دانشگاه آزاد اسلامی واحد تبریز

نام درس: سیستم مدیریت امنیت اطلاعات

بخش: ایمن سازی در مقابل امنیت

نام استاد: دکتر مسعود کارگر

فهرست مطالب

اهداف ایمنی شبکه

- سه هدف ایمنی شبکه (CIA)
- ۱- **محرمانگی(Confidentiality)**: یعنی اطلاعات را به مقصد انتقال داده شود بدون اینکه شخصی آن را ببیند
  - مثال: انتقال اطلاعات حساب بانکی یا کارت اعتباری یا نامه
- ۲-**صحت (Integrity)**: یعنی داده‌هایی که مقصد دریافت می‌کند دقیقا چیزی است که به آن ارسال شده است و در بستر انتقال به آن هیچ تغییری داده نشده باشد.
- ۳- **دسترسی (Availability)**: اطلاعات همیشه در اختیار افراد مجاز قرار گیرد. ممکن است به محرمانگی و صحت اطلاعات خللی وارد نشود ولی از دسترس افراد مجاز خارج شود.

اهداف ایمنی **جدید** شبکه

- سه هدف ایمنی شبکه (CIA+)
- ۱- **محرمانگی(Confidentiality)**
- ۲-**صحت (Integrity)**
- ۳- **دسترسی (Availability)**
- **۴- استفاده قانونی از اطلاعات:** آیا افرادی که از اطلاعات استفاده می‌کنند آیا از نظر قانونی مجاز به استفاده از اطلاعات هستند یا نه؟ آیا همان حدودی که تعریف شده است رعایت می‌شود و با آن حدود در اختیار افراد مجاز قرار می‌گیرد.

تعاریف

- **فضای ایمن:**
- محدوده‌ای از شبکه که در آن سیاست‌های امنیتی اعمال می‌شود.

- **سیاست‌های امنیتی:**
- مجموعه‌ای از قوانین که جهت فراهم آوردن سرویس‌های امنیتی استفاده می‌شود.

- **تهدید:**
- **۱**- هر شخص، پدیده یا حادثه یا ایده‌ای که خطری را در رابطه با اهداف ایمنی شبکه (محرمانگی، صحت، دسترس‌پذیری و استفاده قانونی)اعمال کند را تهدید نامیده می‌شود.
- ۲- هر پدیده یا مفهومی تهدید نامیده می‌شود اگر بتواند به سیاست‌های ایمنی رخنه کند.

تعاریف - ادامه

- **حمله:**
- تحقق یک تهدید است.
- تهدید یک حمله بالقوه است و حمله یک تهدید بالفعل است که اتفاق افتاده و واقع شده است.

- **حفاظت:**
- هر وسیله‌ای که برای محافظت از تهدید به‌کار گرفته شود.
-

- **آسیب‌پذیری:**
- ضعف در مقابل حفاظت یا عدم وجود حفاظت در مقابل تهدید است.

تعاریف - ادامه

- **ریسک:**
- **نشان‌دهنده هزینه آسیب‌پذیری است.**

- **هدف شبکه:**
- هدف شبکه قبل از مطرح شدن مسایل امنیتی، انتقال داده به مقصد با سرعت بالا است .

طبقه‌بندی تهدید و حمله ها

تهدیدها به دو دسته کلی طبقه‌بندی می‌شود:

- ۱- تهدیدهای عمدی
- تهدیدهای تصادفی

حمله‌ها به دو دسته اصلی تقسیم می‌شوند:

۱- حمله‌های عمدی

۲- حمله‌های تصادفی

انواع تهدید

در مقابل تهدیدهای تصادفی، تهدیدهای عمدی قرار دارد.

تهدیدهای عمدی به دو دسته تقسیم می‌شود:

۱- تهدیدهای عمدی

۲- تهدیدهای غیرفعال

تهدیدهای غیر فعال با برداشت اطلاعات، بدون اینکه تغییری در چیزی به وجود آورند، خطر را ایجاد می‌کنند و نقش مانیتور کردن اطلاعات را خواهند داشت.
همچنین دیدن اطلاعات شبکه یک تهدید غیر فعال ساده محسوب می‌شود.

تهدیدهای فعال در پارامترهای شبکه تغییر ایجاد می‌کند به‌عبارتی علاوه بر دیدن اطلاعات شبکه در آن تغییر نیز اعمال می‌کند.

انواع تهدید فعال

تهدیدهای فعال به چهار گروه تقسیم می‌شوند:

۱- تهدیدهای تغییر ظاهر

۲- ارسال اطلاعات تکراری

۳- تغییر محتویات پیام

۴- رد کردن سرویس :

برای مثال می‌خواهیم اطلاعاتی به مقصد ارسال کنیم و پیام عدم وجود مقصد مشاهده می‌شود.

انواع تهدید

۱- نشت اطلاعات:

نشت اطلاعات، رسیدن اطلاعات به افراد غیر مجاز است که نقص محرمانگی است.

۲- عدم صحت اطلاعات:

نقص هدف صحت اطلاعات است.

۳- رد کردن سرویس:

به‌صورت عمدی، جلوی یک سرویس مجاز گرفته می‌شود که نقض دسترسی اطلاعات است.

۴-استفاده غیر قانونی از اطلاعات:

نقض هدف استفاده غیر قانونی اطلاعات است.

