد که فرستنده آن را فرستاده است (محتویات دستکاری، اضافه، حذف، یا بازپخش نشده‌اند). یکپارچگی اتصال همراه با بازیافت برای یکپاچگی همه داده‌های کاربر روی یک اتصال و یافتن هرگونه دستکاری، اضافه، حذف، یا بازپخش داده در توالی داده حاضر و بازیابی موردنیاز مهیا شده است. یکپارچگی اتصال بدون بازیافت همانند بخش بالا ولی تنها یافتن تغییات بدون بازیابی یکپارچگی اتصال فیلد - انتخابی برای یکپارچگی فیلدهای انتخابی بهمراه دادهای کاربر یک بلوک داده‌ای انتقال یافته بر روی یک اتصال به انضمام فرم تعریفی آنکه فیلدهای انتخابی دستکاری، اضافه، حذف و یا بازپخش شده‌اند، مهیا شده‌است. یکپارچگی غیراتصال - محور برای یکپارچگی یک بلوک داده‌ای اتصال مجرد از نوع غیراتصال - محور و شاید به همراه فرم تشیص دستکاری داده مهیا شده‌است. بعلاوه، یک نوع محدود تشخیص بازپخش نیز ممکن است ارائه شود. یکپارچگی غیراتصال - محور فیلد - انتخابی برای یکپارچگی فیلدهای انتخابی در یک بلوک داده اتصال از نوع غیراتصال - محور مجرد بهمراه فرم تشخیص دستکاری فیلدهای انتخابی مهیا گردیده‌است. عدم انکار محافظت در برابر ازکارفتادن بوسیله یکی از موجودیتهای موجود در یک ارتباط که در همه یا بخشی از ارتباط شرکت داشته‌است، را مهیا می‌سازد. عدم انکار، منبع تایید می‌نماید که پیغام از یک بخش خاص ارسال شده‌است. عدم انکار ، مقصد تایید آنکه پیغام توسط بخش خاصی دریافت شده‌است.	احراز هویت اطمینان از اینگه طرفین یک ارتباط همانهایی هستند که ادعا میکنند. احراز هویت موجودیت نظیر بهمراه یک اتصال منطقی برای حصول اطمینان در شناسه موجودیتهای شرکت کننده استفاده می‌گردد. احراز هویت منبع - داده در یک انتقال غیراتصال-محور، اطمینان اینکه منبع داده دریافتی همان منبع مورد نظر است، را ایجاد می‌نماید. کنترل دسترسی جلوگیری از استفاده بدون احرازهویت شده از یک منبع (این سرویس کنترل می‌کند که چه کسی تحت چه شرایطی می‌تواند به یک منبع دسترسی یافته و چه کاری می‌تواند انجام دهد) محرمانگی داده حفاظت داده از افشاشدن بدون تایید. محرمانگی اتصال محافظت از همه داده‌های کاربر در یک اتصال. محرمانگی غیراتصال - محور محافظت از همه داده‌های کاربر در یک بلوک داده‌ای تنها. محرمانگی فیلد - قابل انتخاب محرمانگی فیلدهای انتخابی برای داده‌های کاربر در یک اتصال یا یک بلوک داده‌ای تنها. محرمانگی جریان - ترافیک حفاظت از اطلاعات که ممکن است از مشاهده جریان ترافیک حاصل شده باشد.

جدول 1.2

احراز هویت

سرویس احراز هویت نگران معتبر بودن یک ارتباط است

- در مورد موضوع مربوط به یک پیام منفرد، مانند یک سیگنال آگهی یا زنگ خطر، وظیفه سرویس احراز هویت در واقع حصول اطمینان از دریافت پیام از منبعی است که فرستنده مدعی ارسال آن است.

- در مورد موضوع عمل متقابل درحال پیشرفت، مانند اتصال یک پایانه به یک میزبان، دو جنبه درگیر خواهند بود. اول آنکه، در زمان شروع ارتباط، سرویس اطمینان حاصل می‌نماید که دو موجودیت تایید طلاحیت شده‌اند (یعنی هر موجودیت همانی است که ادعا نموده است). دوم آنکه، سرویس می‌بایست اطمینان حاصل نماید که به هیچ طریقی مداخله‌ای در ارتباط بوجود نیاید که شخص سومی بتواند بطور ناشناس بعنوان یکی از دو طرف اصلی برای مقاصدی چون ارسال و دریافت تایید نشده اقدام نماید.

