



<https://www.alirezataji.ir>



Network Security

آشنایی با مبانی امنیت شبکه

مدرس: علی رضا تاجی



آشنایی با مبانی امنیت شبکه



مقدمه‌ای بر امنیت

اکثر افراد قبل از ارسال نامه، آن را در پاکت قرار می‌دهند. اگر بپرسیم چرا این کار را می‌کنید، برخی پاسخ‌های زیر را می‌شنویم:

"واقعاً نمی‌دانم"، "از روی عادت"، "زیرا، بقیه این کار را می‌کنند".

آیا این پاسخ‌ها واقعاً صحیح هستند؟ یا دلایل دیگری وجود دارد. افراد در اصل برای جلوگیری از خواندن نامه‌ها توسط دیگران آن را درون پاکت قرار می‌دهند. حتی، اگر محتوی نامه شامل اطلاعات مهم یا شخصی نباشد، بسیاری از افراد برای این که مطمئن شوند، مکاتبات شخصی آن‌ها خصوصی می‌ماند آن را در پاکت قرار می‌دهند و مهر می‌کنند تا از دید افراد دیگر مخفی بماند و به دست گیرنده برسد. چون، اگر نامه را در یک پاکت باز قرار دهند و آن را ارسال نمایند، در بین راه افراد به راحتی می‌توانند محتوی آن را بخوانند و تغییر دهند، به طوری که راهی برای تشخیص خواندن و تعویض آن وجود ندارد.

امروزه، اکثر افراد از پست الکترونیک^۱ به جای ارسال نامه‌ها از طریق اداره پست استفاده می‌کنند. پست الکترونیک ابزاری سریع برای انتقال نامه است. اما، در آن پاکتی برای محافظت از محتوی نامه (اطلاعاتی که از طریق پست الکترونیک ارسال می‌شود)، وجود ندارد. در واقع، ارسال نامه از طریق پست الکترونیک شبیه به پست نمودن نامه بدون پاکت است. بنابراین، اگر فردی بخواهد پیام شخصی یا اطلاعات محرمانه را از طریق پست الکترونیک ارسال کند، باید راهی جهت محافظت از نامه خود (جلوگیری از خواندن و تغییر توسط افراد دیگر) پیدا کند.

رایج‌ترین راه‌حل، استفاده از پنهان‌سازی است. زیرا، این روش پیام را رمز می‌کند. در این حالت، اگر پیام رمز شده (کد شده) به دست فرد دیگری (به جز گیرنده) برسد، آن فرد با خواندن پیام چیزی از اطلاعات آن نمی‌فهمد. با چگونگی رمزکردن اطلاعات در فصل‌های دوم و سوم آشنا خواهید شد.

۱-۱. اهمیت امنیت اطلاعات

قبل از این که به اهمیت امنیت اطلاعات بپردازیم، مقوله امنیت را در گذشته مورد بحث قرار می‌دهیم. همان‌طور که می‌دانید، امنیت در زمان‌های ماقبل تاریخ نیز جایگاه ویژه‌ای داشته است. در آن

^۱.Email ^۲.Cryptography



زمان انسان‌ها از جان خود در مقابل حیوانات وحشی محافظت می‌کردند. ابتدا، انسان‌ها برای خودشان خانه‌هایی ساختند تا از گزند حیوانات وحشی در امان بمانند. سپس، برای درب‌های خانه قفل‌ها تعبیه کردند یا نگهبان استخدام نمودند تا از اموال خانه (سرمایه) محافظت نمایند. با توجه به میزان اهمیت چیزی که از آن محافظت می‌شود، امنیت می‌تواند لایه‌ها و سطوح مختلف داشته باشد. به عنوان مثال، یک طلا فروشی را در نظر بگیرید. طلا فروش برای برقراری امنیت سه لایه (سطح) امنیتی را ایجاد می‌کند که عبارت‌اند از:

۱. درب مغازه طلا فروشی را می‌بندد.
۲. طلاها را در گاوصندوق ضد سرقت قرار می‌دهد.
۳. طلا فروشی را به سیستم ضد سرقت مجهز می‌نماید.

حال، یک نانوايي را در نظر بگیرید. نانوا، پس از خاتمه کار نانوايي، فقط درب نانوايي را می‌بندد (يعني نيازي به گاوصندوق و سيستم ضد سرقت ندارد). بنابراین، همان‌طور، که بیان گردید، سطوح امنیتی که برای طلا فروشی ایجاد می‌کنیم، خیلی قوی‌تر و پیچیده‌تر از یک نانوايي است. زیرا، ارزش یک کیلوگرم طلا به مراتب بیشتر از چند کیسه آرد می‌باشد. پس، امنیت برای چیزهایی مطرح می‌شود که مهم هستند و ارزش زیادی دارند. یعنی، برقراری امنیت برای سرمایه‌هایی از قبیل پول، طلا، عکس‌ها و فیلم‌های خانوادگی، رازهای زندگی، رمز کارت‌های حساب بانکی و غیره مهم هستند. اکنون این سوال مطرح می‌شود، آیا اطلاعات در فضای کامپیوتر (مجازی) سرمایه هستند یا خیر؟ آیا این اطلاعات نیاز به محافظت دارند یا نه؟

برای این که به این سوال پاسخ دهیم، به مثال‌های زیر می‌پردازیم:

۱. فرض کنید کارمند شهرداری یکی از شهرهای بزرگ هستید. در سیستم رایانه‌ای شهرداری اطلاعاتی از قبیل طرح‌های نوسازی شهر، اتوبان‌هایی که قرار است در شهر ایجاد شوند و مکان آن‌ها، مکان فضاهای سبز، پارک‌ها و غیره ذخیره شده است. آیا این اطلاعات نیاز به محافظت دارند. در نگاه اول ممکن است فکر کنید، این اطلاعات ارزش چندانی ندارند و نیاز به محافظت ندارند. اما، اگر این اطلاعات به دست افراد خاصی برسند، می‌توانند درآمدهای چند میلیاردی از آن کسب کنند. زیرا، این افراد زمین‌های اطراف این مکان‌ها را به قیمت خیلی پایین می‌خرند و پس از مدت کوتاهی این زمین‌ها را با چندین برابر قیمتی که خریداری کردند، می‌فروشند.
۲. فرض کنید در شرکتی کار می‌کنید که در مناقصات میلیاردی شرکت می‌کند و اطلاعات پیشنهادی قیمتش را در کامپیوتر شرکت ذخیره می‌کند. از طرف دیگر، فرض کنید، فقط چند شرکت در این مناقصات شرکت می‌کنند. اگر یک شرکت بتواند اطلاعات پیشنهاد قیمت شرکت‌های دیگر را به دست آورد، به راحتی می‌تواند در مناقصه برنده شود.
۳. شرکتی را در نظر بگیرید که مواد اولیه کارخانجات کشور را خریداری می‌کند. این شرکت مواد اولیه مورد نیاز را در فایل‌های اکسل و Word ذخیره می‌کند و بروی کامپیوتر شرکت نگهداری

آشنایی با مبانی امنیت شبکه



۲





آشنایی با مبانی امنیت شبکه



۳



می‌نماید. آیا این اطلاعات نیاز به محافظت دارند؟ برای پاسخ به این سوال، سوال دیگری مطرح می‌شود. اگر این اطلاعات در اختیار دشمنان کشورمان قرار بگیرند، چه مشکلی را ایجاد می‌کند؟ چون این مواد از کشور خارجی خریداری می‌گردد و چنانچه مشخص باشد، مواد اولیه از کدام کشور خریداری می‌شود، دشمنان با تنگ کردن حلقه‌ی تحریم، موجب جلوگیری از فروش آن مواد به ایران می‌شوند.

۴. فرض کنید، کارتی دارید که از طریق آن از عابر بانکها پول برداشت می‌کنید. آیا کارت و کلمه عبور آن را در اختیار غریبه قرار می‌دهید؟

۵. فرض کنید، از طریق اینترنت خرید و فروش الکترونیکی انجام می‌دهید. اگر بدانید که فضای اینترنت امن نیست و ممکن است سرمایه‌تان سرقت شود، آیا در این فضا خرید و فروش انجام خواهید داد؟

از طرف دیگر، شاید در خبرها شنیده باشید که بی‌توجهی و سهل‌انگاری در برقراری امنیت اطلاعات، خسارت‌های زیادی را به افراد حقیقی و حقوقی وارد کرده است. چند نمونه از این خبرها در زیر آمده‌اند:

۱. یک هکر هزینه‌ای برابر با دوازده هزار دلار را روی دست آژانس فدرال مدیریت آژانس آمریکا گذاشت.
۲. گروهی از هکرها ادعا می‌کنند که توانسته‌اند به صندوق پست الکترونیکی خانم سارا پلین (معاون نامزد جمهوری خواهان در انتخاب ریاست جمهوری ایالات متحده) دست یابند.
۳. حساب بانکی رئیس جمهور فرانسه (نیکولاسارکوزی) هک شد.
۴. یک هکر که به حساب‌های بانک شهروندان تهرانی نفوذ می‌کرد، به دام افتاد.
۵. به فاصله کوتاهی پس از عبور تانک‌های ارتش روسیه از مرزهای گرجستان، وب سایت دولتی گرجستان آماج حمله قرار گرفت.
۶. بنابر تخمین شرکت سماتیک امروزه ۱/۲ درصد از پیام‌های پست‌الکترونیک حاوی بدافزارهای مخرب هستند.
۷. به تازگی هرزنامه جدیدی در فضای اینترنت منتشر شده است که وانمود می‌کند، از سوی جان پیستول، معاون مدیر FBI صادر شده است.
۸. یک کامپیوتر دست دوم که اطلاعات کارت اعتباری تعدادی از مشتریان بانک انگلیسی بر روی آن ذخیره شده بود، در جریان یک بی‌احتیاطی فروخته شد.
۹. تعداد کل بدافزارهای تولید شده در سال ۲۰۰۷ برابر کل بدافزارهای تولید شده در ۱۵ سال قبل آن بوده است.
۱۰. بنابر اعلام شرکت سماتیک ۷۸ درصد از حجم کل ایمیل‌های جهان از اسپم تشکیل شده است.
۱۱. آیا موساد پشت نرم‌افزارهای اسرائیلی پنهان شده است؟



پیدا کردن برخی اطلاعات شخصی و پاسخ به سوالات امنیتی می‌تواند از طریق جستجو در اینترنت به راحتی صورت گیرد. یکی از هکرها به همین صورت موفق گردید، به پست الکترونیکی خانم سارا پلین دسترسی پیدا کند.

علاوه بر این خبرها، هر روز هزاران خبر دیگر را در زمینه سرقت اطلاعات در اینترنت می‌بینید. از طرف دیگر، امروزه با توسعه رایانه‌ها و گسترش شبکه‌های کامپیوتری مانند اینترنت، امنیت شبکه‌های کامپیوتری و اطلاعات به امری بسیار مهم و حیاتی تبدیل گردیده است.

۲- ۱. مقایسه امنیت اطلاعات در گذشته و حال

امنیت اطلاعات یکی از دغدغه‌های بسیار مهم بشر بوده است. به طوری که در گذشته اطلاعات مهم را در قفسه‌های قفل‌دار نگهداری می‌کردند. این قفسه‌ها را در مکان‌های امن قرار می‌دادند و از نگهبان جهت محافظت از این مکان استفاده می‌کردند. در حالی که امروزه، این اطلاعات در کامپیوترها نگهداری می‌شوند. برای برقراری ارتباط از شبکه‌های کامپیوتری استفاده می‌شود و از روش‌های متعددی از قبیل رمزگذاری، امضای دیجیتال و غیره برای برقراری امنیت اطلاعات استفاده می‌شود. با این روش‌های برقراری امنیت در ادامه بیشتر آشنا خواهیم شد.

به زبان ساده می‌توان گفت در گذشته امنیت با حضور فیزیکی و نظارت تامین می‌گردید. ولی، امروزه از ابزارهای خودکار و مکانیزم‌های هوشمند برای برقراری امنیت و حفاظت از داده استفاده می‌کنند.

۳- ۱. مهاجمان و انگیزه‌ها

سازمان‌ها به منظور جلوگیری از حملات به سیستم‌های اطلاعاتی، باید مهاجمان و انگیزه‌های آن‌ها را بشناسند. به عنوان مثال، فرض کنید بیمار شده‌اید و به پزشک مراجعه کرده‌اید، اگر پزشک بخواهد دارویی تجویز کند، ابتدا باید معاینه‌تان نماید و وضعیت بیماری‌تان را بشناسد و سپس باید برای بهبودیتان دارو تجویز نماید. سازمان‌ها نیز برای مقابله با حملات ابتدا باید دشمنان و انگیزه‌های آن‌ها را بشناسند.

مهاجمان، شامل سارقین اطلاعاتی، مجرمان، دزدان کامپیوتری، شرکت‌های رقیب، سیاست‌مداران، نرم‌افزارهای مخرب (ویروس‌ها)، و غیره می‌باشند. این مهاجمان ممکن است انگیزه‌هایی از قبیل جمع آوری هوشمندان، دستبرد فکری، انکار سرویس (عدم پذیرش سرویس)، کشف کردن، سرگرمی، احساس غرور، مورد توجه واقع شدن، تخریب اطلاعات و غیره را داشته باشند.

آشنایی با مبانی امنیت شبکه





آشنایی با مبانی امنیت شبکه



۵



۴ - ۱. مفاهیم اولیه امنیت اطلاعات

قبل از این که به امنیت اطلاعات و روش‌های برقراری آن بپردازیم، با چند مفهوم در امنیت آشنا می‌شویم. برخی از این مفاهیم در زیر آمده‌اند:

☒ **امنیت**^۱، به حراست و حفاظت از منابع اطلاعات امنیت گویند. امنیت می‌تواند توسط هر شخصی یا برنامه‌ای نقض شود. اگر نتیجه فاجعه آمیزی روی کاربران یا محیط پیش نیاید، می‌گویند سیستم امن خواهد بود.

☒ **تهدید**^۲، پدیده یا رویدادی که بتواند امنیت سیستم را به خطر بی‌اندازد. برخی از این پدیده‌ها و رویدادها سیل، زلزله، آتش‌سوزی، طوفان، تصادف و غیره می‌باشند.

☒ **حمله**^۳، تلاش آگاهانه و حساب شده‌ای است تا بتوان نقاط ضعف سرویس‌های امنیتی را شناخته و از نقص سیستم‌های امنیتی استفاده کرده، سیستم را مورد حمله قرار داد تا به آن آسیب برساند یا از داده‌های آن استفاده کرد. حمله‌ها دو نوع هستند که در ادامه آن‌ها را می‌بینید.

