امنیت تجارت الکترونیک

فصل دهم:
شبکه ارتباطی

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

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

- مدل مرجع OSI
- مدل اینترنت
- تکنولوژی‌های شبکه
- امنیت در لایه‌های مختلف
- ضوابط انتخاب پروتکل
- برنامه‌های مخرب
- کرم اینترنت
- مشکلات امنیتی ارتباطی
- تهدیدهای امنیتی ، گفتگوهای امنیتی
- آسیب‌پذیری‌ها و نقص‌ها

شبکه ارتباطی

شبکه ارتباطی

یک شبکه‌ی ارتباطی، دراصل زیرساختی برای تبادل اطلاعات در قالب الکترونیکی است.

شبکه شامل :

یک زیرساخت فیزیکی است که شامل پیوندهای ارتباطی (سیمها و کابلها)، مسیر یاب‌ها، تکرار کننده‌ها، و دستگاه‌های دیگر،

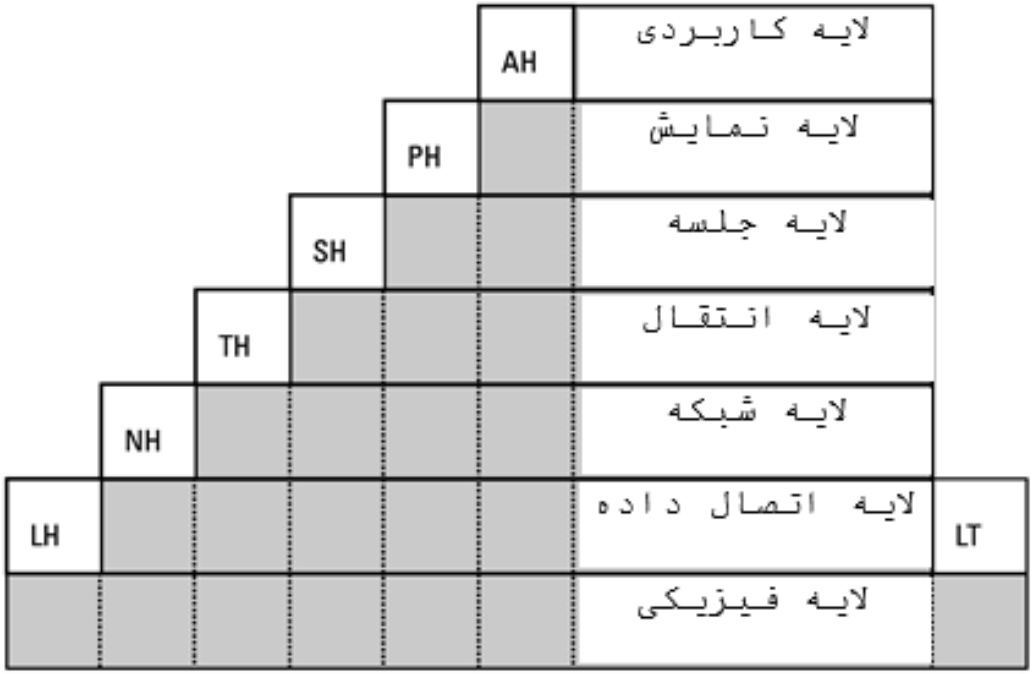
و همچنین یک زیرساخت منطقی است که خود شامل پروتکل‌های ارتباطی است که بستری برای تبادل پالس‌های الکترونیکی یا اطلاعات دودویی در اختیار می‌گذارند.

مدل مرجع OSI:

یکی از پر استفاده ترین مدل‌ها برای توضیح ساختار منطقی شبکه‌های ارتباطی، مدل منبع هفت-لایه‌ای OSIاست.

هر لایه زیر مجموعه‌ای از سرویس‌های ارتباطی را به نحوی فراهم می‌کند که از سرویس‌های لایه‌های پایینتر استفاده نموده و سرویس‌ها را برای لایه‌های بالاتر فراهم نماید.

