جلسه دهم / ۹۳/۹/۲۴ / نظریه طراحی سیستم / اقتداری

جلسه گذشته راجع به بحث امنیت صحبت کردیم، گفتیم امنیت یک هدف سلبی است، یعنی شما برای اثبات اون باید پاسخ به یک سوال بدین که هیچ راه نفوذی وجود نداره، در مقابل اگر بخواین اثبات کنین راه نفوذ وجود داره، شما باید فقط یک راه رو پیدا کنین، اما اگر بخواین اثبات کنین هیچ راه نفوذی وجود نداره، باید تمام راههای ممکن رو احصا کنین و در خصوص هر کدوم اثبات کنین، امکان نفوذ وجود نداره. و این کار مشکل است.

لذا ما امنیت ۱۰۰٪ نداریم، نکته‌ی دیگه‌ای راجع بهش صحبت کردیم بحث موازنه‌ای بود که اهمیت امنیت را در سیستم شما و توی طراحی شما نشون می‌داد، اینکه وقتی شما برای طراحی سیستم تصمیم‌گیری می‌کنید و می‌خواهید feature های امنیتی رو به اون اضافه بکنید، اول باید به این سوال جواب بدهید که امنیت برای شما چه جایگاهی داره و چه اولویتی داره که تا چه حد باید بهش پرداخته بشه این جایگاه و اهمیت در مقابل هزینه و کارایی خودش رو نشان می‌ده حتی قابلیت اطمینان رو هم می‌تونین توی این موازنه دخیل بدونید اما عمده‌ی او نها بحث هزینه و کارایی است.

عوامل مهم در موازنه

- ☐ اهمیت اطلاعات
- ☐ محیط و ابعاد
- ☐
- ☐

کارایی رو باز هم میشه به صورت سرعت سیستم بیان کرد، هم میشه به صورت قابلیت‌های دسترسی و محدودسازی‌هایی بیان کرد که وجود داره. مثال: یه زمانهایی اگرچه سیستم رو امن کردید اما محدود کردید کاربران رو و کار رو برای اونها سخت‌تر کردین، شاید سرعت، سرعت مطلوبی باشه

ارزیابی ریسک

(احتمال و تاثیر)

اما شما کار رسیدن به داده‌ها و بازیابی براتون سخت می‌شه و قابل پیاده‌سازی و عملیاتی شدن در اون حالت خاص نیست، لذا در تعامل بین هزینه و کارایی و امنیت، باید ببینید سیستم شما در کدام جایگاه قرار داره و در نسبت بین اینها امنیت رو داشته باشید.

حالا، در این قسمت می‌خواهیم ببینیم، چه عواملی در امنیت دخیل هستند.

(۱) اولین چیزی که تو موازنه‌ی امنیت وجود داره، اهمیت اطلاعات هست، خود اطلاعات به تنهایی ارزش گذاری می‌شه و ارزشمند است، . سخت‌افزار اگر ارزشش 1 باشد نرم افزار ارزشش 10 هست، یعنی شما یه PC می‌خرین ارزون، بعد windows و office و ... گرون روش نصب می‌کنین، حتی

نرم افزاری مثل هلو و اتوماسیون اداری و ... هم یک هزینه ای دارن برای خرید و نصب. همینطور که دقت می کنید، هزینه نرم افزار خیلی ↑ از سخت افزار خواهد شد و تو حوزه های تخصصی و فنی هم تا ۱۰ برابر ↑ می شه، پس هزینه سخت افزار آلز یا باشد نرم افزار هزینه اش ۱/۱۰ است؛ اطلاعات ارزش ۱۰۰ داره، چه اطلاعاتی! خیلی مواقع شما یک سرور، سخت افزار، با یه قیمتی می خرین

اهمیت اطلاعات

نرم افزار GIS یک هزینه ای داره ولی وقتی یک نرم افزار GIS رو به همراه اطلاعات خیابانهای تهران و خیابانهای جهان و ... می خرین، این اطلاعات خیلی ارزشمنده، بعضی از نرم افزارها اطلاعات کل دنیا رو با Detail داره، این نرم افزار رو می خرین، ممکنه داده هاش رو برای یک ماه اجاره کنید. مثلاً قیمت این یک ماه می شه ۲۰۰ هزار دلار، حتی ممکنه شما به همه ی اطلاعات هم دسترسی نداشته باشین، اطلاعات پردازش شده یا پردازش نشده، قیمتهاش متفاوته و بعضی مواقع سطح اطلاعات مهمه، مثلاً بعضی مواقع شما ممکنه تعداد دانشجویان یک کشور چقدر است که این شامل یه ارزشی است، وقتی شما اطلاعات یک دانشگاه خاص رو می خواین یه ارزش دیگه داره یا اطلاعات هر دانشجو باز خصیص اش فرق می کنه.

