

مبانی رایانش امن

بخش اول – مفهوم ها و تعریف های اولیه

مدرس:

کیارش شکیبائی

عضو هیات علمی گروه کامپیوتر دانشگاه آزاد اسلامی استان آذربایجان شرقی

پاییز ۱۴۰۵

مفاهیم پایه در امنیت

- مجموعه ای از اصول، روش ها و تکنیک هایی که برای محافظت از سیستم های رایانشی و اطلاعات ان ها در برابر تهدیدات و حملات مختلف به کار می روند.
- سیستم های رایانشی مجموعه ای از سخت افزار نرم افزار و شبکه ها هستند که در راستای \ردازش و ذخیره سازی اطلاعات و همچنین انجام محاسبات \یچیده طراحی و اجرا می شوند.

انواع سیستم های رایانشی

- کامپیوترهای شخصی

- سرورها

- ابر رایانه ها

- دستگاه های تعبیه شده

- رایانش ابری

- رایانش مه

مفهوم امنیت

- دوری از هر گونه ریسک ایمنی
- دوری از هر گونه شک ترس و عصبانیت
- وجود حس اعتماد و اطمینان لازم در شبکه و سیستم
- بهره گیری از هر چیزی که به کاربران آرامش، اعتماد، ایمنی و اطمینان می دهد
- رایانش ابری
- رایانش مه

مفهوم امنیت

• به طور غیر رسمی عبارت است از هر چیزی که برای ما دارای اهمیت بالاست.

□ در برابر حملات عمدی

□ در برابر حملات غیر عمدی

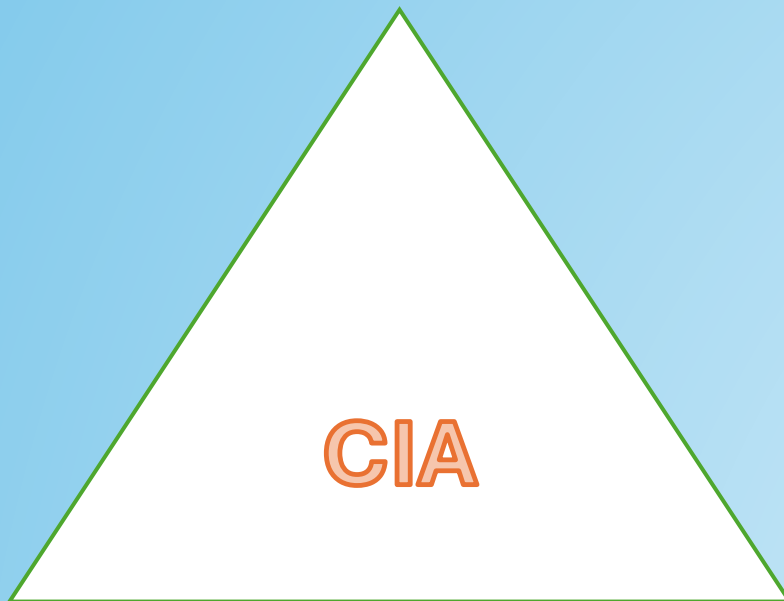
جنبه های اصلی امنیت

محرمانگی
(confidentiality)

CIA

جامعیت
(Integrity)

دسترس پذیری
(Availability)



جنبه های اصلی امنیت

- محرمانگی: دسترسی تنها افراد مجاز به داده ها، منابع، اطلاعات و...
- عدم دسترسی افراد غیر مجاز به داده های افراد مجاز
- یکی از مهم ترین راه کارها استفاده از رمزنگاری است.

جامعیت (Integrity)

- جامعیت یا یکپارچگی عبارت است از مجموعه مکانیزم هایی که برای جلوگیری از تحریف اطلاعات، حذف، آلوده کردن، تکرار، دستکاری و... بکار می رود.
- جامعیت داده: گیرنده همان پیامی را که فرستنده ارسال می کند دریافت نماید.
- جامعیت مبداء: پیام دریافتی دقیقا از همان فرستنده ای باشد که انتظار می رود.
- از جمله راهکارها می توان به مکانیزم های تصدیق اطلاعات و امضای دیجیتال اشاره کرد.

دسترس پذیری (Availability)

- منابع مجاز برای دسترسی یک کاربر همواره در اختیار وی قرار گیرد.
- دسترس پذیری به معنای توانایی تطبیق منابع رایانشی و شبکه جهت کمک به پیاده سازی سیاست های معقول برای بازیابی شرایط پس از وقوع یک رخداد است. بنابراین این اصل زمانی معنی می یابد که علاوه بر جلوگیری از دسترسی افراد غیرمجاز به داده های حساس، افراد مجاز به منابع و اطلاعات مورد نیازشان دسترسی داشته باشند.

میزان دسترس پذیری در لایه‌های مختلف

- لایه دسترسی در برنامه‌های کاربردی به این صورت است که برنامه‌های کاربردی طراحی شده برای کاربران نهایی فقط باید به جریان‌های کاری ضروری کسب و کار دسترسی داشته باشند.
- لایه دسترسی زیرساخت به این مسئله می‌پردازد که اجزای زیرساخت باید فقط به بخش‌های مورد نیاز (یعنی فقط سرورها) دسترسی داشته باشند.
- در لایه دسترسی فیزیکی، دسترسی‌های فیزیکی به هر سیستم، مرکز داده، رایانه یا هر شیء فیزیکی دیگری که حاوی اطلاعات محرمانه است می‌بایست فقط شامل مواردی باشد که برای انجام کار ضروری هستند.
- لایه داده‌های در جریان به امنیت داده‌های در حال انتقال می‌پردازد.

تعریف های مهم

• امنیت اطلاعات:

- ✓ مجموعه تمهیدات جهت جلوگیری از رخدادهای ناخوشایند
 - ✓ مجموعه مکانیزم های مربوط به جلوگیری، پیشگیری و کاهش احتمال وقوع رخدادهای خطرناک
 - ✓ جلوگیری از تمرکز قدرت در هر نقطه از شبکه در حین رخدادهای ناخوشایند
- ## • دارایی: هر موضوعی که ارزش محافظت داشته باشد.
- ## • تصدیق اطلاعات: شامل تامین جامعیت مبدا یعنی کاربر همان فردی است که اداع می کند.
- ## • مجاز شناسی: هر کاربر به اندازه سطح دسترسی تعریف شده در سیستم به اشیاء موردنظر خود دسترسی داشته باشد.

تعریف های مهم

• حفظ حریم خصوصی: مقاومت در مقابل افشای اطلاعات که می تواند از بستر شبکه استنتاج شود.

✓ توجه داشته باشید که محرمانگی و حفظ حریم خصوصی یکی نیستند.

✓ برای نمونه کد ملی و کلمه عبور

• خط مشی امنیتی: به مجموعه بایدها و نبایدهایی که موجب می شود تا دارایی های یک سازمان امن بماند، خط مشی امنیتی گفته می شود.

سیاست امنیت اطلاعات (ISP)

- سیاست امنیت اطلاعات سندی است که یک سازمان بر مبنای نیازها و شرایط خاص خود تهیه می‌کند. این سند، داده‌هایی که باید محافظت شوند و همچنین روش‌های حفاظت از آن‌ها را مشخص می‌کند و راهنمایی‌های لازم برای تأمین ابزارهای امنیت سایبری را در اختیار سازمان‌ها قرار می‌دهد.

