

## ۱) مکانیزم های تأمین امنیت

به منظور تأمین امنیت در سامانه (متاسب با ویژگی های امنیتی مورد دیاز) از تراز  
مکانیزم های امنیتی استفاده می شود.

پیشتر دسته بندی برای مکانیزم هار امعنیر بیان (درین در سالم چهار بخش زیربوده)

① مکانیزم های هشدار (هشدارهای امنیتی)

② مکانیزم های پیگیرانه

③ مکانیزم های مسحیفون

④ مکانیزم های ترمیدم و بازتابی.

درین بخش سعیداریم تا با اجزای سیستمی به این مکانیزم ها بپردازیم:

- ایند این مکانیزم ها روی عوامل فرهای از ساعانه اعمال می شود،

- شامل چه وثای راهی امنیت و ایزابارهای اسن.

سامانه: مجموعه ای از موجودیت های متقابل با اسباب درگیری سایری که یک واحد را سهیل نمایند

۲) مکانیزم های امنیتی و مولفه های ساعانه:

مکانیزم هار امنیت را می توان با زیر دانه های متفاوت بر این مولفه های ساعانه در نظر گرفت.

درین رسم اعمومی برنام دفاع در عمق (Defence in Depth) یا دفاع چندی برنام

ملحوظ می شود. این مفهوم را می توان در معیاس های مختلفی تبلیغ کرد.

سطح کلان - دفاع در عمق درست مکانیزم های سبدار (کلاینت - سروری)

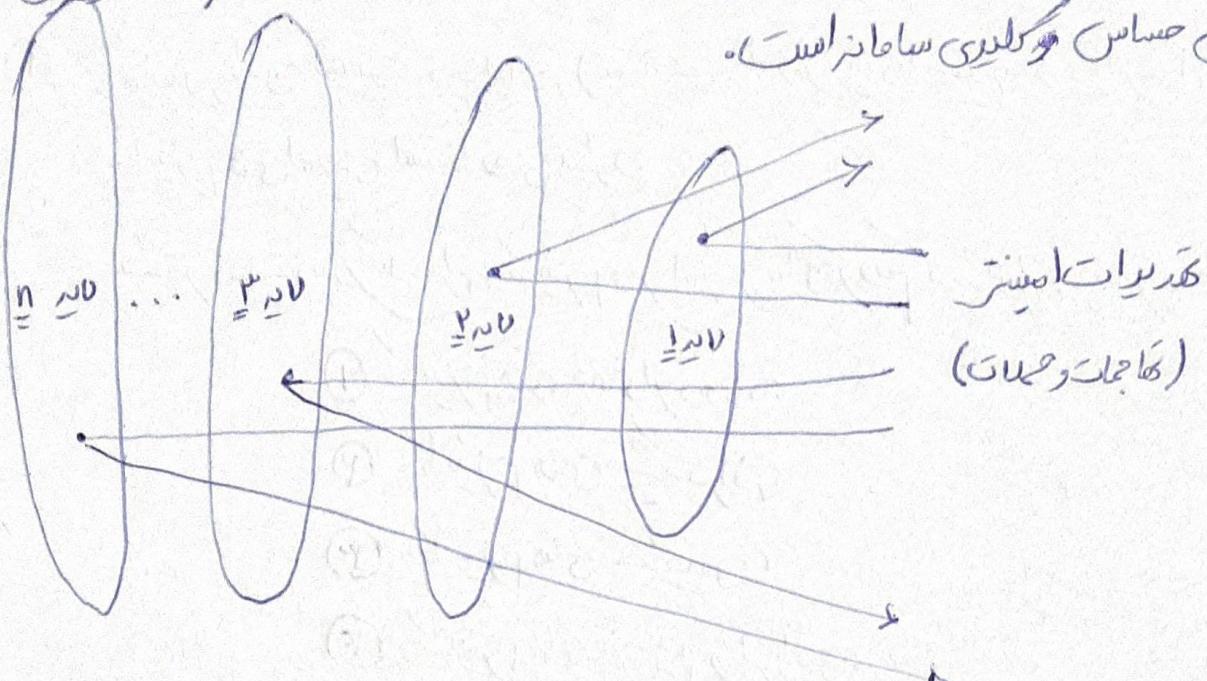
سطح متوسط - دفاع در عمق کلکسیون (کلکسیون موسوی)

سطح خرد - دفاع در عمق در لایک سیستم نرم افزاری (مثل DBMS، OS، ...)

در نظر گرفت.