مثال دیگر: گمرک ایران اتقدر صادرات و واردات داشته، بعد هر جزئیاتش که وارد می شیم می گیم مثلاً مرز بازرگان اتقدر بوده، شاید اطلاعات رو حتی به ما ندن. اینکه ما می گیم چه کالاهایی وارد شده تو چه برهه ای و چه زمانی. اینها اطلاعاتی هستند که تونش خیلی مسایل رو می شه حل آورد.

مسائلی که امروزه در BI رخ می دهد و خیلی مانور می دهند Business intelligent بودن و شما با استفاده از اطلاعات روی وضعیت بازار مسلط می شین، این مقدار وارد شده، این مقدار کسری داریم، پس من روی اینها کار کنم و این باعث سود من هست و اینها باعث می شه اطلاعات رو به شما ندن، اینها شاید بهت راست اطلاعات رو بیان کنه، شاید گاهی اطلاعات خام ارزشش ↑ از اطلاعات پردازش شده و گزارش شده باشد، بعضی مواقع هم بالعکس، اطلاعات خام ارزشی نداره، اینها متفاوت است و بستگی به جایگاه داره

از سوی چه کسی اهمیت داره و بعضی اوقات، اطلاعاتی از جانب برخی بی ارزش است ولی از سوی افراد دیگری با ارزش است، مثلاً اطلاعات حسابداری شرکتتون، می بریدمنزل، برای خانواده شما ممکن است بی ارزش باشد، امّا برای خانواده ی شما موقتاً مهم است و این یک مساله Secure است و شاید شما نذارید اطلاعات این قسمت به دست خانواده برسد، یا ممکن است بالعکس اطلاعات صوتی شما از جانب کارکنان شرکت اهمیت نداشته باشد، امّا اطلاعات حسابداری مالی شرکت تو خود حوزه ی شرکت اهمیت داشته باشه، پس از دید چه کسی اهمیت داره هم مهمه، پس بهتر بگیم چه استفاده ای میشه از اطلاعات که اهمیت اطلاعات تامین می ره یا که زمان انقضاش فرا نرسیده باشه، اطلاعات مالی ۵ سال بعد اهمیتی نداره، ولی بعضی از اطلاعات همیشه مهم هستند، مثلاً بعضی از اطلاعات باعث رشد شرکت می شوند «مایکروسافت تا ۵ سال دیگه کد Win XP رو بیرون نمی ده» بجز اینکه ممکن است اطلاعات برای همیشه Secure باشد امحای آن هم ممکن است با تکنیک خاصی انجام شود.

پس طبیعی داریم از اهمیت اطلاعات، که پایین ترین سطحش می شه افرادی که درگیرش هستند و افرادی که می تونن ازش سواستفاده یا حسن استفاده کنن تا بالاترین سطحش که می تونه امنیتی باشه.

اطلاعات باید ارزش گذاری بشن. احتمال لو رفتن اطلاعات و تاثیر آن.

پس برای پیدا کردن تاثیر لو رفتن اطلاعات، شما باید قیمت بگذارید، ارزش گذاری بکنید، مثلاً شما باید برای هم پیدا کردن تاثیر لو رفتن اطلاعات باید قیمت بگذارید، یعنی به هرکدوم از دسته اطلاعاتتون ارزش بگذارید و ما براساس اون هزینه می کنیم و آن را پوشش می دهیم.

هم ارزش گذاری کنید برای لو رفتن و هم برای نابود شدن، بعضی مواقع ممکن است اطلاعات لو رفتنش مهم نباشه ولی نابود شدنش برای شما دردسر زیادی داشته باشه. مثل اطلاعات مربوط به ورود و خروج افراد، یکسری کارمندان هستند که به صورت روزمرد کار می کنن شما باید نرم افزار بررسی می کنید که چه ساعتی اومده، چه ساعتی رفته؟ حالا آدرس این اطلاعات رو ده نفر هم توی سیستم بدونن اصلاً مهم نیست امّا اگر این اطلاعات از بین بره، آخر ماه نمی دونید براساس چه معیاری باید پرداختها رو انجام بدین پس یه زمانی محرمانگی اطلاعات است یه زمانی نابود شدن اطلاعات.