- نکات کلیدی در مورد سیاست امنیت اطلاعات:

- ✓ توضیحات لازم در خصوص هدف از ارایه طرح امنیت اطلاعات
- ✓ تعریف کلیدواژه‌های موجود در سند برای ایجاد یک درک مشترک بین تمامی افراد
- ✓ تعریف سیاست حفاظت از کلمات عبور
- ✓ تعیین اینکه چه اشخاصی به چه داده‌هایی دسترسی داشته باشند.
- ✓ تعیین نقش و مسئولیت‌های کارمندان برای حفاظت از داده‌ها

ادامه تعریف های مهم

- **مکانیزم امنیتی:** منظور پیاده سازی خط مشی امنیتی است. برای ثبت ورود و خروج کارمندان
- **سرویس امنیتی:** خدمتی است که امنیت سیستم های پرداز داده و انتقال اطلاعات را ارتقاء می دهد این سرویس ها تمایل دارند با حملات امنیتی مقابله کنند. برای نمونه سرویس مجلز شناسی
- **آسیب پذیری:** هر گونه نقطه ضعفی که موجب به خطر افتادن منابع یک سیستم می شود. به عبارات دیگر هر نقطه ضعفی که در توصیف، طراحی، پیاده سازی، پیکربندی و اجرا که بتوان از آن سوء استفاده کرد و در حقیقت نقض خط مشی های امنیتی سیستم.

ادامه تعریف های مهم

- تهدید: احتمال سوء استفاده کردن از یک یا چند آسیب پذیری است. احتمال تهدید

سرویس احراز هویت توسط یک حمله کننده

✓ تهدید های طبیعی، عمدی و غیر عمدی

- حمله امنیتی:

✓ زمانی که یک تهدید از حالت بالقوه به بالفعل تبدیل می شود.

✓ محقق شدن یک تهدید از طریق یک یا چند آسیب پذیری روی یک یا چند دارای اطلاق

می شود

انواع تهدیدات

• طبیعی

✓ سیل، زلزله، آتش سوزی، رعد و برق و...

✓ گستردگی جغرافیایی، ایجاد اختلال و گسترش بحران

✓ استفاده و ایجاد مرکزهای پشتیبان در نقاط مختلف-استفاده از ماهواره به جای

سایر رسانه های انتقال نظیر فیبر

انواع تهدیدات

• غیر عمدی

✓ عوامل انسانی نظیر مدیر شبکه، کارمند، کاربر و...

✓ طراحی نادرست و غیر اصولی زیرساخت شبکه

✓ عدم تهیه پشتیبان به طور منظم از داده ها

✓ سهل انگاری در وظایف محوله

✓ عدم رصد به موقع و مرتب سیستم ها از نظر آلودگی، خرابی، خطا و...

✓ نا آگاهی و عدم آشنایی کاربران از عملیات خطرناک

انواع تهدیدات

• عمدی

✓ هر گونه اقدام برنامه ریزی شده جهت نابودی یا تغییر در داده های حیاتی شبکه

✓ اختلال در خدمات سرویس دهنده

نمونه هایی از مخاطرات امنیتی

- کاربر A فاسلس را برای کاربر B می فرستد که اوی اطلاعات بسیار با اهمیتی است(نظیر اطلاعات مالی) کاربر C که مجاز به دسترسی به ان فایل نیست در حال پایش روند انتقال بوده و نسخه ای فایل را دریافت می کند
- مدیر شبکه D، پیامی به رایانه E مبنی بر به روز کردن فهرستی از کاربران مجاز جهت دسترسی به سیستم می فرستد. کاربر F پیام را دزدیده و اطلاعات دلخواهد خود را جایگزین یا اضافه می نماید و سپس پیام را به E ارسال می کند. رایانه E هم با تصور دریافت پیام از D اقدام لازم را انجام داده و دسترسی افراد غیرمجاز به سیستم فراهم می شود.

نمونه هایی از مخاطرات امنیتی-ادامه

- ارسال یک پیام از طرف یک مشتری به کارگزار جهت خرید سهام و سپس متعاقب با آن پایین آمدن قیمت سهام و انکار توسط مشتری
- به جای دزدین پیام، کاربر F پیام مورد نظر خود با ورودی های دلخواه را ساخته و آن را طوری به E ارسال می کند که وی تصور می کند پیام از طرف d ارسال شده است و تغییرات موجود در فایل را در سیستم اعمال می کند

حمله

- از قوه به فعل در آمدن یک یا چند تهدید
- ممکن است موجب خسارت شود.
- ممکن است تلاش نافرجام باشد.
- دارای تنوع و گوناگونی بسیار بالا

تهدیدات چهارگانه

- **استراق سمع (Interception)**

✓ هر گاه شخص غیرمجاز به هر نحوی نسخه ای از داده های در حال جریان مابین مبدا و مقصد را شنود کند یک حمله استراق سمع رخ داده است.

✓ به خطر افتادن اصل محرمانگی اطلاعات

- **دستکاری (Modification)**

✓ هر گاه داده های در حال جریان بین مبدا و مقصد توسط شخص غیر مجاز به هر نحوی دستکاری یا دچار تحریف شوند، این حمله رخ داده است.

✓ به خطر افتادن صحت اطلاعات

تهدیدات چهارگانه

• جعل (Fabrication)

✓ هر گاه شخص غیرمجاز اقدام به تولید پیام های ساختگی و ارسال آن ها را به شخص مجاز دیگری نسبت دهد، جعل رخ داده است.

✓ به خطر افتادن اصل احراز هویت

• وقفه (Interruption)

✓ هر گاه فردی بتواند سیستم یا خدمتی را از کار بیاندازد یا از روال عادی جریان اجرای آن جلوگیری کرده یا خارج کند وقفه رخ داده است.

✓ به خطر افتادن قابلیت دسترسی

انواع حملات

- حملات فعال (Active Attacks)

- معمولاً در هنگام وقوع کاملاً آشکار می شوند.

- ✓ وقفه

- ✓ دستکاری پیام

- ✓ جعل

- حملات غیر فعال (Passive Attacks)

- هیچ علامت آشکاری در سیستم و شبکه نشان داده نمی شود و برای مدت های طولانی امکان عدم آشکاری وجود دارد که بسیار خطرناک هستند.