☒ **آسیب پذیری**^۴، ضعف‌های موجود در نرم‌افزار، سیستم یا دیگر مکانیزم‌هایی که یک رخنه‌گر برای دسترسی به سیستم یا شبکه می‌تواند از آن بهره بگیرد.

☒ **ریسک**^۵، احتمال این که ضعف‌ها یا آسیب‌پذیری سیستم شناخته شده و از آن‌ها استفاده گردد.

☒ **افشا**^۶، هزینه اتلاف (خسارت) تخمینی حاصل از سوء استفاده یک تهدید از یک آسیب‌پذیری را گویند. افشا وقتی بوجود می‌آید که سیستم رایانه‌ای:

۱. اجازه می‌دهد مهاجم فعالیت‌های جمع‌آوری اطلاعات را انجام دهد.
۲. اجازه می‌دهد مهاجم فعالیت‌هایی را مخفی نماید.
۳. دارای قابلیت است که رفتار مورد انتظار را انجام می‌دهد. ولی، به آسانی در خطر کشف قرار می‌گیرد.

۴. اولین نقطه ورودی است که یک مهاجم ممکن است برای دسترسی به سیستم یا داده استفاده کند.

☒ **شبکه‌های بات**^۷، تعداد زیادی (مثلاً صدها هزار) رایانه اینترنتی سرقت شده که از آن‌ها برای هدایت ترافیک شامل هرزنامه و ویروس به دیگر رایانه‌های اینترنتی استفاده می‌شوند.

☒ **حمله کننده**^۸ **هکر**^۹، فردی است که همواره در صدد استفاده از نقاط ضعف و آسیب‌پذیری موجود در سیستم می‌باشد. این افراد هدف غیرمخرب ندارند و حاصل عملیات آن‌ها می‌تواند اثرات جانی منفی را به دنبال داشته باشد.

☒ **نفوذگران**، افرادی هستند که بدون مجوز از منابع سیستم استفاده می‌کنند.

¹.Security
⁶.Exposure

².Threat
⁷.BotNet

³. Attack
⁸.Attacker

⁴. Vulnerability
⁹.Hacker

⁵ Risk

❑ **بدافزار^۱ یا کد مخرب**، شامل ویروس‌ها، کرم‌ها و برنامه‌های تروجان بوده که هر یک از آنان دارای ویژگی‌های منحصر به فردی هستند.

❑ **ویروس‌ها**، نوع خاصی از کد مخرب هستند که برای آلوده کردن سیستم، عملیات خاصی را انجام می‌دهند. این نوع برنامه‌ها، برای نیل به اهداف تخریبی خود نیاز به یاری کاربران دارند. نمونه‌هایی از همکاری کاربران عبارت‌اند از:

۱. اجرای یک برنامه آلوده در سیستم.
۲. بازکردن یک فایل پیوست آلوده با پست الکترونیک.
۳. مشاهده یک وب سایت آلوده خاص و غیره.

❑ **کرم**، کد مخربی است که بدون نیاز به دخالت کاربر، توزیع و گسترش می‌یابد. کرم‌ها، عموماً با سوء استفاده از نقطه آسیب‌پذیری در سیستم یا نرم‌افزار فعالیت خود را شروع کرده و سعی می‌کنند کامپیوتر را نیز آلوده نمایند. پس از آلوده کردن یک کامپیوتر، تلاش می‌کنند سایر کامپیوترها را آلوده نمایند. مانند ویروس‌ها، کرم‌ها نیز می‌توانند از طریق پست الکترونیک، وب‌سایت‌ها و نرم‌افزارهای مبتنی بر شبکه توزیع و گسترش یابند. یکی از تفاوت‌های بسیار مهم کرم‌ها و ویروس‌ها، توزیع اتوماتیک کرم‌ها می‌باشد.

❑ **برنامه‌های تروجان^۲**، نرم‌افزارهایی هستند که ادعای ارائه خدمات را دارند. ولی در عمل، اهداف خاص خود (تخریب) را دنبال می‌کنند. به عنوان مثال، برنامه‌ای که ادعای افزایش سرعت کامپیوترتان را دارد، ممکن است در عمل اطلاعات مهم کامپیوترتان را برای یک مهاجم و سارق راه دور ارسال نماید.

۵-۱. حمله

حمله تلاش عمدی برای رخنه در یک سیستم و سوء استفاده از آن می‌باشد. به عبارت دیگر، حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل استفاده از شبکه به گونه‌ای توسط فرد غیر مجاز مورد تغییر یا استفاده قرار گیرد. دو نوع حمله وجود دارد که عبارت‌اند از:

۱-۵-۱. حمله غیر فعال

حملات غیر فعال^۳، ذاتاً انتقال‌های پیام را بازبینی و استراق سمع می‌کنند. در این نوع حمله، هدف حمله‌کننده بدست آوردن اطلاعات در حال انتقال می‌باشد. دو نوع حمله غیر فعال وجود دارد که عبارت‌اند از:

❑ **افشاء پیام^۴**، در هنگام انتقال پیام بین فرستنده و گیرنده، فرد یا افراد غیر مجاز دیگری بتوانند پیام را بخوانند (شکل ۱-۱). مکالمه تلفنی، سیستم پست الکترونیک و فایل در حال انتقال ممکن است شامل اطلاعات حساس محرمانه باشند. هدف جلوگیری از مطلع شدن معارضین (افراد غیر

^۱.MalWare

^۲.Trojan

^۳. Passive Attack

^۴. Release of Message

آشنایی با مبانی امنیت شبکه





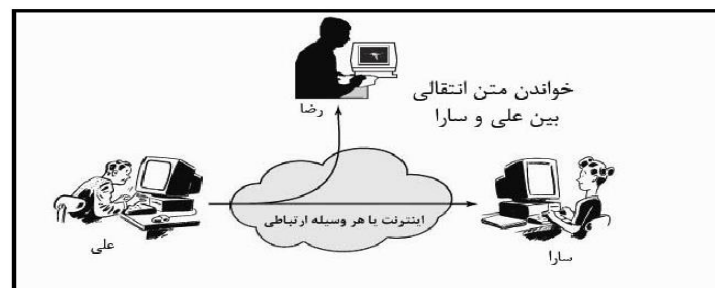
آشنایی با مبانی امنیت شبکه



۷

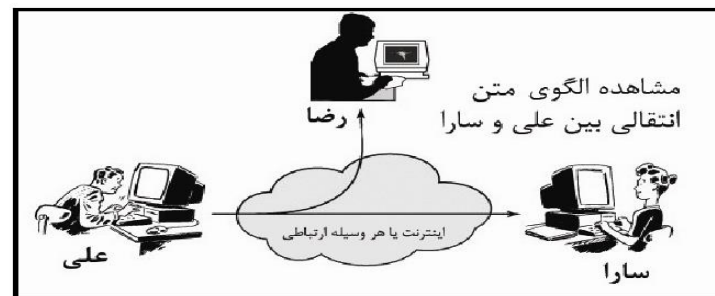


مجاز) از محتوی پیام است. افشاء پیام، به سادگی قابل جلوگیری است. رایج‌ترین راه جلوگیری از این حمله رمزگذاری است. در ادامه رمزگذاری را می‌آموزیم.



شکل ۱-۱ حمله افشاء پیام.

✘ تحلیل ترافیک، فرض کنید داده‌های در حال انتقال رمز شده‌اند. بنابراین، افراد غیر مجاز حتی اگر داده‌ها را بگیرند، نمی‌توانند پیام اصلی را از آن‌ها استخراج کنند. ولی، حمله‌کنندگان می‌توانند اطلاعاتی از قبیل مبداء، مقصد و اندازه پیام را ببینند. این اطلاعات ممکن است برای آن‌ها مفید باشد. این نوع حملات را تحلیل ترافیک گویند (شکل ۱-۲). برای این که با مفهوم تحلیل ترافیک بیشتر آشنا شوید، به این مثال توجه کنید. در جبهه جنگ، فرمان‌ها به صورت رمز ارسال می‌شدند، به طوری که دشمنان آن‌ها را نمی‌فهمیدند. ولی، در شب‌های حمله با توجه به زیاد شدن تعداد پیام‌ها دشمنان می‌فهمیدند که امشب ممکن است حمله‌ای اتفاق بی‌افتد. از آنجایی که داده‌ها در حمله غیر فعال تغییر نمی‌کنند، بنابراین، تشخیص آن‌ها خیلی مشکل است.



شکل ۱-۲ حمله تحلیل ترافیک.



آشنایی با مبانی امنیت شبکه



۸



۲-۵-۱. حملات فعال

حملات فعال^۱، وقتی رخ می‌دهند که حمله کننده علاوه بر دریافت پیام، آن را تغییر داده و برای گیرنده ارسال نماید. چهار نوع حمله فعال وجود دارند که عبارت‌اند از:
☒ بدل^۲، وقتی اتفاق می‌افتد که موجودیتی خودش را به جای موجودیت دیگری جا بزند (شکل ۳-۱). یعنی، فردی هویت فرد دیگری را سرقت کرده و از طرفش پیامی را ارسال می‌نماید یا به منابعی دسترسی می‌یابد.



شکل ۳-۱ حمله بدل.

☒ تغییر پیام^۳، وقتی رخ می‌دهد که بخشی از یک پیام صحیح تغییر یابد یا پیام به تعویق افتاده و یا مجدداً ارسال شود (شکل ۴-۱).



شکل ۴-۱ تغییر پیام.

به عنوان مثال، فرض کنید، پیام اصلی به صورت زیر باشد:
"به آقای احمدی اجازه خواندن فایل محرمانه را بدهید."

^۱.Active Attack

^۲. Masquerade

^۳.Message Modification



آشنایی با مبانی امنیت شبکه



حال ممکن است پیام در هنگام انتقال به صورت زیر تغییر یابد:

"به آقای محمدی اجازه خواندن فایل محرمانه را بدهید."

همان طور که در این پیام‌ها مشاهده می‌کنیم، به جای آقای احمدی، آقای محمدی مجوز خواندن فایل‌های محرمانه را بدست می‌آورد. یعنی، پیام اصلی در هنگام انتقال تغییر یافته است.

☒ **انکار سرویس (DOS)**^۱، از استفاده نرمال منابع ارتباطی و امکانات جلوگیری می‌کند (شکل

۵ - ۱).



شکل ۵-۱ حمله انکار سرویس.

این نوع حملات، هدف خاصی دارند. به عنوان مثال، یک موجودیت مانع از تحویل پیام‌ها به مقصد خاصی می‌گردد. یعنی، شخصی تمام پیام‌های فرستاده شده به مقصد معینی را پنهان می‌کند. فرم دیگر انکار سرویس، قطع کل شبکه، غیر فعال کردن شبکه و ارسال پیام‌های غیر مجاز برای شبکه جهت کاهش کارایی آن می‌باشد. این نوع حملات را از کار انداختن سرویس گویند. در این نوع حملات، فرد غیر مجاز استفاده از سرویس ارائه شده توسط ارائه کننده سرویس را برای کاربران مجاز مختل می‌کند. یعنی، فرد غیر مجاز حجم زیادی از درخواست سرویس به سرویس‌دهنده^۲ می‌فرستد تا امکان سرویس‌دهی به افراد مجاز را از آن سلب کند. در واقع، سرویس‌دهنده مشغول پاسخ‌گویی به درخواست‌های فرد غیر مجاز می‌شود و از پاسخ‌گویی به کاربران مجاز باز می‌ماند یا سرعت پاسخ‌گویی به آن‌ها بسیار پایین می‌آید.

☒ **تکرار**^۳، به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند (شکل ۶-۱).

^۱.Denial of Service

^۲. Server

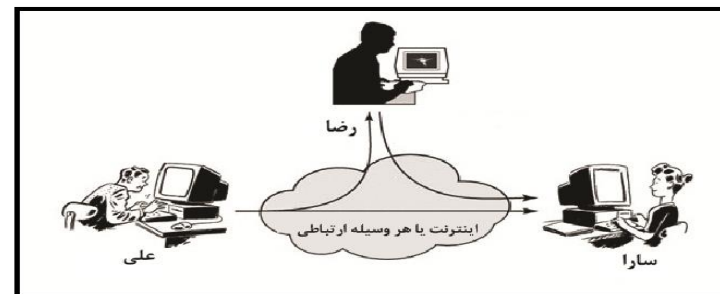
^۳.Replay



آشنایی با مبانی امنیت شبکه



۱۰



شکل ۶-۱ حمله تکرار.

۱-۶-۱. سرویس امنیتی

سرویس امنیتی، سرویسی است که برای ارتقاء امنیت داده مورد استفاده قرار می‌گیرد. تحقق سرویس‌های امنیتی، با استفاده از یک یا چند مکانیزم امنیتی امکان‌پذیر است. سرویس‌های امنیتی، سیاست‌های امنیتی را ارائه کرده و توسط مکانیزم‌های امنیتی اجرا می‌شوند. دو نوع سرویس‌های امنیتی وجود دارد که عبارت‌اند از:

۱. سرویس امنیتی RFC2828

۲. سرویس امنیتی X.800

ممکن است تعریف واضح‌تری از سرویس امنیتی در RFC2828 وجود داشته باشد: سرویس پردازشی یا ارتباطی است که توسط یک سیستم جهت عرضه نوعی محافظت برای منابع سیستم طراحی شده است.

۱-۶-۱-۱. سرویس‌های امنیتی X.800

برخی از سرویس‌های امنیتی X.800 در زیر آمده‌اند:

۱. احراز هویت همتا، این روش تثبیت هویت موجودیت همتا را در یک انجمن مهیا می‌کند.
 ۲. احراز هویت اصل داده، این روش منبع واحد داده را تثبیت می‌کند. این روش حفاظتی علیه تکرار یا تغییر واحدهای داده ایجاد نمی‌کند. این سرویس از برنامه‌های کاربردی مانند پست الکترونیک که فعل و انفعال قبلی بین دو موجودیت ارتباطی وجود ندارد پشتیبانی می‌کند. برخی از این نوع سرویس‌های امنیتی در زیر آمده‌اند:
- ☒ سرویس احراز هویت، در سرویس احراز هویت، هویت طرفین هر ارتباط (فرستنده و گیرنده) صحیح و مستند است. احراز هویت را می‌توان از چند دیدگاه بررسی کرد که عبارت‌اند از:



آشنایی با مبانی امنیت شبکه



۱۱



☒ گیرنده پیام مطمئن شود، آیا پیام ساده از قبیل سیگنال هشدار یا خطر قطع، از منبع مورد نظر می‌آید یا خیر.

☒ در رابطه با فعل و انفعال مداوم از قبیل یک ترمینال به میزبان دو حالت بوجود می‌آید. اول این که، در زمان شروع اتصال سرویس، اطمینان حاصل گردد که موجودیت معتبر است و دوم این که، سرویس باید اطمینان حاصل کند که در اتصال، راهی که شخص سوم (ثالث) بتواند خود را جای یکی از دو طرف قانونی جا بزند، وجود ندارد.