پس داده ها نباید از بین بره.

- محیط و ابعاد: تو کدوم فضا داریم اطلاعات رو ذخیره، بازیابی می کنیم و انتقال می دهیم، یه زمانی پول رو می ذارین داخل کیف پولتون، یا یه زمانی میذارین تو اتاقتون تو صوزه ی کاری، خیلی واهمه ندارین که کسی این پول رو برداره، امّا گاهی این پول رو می ذارین کنار خیابون خوب اینجا محیط شما، محیط امنی نیست محیط مه اینکه شرکت، شاید محیط امنی باشد امّا محیط اینترنت قطعاً امن نیست، وسط فضایی است که ممکن است هرکسی او بنجا بیاد و اطلاعات رو برداره و یا تحریف بکنه. گاهی اطلاعات داخل

Subject:
Year. Month. Date. ( )

wan است امّا اطلاعات داخل اینترانت است ، و این محیط رو با vpn می‌تونیم پیاده کنیم
vpn ها در بستر اینترنت یکجور امن‌سازی هست و یکجور ایزوله‌کردن اطلاعات است امّا نه‌می‌شه
گفت امنیت ۱۰۰٪ رو داره ، نه تا امنی اینترنت رو . یک امنیت نسبی رو برای ایجاد کردن خیلی جاها
می‌شه تقسیمات روب راحتی گرفت . مثلاً برای تراکنشهای مالی نمی‌شه از vpn استفاده کرد ، مثلاً
می‌خوایم انتقال وجهی از طریق اینترنت انجام بدیم یا خریدی از طریق کارت انجام بدیم ، آدرس
از طریق vpn امن هست و امن‌تر از ارتباطهای متعارف و معمول که user و pass می‌زنیم است
امّا کار رو محدود می‌کنه و این محدودکردن کارایی سیستم رو زیر سوال می‌بره - چون کارایی فقط
بحث سرعت نیست . ممکن است دست و پا گیر بودن تراکنشهای مالی باشه و در بعضی حوزه‌ها
نشه از این تر فتد استفاده کرد ، بعضی موقع‌ها ممکن است امنیتی نشود ، مثلاً شما تراکنشهای مالی تو بانک
رو وقتی مشاهده می‌کنید ، گذشته از این که lan رو که یک شبکه امن هست استفاده می‌کنه ، امّا
ممکن است افرادی که در lan هستند هم مشکل زا باشند ، لذا از توکن‌های امنیتی استفاده می‌کنند
به سمت افزار رو انتهای case قرار می‌دن و این در حقیقت یک توکن است که موجب می‌شه کسی که
فقط اون سمت افزار به سیستم‌اش وصل است اجازه دسترسی داشته باشه ، این امنیت رو
افزایش می‌دهد چون شما راهکارهای دیگه‌ای به کار می‌برین مثلاً برای تراکنشهای مالی برای
مشاهده وضعیت account ای که با بانک در اختیارتون می‌زاره یک صفحه اینترنتی با pass دارید که
وارد‌ش می‌شین علیرغم پسورد دومی که وجود داره بعد هر تراکنش مالی که می‌خواهید انجام
انجام دهید ، مشاهدات مشکل نیست ، امّا برای تراکنشها یک pass ای می‌گیرد یعنی در حقیقت
کار رو محکم‌تر می‌کنه چون محیط امن نیست و ممکن است از هرجایی دسترسی داشته باشین .