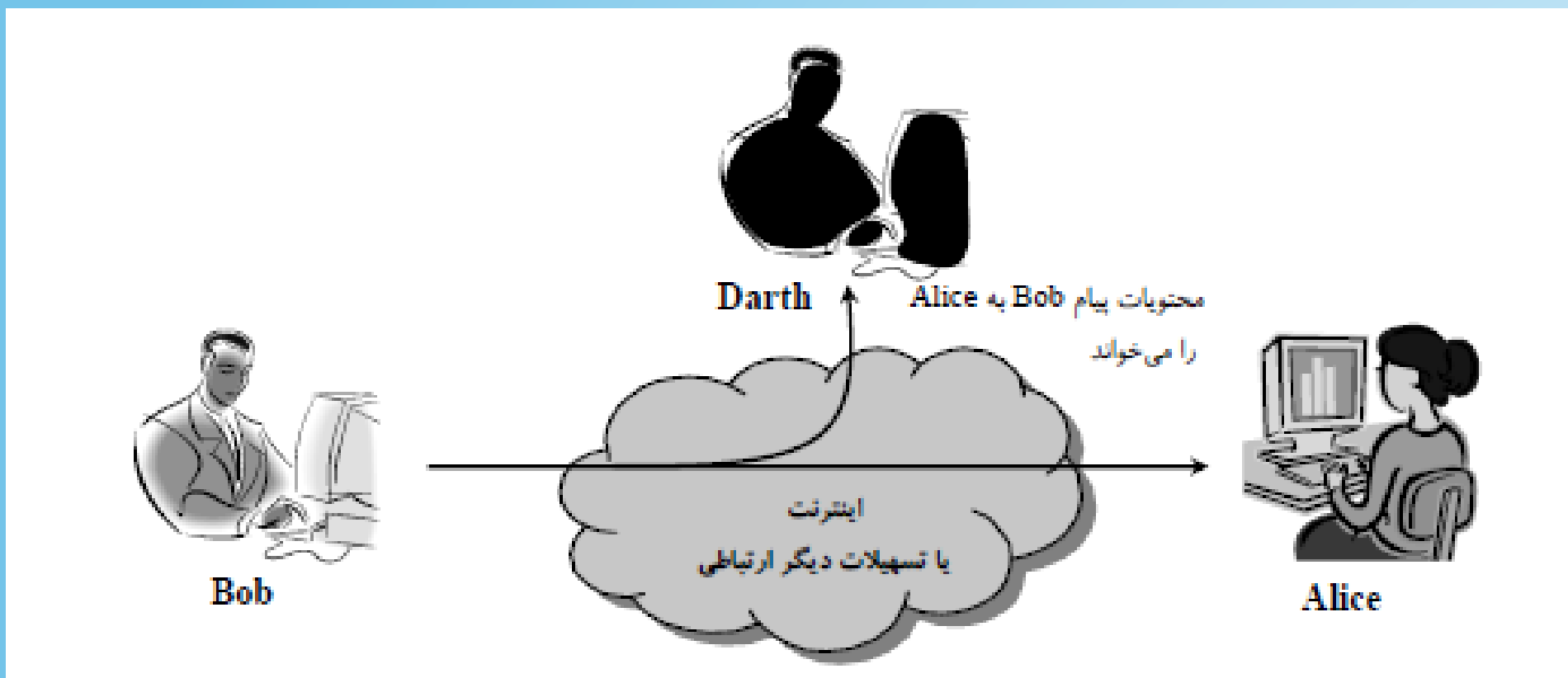
- هیچ ابزاری در برخی موارد قادر به شناسایی نیست.

- ✓ پیشگیری به جای تشخیص: ایجاد یک کانال ارتباطی امن بین طرفین تبادل کننده پیام

- ✓ استراق سمع

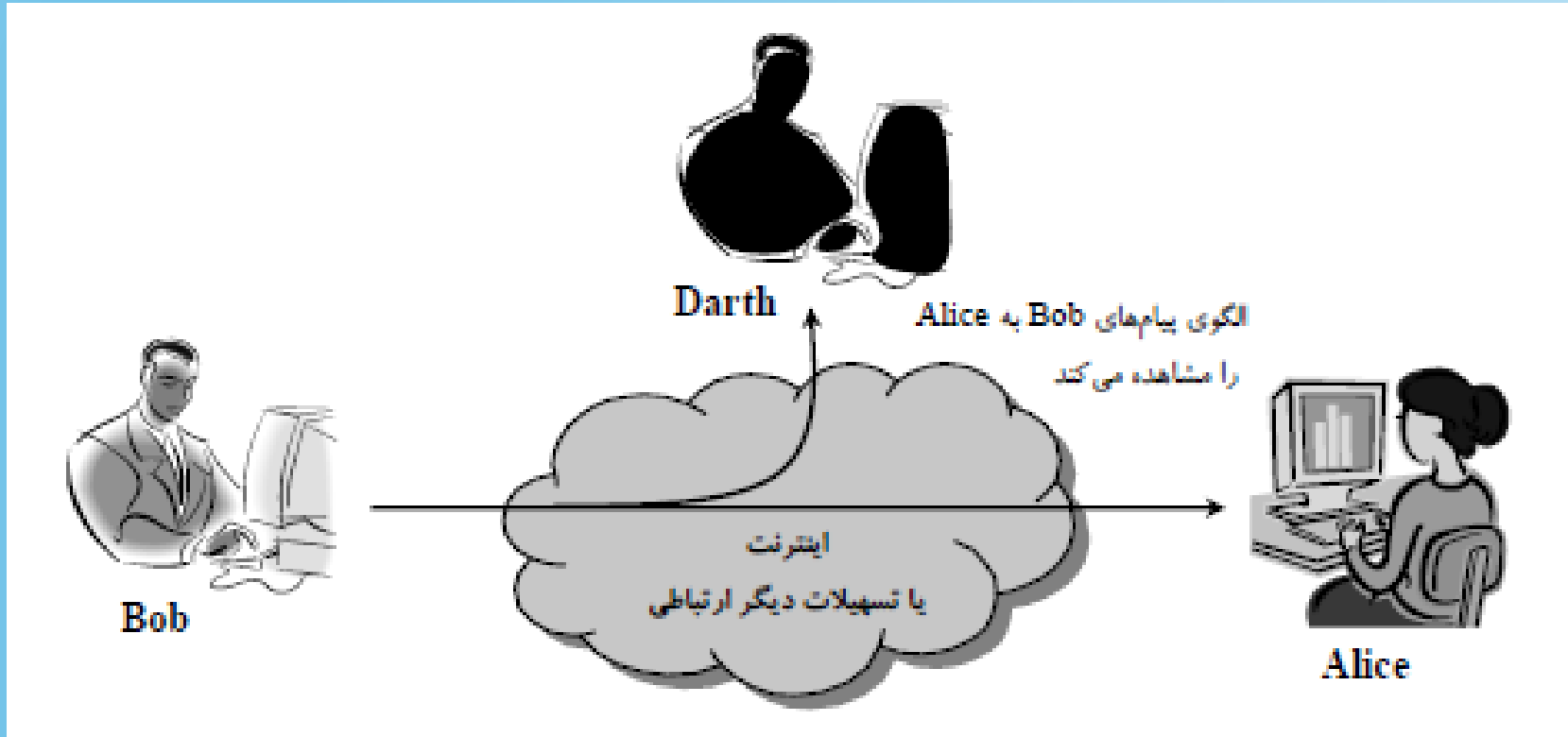
افشای محتویات پیام

- یک مکالمه تلفنی، یک پست الکترونیک و یک فایل انتقال یافته شامل اطلاعات حساس و محرمانه که نمی خواهیم دشمن به آن دسترسی داشته باشد.