۳) هدف از دفاع در عمق را فراسنیده هر امنیت دسترسی را مسدود کرد. مسیر دسترسی نفوذگران

به نواحی حساس گوگلبری ساخته است.



لایه‌های اینترانی → برای پیشگیری اسفاره می‌مورد.

لایه‌های میانی → برای سنهنی اسفاره می‌مورد.

لایه‌های خارجی → برای ترمیم و بازبازی سور را اسفاره می‌کند.

## ۴) دفاع در عمق درین سه سطح

در همین سنتیه می‌باشد براز هدف از مولفه‌های سُنگی (همزه آن را عبارت نهاده):  
۱) مولفه سُنگی را زیارت، مولفه کارگزار (سرور) و مولفه کار طوه (کافیتا) تمهیدات امنیتی  
در تظریق قدر می‌سوند.

به عنوان مثال، براز امنیتی سازی سُنگی را زیارت می‌نمایند تمهیدات زیر را کافد  
کرد:

۱- اسفاره از سُنگی صبیغه برسویج به جای هاب به سبب افزایش محدودیت  
سُنگی‌های اعماق، تعریف نواحی مختلف با مطلع امنیتی مختلف (کامپیوچر  
VLAN) و امکان اعمال سیاست‌های دسترسی (مثل Port security) را تراویح  
می‌کند.

۲- استفاده از ابزارهای معتبر سیکری

۳- توجه بر امنیت و محترمانه ارتباط به سیم

۴- رفع آسیب نیزه‌های سرویس سیکر (Web server, File server, ...)

برای امن سازی کارگزاری تراهندهای امنیت امنیت زیر را کافی نیست:

۱- استفاده از هند برافورد

۲- استفاده از وضله‌های امنیت (Patch) برای تعمیل و رسیدن افزایش امنیت سیم

۳- تغییر در تنظیمات پیش‌فرض،

۴- غیرفعال کردن سرویس‌های غیر ضروری،

۵- قطع دادن تمام پورت‌های TCP/IP به غیر از صوارد لام (برخی از فیلترها می‌توانند پورت ۸۰ برای http و پورت ۴۴۳ برای https را نگذارند، بنابراین پورت‌ها را بیندم).

۶- اجرای سیاست‌های امنیت مختلف در حفظ منابع ارزشی، حسابرسی کاربران و ...

برای امن سازی کارخواه می‌ترانهای امنیت زیر را کافی نیست:

۱- استفاده از هند برافورد،

۲- استفاده از دیواره‌های سیکر (Firewall) سعفی،

۳- استفاده از وضله‌های امنیت بروز برای تعمیل و رسیدن افزایش امنیت سیم

مطلوب تعلیمی - VLAN: سیکر VLAN (virtual LAN) این افعال را برای همین

مشغله‌ها می‌دانند به طور خودکار دسترسی بگیرند و خاص از کاربران را با اینویل کردن بخشن از سیکر محدود نکنند.

۶) مطلب تکمیلی - تعداد هاب و سویچ: هد ندی هاب و سویچ برای انتقال (رسانیدن)

شبکه های دیگر به صورت سلسلی یک بخش واحد از شبکه را بر عهده دارند. با اینحال تعداد  
جهله بین این دو آن است که:

- هاب تمام ترا فیبر و روپی بخود رایه تمام پورت های ارسال می کند. این کار  
سببی سوزار معتبر زدن ترا فیبر بر سبب تکمیل سوزار.

- با اینحال سویچ، ترا فیبر و روپی را کهها به پورت های قابل مراجعت می کند  
در نتیجه اعمال مدیریت تبارات مراهم می سوزار.

~~۷) دفاع در عمق دریافت کامپیوتری~~

۷) دفاع در عمق دریافت کامپیوتری:

برای دستم کامپیوتری نیز با رینگ انفرست بر سنت دستم سبکه ای باست امن سازی

در حامی لایه های نرم افزار دریافت صورت نمی برد:

۱- سکمه (Network)

۲- سیستم عامل (Operating System)

۳- سیستم مدیریت پایگاه راهه (DBMS)

۴- برنامه های کاربری (Application).

۸) دفاع در عمق دریافت کامپیوتری:

در این سطح با رینگ انفرست بر سنت یه در سطح قبل صفات هستیم وی باست مناسب  
پاترمه فزاره های مربوط به مقاوم ساز (Hardening) امنیت آن را انجام دهد.