۲۸:۰۳

امّا وقتی داخل بانک میرین و تراکنشی رو می خواهید انجام دهید چون اطمینان وجود داره که شما صاحب کارت هستین و پسورد رو هم زدین، راحت تر می تونین این تراکنش رو انجام بدین، پس محیط شما در اینترنت با Atm و باجه متفاوت است. پس هر محیطی یک مکانیسم هایی داره که ممکن است سخت گیرانه یا راحت تر باشه. براساس محیط مثلاً شما داخل اتاق هستید و داخل سیستمتان log in کردین ممکنه در log in بمانید امّا در اتاق رو ببندید و از اتاق خارج شوید یا یکی از همکارا داخل اتاق باشه وقتی در رو می بندید و کسی داخل اتاق نیست اگرچه log in کردین امّا چون در رو بستین امنیت داره. پس محیط و ابعاد اون مهمه. در زمانی که اینترنتی وصل می شین رمز اینترنتی میزنین بعد رمز دوم دیگه اطمینان حاصل می شه و دیگه یکسری گزارشات هم دیگه بدون پسورد بهتون می ده، پس محیط ها zone های مختلف باید در نظر بگیریم. zone بندی محیط خودتان هم مهم است اگر یک سیستم دارین باید ببینیم از داخل منزل چه تمهیداتی باید اندیشیده شود، از داخل شعبه به چه ترتیبی هست و با چه تمهیداتی و از داخل اینترنت به چه طریقی و با چه تمهیداتی وصل شود. پس تا محیط مختلف شد.

بحث محیط فیزیکی مطرح می شه مثلاً حوزه تخریب ← مثلاً اتاق سرور در نظر می گیرن و کامپیوتر و سرور هم user و pass داره، امّا ۷۰٪ برای نابود کردن سرور کافیست ولتاژ بالایی رو به case وارد بکنید در این حالت ممکن است power بسوزه یا هارد یا حتی یک ضربه سنگین به سرور بزنید که اطلاعاتی روی هارد هست براساس اون حساسیتی که روی مغناطیسش هست آسیب ببینه و از بین بره، خیلی از موارد بانک CD می تونن user و pass ادمین رو از اول set بکنن و بهش دسترسی پیدا بکنن یا حتی اگر پشت سرور باشین ممکن است اطلاعات Database رو پاک کنن یا ...

برای این مشکلات سرورها رو در مکانهای امنی که اتاق سرور هست قرار می دن و ورود و خروج به اتاق سرور کنترل می شه و access control داره حتی با دو بین کنترل می شه. log هایی که در سرور گرفته می شه برای این است که ببینیم چه کسانی به سرور login کردن. پس ابعاد ممکنه است حتی گذشته از دسترسی به اطلاعات تو بحث محل ذخیره ی اطلاعات هم مطرح بشه یعنی شما ممکن است یکسری تمهیداتی برای دسترسی از طریق اینترنت یا از طریق lan داشته باشین، یکسری تمهیدات برای حفاظت فیزیکی از خود محل ذخیره سازی داده ها داشته باشید، حتی تمهیداتی می تونه وجود داشته باشه برای اینکه به شکلی کاربران رو بترسونه یا اینکه اونها رو از دسترسی به اطلاعات یا تخریب اونها برحذر بداره و اونها رو جلوش رو بگیره مثل log آگیری. log آگیری اگرچه مسائل دیگری هم همراهش هست، شما می تونی ببینی اطلاعات رو کی تغییر داده، چه کسی خونده، چه کسی پاک کرده، اما وجود خود سیستم log آگیری هر سطحی اگر اتفاق بیافته، گذشته از اینکه اطلاعاتی رو به شما می ده یکنوع بازدارندگی هم برای شما ایجاد می کنه، مثل دوربین مداربسته می مونه که باعث می شه جلوی تخریب گرفته بشه.

- نوع کاربران

کاربران را به سه دسته تقسیم می کنیم.

① کاربران سیستم افراد مبتدی و آماتور هستند اینها با سیستم نمی دونن چطور باید برخورد کنن و غالبا روی ناآگاهی کارهایی می کنند که سیستم رو به مخاطره می ندازه مثل بچه ها، که بچه ها برای کار کردن با یک هم چیزهایی رو تغییر می دن یا پاک می کنن که ناآگاهانه هست، بسیاری از چالشهایی که در سیستم های سازمانی رخ می دهد، کارهایی انجام شده که به صورت ناآگاهانه سیستم رو دچار چالش کرده

آگر این افراد در سیستم شما وجود دارند باید یکسری محدودیت براش تعیین بکنید تعیین اجازه ندهید که هرجایی بزن یا اگر نمی‌تونید محدود کنید یا فشار سازمانی روی محدود کردن وجود داره شما باید آموزش بدین که آموزش هم بخشی از امنیت است. که آموزش بخش جدی است.