تحلیل ترافیک

- تغییر محتویات پیام یا سایر اطلاعات ترافیکی به روشی که در صورت سرقت اطلاعات نیز امکان استخراج اطلاعات و داده های صحیح وجود نداشته باشد. (تکنیک عمل رمزنگاری است)



حملات فعال

- شامل ایجاد تغییرات در جریان داده ها یا خلق جریان جدیدی از داده است. می توان چهار دسته زیر را برای آن در نظر گرفت:

✓ نقاب دار

✓ بازخوانی

✓ تغییر پیام

✓ انکار سرویس

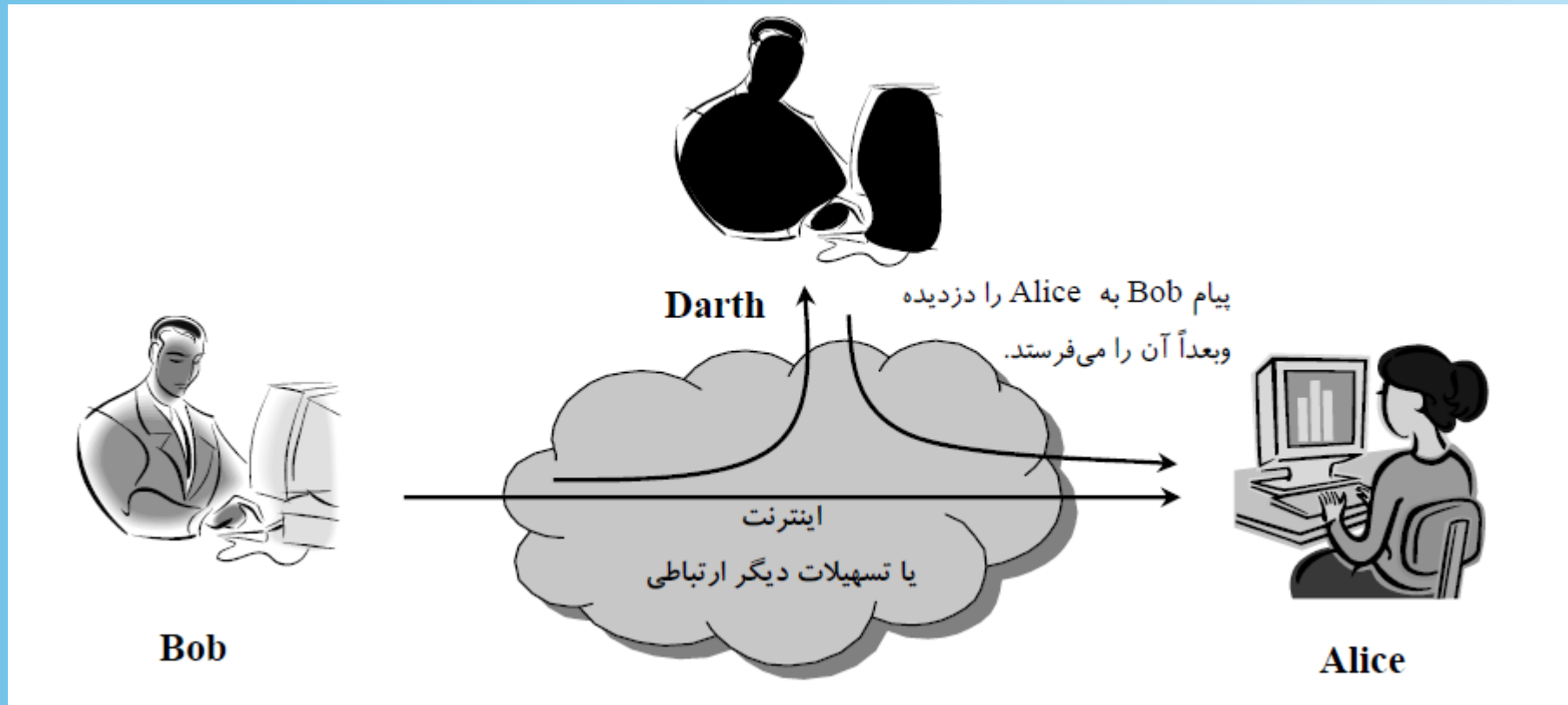
حملات فعال-ادامه

- حمله نقاب دار وقتی صورت می پذیرد که شخصی یا واحدی وانمود کند که شخص یا واحد دیگری است. معمولاً همراه با حمله فعال دیگری است.



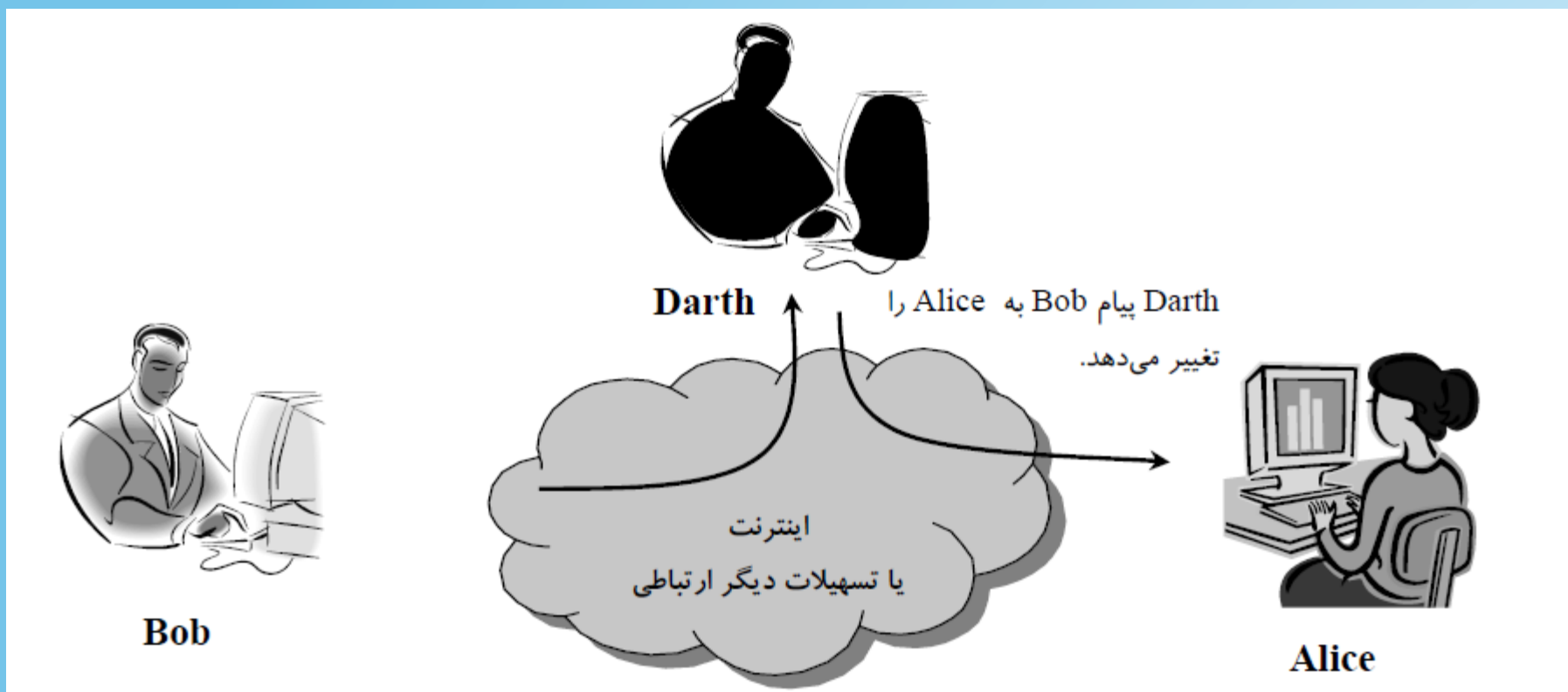
حمله بازخوانی

- شامل دزدیدن غیر فعال واحدهای داده و ارسال مجدد آن ها با تاخیر برای ایجاد یک اثر مخرب است.