کنترل دسترسی

در زمینه امنیت شبکه، کنترل دسترسی عبارت است از محدود کردن و کنترل میزان دسترسی به سیستمها و برنامه‌های کاربردی میزبان ازمیان لینکهای ارتباطی.

برای دستیابی به این نوع کنترل، هر موجودیت که سعی در گرفتن دسترسی دارد ابتدا می‌بایست شناسایی یا تعیین هویت شده و آنگاه دسترسی‌ها و اختیارهای شایسته و صحیح می‌تواند به شخص داده شود.

محرمانگی داده

محرمانگی عبارت است از حفاظت داده ارسال شده در برابر حملات منفعل. بر اساس محتویات ارسال داده می‌توان چندین لایه حفاظتی تعیین نمود.

برای نمونه، وقتی یک اتصال TCP بین دو سیستم برقرار می‌شود، این محافظت گسترده از آزادسازی هر داده انتقالی کاربر بر روی TCP محافظت می‌نماید.

جنبه دیگر محرمانگی در واقع محافظت جریان ترافیک از تجزیه و تحلیل است. برای آنکه مهاجم نتواند منبع و مقصد، پریود، طول، یا سایر مشخصات ترافیک یک ارتباط را زیر نظر داشته باشد، می‌توان از این سرویس استفاده نمود.

محرمانگی روی حملات منفعل کار میکند

یکپارچگی داده

- یک سرویس یکپارچگی با یک رشته پیام کار می‌کند و اطمینان حاصل می‌نماید که پیام ارسالی بدون تکرارشدن، اضافه شدن، تغییر یافتن، مرتب شدن مجدد، و یا بازپخش به مقصد رسیده باشد (اتصال - محور). تخریب داده نیز زیر نظر این سرویس انجام می‌گیرد.
- از طرف دیگر، در یک سرویس غیراتصال - محور با پیامهای مجزا و انفرادی بدون توجه به محتویات بزرگتر کار می‌نماید و بطور عمومی فقط محافظت در برابر تغییر پیام را مهیا می‌نماید.

سرویس یکپارچگی به حملات فعال مرتبط است و لذا تشخیص بیشتر از پیشگیری دارای اهمیت خواهد بود.

عدم انکار

از امکان تکذیب فرستنده و گیرنده یک پیام از ارسال یا دریافت آن جلوگیری می-نماید.

- وقتی یک پیام ارسال می‌گردد، گیرنده می‌تواند ثابت نماید که فرستنده منتصب به پیام درحقیقت آن پیام را ارسال نموده است.

- بطور مشابه، وقتی یک پیام دریافت می‌شود، فرستنده می‌تواند اثبات نماید که گیرنده منتصب در حقیقت آن پیام را دریافت نموده است.

دسترس پذیری

یک سیستم دسترس پذیر خواهد بود اگر سرویسها بر پایه طراحی سیستم برای زمانی که کاربر آنها را تقاضا می‌نماید آماده و مهیا باشند

- تعدادی از این حملات توسط اقدامات متقابل خودکار مانند احراز هویت و رمزگذاری قابل پیشگیری بوده و تعدادی نیز نیازمند اقدامات فیزیکی برای جلوگیری و بازیابی از به هدر رفتن میزان دسترس‌پذیری منابع در یک سیستم توزیع‌شده هستند.
- یک سرویس دسترس‌پذیری در واقع یک سیستم را از دسترس‌پذیر بودن آن مطمئن می‌نماید. این سرویس نشان می‌دهد که نگرانیهای امنیتی با حمله محرومیت – از – خدمات افزایش خواهند یافت.