(۲) کاربران حرفه‌ای: این کاربران کسانی هستند که آموزش لازم دیدن ومی دونن باسیستم چطوری کار کنند. این کاربران، راحت‌تره باهاشون کارکرد ومتوجه می‌شن و سیستم رونگهداری می‌کنند، اینها آموزش کمتری نیاز دارند، برای بخشهای امنیتی توجیه‌ترند و پسوردتون رو به کسی ندین یا پسورد خوب انتخاب می‌کنن

(۳) کاربران خیلی حرفه‌ای: که قصد هک دارن به اطلاعات دیگری در سفود به سیستم‌ها دارند و اگر بخوان تخریب کنند یا فعالیتی که مزاحمت برای سیستم باشه می‌تونن، باید این آدمها رو توی سیستمتون بررسی بکنید اگر توی سیستمی هستید که کسانی که هستند به جوری بدخواه هستند باید مراقب باشید و سیستمتون رو از لحاظ امنیتی ارتقا بدهید. بعضی از سیستم‌ها ممکن است به این ویژگی نیاز باشه، بعضی‌ها نه.

مثلاً بعضی جاها داری نرم افزار انبار می‌نویسی و یه محیط کوچک هست می‌دونیم که اتفاق خواستی نمی‌افته وکسی هم قصد وارد شدن به این سیستم و تغییرات نداره، امّا یجا می‌دونین اطلاعات، اطلاعات مهمی است و تغییرات ممکنه بحثای مالی رو به همراه داشته باشه و می‌دونیم افرادی به سیستم وجود دارند که می‌تونن این کار رو انجام بدهند، لذا باید حواستون باشه، این میزان حساس بودن افراد در سیستم هم باید مورد ارزیابی واقع بشه، همین هم تعداد افرادی که می‌تونن این کار رو انجام بدن، هم قدرت این افراد به علاوه هزینه‌هایی

که دارین ... یه زمانی یه سایتی رو آوردین بالا وسایت یه ذره مشکل امنیتی داشت اما
باهاش کاری نداشتیم، بعد از یه مدت دچار مشکل شد، رفتیم سراغ یک راه حل که از نظر امنیتی
اول سایت رو افزایش دادیم و در حدی شد که گفتیم به هکرها بیاید و این وب رو هک کنید
برای چه کسی این هک نمی شد؟ هکرهای متعارف اما هکر حرفه ای شاید هکش می کرد.
اگر آنالیزه رو یادتون باشه ممکنه دچار خطر بشیم

- شرایط موجود => هم هزینه شما باشه => هم مادی هم معنوی

کارایی => دست و پاگیر نباید باشه اگر داخل lan بحث user و pass و
vpn رو در نظر بگیرین خیلی دست و پاگیره، شاید برای کسایی که
می خوان کار کنن امنیت رو فراهم می کنن اما نارضایتی هم به
همراه داره، این نارضایتی کارایی سیستم رو کاهش می ده و برای
شما هزینه رو افزایش می دهد.

توانایی شما => شما هم به عنوان فردی که در سیستم دارید طراحی انجام می دهید
اگر از طریق mac یا اثر انگشت فرد باید وارد بشه، شاید شما توانایی این طراحی
رو نداشته باشید.

۵۳:۱۹'

ارزیابی ریسک => در خیلی جاها مطرح است و در بحث امنیت پررنگ است در بخش Isms
بحث جدی اش بحث ریسک است، چه خطراتی وجود داره چقدر خطرناکه و احتمالش چقدر است؟
بحثهای امنیتی تکرار داره در هر تکرار میان یکسری مباحث امنیتی رو رعایت می کنند تا امنیت رو برسونن به
۹۹/٪ مثلا در train اول مثلا ۶۰ رو در نظر می گیرین در این حالت میان سراغ اونهایی که ریسکش بالاست (۸)

امنیتش باالست، لذا یکی از پایه‌ترین مباحثی که در بخش امنیت وجود داره بحث مربوطه ارزیابی سیک است و اول این کار انجام می‌شه، بعد میرن سراغ ... باقی چیزهایی که وجود داره.

اسلاید صفحه ۵

ارکان امنیت: توی سیستم‌های مختلف امنیت رو به دسته‌های مختلفی تقسیم کردن ما به ۴ دسته تقسیم می‌کنیم.