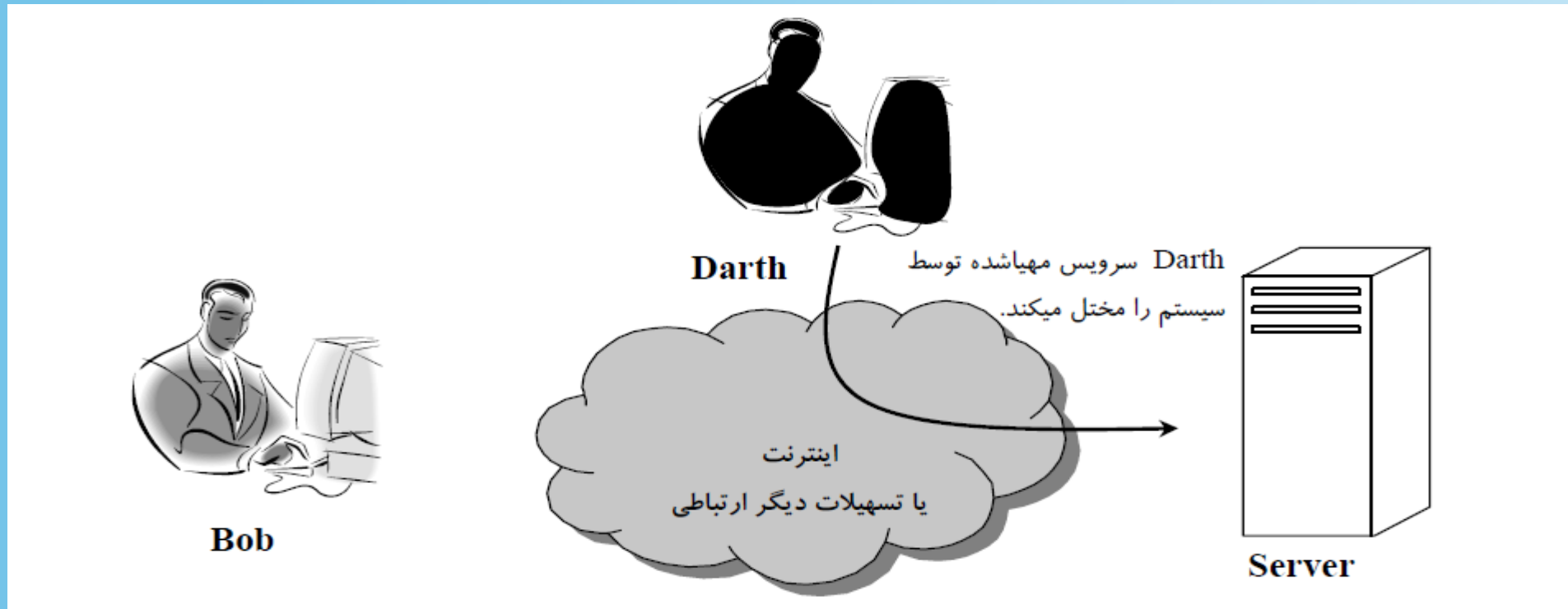
تغییر پیام

- تغییر بخشی از یک پیام قانونی یا تاخیر در پیام یا بر هم خوردن نظم آن ها، نهایتاً مسبب اثر غیر مجاز خواهند شد.
- برای نمونه پیام «به آقای حمید حمیدی اجازه دهید تا فایل حساب های محرمانه را مشاهده کند» به پیام «به آقای مجید مجیدی اجازه دهید تا فایل حساب های محرمانه را مشاهده کند» تغییر می دهد.



انکار سرویس

- مانع کارکرد عادی تجهیزات شده یا از مدیریت تسهیلات ارتباطی جلوگیری می کند.
- نشانه گرفتن یک هدف معین، برای نمونه واحدی تمام پیام هایی که به یک مقصد به خصوص ارسال می شود را حذف کند.
- ایجاد اختلال در تمام شبکه با ارسال پیام های بسیار زیاد به منظور ایجاد اختلال در عملکرد شبکه



جمع بندی بحث حملات

- حملات فعال دارای مشخصاتی خلاف حملات غیر فعال هستند.
- تشخیص حملات غیر فعال دشوار است. روش هایی برای جلوگیری از موفقیت آن ها وجود دارد.
- جلوگیری از حملات فعال کاری بس دشوار است. نیازمند محافظت فیزیکی تمام تسهیلات و مسیرهای ارتباطی در تمام زمان ها است.
- هدف تشخیص حملات فعال، رفع مشکلات یا تاخیر هائی است که این حملات در شبکه ایجاد می کنند.

آسیب پذیری ها (انواع، دسته بندی و برترین ها)

تعریف آسیب پذیری (Vulnerability)

- هر نوع ضعف، نقص یا خلا در یک سیستم رایانشی، نرم افزار، شبکه یا فرآیند
- سوء استفاده توسط مهاجم
- دسترسی غیر مجاز، تخریب اطلاعات، ایجاد اختلال در عملکرد سیستم
- دلایل آسیب پذیری: طراحی نادرست، پیاده سازی ضعیف، عدم پیکربندی مناسب

انواع آسیب پذیری

- آسیب پذیری های نرم افزاری: خطاهای برنامه نویسی، پیکربندی نادرست، عدم به روزرسانی یا به روزرسانی نادرست

- آسیب پذیری های سخت افزاری: طراحی نادرست، تولیدات معیوب

- آسیب پذیری های پیکربندی

- آسیب پذیری های سیاست

OWASP Top 10

- **OWASP مخفف عبارت Open Worldwide Application Security Project به**
معنای «پروژه جهانی متن باز امنیت برنامه‌های کاربردی» است. این سازمان یک بنیاد غیرانتفاعی و بین‌المللی است که با هدف ارتقای امنیت نرم‌افزارها فعالیت می‌کند.
- **هدف OWASP Top 10 شناسایی و معرفی مهم‌ترین آسیب‌پذیری‌های امنیتی برنامه‌های**
تحت وب و افزایش آگاهی توسعه‌دهندگان و متخصصان امنیت نسبت به این تهدیدها است.