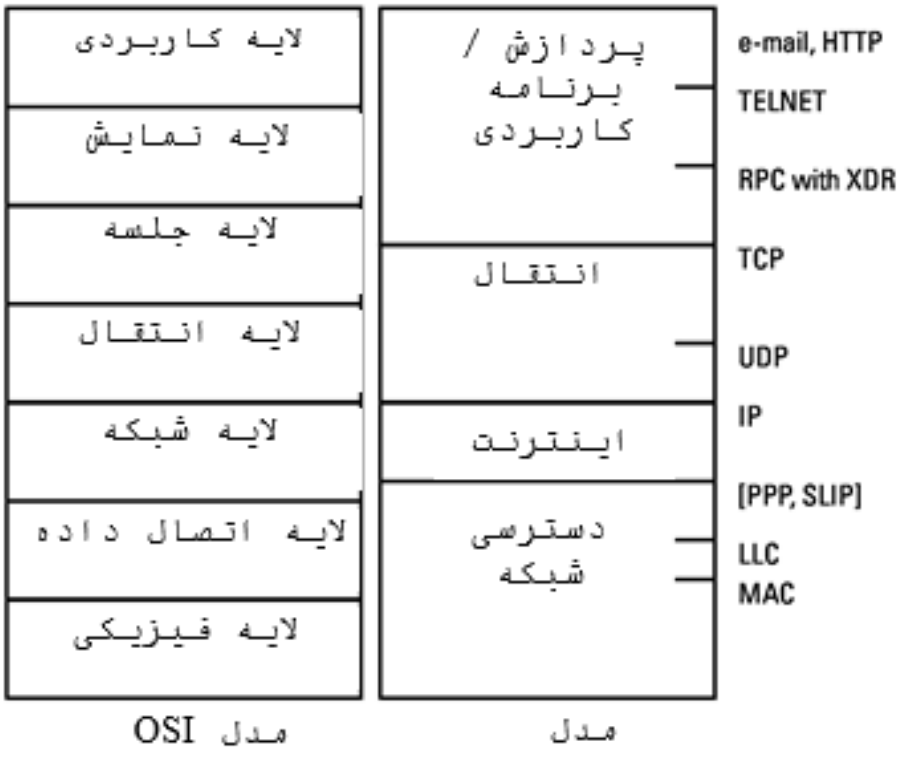
مدل مرجع OSI



شرح و وظیفه هر لایه و نحوه عملکرد آن با لایه های بالاتر و پایین تر.

مدل اینترنت

مدل‌اینترنت نشان داده شده در شکل زیر بر اساس مجموعه پروتکل‌های TCP/IP می‌باشد. یک دنباله پروتکل، یک مجموعه از پروتکل‌های ارتباطی هستند که با یکدیگر همکاری می‌کنند. اسم "اینترنت" به شبکه‌ای اطلاق می‌شود که ارتباطات شبکه‌ای با استفاده از تکنولوژی‌های متفاوت بر اساس دنباله پروتکل‌ها شکل می‌گیرد



- تاریخچه مدل اینترنت
- شرح و وظیفه لایه ها و ارتباط آنها با یکدیگر
- شرح عملکرد پروتکلهای TCP و UDP
- تفاوت اصلی بین دو مدل OSI و اینترنت

تکنولوژی‌های شبکه

یک شبکه ارتباطی شامل تعدادی از گره‌های متصل بوسیله لینکهای ارتباطی است. اگر دو گره از لحاظ جغرافیایی در فواصل دوری از هم قرار داشته باشند، معمولا ارتباط (پیوند) مستقیمی بین آنها نیست.

انواع تکنولوژی ها ، شرح آنها و تفاوت بین آنها:

سوئیچینگ مداری

سوئیچینگ بسته ای

بازپخش فریم

بازپخش سلولی

تکنولوژی شبکه‌های محلی هنوز نمی‌توانند به سرعت بازپخش سلولی دست یابند ولی پشتیبانی بهتری نسبت به بازپخش سلولی ارائه می‌دهند، بخصوص که برای مدت زیادی است که مورد استفاده قرار گرفته‌اند. برای نمونه اترنت Gbit، احتمال بالایی برای مورد قبول واقع شدن وسیع به عنوان تکنولوژی شبکه‌های محلی سریع را دارد.