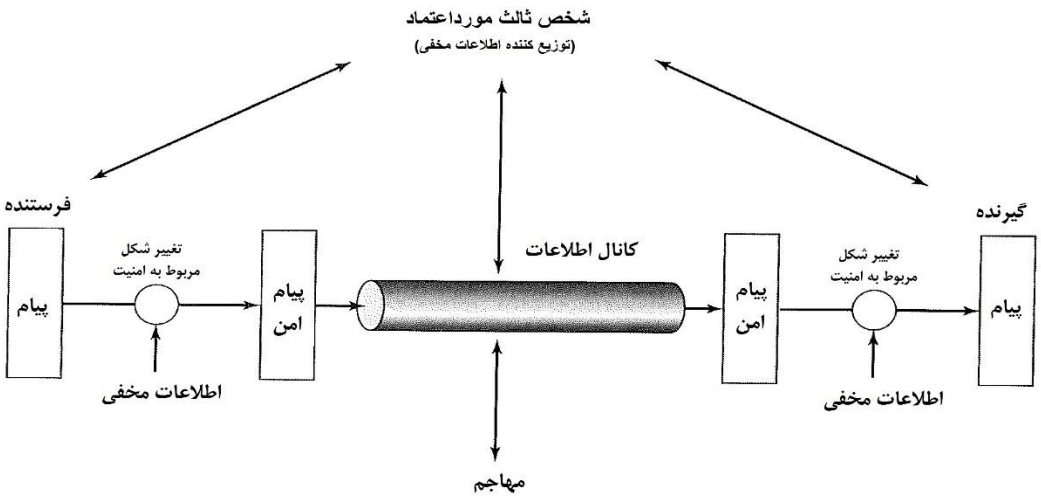
مکانیزمهای امنیتی

مکانیزمهای امنیتی خاص	مکانیزمهای امنیتی فراگیر
شاید در لایه پروتکل خاصی قرار گیرد تا چندین سرویس امنیتی **OSI** را مهیا نماید. برمز درآوردن استفاده از الگوریتمهای ریاضی برای انتقال داده به فرمی که به آسانی قابل فهم نباشد. انتقال و بازیابی توالی داده وابسته به الگوریتم و تعداد کلیدهای رمزگذاری که ممکن است صفر یا بیشتر باشند، خواهد بود. امضاء الکترونیکی داده اضافه شده، یا یک انتقال رمزشده، به یک واحد دادهکه به یک گیرنده واحد داده اجازه میدهد تا فرستنده و یکپارچگی داده را تایید نموده و از در برابر جعل از آنها محافظت نماید. کنترل دسترسی یک تعداد مکانیزمی که میزان دسترسی به منابع را اجرا مینماید. یکپارچگی داده یک تعداد مکانیزمی که برای اطمینان از یکپارچگی یک واحد داده یا رشتهای از واحدهای داده بکار میرود. تبادل احرازهویت یک مکانیزم که قصد دارد از شناسه یک موجودیت جهت تبادل اطلاعات اطمینان حاصل نماید. لایهبندی ترافیک افزودن بیتها به بخشهای خالی یک رشته داده برای ازکار انداختن تلاشهای مربوط به آنالیز ترافیک برای حمله. کنترل مسیریابی فعال نمودن انتخاب مسیرهای امن فیزیکی خاص برای داده خاص و اجازه تغییر مسیر، بخصوص هنگامی که مشکوک به یک نفوذ امنیتی باشد. گواهی رسمی استاده از یک شخص سوم برای حصول اطمینان از خواص مشخص یک تبادل داده.	مکانیزمهایی که مخصوص هیچ یک از سرویسهای امنیتی یا لایه پروتوکل خاص **OSI** نیست. عملکرد قابل اطمینان با توجه به برخی از ضوابط عملکرد صحیح بنظر بیاید. (ایجاد شده بر پایه یک سیاست امنیتی) برچسب امنیتی علامت خاص یک منبع که خواص امنیتی آن منبع را تعیین یا نامگذاری مینماید. تشخیص اتفاق تشخیص اتفاقهای مرتبط با امنیت دنباله ممیزی امنیتی دادهها جمعآوری شده و بطور موثر برای آسان سازی یک بازرسی امنیتی استفاده میشوند، که در واقع یک بازنگری و تست مستقل برای رکورها و فعالیتهای سیستم به حساب میآید. بازیابی امنیت با تقاضاهای مربوط به مکانیزمهایی همانند کنترل رویدادها، و اجرای فعالیتهای بازیابی مرتبط سروکار دارد.