☒ **کنترل دسترسی**، کنترل دسترسی^۱، توانایی محدودکردن و کنترل دستیابی به سیستم‌ها، برنامه‌های کاربردی و داده می‌باشد. در زمینه امنیت شبکه، کنترل دسترسی توانایی محدود سازی و کنترل دسترسی به سیستم‌های میزبان، برنامه‌های کاربردی یا پیوند ارتباطی شبکه است. در کنترل دسترسی، موجودیتی که سعی دارد به منبع یا منابع دسترسی داشته باشد، ابتدا باید شناسایی شده یا تصدیق گردد. برای این منظور، می‌توان از دسترسی یکتا استفاده نمود.

۳. **محرمانگی**، سرویس محرمانگی^۲، بیان می‌کند تمام داده‌های ارسالی، فقط توسط کاربران مجاز قابل دسترسی باشند. محرمانگی، محافظت از داده منتقل شده از حملات غیر فعال است. محرمانگی سرویس گسترده‌ای است که تمام داده‌های انتقالی کاربر بین کاربران را در یک برهه زمانی محافظت می‌کند.

به عنوان مثال، هنگامی که اتصال TCP بین دو سیستم برقرار می‌گردد، این محافظت گسترده از آزادسازی هرگونه انتقال داده کاربر در اتصال TCP جلوگیری می‌کند.

روش‌های محدودتری از این سرویس می‌توانند تعریف شوند که شامل محافظت از پیام ساده یا حتی فیلدهای مشخصی در یک پیام هستند. فرض کنید، حقوق افراد را از طریق شبکه انتقال می‌دهید، می‌خواهید فقط برای فیلد مبلغ حقوق محرمانگی ایجاد کنید.

حالت دیگر محرمانگی، محافظت از جریان ترافیک است. این نوع محرمانگی نیازمند این است که حمله‌کننده قادر نباشد، به منبع (مبدا) و مقصد یا ویژگی‌های دیگر ترافیک در یک شبکه ارتباطی دسترسی یابد. در ادامه با چگونگی انجام این کار آشنا خواهید شد.

۴. **تمامیت داده**^۳ (جامعیت داده)، بیان می‌کند ارسال داده و هرگونه تغییر و دستکاری داده‌های دریافتی (در بین راه) توسط کاربر مجاز انجام شده باشد. یعنی، اولاً داده را کاربر غیر مجاز ارسال نکرده باشد و ثانیاً داده در بین راه (در هنگام انتقال) توسط کاربر غیر مجاز تغییر نکرده است. سرویس تمامیت (جامعیت)، می‌تواند برای پیام‌های ساده یا فیلدهای انتخابی در یک پیام استفاده شود.

^۱.Access Control

^۲.Confidentiality

^۳.Data Integrity



آشنایی با مبانی امنیت شبکه



۱۲

۵. عدم انکار^۱ (سندیت)، یعنی، عمل ارسال، دریافت و نیز محتوی داده و پیام توسط فرستنده و گیرنده قابل انکار نباشد (سرویسی که از انکار فرستنده و گیرنده جلوگیری می‌کند). از این رو، وقتی پیامی ارسال گردید، فرستنده می‌تواند ثابت کند که گیرنده پیام را دریافت کرده است.

۶. دسترس پذیری^۲ (در دسترس بودن)، پیشگیری از محدود شدن یا از دست رفتن منابع داده‌ای به ویژه در سیستم‌های توزیع شده مثل شبکه را بیان می‌کند. هم X.800 و هم RFC2828 دسترسی پذیری را به عنوان یک خصوصیت سیستم تعریف می‌کند.

۲-۶-۱. مکانیزم‌های امنیتی

مکانیزم‌های امنیتی، روش‌ها و راهکارهایی برای تشخیص و جلوگیری از حمله‌های امنیتی هستند. چنانچه، حملات امنیتی اتفاق افتاده باشند، روش‌های ترمیم این حملات را مکانیزم امنیتی گویند. برخی از مکانیزم‌های امنیتی عبارت‌اند از:

۱. رمزکردن^۳، استفاده از الگوریتم‌های ریاضی برای انتقال داده به فرمی که توسط افراد غیر مجاز قابل خواندن (قابل فهم) نباشد.
۲. امضای دیجیتال^۴، داده‌های اضافه شده (انتقالات پنهانی) به واحد داده اصلی است که گیرنده را قادر می‌سازد از صحت داده (دستکاری نشدن داده) و هویت فرستنده آن مطمئن شود. این مکانیزم برای تایید اعتبار فرستنده و صحت اطلاعات فرستاده شده به کار می‌رود.
۳. کنترل دستیابی^۵، اجازه دستیابی به اطلاعات (خواندن و نوشتن) را فقط به افراد مجاز می‌دهد. یعنی، با این مکانیزم افراد غیر مجاز نمی‌توانند داده‌ها را بخوانند یا آن‌ها را دستکاری کنند. روش‌های مختلف کنترل دستیابی اختیاری^۶، کنترل دستیابی مبتنی بر نقش^۷، کنترل دستیابی اجباری^۸ و کنترل دستیابی مبتنی بر HTTP وجود دارند.
۴. کنترل مسیر^۹، مسیریابی امن فیزیکی مقدار مشخصی از داده را ممکن ساخته و تغییرات مسیریابی را وقتی شکاف امنیتی رخ می‌دهد، مجاز می‌سازد.
۵. کنترل ترافیک^{۱۰}، بیت‌هایی در جاهای خالی داده (شکاف‌های داده) جاگذاری کرده تا تلاش تحلیل ترافیک را خنثی نماید.
۶. تعویض هویت^{۱۱}، مکانیزمی که به تشخیص موجودیت توسط تعویض هویت کمک می‌کند.
۷. گواهی^{۱۲}، استفاده از شخص ثالث جهت اطمینان از ویژگی معین تعویض داده است. ارتباط بین سیاست‌های امنیتی و مکانیزم‌های امنیتی در جدول ۱ - ۱ آمده است.

1. Non-repudiation	2. Availability	3. Enchipherment
4. Digital Signature	5. Access Control	6. Discretionary Access Control
7. Role-Based Access Control	8. Mandatory Access Control	
9. Routing Control	10. Traffic Control	11. Authentication Exchanging
12. Authorization		





آشنایی با مبانی امنیت شبکه



۲۲ فصل اول

۲. اطلاعات سرّی به اشتراک گذاشته شده بین دو مسئول، باید از معارض مخفی نگاه داشته شود. یک نمونه، از این اطلاعات سرّی، کلید رمزگذاری و رمزگشایی است که بین فرستنده و گیرنده به اشتراک گذاشته می شود.
- این مدل چهار نکته مهم پایه‌ای را در طراحی سرویس امنیتی نشان می دهد که عبارت‌اند از:
 ۱. الگوریتمی برای اجرای امنیت طراحی می شود. الگوریتم باید به صورتی طراحی شود که معارض نتواند به هدف خود برسد.
 ۲. با استفاده از الگوریتم، اطلاعات سرّی تولید می شوند.
 ۳. روش‌هایی برای تولید و به اشتراک گذاری اطلاعات سرّی ایجاد می شوند.
 ۴. پروتکلی برای استفاده دو مسئول تعریف می شود که کاربرد الگوریتم امنیتی و اطلاعات سرّی برای دستیابی به سرویس امنیتی ویژه را ایجاد می کند.



آشنایی با مبانی امنیت شبکه



رمزگذاری‌های کلاسیک

در فصل اول، انواع حملات را دیدید. یکی از حملات، حمله غیر فعال استراق سمع می‌باشد. برای جلوگیری از این حمله، از رمزنگاری استفاده می‌شود. دو مدل رمزنگاری وجود دارد:

۱. مدل رمزنگاری متقارن (Symmetric Cipher Model).

۲. مدل رمزنگاری نامتقارن (Asymmetric Cipher Model).

۱-۲. مدل رمزگذاری متقارن

در این نوع رمزنگاری یک کلید بین فرستنده و گیرنده اطلاعات مشترک است. فرستنده متن ساده^۱ (اصلی) را با الگوریتم رمزگذاری^۲ و کلید سری^۳ به متن رمز شده^۴ تبدیل می‌کند و گیرنده متن رمز شده را گرفته و با الگوریتم رمز گشایی^۵ و همان کلید آن را به متن ساده و قابل فهم تبدیل می‌کند. (شکل ۱-۲).

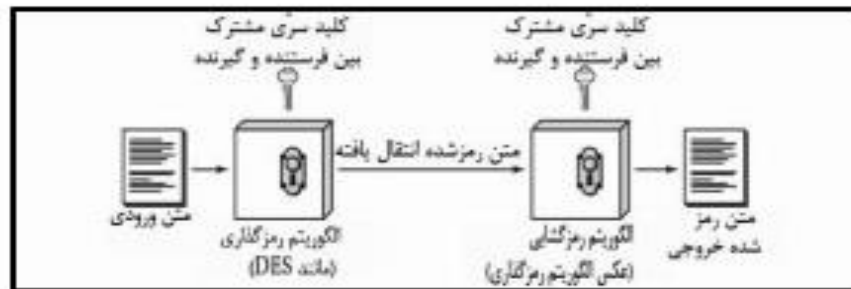
مدل رمزنگاری متقارن از پنج عنصر تشکیل شده است که عبارت‌اند از:

- ☒ متن ساده (اصلی): پیام قابل فهم یا داده‌ای که ورودی الگوریتم رمزگذاری است.
- ☒ الگوریتم رمزگذاری: الگوریتم رمزگذاری که جانشینی‌ها و جابه‌جایی‌های گوناگون را روی متن ساده انجام می‌دهد تا آن را به متن رمز شده (غیر قابل فهم) تبدیل کند.

^۱. PlainText ^۲. Encryption Algorithm ^۳. Secret Key ^۴. CipherText ^۵. Decryption Algorithm



آشنایی با مبانی امنیت شبکه



شکل ۱-۲ مدل ساده شده رمزگذاری مرسوم.

☒ کلید سری: کلیدی که یکی از ورودی‌های الگوریتم رمزگذاری و رمزگشایی است. چون این کلید بین فرستنده و گیرنده پیام مشترک است، باید سری بماند. کلید سری به متن و الگوریتم وابسته نیست. یعنی، جابه‌جایی و جانشینی دقیق توسط الگوریتم وابسته به کلید اجرا می‌شوند.

☒ متن رمز شده: پیامی غیر قابل فهم که خروجی الگوریتم رمزگذاری می‌باشد. غیر قابل فهم بودن این متن، به طول کلید سری و قدرت الگوریتم رمزگذاری وابسته است.

☒ الگوریتم رمزگشایی: در حقیقت این الگوریتم معکوس الگوریتم رمزگذاری است. این الگوریتم متن رمز شده و کلید سری را به عنوان ورودی دریافت می‌کند و خروجی آن متن ساده (متن اصلی قابل فهم) می‌باشد.

برای ایمن سازی رمزگذاری دو نیازمندی وجود دارد:

۱. الگوریتم رمزگذاری قوی: یعنی، الگوریتم باید به گونه‌ای باشد که معارض^۳ نتواند متن رمز شده را رمزگشایی کند یا کلید را کشف کند.
 ۲. فرستنده و گیرنده باید کمی کلید سری را از یک روش امن به دست آورده و کلید را جای امنی نگهداری کنند.
- اگر فردی بتواند کلید را کشف کرده و الگوریتم را بداند، تمام مکاتبات فرستنده و گیرنده که از این کلید استفاده گردد، قابل فهم (خواندن) می‌شود.

^۳.opponent



آشنایی با مبانی امنیت شبکه



۱۶



فرض می‌کنیم دانش الگوریتم رمزگذاری / رمزگشایی مشخص باشد، با این حال رمزگشایی پیام رمز شده، عملی نیست. یعنی، نیازی نیست الگوریتم را مخفی کنیم، فقط باید کلید مخفی باشد. این ویژگی رمزگذاری متقارن آن را جهت استفاده به صورت گسترده عملی می‌نماید. این واقعیت که نیازی نیست الگوریتم مخفی بماند، به این معنی است که سازندگان می‌توانند الگوریتم‌های رمزگذاری و رمزگشایی داده را بر روی یک تراشه ارزان قیمت قرار دهند.

در هنگام استفاده از رمزگذاری متقارن مسئله اصلی امنیت، پنهان نگه داشتن کلید است. شکل ۲-۲ جزئیات رمزگذاری متقارن را نشان می‌دهد. پیام به صورت دنباله‌ای از کاراکترها $(X = [x_1, x_2, \dots, x_n])$ می‌باشد. n ، تعداد حروف الفبای متاهی است (الفبای لاتین از ۲۶ حرف تشکیل شده است).

امروزه از الفبای باینری $\{0, 1\}$ استفاده می‌گردد. کلید به شکل $k = \{k_1, k_2, \dots, k_n\}$ تولید می‌شود. بعد از تولید کلید، باید توسط کاتالی امن به مقصد تحویل داده شود. کلید می‌تواند توسط شخص ثالث تولید شده و به منبع (مبداء) و مقصد تحویل داده شود.

الگوریتم رمزگذاری، پیام X و کلید رمزگذاری K را به عنوان ورودی دریافت کرده، متن رمز $Y = [y_1, y_2, \dots, y_n]$ را تولید می‌کند. یعنی:

$$Y = E(K, X)$$

این فرمول نشان می‌دهد الگوریتم رمزگذاری E (به عنوان یک تابع) با استفاده از کلید K و متن ساده X ، متن رمز شده Y را تولید می‌کند.

همان‌طور که بیان کردیم کلید K بین گیرنده و فرستنده مشترک است. بنابراین، گیرنده با فرمول مقابل می‌تواند متن رمز شده Y را به متن ساده X برگرداند:

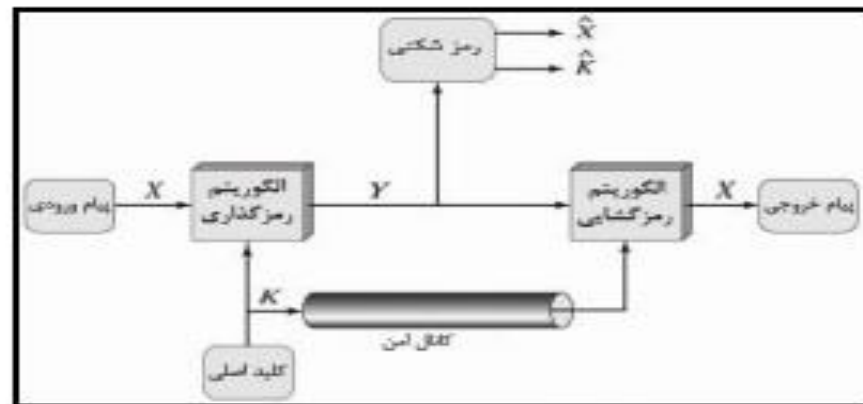
$$X = D(K, Y)$$

در این فرمول D ، معکوس تابع E است.

