

به نام خدا

آزمایشگاه مهندسی نرم افزار

گزارش کار هفتم

استاد: علیرضا محمدی گهر

گروه ۵

نام اعضا:

مهران گل کار

امیررضا ساریخانی

ویژگی های کیفی یک سیستم مهندسی

(۱) در دسترس بودن (Availability)

(۲) امنیت (Security)

(۳) قابلیت ارتقا (Upgradeability)

(۴) اثر بخشی (Effectiveness)

(۵) انعطاف پذیری (Flexibility)

(۱) در دسترس بودن (Availability)

درصدی از زمان در یک بازه زمانی خاص است که در طول آن یک سرور، یک سرویس کلود و یا هر ماشینی که قابل روشن شدن است، برای کاربردی که برای آن در نظر گرفته شده استفاده می شود و به درستی کار می کند.

فرمولی که البته ساده ترین فرمول برای محاسبه Uptime است و اغلب از آن استفاده می شود به صورت زیر می باشد:

$$\text{Availability (\%)} = \text{Uptime} / \text{Total Time}$$

$$\text{Total Time} = \text{Downtime} + \text{Uptime}$$

با این فرمول می توانیم حداکثر میزان Downtime که یک سرویس می تواند داشته باشد تا Service Level Agreement یا SLA خود برسد را به دست آوریم.

Uptime چیست؟

Uptime به میزان زمانی اطلاق می شود که یک سرور، یک سرویس کلود و یا هر ماشینی که قابل روشن شدن است، به درستی کار می کند.

Downtime نیز همان طور که از نام آن مشخص است در واقع معرف مدت زمان خرابی و یا غیر فعال بودن سیستم می باشد.

۲) امنیت (Security)

مهندسی امنیت یک زمینه تخصصی از شاخه مهندسی می باشد که بر روی جنبه های امنیتی در طراحی سیستم هایی که لازم است بتوانند با قدرت در مقابل منابع خرابی بایستند، تمرکز دارد. این خرابی ها می توانند گستره ای از بلایای طبیعی تا فعالیت های بدخواهانه باشند. مهندسی امنیت شبیه به دیگر فعالیت های مهندسی سیستم است که انگیزه اصلی آن پشتیبانی از عرضه راهکارهای مهندسی، که نیازمندی های کاربر و عملکردهای از پیش تعریف شده را برآورده می سازد، است. اما این کار را با ابعاد اضافه ای جهت جلوگیری از سوء استفاده و رفتارهای بدخواهانه انجام می دهد. این محدودیت ها در اکثر اوقات به عنوان سیاست های امنیتی اضافه می شوند.

امنیت شامل سه عنصر پایه ای می باشد :



(۱) محرمانگی (Confidentiality)

(۲) یکپارچگی (Integrity)

(۳) در دسترس بودن (Availability)

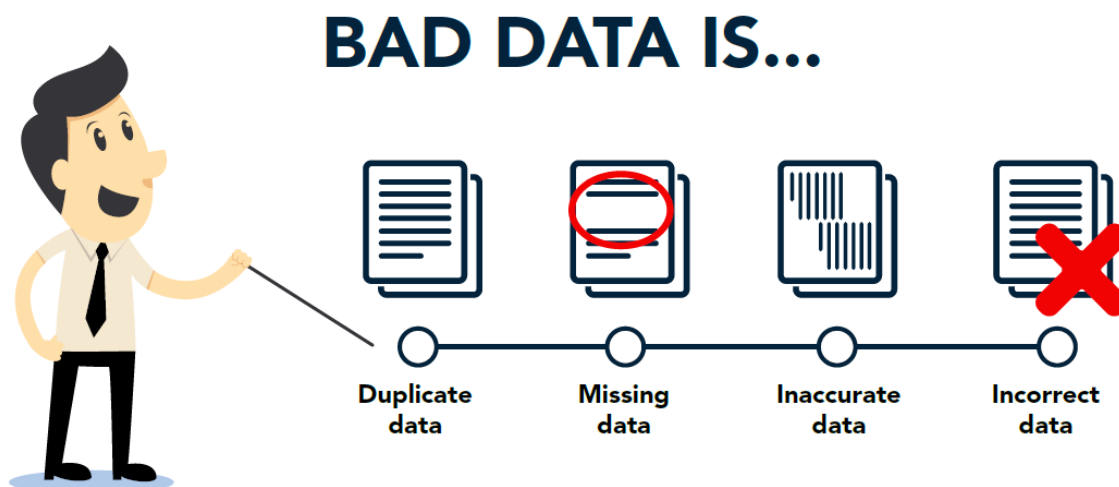
(۱) محرمانگی (Confidentiality)



محافظت از افشای داده در حملات غیر فعال استراق سمع: با کمک شیوه های رمزنگاری و ناخوانا نمودن اطلاعات پیش از ارسال .

محافظت از جریان ترافیک در برابر حملات غیر فعال تحلیل ترافیک با محرمانه نمودن اطلاعات مربوط به مبداء، مقصد، تکرار، طول و ویژگی های ترافیک روی کانال ارتباطی مثل VPN.

۲) یکپارچگی (Integrity)



هدف :

جلوگیری از حذف، اضافه، تکرار و به عبارتی اعمال هر گونه تغییر غیر مجاز در داده ها

داده ها مهم ترین دارایی های سامانه ها و سازمان ها

مهمترین هدف امنیتی سازمان ها :

محافظت از داده ها در برابر مهاجمین با کمک انواع راهکارها و سطوح دسترسی و اجازه عبور و

۳) در دسترس بودن (Availability)



امکان دسترسی کاربران مجاز سیستم با توجه به مشخصات عملکردی سیستم و حقوق دسترسی خود در زمان های مجاز را دسترس پذیری گویند.