مدل امنیت شبکه

چهار وظیفه پایه برای طراحی یک سرویس امنیتی وجود دارد:

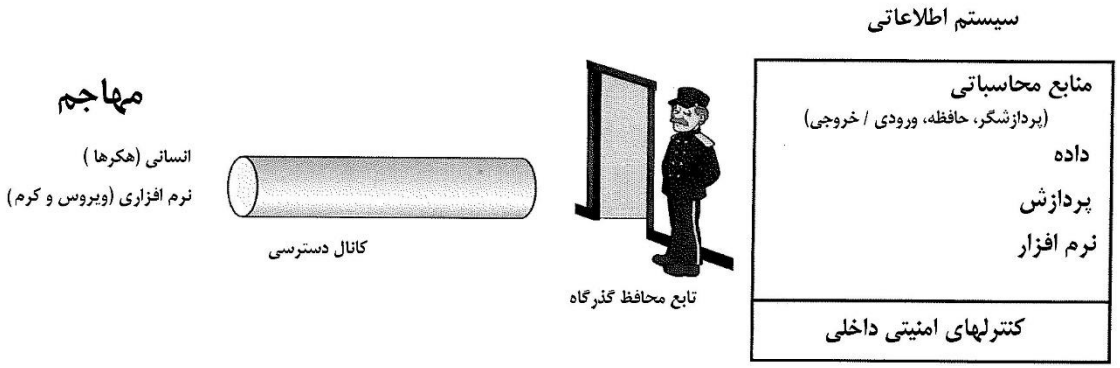
1. طراحی یک الگوریتم برای مهیا نمودن دگرگونیهای مرتبط با امنیت. الگوریتم باید طوری باشد که یک مهاجم نتواند هدف آن را ناقص نماید.
2. تولید اطلاعات محرمانه با استفاده از الگوریتم
3. گسترش روشهایی برای پخش و به‌اشتراک‌گذاشتن اطلاعات محرمانه
4. مشخص نمودن یک پروتکل که توسط دو طرف شرکت کننده برای استفاده از الگوریتم امنیتی و اطلاعات محرمانه جهت دسترسی به یک سرویس امنیتی خاص بکار خواهد رفت.



مدل امنیتی دسترسی شبکه

برنامه‌ها می‌توانند عامل بروز دو نوع از خطرها باشند:

1. خطرهای مربوط به دسترسی اطلاعات: استراق سمع و تغییر داده ازطرف کاربران مجاز توسط کاربری که اجازه دسترسی ندارد.
2. خطرهای سرویس: استفاده از نقصهای سرویس‌های کامپیوتری برای جلوگیری از استفاده کاربران مجاز.



مکانیزمهای دسترسی نیازمند کنترل دسترسی‌های ناخواسته هستند که به دو گروه وسیع دسته‌بندی می‌شوند:

- دسته اول ممکن است با عنوان دروازه‌بان (محافظ گذرگاه) صدا زده شوند. این گروه شامل روش وارد شدن بر پایه رمزعبور است که کار جلوگیری از ورود افراد غیر مجاز و همچنین منطق غربال کردن را برعهده دارد.

دسته دوم دفاع شامل کنترلهای داخلی بسیاری خواهد بود که اطلاعات ذخیره‌شده را به منظور تشخیص حمله نفوذگران ناخواسته کنترل و بازبینی می‌نماید.

سوالات مرتبط

1. اهداف امنیت کامپیوتر را نام برده و شرح دهید؟
2. معماری امنیت OSI چگونه است؟
3. تفاوت بین حملات امنیتی فعال و منفعل چیست؟
4. دسته بندی حملات امنیتی فعال و منفعل را نام برده و بطور مختصر تعریف نمایید؟
5. دسته بندی سرویسهای امنیتی را نام برده و بطور مختصر تعریف نمایید؟
6. دسته بندی مکانیزمهای امنیتی را نام برده و بطور مختصر تعریف نمایید؟

خلاصه:

امنیت شبکه، معماری امنیت، سرویسها، مکانیزمها، حملات و خطرات امنیتی، مدل امنیتی شبکه و مدل دسترسی امنیتی شبکه

جلسه بعدی: رمزنگاری متقارن

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

ترجمه: دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.