مهاجم (معارض)، که Y را در اختیار دارد، ولی K یا X را ندارد، سعی می‌کند X یا K یا هر دو را به دست آورد. فرض شده است که معارض الگوریتم رمزگذاری (E) و رمزگشایی (D) را می‌داند، اگر معارض بخواهد این پیام را رمزگشایی کند، آنگاه روی این پیام متمرکز می‌شود که بتواند پیام را رمزگشایی نماید. در این حالت تلاش می‌کند کلید K را به دست آورد که پیام X را تولید می‌کند (شکل ۲-۲).



آشنایی با مبانی امنیت شبکه



شکل ۲-۲ مدل سیستم رمز قراردادی.

۲-۲. رمز نویسی

سیستم‌های رمز نویسی^۱ از سه بعد زیر با یکدیگر مقایسه می‌شوند:

۱. نوع عملیات استفاده شده برای تبدیل متن ساده به متن رمز، تمام الگوریتم‌های رمز گذاری بر اساس دو اصل کلی (جانشینی و جابه‌جایی) بنا شده‌اند. جانشینی^۲ یعنی، هر عنصر در متن، یک بیت، بایت، حرف، مجموعه‌ای از بیت‌ها یا حروف) با عنصر دیگر جایگزین می‌شود. انتقال^۳ یعنی، جای (مکان) عناصر در متن جابه‌جا می‌شود. در این جابه‌جایی و جانشینی نباید هیچ اطلاعاتی گم شود. یعنی، همه عملیات برگشت پذیر باشند. اکثر سیستم‌هایی که به صورت سیستم‌های محصول^۴ در آمده‌اند، مراحل چندگانه جابه‌جایی و جانشینی را انجام می‌دهند (مانند الگوریتم DES).
۲. تعداد کلیدهای استفاده شده، اگر گیرنده و فرستنده از یک کلید مشترک استفاده کنند، سیستم به صورت متقارن (تک کلید یا کلید سری) تعریف می‌شود (نام دیگر این الگوریتم قراردادی است). ولی، چنانچه گیرنده و فرستنده از کلیدهای متفاوتی استفاده نمایند، سیستم به صورت نامتقارن (دو کلید یا الگوریتم کلیدی عمومی) تعریف می‌شود.
۳. روشی که در آن متن پردازش می‌شود، رمز کننده ممکن است بلوکی^۵ یا دنباله‌ای^۶ باشد. در رمزکننده بلوکی، یک بلوک از عناصر به عنوان ورودی دریافت می‌شود، و بلوکی از عناصر رمز شده

^۱.Cryptography ^۲. Substitution ^۳. Transposition ^۴.Product Systems



آشنایی با مبانی امنیت شبکه



تولید می‌شود. ولی، رمز کتند دنباله‌ای، عناصر ورودی را به صورت متوالی (پشت سرهم) پردازش کرده و یک عنصر خروجی رمز شده را در یک لحظه تولید می‌کند.

۳-۲. رمز شکنی خطی

اساساً، هدف حمله به سیستم رمزگذاری کشف کلید استفاده شده است. یعنی، حمله‌کننده می‌خواهد به جای کشف متن ساده از متن رمز، کلید را به دست آورد. دو روش کلی حمله به الگوریتم مرسوم رمزگذاری وجود دارد که عبارت‌اند از:

۱. رمز شکنی خطی^۲
۲. حمله جستجوی جامع^۳

^۱.Block

^۲.Stream

^۳.Cryptanalysis

^۴.Brute – Force Attack



آشنایی با مبانی امنیت شبکه



فصل ۳ رمزگذاری‌های پیشرفته متقارن و نامتقارن

۱- ۳. رمزگذاری‌های پیشرفته

در فصل دوم، با برخی از رمزگذاری‌های کلاسیک آشنا شدیم. همان‌طور که در این رمزگذاری‌ها دیدید، رمزگشایی بدون داشتن کلید با تلاش امکان‌پذیر بوده است. در این فصل می‌خواهیم برخی از رمزگذاری‌های پیشرفته را بیاموزیم که رمزگشایی بدون کلید مشکل است. برخی از این رمزگذاری‌ها عبارت‌اند از:

- ۱. رمزگذاری بلوکی
- ۲. رمزگذاری DES
- ۳. رمزگذاری AES
- ۴. رمزگذاری RC4
- ۵. رمزگذاری RC5
- ۶. رمزگذاری نامتقارن (کلید عمومی)

۲- ۳. رمزگذاری بلوکی

رمزگذاری بلوکی^۱ یک بلوک از متن را گرفته با روش‌های جایگشتی، جانشینی و کلید آن را رمز کرده، یک بلوک رمز شده را برمی‌گرداند. در ادامه برخی از این نوع رمزگذاری‌ها را می‌بینید.

۱- ۲- ۳. اصول رمزهای بلوکی

این روش ترکیبی از روش‌های ساده جانشینی و جایگشت است که ترکیب آن‌ها الگوریتم پیچیده و امنی را ایجاد می‌کند. اغلب الگوریتم‌های بلوکی متقارن از ساختار رمز بلوکی فیستل^۲ استفاده می‌کنند.

این فصل را با مقایسه رمزکننده دنباله‌ای^۳ و رمزکننده‌های بلوکی آغاز می‌کنیم. سپس، راجع به هدف ساختار رمزکننده بلوکی فیستل بحث می‌کنیم. در پایان به برخی مفاهیم و رمزگذاری‌های پیشرفته می‌پردازیم.

۲- ۲- ۳. رمزکننده دنباله‌ای و بلوکی

دو نوع رمزگذاری وجود دارد که عبارت‌اند از:

^۱.Block cipher ^۲.Feistel Cipher ^۳.Stream Ciphers ^۴.Vernam Cipher



آشنایی با مبانی امنیت شبکه



رمزگننده دنباله‌ای، نوعی از رمزگذاری است که دنباله داده دیجیتال را به صورت یک بیتی یا یک بایتی در یک مرحله رمزگذاری می‌کند. یک نمونه از رمزگننده دنباله‌ای کلاسیک رمز وینچرو رمز ورنام^۱ است.

رمزگننده بلوکی، بلوک‌های متنی را به بلوک‌های رمز شده با طول یکسان تبدیل می‌کند. در کل، در این نوع رمزگننده اندازه بلوک ۶۴ بیتی یا ۱۲۸ بیتی است. رمزگننده‌های بلوکی کاربرد بیشتری نسبت به رمزگننده‌های دنباله‌ای دارند. بنابراین، روی این رمزگننده‌ها تمرکز می‌شود.

۳-۲-۳. هدف ساختار رمزگننده فیستل

رمزگننده بلوکی، بلوک n بیتی متن را به بلوک رمز شده n بیتی تبدیل می‌کند. اکنون 2^n بلوک متنی مختلف برای برگرداندن متن اصلی وجود دارد. این نوع تبدیل‌ها، برگشت‌پذیر^۲ یا غیر یکتا^۳ نامیده می‌شوند. به عنوان مثال، تبدیل‌های برگشت‌پذیر و برگشت‌ناپذیر را به صورت زیر مشاهده می‌کنید.

نگاشت برگشت‌پذیر		نگاشت برگشت‌ناپذیر	
متن اصلی	متن رمز شده	متن اصلی	متن رمز شده
00	11	00	11
01	10	01	10
10	00	10	01
11	01	11	01

در نگاشت برگشت‌ناپذیر، متن رمز شده "01" توسط یک یا دو بلوک متنی بوجود آمده است، بنابراین، اگر به نگاشت‌های برگشت‌پذیر محدود شویم تعداد تبدیل‌های مختلف 2^n می‌شود. شکل ۳-۱ منطق رمز جایثینی برای $n = 4$ را نشان می‌دهد. ورودی ۴ بیتی یکی از ۱۶ حالت ممکن ورودی را تولید می‌کند، که توسط رمز جایثینی به یکی از ۱۶ حالت ممکن خروجی یکتا نگاشت می‌شود، که هر کدام با ۴ بیت رمز شده نشان داده می‌شود.

^۱Reversible ^۲Nonsingular



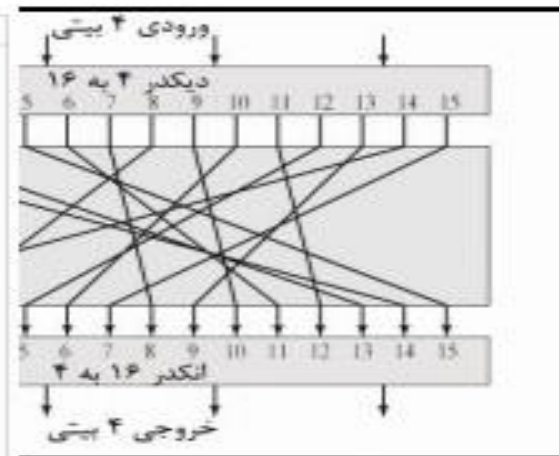
آشنایی با مبانی امنیت شبکه



۲۱



متن اصلی	متن رمز شده
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101



شکل ۱- ۳ جانشینی بلوکی n بیت جامع.

این کلی‌ترین شکل رمزگذاری بلوکی است و می‌توان آن را برای هر نگاشت برگشت‌پذیر برای متن اصلی و متن رمز شده تعریف کرد. لیست از این روش به عنوان رمز بلوکی مطلوب استفاده می‌کند، زیرا حداکثر تعداد نگاشت‌های رمزگذاری ممکن را از بلوک متنی می‌پذیرد. نگاشت‌های رمزگذاری و رمزگشایی با جدول‌بندی قابل تعریف هستند، که در شکل ۲-۳ نشان داده شده است. اما یک مشکل اصلی برای رمز بلوکی وجود دارد. اگر اندازه کوچکی

از بلوک مانند 4-n بکار رود، سیستم مانند یک سیستم رمز جانشینی کلاسیک عمل می‌کند.

همان‌طور که دیدیم، این گونه سیستم‌ها با تحلیل آماری متن آسیب‌پذیرند. این ضعف در استفاده از رمز جانشینی همیشگی نیست، اما به نسبت بلوک‌های کوچک حاصل می‌شود. اگر n به اندازه کافی بزرگ باشد و جانشینی برگشت‌پذیر مطلق بین متن اصلی و متن رمز شده مجازی باشد، ویژگی‌های آماری متن اصلی به کلی پوشیده می‌شود که این نوع رمز جانشینی برگشت‌پذیر مطلق برای بلوک با اندازه بزرگ از نظر کارایی و اجرا کاربردی نیست.

در این نوع تبدیل، نگاشت خودش کلید را ترکیب شکل ۲-۳ جدول رمزگذاری و رمزگشایی



آشنایی با مبانی امنیت شبکه

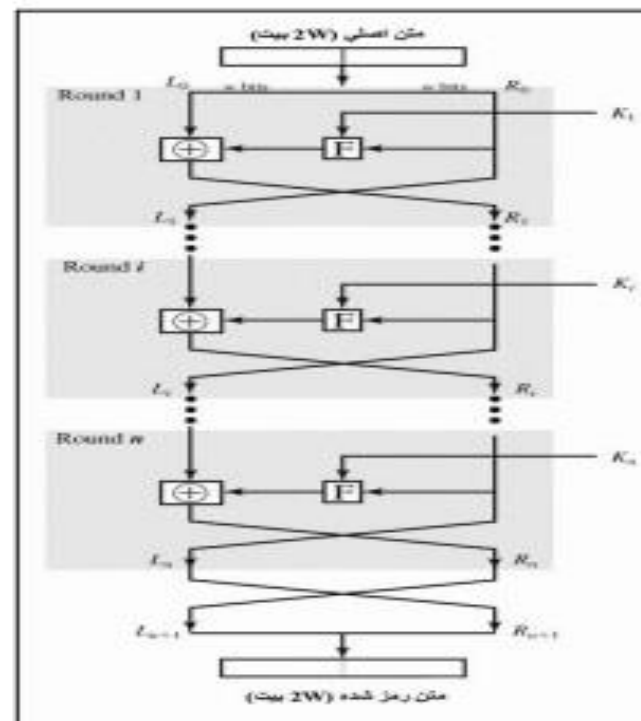


می‌کند. با برگشت به شکل ۲-۳ که نگاهت
برگشت‌پذیر را تعریف می‌کند، می‌بینیم که نگاهت می‌تواند توسط ورود در ستون دوم تعریف شود.
که مقدار متن رمز شده را برای هر بلوک متنی نشان می‌دهد. این اساساً کلیدی است که نگاهت
بخصوصی از میان نگاهت‌های موجود را تعیین می‌کند. در این حالت، طول کلید مورد نیاز
بیت $64 - 16 \times 4$ بیت می‌باشد.
در کل، برای رمز بلوکی ایده‌آل n بیتی، طول کلید تعریف شده در این روش $n \times 2^2$ بیت است.
برای بلوک ۶۴ بیتی که طول مناسبی برای خشی کردن حملات آماری است، طول کلید مورد نیاز
 $2^{10} = 64 \times 4^2 = 1024$ بیت است.
با ملاحظه این مشکلات، فستل مولفه‌های لازم برای تولید رمز بلوکی نزدیک به سیستم رمز بلوکی
مطلوب برای n های بزرگ را نشان می‌دهد.

۳-۳. رمز فستل

فستل در رابطه با رمز بلوکی، پیشنهادی را مطرح نمود که می‌توان رمز بلوکی مناسبی را با
یکارگیری رمز تولید شده تقریب زد، اجرای دو یا چند رمز ساده بطور متوالی است. در این روش،

نتیجه نهایی قوی‌تر از رمزهای ترکیبی
است.



در این روش طول کلید K بیت
بوده و طول بلوک n بیت است که
 2^4 تبدیل ممکن را بیشتر از 2^1
تبدیل موجود با رمز بلوکی مناسب
مجاز می‌کند. در سیستم رمز فستل
جانیشنی‌ها و جایگشت‌ها به نوبت
انجام می‌شود.

۳-۳-۱. ساختار رمز فستل

در شکل ۳-۳ ساختار
پیشنهادی فستل را می‌بینید.
ورودی‌های الگوریتم رمز گذاری،
بلوک متن اصلی با طول $2w$ بیت و



آشنایی با مبانی امنیت شبکه



کلید k بیتی است. متن اصلی به دو نیمه L_0 و R_0 تقسیم می‌شوند. این دو نیمه از یک فرآیند n مرحله‌ای عبور کرده و سپس، جهت تولید بلوک متن رمز شده باهم ترکیب می‌شوند که در شکل ۳-۳ این مراحل را مشاهده می‌کنید. شکل ۳-۳ شبکه فیستل کلاسیک.