CIA ⇐ محرمانگی (confindentiality)، جامعیت (Integrity)، احراز هویت (Authentication)

خیلی جاها این سه مورد رو به عنوان ارکان امنیت در نظر می‌گیرن،

- احراز هویت ⇐ "Authentication" ⇐ چه کسی وارد سرم افزار شده؟

AAA

- سطح اختیارات ⇐ "Authorization" ⇐ چه دسترسی‌هایی داره؟
- نظارت "Auditing" ⇐ براساس دسترسی‌هایی انجام بده نظارت می‌کنیم ببینیم چه کاری رو انجام بده.

AAA ⇒ Authentication, Authorization, Auditing

- محرمانگی (Confidentiality) ⇐ مخفی بودن اطلاعات، انواع محرمانگی وجود داره، محرمانگی ← افشای اطلاعات
- جامعیت (Integrity) ⇐ تغییر اطلاعات
- عدم انکار (non-repudiation) ⇐ مربوط می شه به این که فرستنده و گیرنده اعمال کننده تغییرات، منکر نتونه بشه تغییراتی که انجام داده یا ارسالی که انجام داده
- قابلیت دسترسی (Availability) ⇐ تمام ۳ رکن بالایی به یه شکلی محدود کننده هستند و رکن آخر، قابلیت دسترسی در مقابل اینها قرار گرفته، چون باید باسطحی بده به کسی که قراره امراز هویت اش انجام بشه و آدم مقبولی است، سطح اختیاراش هم درست است و محرمانگی هم رعایت کرده، جامعیت هم رعایت کرده، عدم انکار هم رعایت شده، حالا این آدم باید راحت با سیستم کار کنه، قرار نیست این آدم هم باسطحی با سیستم کار کنه.

ارکان امنیت

- احراز هویت (Authentication)
- سطح اختیارات (Authorization)
- Confidentiality
- Integrity
- عدم انکار (non-repudiation)
- قابلیت دسترسی (Availability)

احراز هویت ⇐ اولین رکن امنیت

ممکنه سیستم باشه ، ممکنه شخص حقیقی/حقوقی باشه .

✓☐ فرآیندی است که صحت ادعای کسی یا چیزی در خصوص هویتش را تعیین می کند. یک زمانی شما داخل بانک اطلاعاتی یا نرم افزار کار می کنین و می آین من اعتباری با این مشخصات user, pass ولی می شم و اطلاعات رو داشته باشم ، یه زمانی یک سیستم وارد یک سیستم دیگه می شه مثل web-service

✓☐ روش های کلی برای احراز هویت :

✓☐چیزی که شما می دانید

✓ ▨کلمه عبور، سوالات خصوصی ⇐ مثلاً وقتی user, pass در سطح سازمانی می گیرین برای یک سیستم ، اون چیزی هست که در حافظه شما آنرا می دانید ، و دیدید که برای ایمیل ها هم یکسری سوال از شما می پرسن ، مثلاً اولین مدرسه یا مثلاً وقتی pass یادتون می ره عکس نشون می ده که اسم این دوست چیه؟ این روشها خوب است چون قابل دسترس (Available) است ، اما از جهت امنیتی یه ذره مشکل داره چون ممکنه اون چیزی که تو می دونی دیگران هم بدونن ، یا بفهمن ، پس ممکنه مرکنار دسترسی سریع ، مخاطره هم داشته باشه ، ایسک هم داره به سمت پایین ترکه میایم انعطاف پذیری کاهش پیدا می کنه ، ریسک هم کاهش پیدا می کنه ، مثل کارت بانک ، کارت شناسایی ، توکن امنیتی ، دیگه منظور کلمه عبور نیستید . وقتی دارین با کارت کار می کنین یعنی شما چیزی

☐چیزی که شما دارید

▨کارت بانک، کارت شناسایی، توکن امنیتی

☐چیزی که شما هستید

▨اثر انگشت، چهره، صدا، محل کنونی

دستتون دارین و علاوه براون ، مرد دوم هم می زنن ،
فراتر از چیزی هست که شما هستین ، چیزی که شما دارین رو شاید به یکی دیگه بدین
مثل کارت ، اما چیزی که هستید / بین تو بین به کسی و آنالز کنین

اون چیزی که شما هستین خیلی مطمئن تره و این قابلیت باعث می‌شه هزینه بره بالاتر ، مثلاً اگر کارت کسی رو بردارین این می‌شه مزدی کارت وخیلی هزینه داره

چهره، صدا یا مثل کنونی هم راههایی برای احراز هویت است .

