دانشکده علوم ریاضی و آمار

مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۸

نگارنده: فاطمه سلاجقه

۱ اردیبهشت ۱۴۰۱

فهرست مطالب

۱ مکانیزم‌های تامین امنیت

به منظور تأمین امنیت در سامانه (متناسب با ویژگی‌های امنیتی مورد نیاز) از توالی از مکانیزم‌های امنیتی استفاده می‌شود. پیشتر دسته‌بندی کلی برای مکانیزم‌های امنیتی بیان کردیم که شامل چهار بخش زیر بود:

۱. مکانیزم‌های هشداردهنده،

۲. مکانیزم‌های پیشگیرانه،

۳. مکانیزم‌های تشخیص،

۴. مکانیزم‌های ترمیم و بازیابی.

در این بخش سعی داریم تا با جزئیات بیشتری به این مکانیزم‌ها بپردازیم:

- اینکه این مکانیزم‌ها روی چه مؤلفه‌هایی از سامانه اعمال می‌شود،
- و شامل چه ویژگی‌های امنیتی و ابزارهایی است.

سامانه: مجموعه‌ای از موجودیت‌های متعامل یا وابسته در محیط سایبری که یک واحد را تشکیل می‌دهند.

۲ مکانیزم‌های امنیتی و مؤلفه‌های سامانه

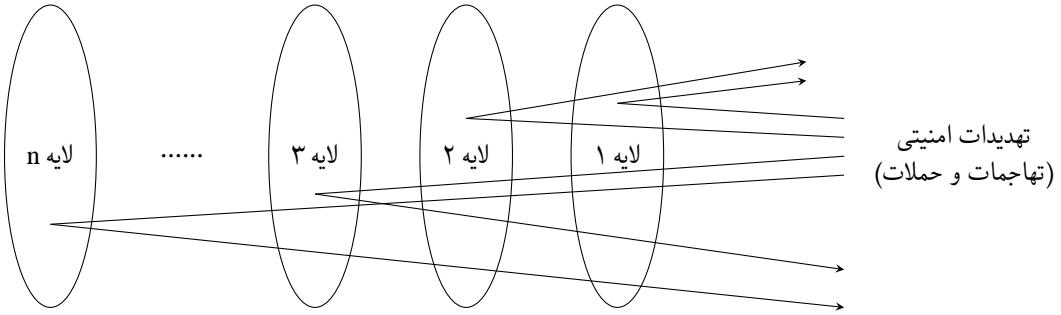
مکانیزم‌های امنیتی را می‌توان با ریزدانگی‌های متفاوت برای مؤلفه‌های سامانه در نظر گرفت. در این راستا مفهومی به نام دفاع در عمق (Defense in Depth) یا دفاع لایه به لایه مطرح می‌شود. این مفهوم را می‌توان در مقیاس‌های مختلفی نظیر موارد زیر در نظر گرفت:

سطح کلان - دفاع در عمق در یک سیستم شبکه‌ای(کلاینت-سروری)،

سطح متوسط - دفاع در عمق در یک سیستم کامپیوتری،

سطح خرد -دفاع در عمق در یک سیستم نرم‌افزاری(مثل DBMS ، OS ، و...)

هدف از دفاع در عمق و افزایش لایه های امنیتی، دشوار کردن مسیر دسترسی نفوذگران به نواحی حساس و کلیدی سامانه است.



لایه‌های ابتدایی : برای پیشگیری استفاده می‌شود.

لایه‌های میانی : برای تشخیص استفاده می‌شود.

لایه‌های انتهایی : برای ترمیم و بازیابی مورد استفاده قرار می‌گیرند.

۱.۲ دفاع در عمق در یک سیستم شبکه‌ای

در چنین سیستمی می‌بایست برای هر بک از مؤلفه‌های تشکیل‌دهنده آن که عبارتند از:

- مؤلفه شبکه و ارتباطات،
- مؤلفه کارگزار(سرور)،
- مؤلفه کارخواه (کلاینت)،

تمهیدات امنیتی در نظر گرفته شود. به عنوان مثال، برای امن‌سازی شبکه و ارتباطات می‌توان تمهیدات زیر را لحاظ کرد:

۱- استفاده از شبکه مبتنی بر سوئیچ به جای هاب که سبب افزایش مصونیت شنود بسته‌ها، امکان تعریف نواحی محتلف با سطوح امنیتی مختلف(مکانیزم VLAN) و امکان اعمال سیاست‌های دسترسی(مثل Post Security) را فراهم میکند،

۲- استفاده از ابزارهای مدیریت شبکه،

۳- توجه به امنیت و محرمانگی ارتباط بی‌سیم،

۴- رفع آسیب‌پذیری‌های سرویس شبکه(File Server، Web Serverو...)