ورودی هر مرحله (k) ، R_{i-1} و L_{i-1} و زیر کلیدها است. این ورودی‌ها از مرحله قبلی و کلید اصلی k مشتق شده‌اند.

در واقع، زیر کلیدهای k_i با کلید اصلی k و همچنین با خودشان متفاوت هستند. تمامی مراحل ساختار مشابه دارند. جانشینی روی نیمه چپ داده انجام می‌شود. این عمل با بکارگیری تابعی گردکننده^۱ به نام

F روی نیمه راست داده انجام می‌شود و سپس، خروجی تابع F با نیمه چپ داده OR انحصاری (XOR) می‌شود. تابع گردکننده F همان ساختار را برای هر مرحله دارد. اما با زیر کلید k_i هر مرحله مقداردهی می‌شود. به دنبال این جانشینی، جایگشت اجرا می‌شود که از تعویض دو نیمه داده تشکیل شده است. این ساختار روش شانون^۲ را بری شبکه جانشینی - جایگشتی^۳ نشان می‌دهد.

^۱ .Round Function ^۲ .Shannon ^۳ .Substitution - Permutation Network (SPN)



آشنایی با مبانی امنیت شبکه



قبل از این که به امنیت شبکه و محیط کاری بپردازیم، ابتدا تهدیداتی که برای شبکه وجود دارند، را بررسی می‌کنیم. دو نوع تهدید موجود در شبکه عبارتند از:

۱. دسترسی افراد غیر مجاز در شبکه.
۲. تخریب داده‌ها در شبکه.

بنابراین، در این فصل ابتدا به روش‌های دسترسی غیر مجاز در شبکه و دلایل تخریب اطلاعات می‌پردازیم. سپس، لیست‌های کنترل امنیتی که سازمان‌ها و اشخاص باید چک کنند تا از دسترسی افراد غیر مجاز به شبکه و تخریب داده‌ها جلوگیری نمایند را می‌بینید.

۴-۱. دسترسی افراد غیر مجاز در شبکه

امروزه یکی از رایج‌ترین و مهم‌ترین تهدیداتی که در شبکه‌های کامپیوتری وجود دارد، دسترسی افراد غیرمجاز است. دسترسی افراد غیر مجاز در یکی از بخش‌های زیر رخ می‌دهد:

۱. اتصالات فیزیکی شبکه
۲. سرورها و زیرساخت‌های مرکزی و اصلی
۳. کامپیوترهای رومیزی

۴-۱-۱. اتصالات فیزیکی شبکه

امروزه کامپیوترها در شبکه به روش‌های مختلفی با یکدیگر متصل می‌گردند. برخی از این روش‌ها عبارتند از:

۱. شبکه‌های کابلی
۲. شبکه‌های فیبر نوری
۳. شبکه‌های بی‌سیم
۱. شبکه‌های کابلی

اکثر شبکه‌های محلی از کابل‌های مسی مانند کابل‌های شبکه معمولی و کابل‌های تلفن برای اتصال رایانه‌ها به شبکه‌ها استفاده می‌کنند. از آنجائی که در کابل‌های مسی امکان شنود و استراق سمع وجود



آشنایی با مبانی امنیت شبکه



دارد، لذا، به کارگیری آنها در محیط‌های ناامن جهت تبادل و انتقال اطلاعات محرمانه، خطرناک می-باشد.

۲. شبکه‌های فیبرنوری

شبکه‌هایی که از فیبرنوری^۱ تشکیل شده‌اند، بندرت جهت اتصال کامپیوترها در شبکه‌ها استفاده می‌شوند. زیرا، هزینه راه‌اندازی و نگهداری آنها بسیار بالا است. اما، شبکه‌هایی که از فیبرنوری برای اتصال کامپیوترها استفاده می‌کنند، نسبت به روش‌های دیگر شنودپذیری و استراق سمع کمتری دارند.

۳. شبکه‌های بی‌سیم

استفاده از شبکه‌های بی‌سیم^۲ به مراتب خطرناک‌تر از شبکه‌های کابلی و فیبرنوری است. زیرا، از آنجائی که دسترسی به شبکه، خارج از ساختمان و در محل دیگر امکان‌پذیر است، امکان شنود در این شبکه‌ها را به مراتب بیشتر از شبکه‌های دیگر افزایش می‌دهد.

روش‌های ایجاد ارتباط ایمن در شبکه

روش‌های متعددی برای ایجاد ارتباط ایمن در شبکه وجود دارند. دو روش ایجاد ارتباط ایمن را در زیر می‌بینید:

۱. استفاده از شبکه‌های محلی مجازی^۳

۲. استفاده از شبکه‌های خصوصی مجازی^۴

۱. استفاده از شبکه‌های محلی مجازی

اگر بدون تغییر ساختار فیزیکی شبکه با تنظیم روی سوییچ‌های شبکه، بتوانیم شبکه‌ای مستقل ایجاد کنیم، به صورتی که کامپیوترهای دیگر موجود در شبکه نتوانند به این شبکه دسترسی داشته باشند، تشکیل شبکه VLAN را داده‌ایم. در شکل ۱ - ۴ نمونه‌ای از شبکه VLAN را می‌بینید. در این شکل کامپیوترهای عضو VLAN1 نمی‌توانند به کامپیوترهای عضو VLAN2 دسترسی داشته باشند.

^۱.Fiber Optic

^۲.Wireless

^۳.Virtual LAN

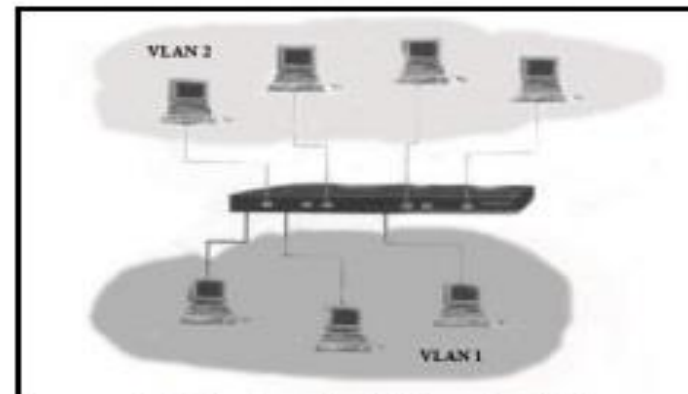
^۴.Virtual Private Network



آشنایی با مبانی امنیت شبکه



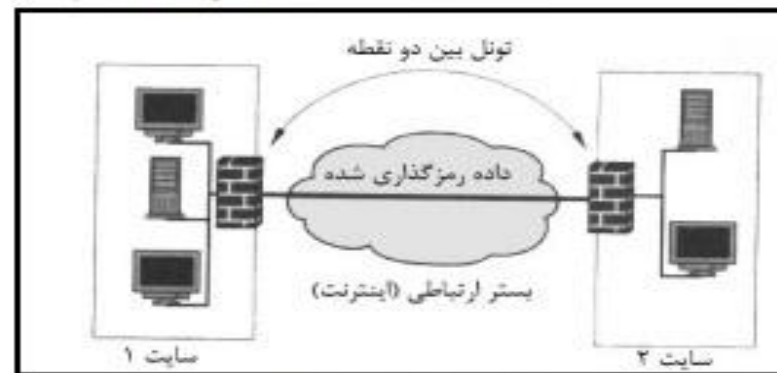
۲۶



شکل ۱-۲ محیط شبکه محلی مجازی (VLAN)

۲. شبکه خصوصی مجازی

همانطور که می‌دانید، گاهی اوقات نیاز است که اطلاعات از طریق فضای ناامن مانند اینترنت تبادل شوند. برای جلوگیری سرت اطلاعات بین کامپیوترهای مبداء و مقصد، یک شبکه VPN ایجاد می‌نماییم. این عمل، به تونل زدن معروف است. در شکل ۲-۴ نمونه‌ای از تونل زدن را می‌بینید. در این شکل اطلاعات در محیط اینترنت بین دو کامپیوتر با رمزگذاری و تونل زدن انتقال می‌یابند.



شکل ۲-۴ تونل مجازی

۲-۱-۴ سرور و زیر ساخت مرکزی و اصلی

سرورها معمولاً در اتاق‌های ظاهراً خوبی محافظت شده، در زیر زمین یا طبقه همکف قرار داده می‌شوند و در مقایسه با اتاق‌ها در یک طبقه بالاتر، خطر دزدی و ورود سیلاب را به عنوان نکته‌ای مهم باید در نظر داشت.



آشنایی با مبانی امنیت شبکه



به خصوص، تخصیص مناسب اتاق‌ها و طرح‌هایی که دستیابی عموم را به طبقات آسان می‌سازد، باعث می‌شوند که پیدا کردن اتاق سرور حتی برای غریبه‌ها آسان شود و اگر تعداد افراد غیر عضو یا غریبه (مانند مشتریان تامین کنندگان) به این طبقه دسترسی داشته باشند، حضور آن‌ها در جلوی اتاق‌های سرور باعث جلب توجه نمی‌شود. در کمپانی‌های کوچک، اتاق‌های سرور غالباً به عنوان محل‌های انبار نیز استفاده می‌شوند که این امر بدین معنی می‌باشد که افرادی که نباید وارد اتاق‌های سرور بشوند، می‌توانند به آن‌ها دستیابی پیدا کنند. در بیشتر موارد، تفکیک اتاق یا محل انبار مستلزم هزینه و تلاش زیادی نمی‌باشد. همچنین، پرینترهای مرکزی و اصلی (مانند پرینترهای لیزری رنگی، پرینترهای با سرعت بالا) نباید برای پایین نگهداشتن تعداد افراد که به آن‌ها دسترسی دارند، در اتاق سرور قرار داده شوند و بلکه بهتر است که دو یا سه اتاق جداگانه داشته باشیم که اولی می‌تواند محل قرار دادن وسایل مرکزی و اصلی باشد که توسط تعداد زیادی از کارکنان (لیزر رنگی، پلاتر یا رسام) مورد استفاده قرار می‌گیرد. در اتاق دوم نیز وسایلی قرار داده می‌شوند که ضروری و مهم نمی‌باشند که در بعضی از شرکت‌ها می‌تواند شامل سرورهای وب باشد. در اتاق سوم نیز ایمن‌ترین وسایل و تجهیزات یعنی فایل سرور¹⁰ و سرور مجوز و تایید اعتبار (مانند کربروس¹¹، Active Directory) قرار داده می‌شوند. با مفهوم سرویس کربروس در ادامه آشنا خواهید شد.

در سازمان‌های کوچک، پشتیبان‌ها نیز مستقیماً در فایل سرور انجام می‌شوند و به منظور حفاظت قویاً توصیه می‌شود که آن‌ها را در محل دیگری نگهداری و ذخیره کنید و ضروری است که این محل نیز باید بسیار مطمئن و ایمن باشد. حفاظت از نسخه‌های پشتیبان در برابر تخریب توسط آتش، سیل، زلزله و موارد مشابه غالباً زیاد مهم نمی‌باشد، زیرا احتمال اینکه نسخه‌های پشتیبان و همچنین داده‌های اصلی در یک زمان از بین بروند نسبتاً کم می‌باشد.

به هر حال این خطر که افراد غیر مجاز بتوانند به نسخه‌های پشتیبان دسترسی پیدا کنند، بسیار زیاد می‌باشد. بهترین سیستم‌های کنترل دستیابی و تایید مجوز در شبکه داخلی اگر تمام داده‌ها در روی نوارها قابل دسترسی باشند، بی‌فایده هستند. زیرا برای مثال، شخصی می‌تواند آن‌ها را به سادگی در یک کیف دستی یا روی صندلی عقب اتومبیل خود جا بگذارد.

¹⁰.File Server

¹¹. Kerberos

¹².Workstation



آشنایی با مبانی امنیت شبکه



۲۸



فصل ۵ بدافزارها

کلمه ویروس به عنوان یک عبارت عمومی برای انواع مختلف حمله‌های رایانه‌ای با کد مخرب استفاده می‌شود. به عنوان مثال، ویروس‌های رایانه‌ای، تروجان‌ها، کرم‌ها و سایر بدافزارهایی که در این فصل می‌بینید، همگی نوعی ویروس محسوب می‌شوند.

اغلب کاربران حداقل یک بار با یکی از انواع ویروس‌ها دچار آلودگی شده‌اند. ویروس می‌تواند از طریق نصب یک نرم‌افزار آلوده، یک دستگاه آلوده (مانند فلش)، باز کردن پست الکترونیکی آلوده، وارد شدن به وب سایتی که آلوده است، به رایانه‌تان منتقل شود.

به طور کلی ویروس‌ها نرم‌افزارهای مخربی هستند که می‌توانند رایانه‌تان را آلوده کرده، منابع آن را به نفع خودشان استفاده کرده، داده‌های رایانه‌تان را سرقت یا خراب کنند. در این فصل با مفاهیم بدافزار^{۱۱} (برنامه‌های مخرب^{۱۲}) و انواع آن‌ها آشنا می‌شویم.

بدافزار، نرم‌افزاری مخرب است. برخی از بدافزارها که نیت تخریب دارند در زیر آمده‌اند:

۱. ویروس‌ها (Virus)
۲. کرم‌ها (Worms)
۳. تروجان‌ها (Trojans)

۱-۵. ویروس

ویروس، قطعه کدی (برنامه نرم‌افزاری) است که خود را در برنامه‌های بزرگ‌تر کپی کرده، آن‌ها را تغییر می‌دهد. برنامه‌هایی که ویروس خودش را در آن‌ها کپی می‌کند، میزبان نام دارند. بنابراین، ویروس‌ها مستقل نیستند. یعنی، زمانی که برنامه‌های میزبان اجرا می‌شوند، ویروس‌ها نیز اجرا می‌گردند و شروع به تکثیر خود و آلوده نمودن برنامه‌های دیگر می‌نمایند. ویروس دو جزء مهم دارد: ۱. مکانیزم انتشار، مکانیزمی است که ویروس را تکثیر می‌کند و برنامه‌ها و رایانه‌های مختلف را آلوده می‌نماید. ۲. مکانیزم اجرا، مکانیزمی است که موجب می‌شود ویروس اجرا شده، عمل تخریب خودش را شروع کند. به عنوان مثال، ویروس میکلاتز در تاریخ تولد میکلاتز فعال گردید و عمل تخریب‌اش را شروع نمود.