۹) مکانیزم های امنیتی (پیلگرانه، تصحیف، ترمیم و بازگردان) در مرحله از سطح علاوه بر امنیت محدود  
قابل اعمال هستند

جمع بندی: مانع از به سطح رکابندهای معرفی شده، موارد سعی برآن است که قدریات را حفظ  
در سطح علاج را استفاده از مکانیزم های پیلگرانه مقابله شود لی با اینحال هزاره را سطح خرد  
مکانیزم های ترمیم و بازگردان فراخنده را صنعت را فرید و وزیرساخت نژام را مهیا ننمی  
کند.

۱۰) مکانیزم های امنیتی - پیلگرانی:

برخی از ابزارهای ضروری به مکانیزم پیلگرانی عبارتند از:

(Identification and Authentication) -  
- مناسایی و اثبات امتالات (Access control)

- کنترل (سترسی) (Firewall)

- دیواره آتش (Cryptography)

- رمزگاری (Digital signature)

- امضای دیجیتال

در ادامه هر یک از ابزارهای فوق به مورخ مختصر معرفی می شوند.

۱۱) مناسایی و اثبات امتالات: پیشیگیری از کنترل دسترسی در هر سطح، مناسایی و اثبات  
هویت کاربر است. در این فرآیند کاربری باست ابتدا خود را به سطح معرفی کند و سپس  
امنیت کنترل های مذکوری اسکرین کر ادعایی کند.  
(از طرف مسناه)

بعنوان مثال، برای ورود به حساب کاربری ایمیل خود با وارد کردن نام کاربری  
خود را به سطح معرفی کنیم و از مدرسین کلمه عبور که بین ما و ایمیل سرویس صورت  
تلخ ترافق کرده ایم، ادعای خود را برای ورود ایجاد کرده و وارد حساب کاربری  
خود می شویم.

(۱۲)

اهراز هویت (Authentication) کاربر باید این می تواند براساس داشته های خود از مختلفی قدرت پذیرد که در ادامه برح از آنها خواسته شده اند:

- اهراز هویت براساس داشته های کاربر (What you know)

- اهراز هویت براساس داشته های کاربر (What you have)

- اهراز هویت براساس آنچه هست (What you are)

- اهراز هویت چند فاکتوری Authentication (Multifactor Authentication)

(۱۳)

اهراز هویت براساس داشته های کاربر؛ ساده ترین و معمولی ترین فاکتور اهراز هویت به سه این اکیده واقع ادعای مطابق با آنچه نیز است که در ذهن خود داریم، مثل گذرواژه یا پسورد را دارد.

• Personal Identification Number

مسئل اعلی این اهراز هویت؛ مقابل حرس بورن یا افتخار داشتم فراست. بالفعال با تغییر در راسته، ترکیب با سایر روش های اهراز اعمال و داشتن سیاست های امنیتی برای داشتن رمز عبور پیچیده می تواند مسئل فرق را کمتر نماید.

(۱۴)

اهراز هویت براساس داشته های کاربر؛ در این نوع اهراز هویت، نزد دارنده سگه متنزه کسر تغییر کارت های هوشمند، ترکیب های امنیتی، OTP، ... است و این رسماً مزد را اهراز هویت می نماید. بنابراین در صورت های روش قبل، نزد نیاز نیست داشتم فراز را در این رایه در زمان خوب سپارند.

با اینحال معمول در سال داشتم فراز، مسئل اعلی این اهراز هویت به سه این اکیده.

ب مطور مجهول برای رفع این مسئله، این روش را با ترکیب دو روش اهراز هویت به کار گیری می نماید.

(۱۵)

۱۵ احرازه ویت ابراساس آن چیز است: در این نوع احرازه ویت از مستحقه های بیولوژیکی  
نتیجه: اثرا نشست، عینی حسنه، چهره، قدرت و موارد غایبیه بای احراز افعال  
استفاده می شود. این نوع احراز افعال در مقایسه با دونوی قبل آن است که فرد  
مکن است ~~آنکه~~ اثرا نشست خود را برتر سینه فراسوس با گفتم لذات  
خواص بیولوژیکیه همراه هر راه اوست.

پایین حالت مصالح افعال استفاده از جنین احرازه ویت، همینه بالا و متصدیه رسمیه بود  
بای آن است.

۱۶) از عمده زر است مر همراه می باشد از افعالات مر بوده احرازه ویت (گذر و ایله، ترک، حضنیه های  
بیولوژیکی) که در غالب راه در شبکه جریان دارد و با بر روی ستم در راه است که نهاده مسخر است  
(احرازه ویت لفظه)