تکنیکهای تسهیم داده

اگر دو یا چند منبع داده یک رسانه انتقال رایج را به اشتراک بگذارند، کارآمدترین راه برای استفاده از رسانه، تسهیم داده روی آن است.

شرح روشهای تسهیم داده و بررسی کیفیت سرویس:

تسهیم تقسیم زمانی (TDM)

تسهیم تقسیم فرکانسی (FDM)

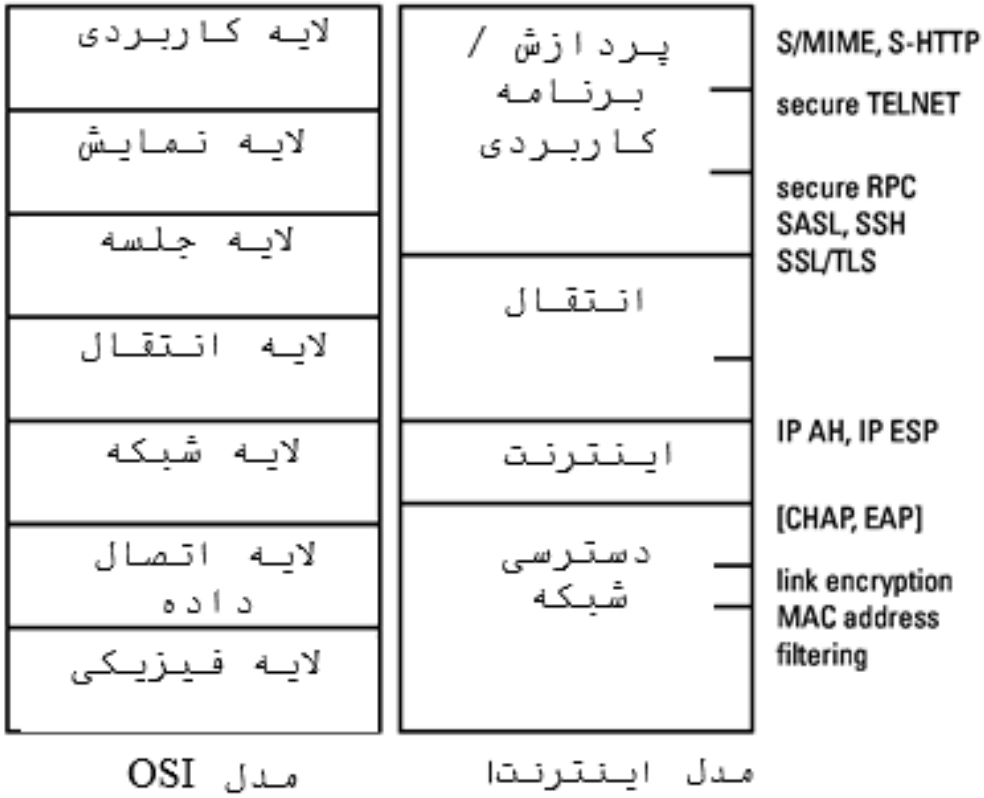
کیفیت سرویس (QoS) معمولا به عنوان مجموعه‌ای از پارامترهایی که کیفیت انتقال مورد نیاز کاربر را تعریف می‌کند بیان می‌شود و می‌تواند برای نمونه، خطای مورد قبول و سطوح گم شده، یا میانگین خواسته شده و حداقل توان عملیاتی باشد.

امنیت در لایه‌های مختلف

شکل روبرو جایگاه برخی از مکانیزم‌های رایج امنیتی استفاده شده دراینترنت را نشان می‌دهد.

با مقایسه این شکل با شکل قبلی، می‌توان دید کدام پروتکل می‌تواند با کدام مکانیزم امنیتی‌ایمن گردد.