^{۱۱} Malware ^{۱۲} Malicious Software



آشنایی با مبانی امنیت شبکه



۲۹



۲-۵. کرم

کرم، برنامه‌ای است که به صورت مستقل اجرا می‌گردد (برای اجرا نیاز به میزبان ندارد). برخلاف ویروس‌ها که خودشان را در فایل‌های دیگر کپی می‌کردند، کرم‌ها استقلال خود را حفظ نموده، برنامه‌های دیگر را تغییر نمی‌دهند. کرم‌ها برای بقای خودشان، منابع میزبان از قبیل پهنای باند شبکه، منابع محلی را مصرف می‌کنند و منجر به حملات انکار سرویس می‌شوند. برخی از کرم‌ها، بدون مداخله کاربر اجرا شده، خودشان را تکثیر می‌کنند. در حالی که برخی دیگر از کرم‌ها، نیاز دارند کاربر آن‌ها را مستقیماً اجرا نموده تا بتوانند خودشان را تکثیر کنند. کرم‌ها علاوه بر تکثیر خود می‌توانند خرابکاری را نیز در سیستم انجام دهند.

۳-۵. تروجان

یک اسب تروا^۱ (تروجان)، قطعه برنامه‌ای است که در ظاهر کار مفید انجام می‌دهد، ولی دارای کد مخفی است که عمل تخریب را انجام می‌دهد.

اسب تروا، خودش را منتشر نمی‌کند، بلکه معمولاً برای کپی کردن خودش، از یک ویروس یا کرم استفاده می‌کند. هدف اصلی یک اسب تروا، تخریب کار کاربر یا عملیات معمولی سیستم است. به عنوان مثال، اسب تروا ممکن است یک درب پستی^۲ را در سیستم باز کند تا هکر از طریق آن بتواند سرعت اطلاعات را انجام داده یا پیکربندی سیستم را تغییر دهد (تروجان‌هایی که به هکرها اجازه دسترسی از راه دور را می‌دهند، تروجان‌های دسترسی راه دور^۳ نام دارند).

۴-۵. نرم افزار Bonus

نرم افزار Bonus، نرم‌افزاری است که علاوه بر نرم‌افزار اصلی شامل بسته‌های دیگر نرم‌افزاری است. وجود بسته‌های دیگر در یک نرم‌افزار تجاری رایج است. به عنوان مثال، فرض کنید یک مرورگر^۴ نصب می‌کنید. این برنامه ممکن است شامل بسته‌هایی نظیر نرم‌افزارهای چند رسانه‌ای یا Adobe Acrobat باشد. بنابراین، گاهی اوقات نیاز است برای نصب یک نرم‌افزار، بسته‌های دیگری را نصب نمایید. در هنگام نصب برنامه اصلی، نصب نرم‌افزارهای جانبی (نرم‌افزارهای اضافی علاوه بر نرم‌افزار اصلی) به اطلاع کاربر می‌رسد. چون عملکرد نرم‌افزارهای Bonus معمولاً متفاوت از نرم‌افزار اصلی است، اگر کاربر چاره‌ای داشته باشد، مسلماً نباید آن‌ها را نصب کند.

^۱ در اسطوره‌های قدیمی، اسب تروا، اسب توغالی ساخته شده از چوب است که توسط سردار سپاه یونان در جنگ امپراتوری تروا ساخته شد. سربازان یونان در این اسب مخفی شدند و از طریق آن وارد شهر شدند. در شب هنگام، از داخل اسب بیرون آمدند و دروازه شهر را برای سربازان یونان باز کردند و به این ترتیب در جنگ پیروز شدند.

^۲.Back door ^۳.Remote Access Trojans ^۴.Browser



آشنایی با مبانی امنیت شبکه



۵-۵. انواع عملیات نرم افزار مخرب (بد افزار)

محدودیتی در چگونگی فعالیت بدافزارها روی کامپیوترتان وجود ندارد، اما، این برنامه‌ها در برخی از فعالیت‌ها مشترک هستند. این فعالیت‌ها در زیر آمده‌اند:

۱. رونویسی یا حذف داده‌ها
بعضی از بدافزارها، واقعاً مخرب هستند. این گونه بدافزارها یا نصب نرم افزارها روی کامپیوترتان سریع می‌توانند فایل‌های ذخیره شده در دیسک سخت را پاک یا با اطلاعات غلط رونویسی کنند. به طوری که اطلاعات رونویسی یا حذف شده قابل بازیابی نباشند.
۲. نصب یک برنامه تروا
امروزه، این عملکرد بدافزارها خیلی رایج شده است. اگر روی رایانه‌تان برنامه‌ای نصب شده است که سیستم عامل استفاده زیادی از آن می‌کند، بدافزار می‌تواند به جای این برنامه، برنامه خود را جایگزین کند تا تاثیر مخربش را بگذارد.
- علاوه بر این، بدافزارها می‌توانند برنامه‌های دیگر را در سیستم‌تان نصب کنند تا در زمان از پیش تعیین شده نظیر زمان روشن شدن رایانه یا تاریخ خاص فعال و اجرا گردند.
۳. نرم افزارهای سریار
نرم افزارهای سریار^{۱۳}، نرم افزارهایی هستند که بدافزارها بر روی رایانه‌تان نصب می‌کنند و هنگامی که رایانه‌تان روشن می‌شود یا برنامه خاصی را اجرا می‌کنید، اجرا می‌شوند.
۴. ثبت کلیدهای تایپ شده
گاهی بدافزارها، نرم افزارهایی بر روی رایانه‌تان نصب می‌کنند که تمام کلیدهای تایپ شده را در فایلی ذخیره می‌کنند. این نرم افزارها، ثبت کننده کلید^{۱۴} نام دارند. فایلی که کلیدهای ثبت شده در آن ذخیره شده است، می‌تواند از طریق درب پستی مورد استفاده قرار گیرد یا از طریق پست الکترونیکی یا وب به نویسنده نرم افزار فرستاده شود. پس اگر در هنگامی که در وب شماره کارت اعتباری یا کلید عبور خود را تایپ می‌کنید و صفحه وب ایمن نباشد (اطلاعات در هنگام انتقال رمزگذاری نشود)، این برنامه هر چه را تایپ می‌کنید، دقیقاً ثبت می‌کنند. بنابراین، در هنگام تایپ شماره کارت اعتباری و کلمه عبور در صفحات وب دقت لازم را داشته باشید یا اگر صفحه وب علاوه بر صفحه کلید کامپیوترتان، صفحه کلید مخصوص به خود را طراحی نموده است که مکان کلیدها به طور تصادفی انتخاب می‌شوند، حتماً از این صفحه کلید استفاده کنید.



آشنایی با مبانی امنیت شبکه



فصل ۶ فایروال

فایروال (دیواره آتش)^{۱۴}، موانعی بین شبکه یا رایانه شخصی قابل اعتماد و اینترنت غیر قابل اعتماد است. به عبارت دیگر، فایروال، ابزاری است که کنترل دستیابی به سیستم محلی یا سیستم‌های شبکه را بنابر سیاست امنیتی تعریف می‌کند.

از لحاظ فنی، یک گره شبکه شامل نرم‌افزار و سخت‌افزاری است که شبکه خصوصی را از شبکه عمومی ایزوله می‌کند. در اینترنت، داده‌ها و درخواست‌های فرستاده شده از یک رایانه به دیگری به قسمت‌هایی به نام بسته^{۱۵} شکسته می‌شوند. هر بسته شامل آدرس اینترنتی رایانه فرستنده داده‌ها، آدرس اینترنتی رایانه گیرنده داده و حاوی اطلاعات دیگری است که بسته‌ها را از یکدیگر متمایز می‌کند. فایروال، همه بسته‌هایی که از آن عبور می‌کنند را بررسی می‌کند و سپس یکی از اعمال اجازه عبور یا اجازه عبور ندادن را با توجه به سیاست امنیتی تعریف شده می‌دهد. فایروال‌ها برای محافظت از موارد زیر طراحی شده‌اند:

۱. ورود از راه دور، وقتی فردی از راه دور به رایانه‌تان متصل می‌گردد و کنترل آن را به دست می‌گیرد، می‌تواند اطلاعات رایانه‌تان را خوانده یا تخریب نماید.
۲. درب‌های پشتی برنامه کاربردی، بعضی از برنامه‌ها می‌توانند امکان دسترسی از راه دور را فراهم کنند. در برخی از برنامه‌ها خطاهایی وجود دارد که یک درب پشتی (دسترسی مخفی) را فراهم می‌کند.
۳. همه بسته‌های ارسال شده از یک آدرس معینی متوقف شوند. گاهی اوقات شرکت‌ها از این روش برای مسدود کردن درخواست‌های رسیده از شرکت‌های رقیب استفاده می‌کنند.
۴. ویروس‌ها، مفهوم ویروس‌ها را قبلاً دیدید. برخی از فایروال‌ها از ورود ویروس‌ها به شبکه جلوگیری می‌کنند.
۵. هزینه‌ها، همان طور که بیان کردید، پست‌های الکترونیکی ناخواسته، هزینه هستند. هزینه‌ها می‌تواند خطرناک باشند، زیرا حاوی پیوند به سایت‌های خطرناک هستند.

^{۱۴} Firewall ^{۱۵} Packet



آشنایی با مبانی امنیت شبکه



۶. هر بسته‌ای که از بیرون می‌آید و آدرس رایانه درونی را دارد متوقف نماید. بعضی اوقات نفوذگر رایانه خود را به جای رایانه درون سازمان جا می‌زند. بنابراین، با این روش شرکت‌ها می‌توانند درخواست‌های این چنینی را مسدود کنند.

فایروال ممکن است دستگاهی سخت‌افزاری یا نرم‌افزاری نصب شده بر روی رایانه باشد. در هر حالت، فایروال در محل اتصال دو شبکه قرار می‌گیرد. یعنی، فایروال معمولاً بین شبکه محلی و عمومی (اینترنت) قرار می‌گیرد.

در شکل ۱-۶ فایروال و محل قرار گرفتن آن را مشاهده می‌کنید. برای آشنایی بهتر با مفهوم فایروال، چهار ناحیه^{۱۵} شکل ۱-۶ را در زیر می‌بینید:

۱. شبکه خصوصی^۱ (LAN) ، ناحیه‌ای است که فقط کارکنان و مدیران سازمان در آن قرار دارند. بنابراین، باید حفاظتی ایجاد گردد تا به جز کارکنان و مدیران سازمان افراد دیگر نتوانند از طریق اینترنت وارد این شبکه شوند و به منابع و داده‌های آن دسترسی داشته باشند.

۲. ناحیه بی‌طرف^۲ (DMZ) ، ناحیه‌ای از شبکه است که بین شبکه داخلی سازمان و شبکه خارجی (اینترنت) قرار دارد و این دو شبکه را از لحاظ فیزیکی جدا (ایزوله) می‌سازد. این ایزوله‌سازی با قوانین اعمال شده از طرف فایروال کنترل می‌گردد. به عنوان مثال، فرض کنید، سازمانی می‌خواهد وب سایت خود را اداره نماید. در پیکربندی DMZ، سازمان سرویس‌دهنده وبش را در شبکه‌ای قرار می‌هد تا عموم بتوانند به آن دسترسی داشته باشند و بقیه سرویس‌دهنده‌ها را در شبکه خصوصی قرار می‌دهد. سپس، فایروالی را پیکربندی می‌کند تا درخواست‌های رسیده از بیرون (عموم) را به سرویس‌دهنده مورد نظر هدایت نماید. در اکثر اوقات فایروال دومی، در دروازه ورود شبکه داخلی قرار می‌گیرد تا از ورود درخواست‌های نفوذگران به شبکه داخلی با تضمین بیشتری جلوگیری شود. در شکل ۲-۶ نمونه‌ای از ناحیه بی‌طرف (DMZ) را می‌بینید.

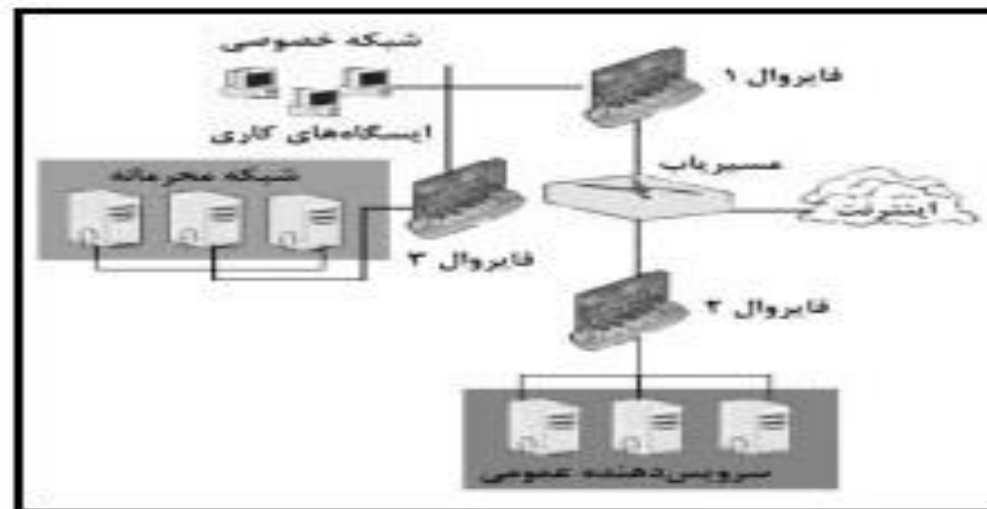
¹⁵ Zone ² Private Network ¹ Demilitarized Zone



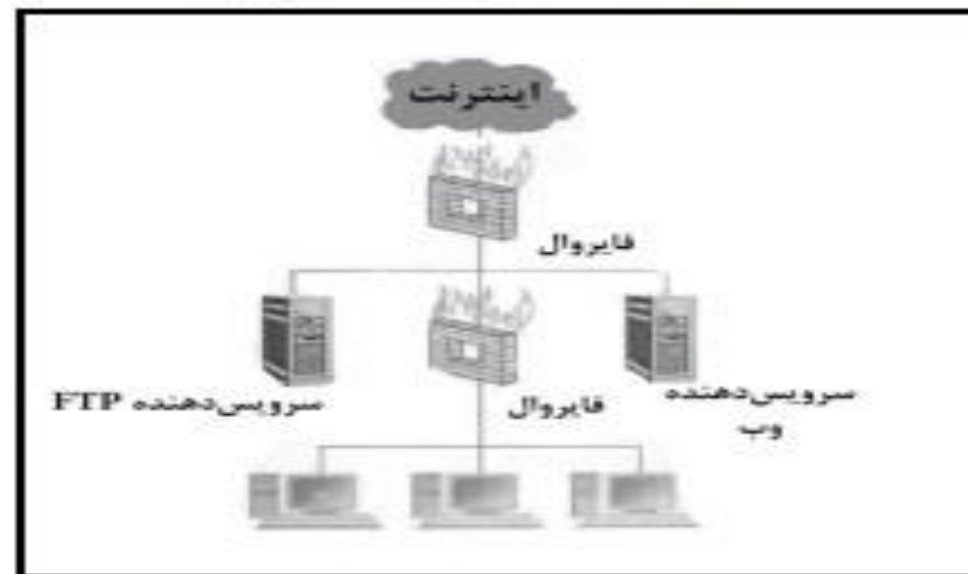
آشنایی با مبانی امنیت شبکه



۳۳



شکل ۱ - ۶ تاحیه‌های مختلف فایروال



شکل ۲ - ۶ نمونه‌ای از تاحیه بی طرف



آشنایی با مبانی امنیت شبکه



۲۴

پرداخت‌های الکترونیکی مانند پرداخت‌های سستی، مشکلاتی از قبیل احتمال کپی نمودن اسناد مالی دیجیتالی، احتمال ایجاد امضای دیجیتال جعلی یا الحاق اطلاعات هویتی شخص پرداخت‌کننده به تراکنش مالی را دارد. یک تاجر باید موارد بیان شده را در نظر بگیرد. سیستم انتخابی باید بالاترین سطح امنیتی را داشته باشد و در عین حال، نیازهای مشتریان را برآورده نماید. البته، ایجاد این امکانات وظیفه تاجر نیست، بلکه نهادهای سیاست‌گذار و مجری هر کشور باید بسترهای آن را فراهم کنند تا استفاده‌کنندگان در شرایط امن و قابل اعتماد بتوانند یکی از روش‌های پرداخت را انتخاب کنند.