فرآیند تهیه و به روز رسانی فهرست های OWASP

- ۱- جمع آوری داده از منابع معتبر
- ۲- تحلیل فراوانی و شدت آسیب پذیری ها
- ۳- بررسی نظر متخصصان امنیت
- ۴- رتبه بندی آسیب پذیری ها
- ۵- انتشار نسخه جدید

۱۰ آسیب پذیری برتر امنیتی برنامه های تحت وب فهرست OWASP

- 1 نقص در کنترل دسترسی (Broken Access Control)
- 2 پیکربندی نادرست امنیتی (Securiyt Misconfiguration)
- 3 نقص در زنجیره تامین نرم افزار (Software Supply Chain Failures)
- 4 خطاهای رمزنگاری (Cryptographic Failures)
- 5 حملات تزریق (Injection)
- 6 طراحی ناامن (Insecure Design)
- 7 نقص در احراز هویت (Authentication Failure)
- 8 نقص در یکپارچگی نرم افزار و داده ها (Software and Data Integrity Failure)
- 9 ضعف در ثبت رویدادها و هشدار امنیتی (Security logging and Alerting Failures)
- 10 مدیریت نادرست شرایط استثنائی (Mishandling of Exceptional Conditions)

نقص کنترل دسترسی

- **Broken Access Control** زمانی رخ می‌دهد که محدودیت‌های دسترسی کاربران به‌درستی پیاده‌سازی نشده باشند. در این شرایط، یک کاربر می‌تواند به بخش‌ها، فایل‌ها یا اطلاعاتی دسترسی پیدا کند که مجوز مشاهده یا ویرایش آن‌ها را ندارد. برای مثال، اگر کاربر عادی بتواند با تغییر یک شناسه در آدرس URL به اطلاعات سایر کاربران یا پنل مدیریت دسترسی پیدا کند، این آسیب‌پذیری رخ داده است.
- برای جلوگیری از **Broken Access Control** باید بررسی مجوزها در سمت سرور انجام شود، اصل حداقل دسترسی (Least Privilege) رعایت شود، از کنترل دسترسی مبتنی بر نقش (RBAC) استفاده شود و تمامی درخواست‌ها پیش از دسترسی به منابع حساس اعتبارسنجی شوند.

پیکر بندی نادرست امنیتی

- زمانی رخ می‌دهد که تنظیمات امنیتی سرورها، پایگاه‌های داده، فریمورک‌ها، سرویس‌های ابری یا سایر اجزای نرم‌افزار به‌درستی پیکربندی نشده باشند. فعال بودن تنظیمات پیش‌فرض، استفاده از رمزهای عبور پیش‌فرض، نمایش پیام‌های خطای حساس، فعال بودن سرویس‌ها و قابلیت‌های غیرضروری، تنظیم نادرست مجوزها یا نبود هدرهای امنیتی، از رایج‌ترین نمونه‌های این آسیب‌پذیری هستند.

- برای جلوگیری از این مشکل، باید تنظیمات امنیتی به‌صورت منظم بازبینی شوند، قابلیت‌ها و سرویس‌های غیرضروری غیرفعال شوند، به‌روزرسانی‌های امنیتی به‌موقع نصب شوند و تمامی محیط‌های توسعه، آزمایش و عملیاتی بر اساس یک پیکربندی امن و استاندارد مدیریت شوند.

نقص در زنجیره تامین نرم افزار

- به مشکلات و ضعف‌های امنیتی در فرایند توسعه، ساخت، به‌روزرسانی و انتشار نرم‌افزار اشاره دارد. این آسیب‌پذیری معمولاً زمانی رخ می‌دهد که از کتابخانه‌ها، فریمورک‌ها، ابزارها یا سایر وابستگی‌های شخص ثالث آسیب‌پذیر، قدیمی یا غیرقابل اعتماد استفاده شود. برای مثال، اگر یک کتابخانه متن‌باز دارای یک آسیب‌پذیری شناخته‌شده باشد و بدون به‌روزرسانی در نرم‌افزار استفاده شود، مهاجمان می‌توانند از همان ضعف برای نفوذ به سیستم سوءاستفاده کنند.

- برای کاهش این خطر، باید تمامی وابستگی‌ها به‌طور مداوم شناسایی و پایش شوند، تنها از منابع معتبر استفاده شود، به‌روزرسانی‌های امنیتی به‌موقع نصب شوند و امنیت فرایند توسعه و استقرار نرم‌افزار (CI/CD) نیز به‌دقت محافظت شود.

خطاهای رمزنگاری

به استفاده نادرست از رمزنگاری یا به کارگیری الگوریتم‌ها، پروتکل‌ها و روش‌های نامناسب برای محافظت از اطلاعات حساس اشاره دارد. ذخیره رمزهای عبور به صورت متن ساده، استفاده از الگوریتم‌های رمزنگاری قدیمی یا ضعیف، مدیریت نادرست کلیدهای رمزنگاری و انتقال اطلاعات بدون استفاده از **HTTPS** یا **TLS**، از رایج‌ترین نمونه‌های این آسیب‌پذیری هستند.

در صورت سوءاستفاده از این ضعف امنیتی، اطلاعات محرمانه مانند رمزهای عبور، اطلاعات بانکی، داده‌های شخصی و سایر اطلاعات حساس ممکن است افشا شوند. برای جلوگیری از این مشکل، باید از الگوریتم‌های رمزنگاری استاندارد و به‌روز، پروتکل **TLS** برای انتقال امن داده‌ها، مدیریت صحیح کلیدهای رمزنگاری و الگوریتم‌های هش امن مانند **Argon2**، **bcrypt** یا **PBKDF2** برای ذخیره رمزهای عبور استفاده شود.

حملات تزریق

- یکی از رایج‌ترین و خطرناک‌ترین آسیب‌پذیری‌های امنیتی است که زمانی رخ می‌دهد که داده‌های ورودی کاربران بدون اعتبارسنجی یا پردازش مناسب، در دستورات SQL، سیستم‌عامل یا سایر مفسرها اجرا شوند. در این شرایط، مهاجم می‌تواند دستورات مخرب خود را اجرا کرده و به اطلاعات حساس دسترسی پیدا کند یا عملکرد برنامه را تغییر دهد.
- **SQL Injection** شناخته‌شده‌ترین نوع این آسیب‌پذیری است، اما حملاتی مانند **NoSQL Injection**، **Command Injection** و **LDAP Injection** نیز در این دسته قرار می‌گیرند. برای جلوگیری از حملات تزریق، باید داده‌های ورودی اعتبارسنجی شوند، از **Query**های پارامتری (**Prepared Statements**) یا **ORM** های امن استفاده شود و از ترکیب مستقیم ورودی کاربران با دستورات یا **Query**ها خودداری شود.

طراحی نا امن

- به ضعف‌های امنیتی در معماری و طراحی نرم‌افزار اشاره دارد؛ یعنی از همان ابتدا کنترل‌های امنیتی لازم در طراحی سیستم در نظر گرفته نشده‌اند. در این حالت، حتی اگر کدنویسی بدون خطا انجام شود، طراحی نادرست برنامه می‌تواند زمینه سوءاستفاده مهاجمان را فراهم کند. برای مثال، نداشتن محدودیت برای تعداد دفعات ورود ناموفق، نبود مکانیزم مناسب برای تأیید هویت یا طراحی نادرست منطق کسب‌وکار، از نمونه‌های رایج طراحی ناامن هستند.

- برای جلوگیری از این مشکل، باید از ابتدای پروژه الزامات امنیتی مشخص شوند، مدل‌سازی تهدید (Threat Modeling) انجام شود و امنیت به‌عنوان بخشی از چرخه توسعه نرم‌افزار (Secure SDLC) در تمام مراحل طراحی و توسعه در نظر گرفته شود.

نقص در احراز هویت

- زمانی رخ می‌دهد که فرآیند احراز هویت کاربران به‌درستی پیاده‌سازی نشده باشد و مهاجمان بتوانند به حساب کاربران دسترسی غیرمجاز پیدا کنند. استفاده از رمزهای عبور ضعیف، نبود احراز هویت چندمرحله‌ای (MFA)، ضعف در فرآیند بازیابی رمز عبور، مدیریت نادرست نشست‌های کاربری (Session) یا نبود محافظت در برابر حملاتی مانند Brute Force و Credential Stuffing، از رایج‌ترین نمونه‌های این آسیب‌پذیری هستند. برای جلوگیری از این مشکل، باید از رمزهای عبور قوی، احراز هویت چندمرحله‌ای، مدیریت امن نشست‌ها، محدود کردن تلاش‌های ناموفق برای ورود و استفاده از مکانیزم‌های استاندارد احراز هویت استفاده شود.