مثل کنونی ← مثلاً شما یکجا هستین لو می‌گین با ... این ZP ها می‌تونی وارد شبکه نبشی، خیلی جاها کشورها بخاطر بحثهای تحریم ایران و تحریم کردن مثل سایت اندرویدیا مثلب

البته در بحث مثل کنونی، احراز هویت یک احراز هویت کلی هست ، فردی نیست ، مثلاً همه‌ی کسانی که در شرکت هستن دسترسی به این دارند یا همه کسانی که از فلان شبکه تماس می‌گیرن یا ZP اگه به آن مثل است به آن دسترسی دارن .

پس دسترسی خیلی عمومی تعریف می‌شه ، مگر اینکه اینها رو بیاین با توکن و ... ترکیبشان کنیم .

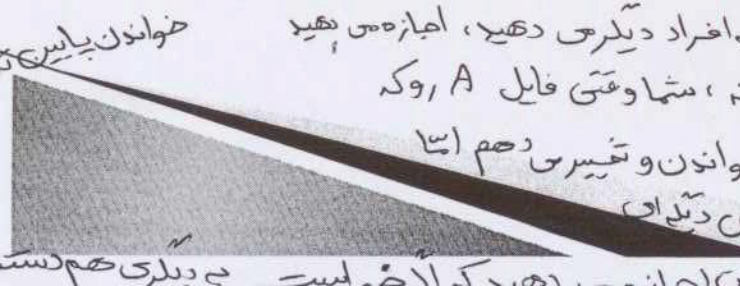
سطح اختیارات

(Authorization) ← حاکد وا دسیستم‌شدین چه دسترسی هایی دارین، به چه منابعی دسترسی داره و تو چه سطحی ؟

- ☑ فرآیند تصمیم گیری در خصوص حق دسترسی به منابع بر اساس سطح دسترسی افراد مجاز
- ☑ Access control ← کنترل دسترسی به منابع
- ☑ دسته بندی منابع و کاربران ← یعنی شما یک موجودیت کاربرد هم یک موجودیت کاربرد این، این که چه کاربر به چه منبعی و چه سطحی دسترسی داشته باشه، مفاهیمی مثل Access list (ACL) مطرح می‌شه، لیستی از دسترسی افراد به منابع
- ☑ انواع دسترسی شامل: خواندن، نوشتن (ایجاد، بهنگام سازی، حذف)
  - ☐ CRUD ← تفسیر دادن داده شامل ایجاد «create»، بهنگام سازی «update» و حذف «Delete» بازیابی است — شاید بعضی از دسترسی ها به فرد دیگری ندهید
  - ☐ Full Control ← به کسی که امکان ایجاد، update و delete می دهید، یعنی می‌گن دسترسی کامل crud
  - ☐ Execute

CRUD => create read ...

مجموع تمام خواندن پایین‌ترین سطح دسترسی است.



crud با full control یک تفاوت دارد و وقتی full control به افراد دیگری دهید، اجازه می‌دهید که اون هم full control به افراد دیگر بدهد و براشون تعریف کنه، شما وقتی فایل A رو که تولید کننده‌ش هستین می‌گین من به شخص X اجازه خواندن و تغییر هم اینا رو بکس دیگه‌ای 7 اون شخص دیگه نمی‌تونه اون اختیارات یا Permision ها رو به کس دیگه‌ای و اگذار کنه، اما وقتی full control می‌دهید یعنی به اون شخص این اجازه رو هم می‌دهید که به دیگری هم دسترسی بدهد و به محیط

مختلف متفاوت است. مثلا در بعضی FTP ها اومدن execute کردن رو از خواندن جدا کردند، یا مثلا در FTP لیست کردن فایل هم اجازه می خواهد، ممکنه شخصی در FTP فایلی اضافه کند، اما خود شخص اجازه ی مشاهده و لیست کردن اون فایل رو نداشته باشه.

مثل صندوق پستی که شما نامه می نویسید و در صندوق پستی می اندازید، اما بعد ارسال دیگه نمی توانین داخل صندوق پستی رو ببینین، و نمی توانین تغییر بدین یا بخونینش