از طرف دیگر، تراکنش‌های الکترونیکی و سایت‌ها ریسک‌های بازرگانی ایجاد می‌نمایند. مجرمان در هر نقطه دنیا خیلی بیشتر از گذشته اطلاعات کارت اعتباری، کلمه عبور حساب بانکی و دیگر اطلاعات شخصی را می‌دزدند. دامنه تهدیدات از حملات ترکیبی فرا مدون تا ضربه‌های جازدن فرودناوری تغییر می‌کنند. به همین دلیل، یک استراتژی امنیت تجارت الکترونیکی (شامل چندین لایه امنیتی) لازم است. این استراتژی امنیت تجارت الکترونیکی را به عنوان فرآیند جلوگیری و تشخیص استفاده غیر مجاز از نام تجاری، هویت، سایت، نام الکترونیکی، اطلاعات یا اموال با ارزش سازمان و تلاش برای کلاهبرداری از سازمان، مشتریان یا کارمندان آن سازمان می‌بیند. از اقدامات جلوگیری، برای جلوگیری از ورود کاربران غیر مجاز (نفوذ گران یا مهاجمان)، به هر بخشی از تجارت الکترونیک استفاده می‌شود. از اقدامات تشخیص جهت تشخیص، این که آیا نفوذ گران تلاش کردند وارد سیستم شوند یا این که موفق بودند، و این که چه کاری ممکن است انجام داده باشند، استفاده می‌شوند.

بخش مهم بهبود تجربه خریدار، اطمینان حاصل کردن از این است که خرید ایمن و بی‌خطر باشد. معمولاً هدف نهایی امنیت تجارت الکترونیک **تضمین اطلاعات**^۱ است. تضمین اطلاعات، محافظت سیستم‌های اطلاعاتی از دسترسی غیر مجاز یا تغییر اطلاعات در ذخیره، پردازش، انتقال، محافظت از انکار سرویس به کاربران مجاز، و اقدامات لازم برای تشخیص، مستند کردن و مقابله با تهدیدات می‌باشد.

در این فصل مطالبی درباره استراتژی‌های امنیتی تجارت الکترونیک، اقدامات جلوگیری و تشخیص و نیاز به رویکرد امنیتی دفاع کامل را می‌آموزید. به عنوان مثال، فایروال^۲ (دیوارهای آتش)

^۱. (IA = Information Assurance)

^۲. Firewall

^۳. Human Firewalls





آشنایی با مبانی امنیت شبکه



محافظ شبکه‌های بازرگانی نمی‌تواند از تمام حملات جلوگیری کند. اگر شرکت فایروال‌های انسانی^۲ نداشته باشد (فایروال‌های انسانی، دسترسی کارمندان به اسناد حیاتی بازرگانی را محدود می‌کنند و سیاست‌های سخت‌گیر امنیتی را اجرا نمایند) نمی‌تواند امنیت را به طور کامل اجرا نماید. شرکت‌ها، علاوه بر چندین لایه دفاعی به چندین لایه بازایی نیز نیاز دارند.

بنابراین در این فصل به مفاهیم امنیت و روش‌های ایجاد آن در تجارت الکترونیک می‌پردازیم.

۱-۷. لایه سوکت امن (SSL)

تکنولوژی SSL^۱ اساس وب گسترده جهانی^۲ امن را تشکیل می‌دهد. لایه سوکت امن، پروتکلی است که از گواهی‌های استاندارد جهت احراز هویت و رمزنگاری داده استفاده می‌کند تا اطمینان از محرمانگی داده را ایجاد کند. امروزه، یکی از پروتکل‌های اصلی در حال استفاده برای ایمن‌سازی تجارت الکترونیک SSL می‌باشد که به عنوان امنیت لایه انتقال (TLS)^۳ نیز شناخته می‌شود.

SSL، توسط شرکت نت‌اسکیپ تولید گردید تا از گواهی استاندارد جهت احراز هویت و رمزگذاری داده برای اطمینان از محرمانگی داده استفاده گردد. SSL، استاندارد اصلی مورد استفاده پرداخت‌های کارت اعتباری است. یعنی، SSL رمزگذاری شماره‌های کارت اعتباری و دیگر انتقال‌های بین سرویس‌دهنده وب و مرورگر وب را امکان‌پذیر می‌نماید. در مورد تراکنش‌های کارت اعتباری، جهت خرید در وب، باید کارهای دیگری علاوه بر دادن شماره کارت به فروشنده انجام گردد. برخی از این کارها عبارت‌اند از:

۱. اعتبار شماره باید بررسی گردد.
 ۲. بانک مشتری باید به مشتری اجازه دهد تا فرآیند خرید انجام شود.
- SSL، به جز انتقال شماره کارت، هیچ یک از اعمال بیان شده را مدیریت نمی‌کند. مهمترین اجزای پروتکل SSL، جلسه SSL و اتصال SSL هستند که به صورت زیر تعریف می‌شوند:
- ☒ اتصال، انتقالی است (در مدل لایه‌بندی OSI) که یک سرویس مناسب را فراهم می‌کند در SSL اتصالات نقطه به نقطه و گذرا هستند هر اتصال تنها به یک جلسه متصل می‌شود.
 - ☒ جلسه، جلسه SSL ارتباطی بین یک کلاینت و یک سرور است. جلسات با پروتکل دست دادن^۴ تولید می‌شوند، جلسات پارامترهای امنیت رمزگذاری را تعریف می‌کنند که بین اتصالات به صورت مشترک استفاده می‌شود. جهت ایجاد هر جلسه به پارامترهایی نیاز است که به صورت زیر می‌بینید:
 - ☒ شناسه جلسه^۵، رشته دلخواه یکتایی که توسط سرور برای تعیین جلسه قابل استفاده انتخاب می‌شود.
 - ☒ گواهی گره^۶، گواهی x509.V3 مربوط به طرف اتصال که می‌تواند تهی باشد.

¹. Secure Socket Layer ². WWW (World Wide Web) ³. Transport Layer Secure
⁴. Hand Shaking ⁵. Session Identifier ⁶. Peer Certificate



آشنایی با مبانی امنیت شبکه



- ❑ روش فشرده‌سازی، الگوریتمی که برای فشرده‌سازی قبل از رمزگذاری استفاده می‌شود.
- ❑ مشخصات رمز، شامل الگوریتم رمزگذاری از قبیل AES و الگوریتم درهم‌سازی از قبیل SHA-1 است.
- ❑ کلید اصلی، کلید ۶۴ بیتی که بین دو طرف (کلاینت سرور) مشترک است.
- ❑ پرچم ادامه^{۱۸}، پرچمی که نشان‌دهنده این است که جلسه می‌تواند بین دو اتصال جدید استفاده شود یا خیر.

پارامترهای مورد نیاز در یک اتصال را به صورت زیر می‌بینید:

- ❑ اعداد تصادفی انتخاب شده در دو طرف اتصال.
- ❑ کلید استفاده شده برای محاسبه MAC در سرور
- ❑ کلید مشابه در طرف کارفرما
- ❑ کلید متقارن رمزگذاری داده توسط سرور
- ❑ کلید مشابهی در طرف کارفرما
- ❑ بردار اولیه برای رمز در حالت CBC

شماره سریال، هر طرف یک شماره سریال دارد که حداکثر ۱ - ۲^{۳۲} است.

۲-۷. تراکنش الکترونیکی امن

تراکنش الکترونیکی امن (SET)^۲، یک رمزگذاری از دو مشخصات امن است که برای تامین امنیت تراکنش‌های کارت اعتباری در اینترنت طراحی گردید. نسخه اولیه SET، ناشی از فراحوانی استاندارد امنیتی توسط شرکت‌های ویزا کارت و مستر کارت در فوریه ۱۹۹۶ می‌باشد. شرکت‌های متعددی از قبیل JBM مایکروسافت، نتاسکیپ، RSA و غیره در ایجاد مشخصات اولیه SET نقش داشته‌اند و تست‌های متعددی روی آن انجام دادند تا در سال ۱۹۹۸ اولین محصول سازگار با SET ارائه گردید.

برخلاف اشتباه بعضی‌ها، SET یک سیستم پرداخت نیست، بلکه یک سری از پروتکل‌های استاندارد و فرمت‌های امنیتی است تا کاربران را قادر سازد، زیرساخت‌های پرداخت کارت اعتباری موجود را روی شبکه‌های نظیر اینترنت استفاده کنند. در اصل SET سه سرویس زیر را فراهم می‌نماید:

- ❑ **محرمانگی اطلاعات**، چون کانال امنی بین شرکت‌کنندگان در تراکنش فراهم می‌کند، بنابراین، محرمانگی برقرار می‌شود. یعنی، اطلاعات پرداخت و حساب صاحب کارت، در هنگام انتقال در شبکه دارای امنیت است. زیرا، مانع از این می‌گردد که بازرگانان، شماره کارت اعتباری صاحب کارت

¹⁸.Is presumable ².Secure Electronic Transaction



آشنایی با مبانی امنیت شبکه



را ببینند. این اطلاعات فقط در اختیار صادرکننده کارت می‌باشد. SET، برای تامین محرمانگی از رمزگذاری DES استفاده می‌نماید.

تعمیم داده‌ها (جامعیت)، اطلاعات پرداخت از قبیل اطلاعات سفارش، داده‌های شخصی، و دستورالعمل‌های پرداخت از صاحبان کارت به فروشندگان فرستاده می‌شود. SET، از طریق امضای دیجیتال RSA و با کدهای درهم سازی SHA-1 تعمیم پیام را در هنگام انتقال تامین می‌کند. یعنی، تضمین می‌کند اطلاعات در هنگام انتقال تغییر نمی‌یابند.

احراز هویت، سرویس احراز هویت SET دو نوع احراز هویت را انجام می‌دهد که عبارت‌اند از:
۱. احراز هویت بازرگان (فروشنده)، صاحب کارت را قادر می‌سازد تا اثبات نماید که فروشنده یا موسسه مالی‌ای که اجازه می‌دهد کارت‌های اعتباری پرداخت را بپذیرد.

۲. احراز هویت صاحب کارت، فروشنده را قادر می‌سازد تا بررسی نماید آیا صاحب کارت، کاربر قانونی شماره حساب کارت اعتباری است یا خیر.

SET، برای تامین هر دو نوع احراز هویت از گواهی نامه‌های دیجیتال X.509V3 با امضای دیجیتال RSA بهره می‌گیرد.

تجارت الکترونیک امن (SET) رمزگذاری باز بوده و امنیتی را برای دو طرف ارتباط تعیین می‌کند که برای محافظت از تراکنش‌های کارت اعتباری در اینترنت طراحی شده است. SETV1 از یک تماس برای استاندارد امنیتی توسط کارت اعتباری و ویزا در فوریه سال ۱۹۹۶ پدید آمده است. حوزه وسیعی از شرکت‌ها از قبیل IBM، مایکروسافت، نتاسکیپ، RSN با این تکنولوژی سروکار دارند.

در آغاز سال ۱۹۹۶ آزمایشات متعددی انجام شد تا در سال ۱۹۹۸ اولین موج محصولات ترکیبی SET بوجود آمدند.



آشنایی با مبانی امنیت شبکه



امنیت شبکه و اطلاعات توسط سرویس‌ها و برنامه‌های کاربردی تامین می‌شود. هر یک از بخش‌های شبکه برای تامین امنیت از سرویس‌ها و برنامه‌های کاربردی مخصوص به خود استفاده می‌کنند. بنابراین، در این فصل، برخی از سرویس‌ها و برنامه‌های کاربردی امنیت شبکه را می‌آموزیم. این سرویس‌ها و برنامه‌های کاربردی عبارت‌اند از:

۱. سرویس‌های امنیت پست الکترونیک
۲. امنیت معماری IP
۳. سرویس‌های کنترل دسترسی داده
۴. سیستم زیست‌سنجی
۵. احراز هویت
۶. مدیریت شبکه آسان (SNMP)

۸-۱. سرویس‌های امنیت پست الکترونیک

امروزه سازمان‌ها برای ارسال داده‌ها و نامه‌ها از پست الکترونیک استفاده می‌کنند تا در زمان و هزینه صرفه‌جویی نمایند. بنابراین، باید امنیت داده‌های ارسالی و محرمانه ماندن محتویات آن‌ها مورد توجه ویژه‌ای قرار گیرد. اکثر کاربران سرویس احراز هویت را جهت محرمانه ماندن پیام-هایشان به کار می‌برند. دو ابزار مهم برای ایمن نگه داشتن پست الکترونیک وجود دارد:

۱. سرویس PGP¹⁹
۲. سرویس S/MIME²⁰

¹⁹.Pretty Good Privacy ²⁰. Secure/ Multipurpose Internet Mile Extension



آشنایی با مبانی امنیت شبکه



۱-۱-۸. سرویس PGP

سرویس PGP توسط آقای فیل زیمرمان ارائه گردید. این سرویس قابلیت اعتماد و سرویس احراز هویت که در برنامه‌های پست الکترونیک و ذخیره فایل استفاده می‌شود را فراهم می‌کند. اهداف سرویس PGP عبارت‌اند از:

- 1. برای ایجاد بلوک‌ها از بهترین الگوریتم‌های رمزگذاری استفاده شود.
 - 2. الگوریتم‌های مورد استفاده در قالب یک برنامه کاربردی مجتمع شوند و با مجموعه‌ای دستورات ساده بتوان از آنها استفاده کرد.
 - 3. در قالب یک بسته نرم‌افزاری به همراه مستندات که کد برنامه را نیز شامل می‌شود به سادگی از طریق اینترنت، تابلوی اعلانات و شبکه تجاری از قبیل AOL²⁰ قابل دسترسی باشد.
 - 4. با هر نسخه‌ای سازگاری داشته و کم هزینه باشد.
- سرویس PGP خیلی سریع گسترش یافت و مورد استفاده قرار گرفته است. زیرا، این سرویس به طور رایگان قابل دسترس بوده و روی سیستم عامل‌های مختلفی از قبیل ویندوز، یونیکس، مکینتاش و بسیاری دیگر قابل اجرا است.