نقص در یکپارچگی نرم افزار و داده ها

- زمانی رخ می دهد که نرم افزار نتواند از صحت و یکپارچگی کدها، فایل ها یا داده های دریافتی اطمینان حاصل کند. در این شرایط، ممکن است برنامه بدون بررسی اعتبار، فایل ها، به روزرسانی ها، کتابخانه ها یا داده های دریافتی از منابع خارجی را اجرا یا پردازش کند و در نتیجه، مهاجم بتواند کد مخرب یا داده های دستکاری شده را وارد سیستم کند.
- برای جلوگیری از این آسیب پذیری، باید از امضای دیجیتال و مکانیزم های بررسی صحت فایل ها استفاده شود، تنها از منابع معتبر برای دریافت نرم افزار و وابستگی ها استفاده گردد و امنیت فرآیند توسعه و استقرار نرم افزار (CI/CD) نیز به طور کامل محافظت شود.

ضعف در ثبت رویدادهای و هشدار امنیتی

- زمانی رخ می‌دهد که برنامه رویدادهای امنیتی را به‌درستی ثبت نکند، فعالیت‌های مشکوک را پایش نکند یا در زمان مناسب هشدارهای لازم را ارسال نکند. در این شرایط، حملات ممکن است برای مدت طولانی بدون شناسایی ادامه پیدا کنند و واکنش به رخدادها امنیتی با تأخیر انجام شود.

- برای جلوگیری از این آسیب‌پذیری، باید تمامی رویدادهای مهم امنیتی به‌طور کامل ثبت شوند، لاگ‌ها در برابر دستکاری محافظت شوند، فعالیت‌های مشکوک به‌صورت مداوم مانیتور شوند و با استفاده از ابزارهایی مانند SIEM، هشدارهای امنیتی به‌موقع ایجاد و بررسی شوند.

مدیریت نادرست شرایط استثنائی

- زمانی رخ می‌دهد که نرم‌افزار نتواند خطاها و شرایط غیرعادی را به‌درستی شناسایی، مدیریت یا از آن‌ها بازبازی کند. در این شرایط، برنامه ممکن است دچار رفتارهای غیرمنتظره، از کار افتادن یا ایجاد آسیب‌پذیری‌های امنیتی شود. برای مثال، مدیریت نادرست خطاهای ورودی، قطعی شبکه، کمبود حافظه یا خطاهای پردازشی می‌تواند باعث شود سیستم در وضعیت نامشخصی قرار گیرد و مهاجمان از این شرایط سوءاستفاده کنند.

- برای جلوگیری از این مشکل، باید اعتبارسنجی مناسب ورودی‌ها انجام شود، مدیریت خطا و استثناها به‌صورت متمرکز پیاده‌سازی شود، تراکنش‌های ناقص به‌درستی بازگردانی (Rollback) شوند و تمامی خطاهای مهم ثبت، پایش و در صورت لزوم برای آن‌ها هشدار امنیتی صادر شود.

جلوگیری از آسیب پذیری های OWASP Top 10

- رعایت اصول کد نویسی امن
- اعتبارسنجی و پاکسازی ورودی کاربران
- مدیریت صحیح احراز هویت و کنترل دسترسی
- استفاده از رمزنگاری استاندارد
- به روزرسانی مداوم نرم افزارها و کتابخانه ها
- انجام آزمون نفوذ و پایش امنیتی
- ثبت و نظارت و بررسی رویدادهای امنیتی

مکانیزم های امنیتی

- سیاست

- ✓ بیانیه

- ✓ مجاز و غیرمجاز

- مکانیزم

- ✓ متد، ابزار یا روش

- ✓ اجرای سیاست امنیتی

مکانیزم های امنیتی

- مکانیزم های پیشگیرانه (Preventive Mechanisms)
- مکانیزم های تشخیص (Detective Mechanisms)
- مکانیزم های ترمیمی (Corrective Mechanisms)
- مکانیزم های بازیابی (Recovery Mechanisms)

• مکانیزم های پیشگیرانه (Preventive Mechanisms)

• کنترل های دسترسی (Access Controls)

• رمزنگاری (Encryption)

• فایروال ها (Firewalls)

• آموزش و آگاهی بخشی (Education and Awareness)

• پیکربندی ایمن (Secure Configuration)



مکانیزم های تشخیص (Detective Mechanisms)

- سیستم های تشخیص نفوذ (Intrusion Detection Systems-IDS)



- لاگینگ و نظارت (Logging and Monitoring)

- فایروال ها (Firewalls)

- حسگرهای امنیتی (Security Sensors)

- آنتی ویروس ها و آنتی بدافزارها (Antivirus and AntiMalware)

مکانیزم های ترمیمی (Corrective Mechanisms)

- پیچ و به روز رسانی (Patch and Update)
- اصلاح پیکربندی (Configuration Correction)
- تجزیه و تحلیل بعد از حادثه (Post-Incident Analysis)
- حذف بدافزارها (Malware Removal)



مکانیزم های بازیابی (Recovery Mechanisms)