انواع تهدید

تهدیدهای نفوذی:

۱- تهدید تغییر ظاهر

۲- تهدید دور زدن کنترل شبکه

۳-تهدید تخطی از حقوق و قوانین شبکه

تهدیدهای طراحی شده:

۴- اسب تراوا

۵- دریچه Trapdoor

انواع سرویس‌های امنیتی

سرویس‌های امنیتی به پنج دسته کلی تقسیم می‌شوند.

۱- سرویس‌های اعتبار سنجی یا احرازهویت Authentication

۲- سرویس‌های کنترل دستیابی Access control

۳- سرویس‌های محرمانگی اطلاعات Data confidentiality

۴-سرویس‌های صحت داده Data Integrity

۵-سرویس‌های عدم رد سرویس Non repudation

تعریف سرویس اعتبارسنجی یا احراز هویت
Authenticatian

اعتبارسنجی یعنی:

آیا طرف مقابل همانی که ادعا می‌کند، هست یا نه؟

آیا این بسته‌ای که فرستاده شده است، از نظر هویت فرستنده آن، با چیزی که ادعا می‌شودیکی هست یا نه؟

انواع سرویس اعتبارسنجی

سرویس‌های اعتبار سنجی به دو گروه طبقه‌بندی می‌شوند:

۱- اعتبارسنجی موجودیت Entity Authentication:

تعیین هویت و اصلیت کاربر با هویت ادعا شده در زمان‌های مشخصی همچون شروع یا درعین ارتباط بررسی می‌شود.

۲- اعتبار سنجی اصالت Origin Authentication:

تعیین مبدا داده است. مشخص می‌کندکه کسی که این اطلاعات را تولید کرده چه کسی بوده است. نشان نمی‌دهد که این اطلاعات از کجا آمده است.

سرویس کنترل دستیابی
Access control

سرویس کنترل دستیابی:

جلوی دسترسی‌های غیر مجاز را از منابع می‌گیرد. انواع دسترسی‌های غیر مجاز که می‌تواند وجود داشته باشد، مثل خواندن، نوشتن و منابع پردازشی.

سرویس محرمانگی اطلاعات
Data Confidentiality

سرویس‌های محرمانگی به چهار گروه طبقه‌بندی می‌شوند:

۱- انفصال‌گرا Connectionless.

۲- اتصال‌گرا Connection Oriented.

۳-محرمانگی یک حوزه خاص.

۴- محرمانگی جریان ترافیک.

انواع سرویس صحت
Integrity

سرویس‌های صحت به پنج گروه طبقه‌بندی می‌شوند:

۱- صحت اطلاعات با ترمیم.

۲- صحت اطلاعات بدون ترمیم.

۳-صحت اطلاعات در یک حوزه خاص.

۴- صحت اطلاعات در یک ارتباط بدون اتصال.

۵- صحت اطلاعات حوزه خاص در یک ارتباط بدون اتصال.

سرویس عدم رد

سرویس‌های عدم رد به دو گروه طبقه‌بندی می‌شوند:

۱- عدم انکار مبدا.

۲- عدم انکار تحویل.

عدم انکار مبدا

عدم انکار مبدأ:

سرویسی که مبدأ ارسال کننده اطلاعات، نتواند ارسال اطلاعات را انکار کند. یعنی گیرنده نشانه‌ای از فرستنده داشته باشد که نشان دهد این اطلاعات از او بـــوده است.

این کار، از ارسال اطلاعات توسط یک فرستنده به اشتباه، برای یک مقصد نا بجا جلوگیری می‌کند.

ممکن است بسته اطلاعاتی را دریافت کنیم و مبدا ارسال آن را انکار کند. بسیاری از بسته‌های دریافت شده در شبکه، به دلیل معلوم نبودن فرستنده آن، حمله ای را انجام می‌دهند که قابل پیگیری نمی‌باشد.

عدم انکارتحویل

عدم انکار تحویل:

هیچ گیرنده‌ای نتواند دریافت اطلاعات را انکار کند.

به طور مثال: ممکن است بسته‌ای را برای کسی ارسال کرده باشیم و گیرنده آن را دریافت کرده باشد، ولی دریافت آن را انکار کند.گیرنده رسیدی را مبنی بر دریافت اطلاعات، صادر می‌کند.

مکانیزم های امنیتی

مکانیزم‌های امنیتی، روش فراهم آوردن سرویس‌ها است.

انواع مکانیزم‌ها

۱. مکانیزم‌های خاص

- رمزکردن اطلاعات
- امضای دیجیتال
- کنترل دستیابی
- صحت داده
- انتقال هویت
- پرکردن ترافیک
- کنترل مسیر دستیابی
- گواهی

۲. مکانیزم‌های عام یا فراگیر

- توابع قابل اعتماد
- برچسب‌های ایمنی
- تشخیص حوادث
- بازبینی دنباله‌ها
- بازیابی

تفاوت مکانیزم خاص و عام

تفاوت بین مکانیزم‌های امنیت خاص و امنیت عام:

مکانیزم‌های‌خاص برای فراهم آوردن سرویس‌خاص استفاده می‌شوند، ولی مکانیزم‌های عام، ممکن است برای ایجاد هر نوع سرویسی استفاده شوند. این تقسیم‌بندی نیز بر این اساس انجام گرفته است.