امنیت تجارت الکترونیک

فصل چهاردهم:
امنیت لایه کاربردی

تهیه و تنظیم: دکتر آرش حبیبی لشکری
منبع: کتاب "اصول امنیت برای تجارت الکترونیکی"

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

- دروازه‌های برنامه‌کاربردی و فیلترهای محتوا
- کنترل دسترسی و صدور مجوز
- امنیت سیستم عامل
- تشخیص نفوذ برپایه – میزبان
  - رکوردهای ممیزی
  - انواع نفوذگرها
  - تشخیص نفوذ آماری
- ارزیابی امنیتی

امنیت لایه کاربردی

دروازه‌های برنامه‌کاربردی و فیلترهای محتوا

دروازه‌های برنامه کاربردی مکانیزم‌هایی هستند که توسط دیوارهای آتش برای کنترل گذردهی ترافیک از میان دژ لایه کاربردی میزبان استفاده می‌شوند.

اغلب به *پروکسی* معروف هستند. یک پروکسی یک برنامه واسطی است که هم نقش یک سرویس دهنده (به سرویس‌گیرنده اصلی) و هم یک سرویس‌گیرنده (به سرویس دهنده‌ی که سرویس‌گیرنده اصلی می‌خواهد به آن متصل شود) را بازی می‌کند.

هم درخواستهای سرویس‌گیرنده را قبول می‌کند و همچنین بعد از آن:

- آنها را (درون خود) پردازش می‌کند و پاسخی به سرویس‌گیرنده ارسال می‌کند، یا
- درخواست را به سرویس‌دهنده دیگری ارسال می‌کند، یا
- درخواست را ترجمه و آن را به سرویس‌دهندهی که در سمت سرویس‌گیرنده است ارسال می‌کند.

البته در دو مورد آخر پروکسی درخواست را دریافت و برای سرویس‌گیرنده ارسال می‌کند.

شرح فیلترهای محتوا

شرح سیستم های بررسی و ردیابی وضعیت

کنترل دسترسی و صدور مجوز

از اینکه یک سرویس‌گیرنده و سرویس‌دهنده، برای نمونه از طریق PPP، SLIP یا TELNET که با موفقیت تایید اعتبار شده‌اند، تماس برقرار می‌کند، سرویس‌دهنده باید تشخیص دهد که آیا سرویس‌گیرنده مورد نظر برای آن ارتباط مجاز است یا خیر؟

بسیاری از محصولات دیوارآتش مانند RADIUS [1] و TACACS [2] را برای انجام اعتبار سنجی و صدور مجوز پیاده سازی می‌کنند.

تعریف RADIUS و NAS

شرح نحوه عملکرد این دو

امنیت سیستم عامل

سیستم‌های عامل برای اینکه بطور رسمی مشخص و تایید اعتبار شوند، خیلی پیچیده‌اند. بنابراین غیرممکن است که آنها را بطور کامل ایمن ساخت. با این حال، مکانیزم‌هایی برای بهبود امنیت سیستم‌های عامل وجود دارد.

در محیطهای نظامی مدل‌های کنترل دسترسی محدود کننده بیشتری از قبیل مدل Bell-La Padula که در بخش اول به آن اشاره شده، استفاده شده است. این مدل یک سیاست امنیتی چند لایه را تعریف می‌کند.

به هر کاربر یک برچسب امنیتی به نام *صلاحیت* که معرف سطح امنیتی کاربر است، اختصاص داده شده است.

به هر منبع یک برچسب امنیتی به نام *طبقه بندی یا حساسیت* که معرف سطح امنیتی منبع است، اختصاص داده میشود.

شرح عملکرد سیستم عاملهای امن و نحوه استفاده الگوریتم های رمزنگاری در آنها

تشخیص نفوذ برپایه - میزبان

رکورهای ممیزی

یک رکورد ممیزی، یک ورودی از یک قالب (فرمت) خاصی است که وقتی یک کار بحرانی امنیتی توسط شخصی روی منبعی انجام می‌شود، ایجاد می‌شود.

انواع نفوذگرها

- *فریبکار*، یک شخص (طرف، مسئول) غیرمجاز که به کنترل دسترسی سیستم‌های‌عامل نفوذ می‌کند تا اختیارات قانونی برای دسترسی کاربران به استفاده از منابع را بدست بیاورد.
- *متجاوز*، کاربری قانونی که یا به منابع غیر مجاز (از روشی غیر مجاز به آن منابع) دسترسی می‌یابد، یا از اجازه‌ای که برای دسترسی به منابع دارد، سوء استفاده می‌کند.
- *کاربر مخفی*، شخصی که کنترل نظارت سیستم عامل را بدست می‌گیرد و از آن برای اجتناب از ممیزی استفاده می‌کند.

زمان	مصرف منابع	شرایط استثنا	شی	فعالیت	اجرا کننده
945869598	RECORDS=0	read violation	secret.txt	read	Smith

تشخیص نفوذ برپایه - میزبان

تشخیص نفوذ آماری

- روش‌های شناسایی از طریق بررسی نابرابری: انحرافات موجود را با استفاده الگوهای استفاده (پروفایل کاربران، انحرافات حد واسط و استاندارد) قبلی شناسایی می‌کند.
- روش‌های شناسایی آستانه: از مقادیر آستانه برای دفعات وقوع بعضی مقادیر (برای مثال، تعداد تلاشهای ناموفق ورود به سیستم) استفاده می‌کند.
- شناسایی تناظر: وقایع ظاهرا نامربوط را مقایسه می‌کند و دنبال ارتباطات مشکوک می‌گردد. (برای مثال: زمان CPU و واحدها ورودی/ خروجی استفاده شده توسط یک برنامه، دفعات ورود به سیستم و طول مدت جلسات ورود به سیستم.

شرح مدل شناسایی مدل آماری

ارزیابی امنیتی

- ارزیابی امنیت و آزمون امنیت حائز اهمیت بوده، اگرچه، برای همه برنامه‌های کاربردی امن. اساسا، دو نوع آزمون وجود دارد:
- آزمون جعبه سیاه، که در آن خروجی یک برنامه با ورودی آن مقایسه می‌شود.
- آزمون جعبه سفید، که در آن رفتار و ساختار درونی سیستم آزموده می‌شود (برای مثال، آزمونهای متن باز)

آزمون جعبه سفید سخت‌تر و طولانی‌تر از آزمون جعبه سیاه است، اما احتمال بیشتری می‌رود که اشکالات پنهان و کدهای مخرب را پیدا کند.

شرح نحوه عملکرد آزمون جعبه سیاه و سفید

خلاصه: دروازه‌های برنامه‌کاربردی و فیلترهای محتوا، کنترل دسترسی و صدور مجوز، امنیت سیستم عامل، تشخیص نفوذ برپایه – میزبان، رکوردهای ممیزی، انواع نفوذگرها، تشخیص نفوذ آماری، ارزیابی امنیتی

جلسه بعدی: پروتکل HTTP

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.