تضمین های سرویس دسترس پذیری :

امکان استفاده کاربر مجاز از منابع سیستم طبق ضوابط ، تحت هر شرایطی

(۳) قابلیت ارتقا (Upgradeability)

ارتقا در واقع فرآیند جایگزینی یک محصول یا کالا که در مقایسه با کالای پایه دارای نسخه جدیدتر است، می باشد. در الکترونیک محاسباتی و مصرفی، به صورت کلی و عمومی، ارتقا به معنای جایگزینی سخت افزار و نرم افزار که دارای نسخه جدیدتر و با عملکرد بهتر نسبت به نسخه اولیه است، می باشد. ارتقا در سیستم به منظور به روز رسانی سیستم می باشد تا خصوصیات سیستم بهبود و ارتقا یابد.

(۴) اثربخشی (Effectiveness)

اثربخشی با توجه به میزان همسو بودن فعالیت‌ها با هدف‌های تعیین شده سنجیده می‌شود. بنابراین افزایش اثربخشی به این معناست که فعالیت‌های ما، بیش از گذشته با هدف‌هایمان همسو شده است.

همانطور که در تصویر زیر مشخص است، هرچه زاویه بزرگتر شود، می توان گفت اثر بخشی کاهش یافته است.



۵) انعطاف پذیری (Flexibility)

انعطاف پذیری را در واقع می توان میزان توانایی سازمان در تطبیق با تغییرات مهم و آنی یک سیستم مهندسی تعریف کرد. در این تعریف منظور از تغییرات، آن دسته از وقایع محیط می باشد که بر روی عملکرد سیستم تاثیرات معناداری خواهند داشت.

میزان انعطاف پذیری یک سیستم اغلب به عنوان یک اولویت رقابتی در کنار هزینه، کیفیت و نوآوری تفسیر می شود. همانطور که هزینه پایین و کیفیت بالا از نیازهای ورود به یک بازار هستند، انعطاف پذیری را می توان کلید نهایی ایجاد قابلیت های رقابتی بین سیستم ها دانست. همچنین با توجه به افزایش پویایی و تغییرات به وجود آمده، موضوع انعطاف پذیری جایگاه مهمتری در بحث های سیستمی کسب نموده است که می بایست با اخذ تدابیر هوشمندانه مورد توجه قرار گیرد.

بررسی پارامتریک در سیستم کتابخانه

(۱) در دسترس بودن (Availability)

کتابخانه از طریق اقدامات زیر این خصوصیت را در سیستم خود تامین می کند:

- ✓ حفظ رکوردهای مربوط به دسته بندی های مختلف مانند: کتاب ها، ژورنال ها، روزنامه ها، مجلات و ...
- ✓ اتخاذ ساز و کار آسان برای ورود کتاب های جدید به سیستم

- ✓ اتخاذ ساز و کار آسان به منظور عضویت و خروج کاربران از سیستم
- ✓ دارا بودن ضوابط مختلف و متنوع برای جستجوی کاربران
- ✓ حفظ رکوردها و اطلاعات کامل مربوط به کتاب ها شامل: نام کتاب، نویسنده، ناشر، ماه و سال نشر، بهای کتاب، تاریخ خرید و رسید خرید کتاب
- ✓ انواع مختلف گزارشات شامل: تعداد کل کتاب مورد نظر، تعداد کتاب های مرتبط، تعداد ژورنال ها و ...
- ✓ وجود ساز و کار ساده برای دانستن وضعیت یک کتاب
- ✓ وجود یک تقویم دقیق همراه با مناسبات برای کتابخانه دار برای به یاد داشتن تاریخ ها
- ✓ دسترسی آسان برای کاربر عضو کتابخانه برای مشاهده وضعیت کتاب های خود
- ✓ وجود سیستم مدیریت کتابخانه ای بر مبنای کلود برای ماندگاری همیشگی اطلاعات سیستم
- ✓ سهولت در سیستم و عدم نیاز به بررسی های مفصل و طاقت فرسا در سخت افزار سیستم

۲) امنیت (Security)

همانطور که در بخش امنیت بیان شد، این بخش از سه قسمت پایه ای تشکیل شده است:

(۱) محرمانگی (Confidentiality)

یک کتابخانه متعهد می شود که اطلاعات حقیقی و همچنین اطلاعات مربوط به حساب کاربری کاربران را با لحاظ نمودن تدابیر امنیتی مناسب و هوشمندانه حفظ نماید و تحت هر شرایطی از آنها محافظت نماید.

(۲) یکپارچگی (Integrity)

کتابخانه موظف است از حذف، اضافه، تکرار و یا به عبارت دیگر از اعمال هرگونه تغییر غیرمجاز در داده های مربوط به کاربران خودداری نماید. کتابخانه برای رسیدن به این یکپارچگی از راهکارهای مختلف مانند سطوح دسترسی و اجازه عبور در سیستم خود استفاده می کند.

(۳) در دسترس بودن (Availability)

کتابخانه موظف است امکان دسترسی کاربران مجاز کتابخانه را با توجه به مشخصات آن ها در زمان های مجاز و تعیین شده از سوی کتابخانه و مراجع بالاتر را به کاربران و متقاضیان خود بدهد.