برای امن‌سازی کارگزار می‌توان تمهیدات امنیتی زیر را لحاظ کرد:

۱- استفاده از مند بدافزار،

۲- استفاده از وصله‌های امنیتی(Patch) برای سیستم‌عامل و دیگر نرم‌افزارهای نصب شده بر روی سرور،

۳- تغییر در تنظیمات پیش‌فرض،

۴- غیر فعال کردن سرویس‌های غیر ضروری،

۵- مسدود کردن تمام پورت‌های TCP/IP غیر از موارد لازم(به عنوان مثال برای یک وب‌سایتی که داریم مثلاً پورت ۸۰ برای http و پورت ۴۴۳ را برای https باز نگه داشته و بقیه پورت‌ها را می‌بندیم)،

۶- اجرای سیاست‌های امنیتی مختلف در خصوص گذرواژه، حسابرسی کاربران و...

برای امن‌سازی کارخواه می‌توان تمهیدات امنیتی زیر را لحاظ کرد:

۱- استفاده از مند بدافزار،

۲- استفاده از دیوار آتش(Firewall) شخصی،

۳- استفاده از وصله‌های امنیتی به‌روز برای سیستم‌عامل و دیگر نرم‌افزارهای نصب شده بر روی سیستم کلاینت.

مطلب تکمیلی - VLAN: شبکه‌ی VLAN(virtual LAN) این امکان را برای مدیران شبکه فراهم می‌کند که می‌توانند به طور خودکار دسترسی یک گروه خاص از کاربران را با ایزوله کردن بخشی از شبکه محدود کنند.
مطلب تکمیلی - تفاوت هاب و سوئیچ: هردوی هاب و سوئیچ برای اتصال دستگاه‌های شبکه به یکدیگر به منظور تشکیل یک بخش واحد از شبکه را به عهده دارند. با این حال تفاوت عمده بین این دو است که:

- هاب تمام ترافیک ورودی بر خود را به تمام پورت‌هایش ارسال می‌کند. این کار سبب می‌شود که مقدار زیادی ترافیک به شبکه تحمیل شود.
- با اینحال سوئیچ، ترافیک ورودی را تنها به پورت‌های مرتبط هدایت میکند و در نتیجه امکان مدیریت تبادلات فراهم می‌شود.

۲.۲ دفاع در عمق در یک سیستم کامپیوتری

برای یک سیستم کامپیوتری نیز با ریزدانگی بیشتری نسبت به سیستم شبکه‌ای می‌بایست امن‌سازی در تمام لایه‌های نرم‌افزاری یک سیستم صورت پذیرد.

۱- شبکه(Network)،

۲- سیستم‌عامل(Operating System)،

۳- سیستم مدیریت پایگاه داده(DBMS)،

۴- برنامه‌های کاربردی(Application).

۳.۲ دفاع در عمق در یک سیستم نرم‌افزاری

در این سطح با ریزدانگر بیشتری نسبت به دو سطح قبل مواجه هستیم و می‌بایست متناسب با نرم‌افزار تمهیدات مربوط به مقاوم سازی(Hardening) امین‌تر آن را انجام دهیم. مکانیزم‌های امنیتی (پیشگیرانه، تشخیص، ترمیم و بازیابی) در هریک از سطوح کلان تا خرد به صورت لایه‌ای قابل اعمال هستند.
جمع‌بندی: با توجه به سطوح و مکانیزم‌های معرفی شده، همواره سعی بر آن است تا با تهدیدات و حملات در سطح کلان و با استفاده از مکانیزم‌های پیشگیرانه مقابله شود ولی با اینحال همواره می‌بایست تا سطح خرد و مکانیزم‌های ترمیم و بازیابی فرآیندهای امنیتی را مدیریت و زیرساخت لازم را مهیا کنیم.