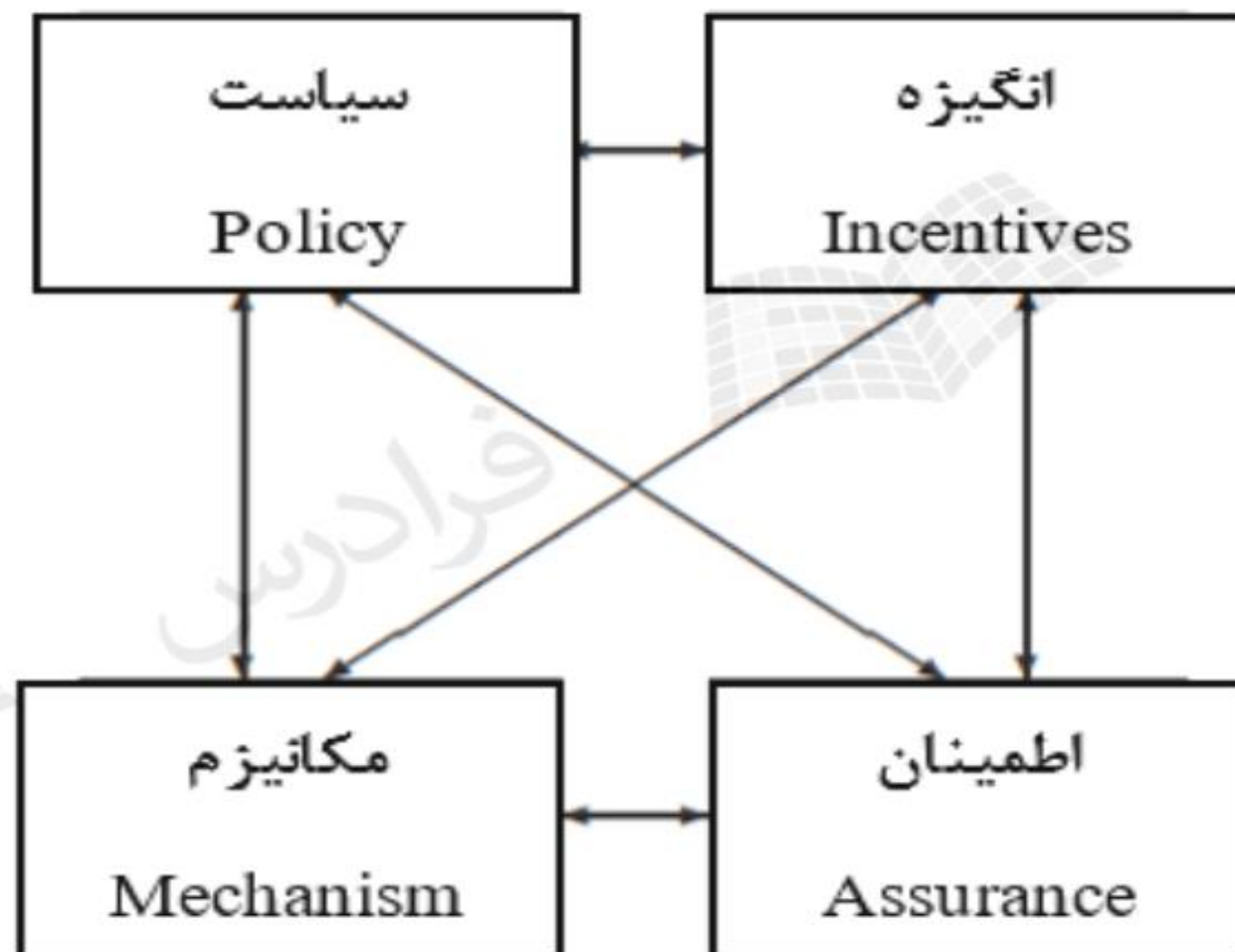
- پشتیبان گیری و بازیابی (Backup and Recovery)
- تداوم کسب و کار (Business Continuity Planning-BCP)
- برنامه های بازیابی از بحران (Disaster Recovery Planning-DRP)
- آزمون ها و تمرین های بازیابی (Recovery Drills and Tests)



اصول مهندسی امنیت

- مواجهه با سوء نیت، خطا یا اشتباه
- باقی ماندن به شکل قابل اعتماد
- به عنوان یک رشته
- تمرکز بر ابزارها، فرآیندها و روش ها جهت طراحی، پیاده سازی و آرامش
- تطبیق سیستم های موجود با تکامل محیطشان
- تخصص بین رشته ای

مهندسی امنیت



چگونگی طراحی امن سیستم ها از ابتدا

- تحلیل نیازهای امنیتی
- انتخاب معماری امن
- اجرای کنترل های امنیتی
- تست و ارزیابی امنیت
- آموزش و آگاهی

تحلیل نیازهای امنیتی

- اولین قدم در طراحی سیستم‌های امن، شناسایی نیازهای امنیتی است. این شامل تعیین دارایی‌های مهم، تهدیدات بالقوه و سطح ریسک قابل قبول می‌شود. برای مثال، یک سیستم بانکی نیاز به سطح بالایی از امنیت دارد، در حالی که یک وبسایت شخصی ممکن است نیازهای امنیتی کمتری داشته باشد.
- در این مرحله، تیم طراحی باید با کاربران نهایی و متخصصان امنیتی همکاری کند تا نیازهای واقعی را شناسایی کند. این تحلیل می‌تواند شامل بررسی استانداردهای صنعتی مانند ISO 27001 یا NIST باشد.

انتخاب معماری امن

- **اصول حداقل دسترسی:** هر کاربر یا سیستم تنها به حداقل دسترسی لازم برای انجام وظایف خود دسترسی داشته باشد.
- **جداسازی:** سیستم‌ها و داده‌ها باید به گونه‌ای طراحی شوند که در صورت نفوذ به یک بخش، سایر بخش‌ها آسیب نبینند.
- **تکرارپذیری:** سیستم باید بتواند در صورت خرابی یا حمله، به سرعت بازیابی شود.
- **شفافیت:** طراحی سیستم باید به گونه‌ای باشد که امکان بررسی و تست امنیت آن وجود داشته باشد.
- **در این مرحله، استفاده از مدل‌های امنیتی مانند Zero Trust یا Defense in Depth می‌تواند بسیار مفید باشد. این مدل‌ها به سیستم اجازه می‌دهند تا در برابر حملات مختلف مقاوم‌تر باشد.**

اجرای کنترل های امنیتی

- احراز هویت و کنترل دسترسی: استفاده از روش های احراز هویت قوی مانند احراز هویت چند عاملی (MFA).
 - شفافیت: ثبت فعالیت های سیستم و تحلیل آن ها برای شناسایی فعالیت های مشکوک.
 - به روز رسانی و پیچ: اطمینان از به روز رسانی مداوم نرم افزار و سیستم عامل برای محافظت در برابر آسیب پذیری های جدید.
 - پشتیبان گیری و بازیابی: ایجاد کپی های پشتیبان از داده ها و طراحی برنامه های بازیابی در صورت بروز فاجعه.
- در این مرحله، استفاده از ابزارهای امنیتی مانند سیستم های تشخیص نفوذ (IDS)، دیوار آتش (Firewall) و سیستم های مدیریت اطلاعات و رویدادهای امنیتی (SIEM) ضروری است.

تست و ارزیابی امنیت

- **تست نفوذ:** شناسایی آسیب‌پذیری‌های سیستم توسط متخصصان امنیتی.
 - **تست عملکرد:** بررسی عملکرد سیستم در شرایط مختلف، از جمله تحت بار سنگین.
 - **تست امنیت:** بررسی سیستم برای شناسایی نقض‌های امنیتی بالقوه.
- این تست‌ها باید به صورت مداوم و دوره‌ای انجام شوند تا از امنیت سیستم در طول زمان اطمینان حاصل شود.

آموزش و آگاهی

- یکی از مهم‌ترین بخش‌های طراحی سیستم‌های امن، آموزش کاربران و تیم‌های فنی است .
کاربران باید در مورد بهترین روش‌های امنیت آگاه باشند و تیم‌های فنی باید با آخرین تهدیدات و روش‌های دفاعی آشنا باشند.
- آموزش‌های دوره‌ای در زمینه امنیت سایبری، مدیریت رمز عبور، شناسایی فیشینگ و سایر تهدیدات رایج می‌تواند به کاهش ریسک‌های امنیتی کمک کند.

چالش های مهندسی امنیت

- **تغییرات مداوم:** تهدیدات سایبری با سرعت زیادی تغییر می کنند و سیستم های امنیتی باید بتوانند با این تغییرات سازگار شوند.
- **محدودیت های بودجه:** اجرای کنترل های امنیتی کامل ممکن است هزینه های بالایی داشته باشد و سازمان ها باید بین امنیت و سایر نیازهای تجاری تعادل برقرار کنند.
- **کمبود تخصص:** پیدا کردن متخصصان امنیتی با تجربه و مهارت کافی می تواند چالش برانگیز باشد.
- **پیچیدگی:** سیستم های مدرن بسیار پیچیده هستند و طراحی امنیت در چنین سیستم هایی می تواند بسیار دشوار باشد.