برای مثال، S/MIME می‌تواند برای محافظت از یک پیام پست الکترونیکی استفاده شود، و S-HTTP برای محافظت از پیام‌های HTTP بکار رود.



ضوابط انتخاب پروتکل

تصمیم‌گیری در مورد اینکه در کدام لایه امنیت باید پیاده شود، فاکتورهای زیادی را باید در نظر گرفت:

- چه کسی باید احراز هویت شود
- آیا امنیت انتها به انتها یک نیازمندی می‌باشد، یا پیاده‌سازی یک محیط حفاظتی کافی است؟
- هزینه‌های پیاده سازی و نگهداری چقدر باید باشد؟
- آیا توسعه‌های امنیتی قابلیت همکاری بین چندین پلتفرم را ایجاد می‌کند؟
- آیا پروتکل‌های امنیتی بر اساس استانداردهای میان - صنعتی بوده و توسط چندین تولید کننده پشتیبانی می‌شوند؟

برنامه‌های مخرب

برنامه‌های مخرب از آسیب پذیریهای تجهیزات محاسباتی و ارتباطی بهره برداری می‌کنند. برنامه‌های مخرب متفاوتی وجود دارند :

- *باکتری* قابلیت تکرار و استفاده از منابع سیستم را دارد. آنها معمولا باعث محرومیت – از- خدمات می‌شوند.
- یک *بمب منطقی*، برنامه‌ای است که منتظر شرایط خاصی می‌شود تا کارکرد واقعی خود را به نمایش بگذارد.
- درب تله که معمولا توسط کسانی مورد استفاده قرار می‌گیرد که از یک "راه کوتاه" برای دسترسی به منابع سیستم استفاده نمایند. معمولا یک ویژگی پنهان از یک برنامه بوده و نیازمند دانش خاصی برای فعال سازی می‌باشد.
- یک *اسب تروا* ویرایش تغییر داده شده یک نرم‌افزار غیرمخرب و پر استفاده است. ویرایش تغییر داده شده شبیه به همان برنامه تغییر داده نشده است، ولی کارکردی جدید دارد که کاربر از آن آگاه نیست .
- یک *ویروس* برنامه‌ای است که برنامه‌های دیگر مانند سیستم‌های عامل را "آلوده" می‌کند.
- یک کرم یکی از خطرناک‌ترین نوع برنامه‌های مخرب است. که به خودی خود اجرا نمی‌شود ولی کپی‌های خود را در شبکه به سایر ماشین‌ها پخش می‌کند.

تهدیدهای امنیتی

- استراق سمع روی محتوی یک بسته
- دستکاری محتوی یک بسته
- دستکاری به کمک اطلاعات کنترلی
- بازپخش
- تحلیل ترافیک
- محرومیت- از - خدمات
- ماسک گذاری و تغییر
- نفوذ

آسیب‌پذیری‌ها و نقص‌ها

آسیب پذیری‌های بالقوه‌ای که ممکن است در یک سیستم امن رمزنگاری شده یافت شود:

- الگوریتمهای رمزنگاری ضعیف
- آسیب‌پذیری‌های طراحی رمزنگاری
- آسیب‌پذیری‌های پیاده‌سازی نرم‌افزار
- آسیب پذیری‌های پیاده‌سازی سخت افزار
- آسیب‌پذیری مدل اعتماد
- مهندسی اجتماعی و فاکتورهای اجتماعی
- رویه‌های بازیابی- شکست نامناسب

خلاصه: مدل منبع OSI، مدل اینترنت، تکنولوژی‌های شبکه ، امنیت در لایه‌های مختلف ،ضوابط انتخاب پروتکل ، برنامه‌های مخرب ،کرم اینترنت، مشکلات امنیتی ارتباطی ،تهدیدهای امنیتی ،گفتگوهای امنیتی ، آسیب‌پذیری-ها و نقص‌ها

جلسه بعدی: امنیت لایه دسترسی شبکه

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