۳ مکانیزم‌های امنیتی-پیشگیری

برخی از ابزارهای مروبوط به مکانیزم پیشگیری عبارتند از:

- شناسایی و احراز اصالت(Identification and Authentication)،
- کنترل دسترسی(Access Control)،
- دیوار آتش(Firewall)،
- رمزنگاری(Cryptography)،
- امضای دیجیتال(Digital Signature).

در ادامه هریک از ابزارهای فوق به طور مختصر معرفی می‌شوند.

۱.۳ شناسایی و احراز اصالت

پیشنیاز کنترل دسترسی در هر سیستم، شناسایی و احراز هویت کاربر است. در این فرآیند کاربر می‌بایست ابتدا خود را به سیستم معرفی کرده (از طریق شناسه) و سپس اثبات کند که همان فردی است که ادعا می‌کند.
به عنوان مثال، برای ورود به حساب کاربری ایمیل خود با وارد کردن نام کاربری خود را به سیستم معرفی می‌کنیم و از طریق کلمه‌ی عبور که بین ما و ایمیل سرور مورد نظر توافق کرده‌ایم، ادعای خود را برای ورود اثبات کرده و وارد حساب کاربری خود می‌شویم.
احراز هویت(Authentication): احراز هویت(Authentication) کاربر به یک سیستم می‌تواند بر اساس پارامترهای مختلفی صورت گیرد که در ادامه برخی از آن‌ها فهرست شده‌اند:

- احراز هویت بر اساس دانسته‌های کاربر(What you know)،
- احراز هویت بر اساس داشته‌های کاربر(What you have)،
- احراز هویت بر اساس آنچه هست(What you are)،
- احراز هویت چند فاکتوری(Multifactor Authentication).

احراز هویت بر اساس دانسته‌های کاربر: ساده‌ترین و ضعیف‌ترین فاکتور احراز هویت به شمار می‌آید و در واقع ادعای ما برای ورود به سیستم آن چیزی است که در ذهن خود داریم مثل گذرواژه یا شماره شناسایی شخصی(Personal Identification Number).
مشکل اصلی چنین احراز هویتی، قایل حدس بودن یا افشای دانسته فردی است. با اینحال با تغییر دوره‌ای دانسته، ترکیب با سایر روش های احراز اصالت و داشتن سیاست‌های امین‌تر برای داشتن رمز عبور پیچیده می‌تواند مشکل فوق را کم‌رنگ‌تر نماید. **احراز هویت بر اساس داشته‌های کاربر**: در این نوع احراز هویت، فرد دارای یک دستگاه فیزیکی نظیر کارهای هوشمند، توکن‌های امنیتی، OTP و ...است و این دستگاه فرد را احراز هویت می‌کند بنابراین در مقایسه روش قبل، فرد نیاز نیست دانسته‌ای را در این رابطه در ذهن خود بسپارد.
با این حال مفقود شدن داشته‌ی فرد، مشکل اصلی چنین احراز هویتی به شمار می‌آید. به طور معمول برای رفع چنین مشکلی، این روش را با ترکیب دیگر روش‌های احراز هویت به کار می‌برند.
احراز هویت بر اساس آنچه هست: در این نوع احراز هویت از مشخصه‌های بیولوژیکی فرد، نظیر: اثر انگشت، عنبیه چشم، چهره، صوت و

موارد مشابه برای احراز اصالت استفاده می‌شود.رهآورد این نوع احراز اصالت در مقایسه با دو نوع قبل آن است که فرد ممکن است دانسته یا داشته‌ی خود را به ترتیب فراموش یا گم کند اما خواص بیولوژیکی او همواره همراه اوست. با این حال مسأله اصلی استفاده از چنین احراز هویتی، هزینه بالا و پیچیدگی مربوط به آن است.
لازم به ذکر است که همواره می‌بایست از اطلاعات مربوط به احراز هویت(گذرواژه، توکن خصیصه‌های بیولوژیکی) که در قالب داده در شبکه جریان دارد و یا بر روی سیستم دریافت‌کننده(احراز هویت کننده) مستقر است اطمینان حاصل کرد.