نماد	توضیح
K_u	کلید جلسه استفاده شده در الگوریتم‌های متقارن.
PR_u	کلید خصوصی کاربر A.
PU_u	کلید عمومی کاربر A.
EP	رمزگذاری کلید عمومی (نامتقارن).
DP	رمزگشایی کلید عمومی (نامتقارن).
EC	رمزگذاری متقارن.
DC	رمزگشایی متقارن.
H	تابع درهم‌ساز.
	الحاق (بهم چسباندن) ²¹ .
Z	فشرده‌سازی یا استفاده از الگوریتم ZIP.
R64	تبدیل قالب radix64 به ASCII.

²⁰America on Line

²¹.Concatenation



آشنایی با مبانی امنیت شبکه



۴۰

در این سرویس، از الگوریتم‌های رمزگذاری کلید عمومی متقارن قوی و معروفی از قبیل DES، RSA، IDEA، CAST-128 و SHA-1 استفاده شده است و در حوزه وسیعی از برنامه‌ها قابل استفاده است. به خصوص سازمان‌هایی که از یک استاندارد برای رمزگذاری فایل‌ها و پیام‌های محرمانه به افراد استفاده می‌کنند. این سرویس، توسط دولت بخصوصی طراحی و کنترل نمی‌شود. جهت توصیف عملکرد سرویس PGP ابتدا باید نمادهای آن را بشناسیم. این نمادها در جدول ۸-۱ آمده‌اند.

PGP، سرویس‌های متعددی ارائه می‌کند که آن‌ها را در جدول ۲-۸ می‌بینید.

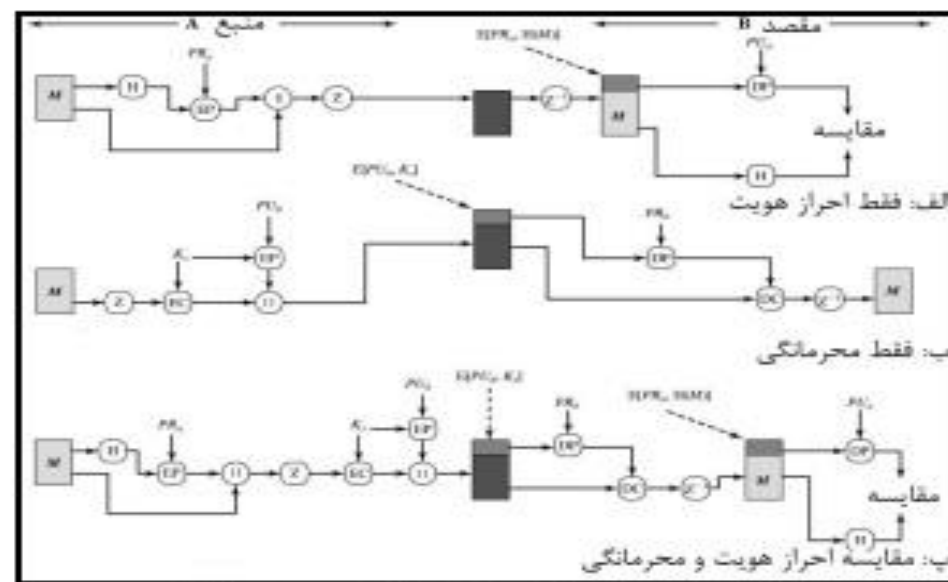
توضیح	الگوریتم	تابع
کد درهم‌ساز خلاصه پیام یا استفاده از الگوریتم SHA-1 ایجاد می‌شود. خلاصه پیام یا استفاده از DSS یا RSA یا کلید خصوصی فرستنده رمزگشایی شده و خلاصه پیام به همراه پیام ارسال می‌شود.	DSS/ SHA RSA/SHA یا	امضای دیجیتال (Digital Signature)
پیام توسط فرستنده رمزگذاری می‌شود. کلید جلسه با استفاده از RSA یا کلید عمومی گیرنده به همراه پیام رمزگذاری می‌شود.	CAST IDEA یا DES یا گانه یا RSA	رمزگذاری پیام (Message Encryption)
ممکن است پیام جهت ذخیره‌سازی یا انتقال با الگوریتم ZIP فشرده‌سازی شود.	ZIP	فشرده‌سازی (Compression)
جهت فراهم کردن شفافیت در برنامه‌های پست الکترونیکی، پیام رمزگذاری شده باید توسط تبدیل Radix64 به رشته اسکی تبدیل شود.	تبدیل Radix64	سازگاری با پست- الکترونیک (Email) (Compatibility)
جهت غلبه بر محدودیت‌های حداکثر اندازه پیام، PGP پیام را تکه‌تکه کرده و سپس، در مقصد مجتمع می‌کند.		تقسیم و ترکیب (Segmentation)

در شکل ۸-۱ فرآیند ایجاد احراز هویت و محرمانگی را در سرویس PGP می‌بینید.





آشنایی با مبانی امنیت شبکه



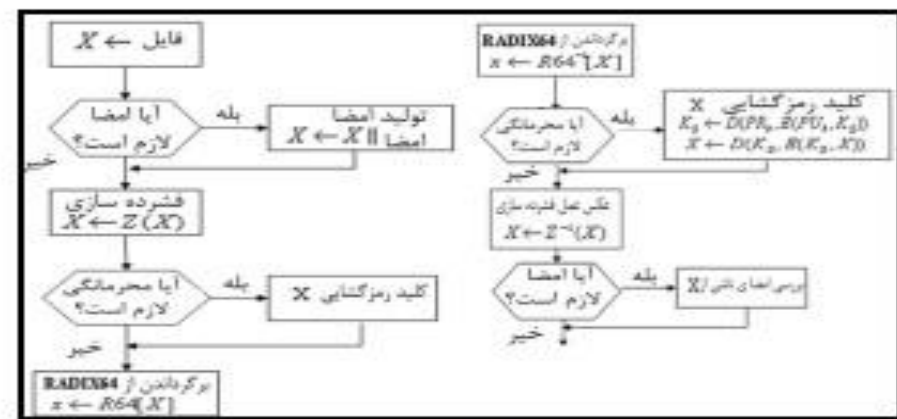
شکل ۱-۸ ایجاد احراز هویت و محرمانگی در سرویس PGP.

روند ایجاد این سرویس به صورت زیر است:

۱. فرستنده پیام را تولید می کند.
 ۲. تابع SHA-1 برای ایجاد خلاصه پیام 160 بیتی استفاده می شود.
 ۳. کد درهم توسط RSA و یا استفاده از کلید خصوصی فرستنده رمزگذاری شده و نتیجه به پیام اضافه می شود.
 ۴. گیرنده با استفاده از RSA و کلید عمومی فرستنده خلاصه پیام را رمزگشایی و بازیابی می کند.
 ۵. گیرنده، خلاصه پیام جدیدی از پیام ایجاد کرده و آن را با خلاصه پیام رمزگشایی شده مقایسه می کند. اگر باهم برابر بودند، پیام به عنوان پیام معتبر پذیرفته می شود.
- به هنگام ارسال و دریافت پیام در سرویس PGP چهار سرویس PGP که قبلاً دیدید با هم ارتباط برقرار می کنند. این ارتباط را در شکل ۲-۸ می بینید.



آشنایی با مبانی امنیت شبکه



شکل ۲-۸ فرآیند ارتباط چهار سرویس اصلی PGP با یکدیگر.

هنگام انتقال اگر لازم باشد، امضا یا استفاده از خلاصه پیام متن غیر فشرده تولید می شود. آن-گاه، پیام به همراه امضا فشرده می شود. سپس، اگر قابلیت اعتماد نیاز باشد، بلوک (متن فشرده شده یا امضای فشرده شده به همراه پیام) رمزگذاری شده و با کلید رمزگذاری متقارن رمزگذاری شده کلید عمومی به پیام اضافه می شود. در پایان، کل بلوک به قالب Radix 64 تبدیل می شود. هنگام دریافت پیام، بلوک دریافتی ابتدا از فرمت Radix64 به فرمت باینری تبدیل می شود. آن گاه، بلوک حاصل از حالت فشرده خارج می شود. اگر پیام امضا شده بود، گیرنده، خلاصه پیام انتقالی را بازیابی کرده و آن را با خلاصه پیام محاسبه شده خود مقایسه می کند. در صورت تطابق، پیام تصدیق می شود.

۲-۱-۸. سرویس توسعه پست الکترونیکی چند منظوره (S/MIME)

سرویس S/MIME، برای افزایش امنیت به استاندارد قالب پست الکترونیکی طراحی گردید که براساس تکنولوژی امنیت داده RSA عمل می کند. گرچه، هم PGP و هم S/MIME براساس استاندارد IETF هستند، اما S/MIME به عنوان استاندارد صنعتی برای استفاده تجاری و سازمانی به کار می رود، درحالی که PGP، برای امنیت پست الکترونیکی شخصی کاربران استفاده می شود. S/MIME از دو استاندارد RFC822 و MIME استفاده می کند. شرح این دو استاندارد

را در زیر می بینید:
استاندارد RFC822



آشنایی با مبانی امنیت شبکه



RFC822. قالبی برای پیام‌های متنی که از طریق پست الکترونیک ارسال می‌شوند. تعریف می‌کند. در این استاندارد، قالب پیام و محتوی آن به صورت بسته است. یک بسته شامل اطلاعات مورد نیاز برای ارسال و دریافت است. محتویات شامل اطلاعاتی است که باید به گیرنده تحویل داده شود.

RFC822. فقط برای امنیت محتویات به کار می‌رود. پس، استاندارد محتویات شامل مجموعه‌ای از فیلدهای سرآیند است که توسط سیستم پست جهت ایجاد بسته استفاده می‌شوند و این استاندارد جهت آسان نمودن فهم پیام توسط برنامه‌ها استفاده می‌شود. سرآیند شامل تعدادی کلمات کلیدی است که با کاراکتر ":" از هم جدا می‌شوند. کلیدهای اصلی از سرآیند شامل From, TO, Subject و Date می‌باشند.

مثال: پیام زیر با استفاده از استاندارد RFC822 ایجاد می‌شود:

Date : Tue, 16/04/2010 Time : 14 : 20 : 17 pm

From : "fanavarie novin"

Subject : RFC822

TO : "Ramazan Abbasnezhad"

Hello. This is a Sample of RFC822 Standard That is Sent For you.

استاندارد MIME

این استاندارد برای رفع محدودیت‌های RFC822 تحت پروتکل انتقال SMTP طراحی گردید. برخی از محدودیت‌های SMTP/822 را در زیر می‌بینید:

۱. SMTP قادر به عبور فایل‌های اجرایی یا اطلاعات دودویی نمی‌باشد. برای رفع این مشکل باید از راهکارهای Unencode / Undecode استفاده نمود.
۲. SMTP داده‌های متنی که شامل کاراکترهای زبان ملی هستند را عبور نمی‌دهد. چون، این کاراکترها به صورت کدهای ۸ بیتی با ارزش ۱۲۸ دسیمال یا بالاتر نشان داده می‌شوند. ولی، SMTP تا ۷ بیت اسکی محدود شده است.
۳. سرورهای SMTP ممکن است پیام‌های بزرگتر از یک طول معین را قبول نکنند.
۴. SMTP پیاده‌سازی یکسانی را براساس استاندارد RFC821 از قبیل حذف، اضافه، شکستن، حذف فاصله و Tab را بین خطوط و کاراکترها انجام نمی‌دهد.

²¹ Simple Mile Transfer Protocol



آشنایی با مبانی امنیت شبکه



۴۴



استاندارد MIME برای رفع این مشکلات طراحی شد. این استاندارد از مولفه‌های زیر تشکیل شده است:

- ❑ پنج فیلد جدید در سرآیند پیام تعریف می‌شوند. این فیلدها، اطلاعاتی در مورد بدنه پیام ایجاد می‌کنند.
- ❑ تعدادی قالب‌بندی محتوی تعریف می‌شوند که از طریق آن‌ها پست الکترونیک چند رسانه‌ای استاندارد می‌شود (ارسال صدا، فیلم، تصویر).
- ❑ کدگذاری‌های محتوی تعریف می‌شوند تا تبدیل هر قالب‌بندی محتوی، به شکلی که از حذف توسط سیستم پست محافظت شوند، ممکن شود.
- ❑ پنج فیلد سرآیند در MIME به صورت زیر تعریف می‌شوند:
- ❑ نسخه MIME²²، مقدار آن حتماً باید 0 و 1 باشد. این فیلد نشان دهنده این است که پیام با RFC2045 و RFC2046 مطابقت دارد.
- ❑ نوع محتوی¹، محتوی داده‌های جزئی در مورد نوع محتوی پست الکترونیک است، به طوری که قابل شناسایی باشد.
- ❑ کدگذاری روی محتوی²، نوع کدگذاری که بدنه پیام را نشان می‌دهد، به طوری که پیام قابل انتقال باشد.
- ❑ شناسه محتوی³، جهت شناسایی عناصر MIME به صورت یکتا در مواقعی که چند قطعه هم زمان در یک پیام درج شده باشند، تعریف می‌شود.
- ❑ توصیف محتوی⁴، نوع محتوی پیام را توصیف می‌کند. این فیلد وقتی که پیام قابل خواندن نیست (مانند پیام صوتی)، قابل استفاده است.
- ❑ جدول ۳ - ۸ محتوی استفاده شده در MIME را نشان می‌دهد.
- ❑ یک مثال از محتوی چند قسمتی (Multipart) را در زیر می‌بینید:

```

From : Nathaniel Boreenstein
To : Ned Freed
Subject : Sample Message
MIME - Version 10
Content -type : multipart / mixed ; boundary = " Simple boundary"
This is The preamble. It is to be ignored, Though it is a handy place for mail
Composers to include an explanatory note to non-MIME Conformant readers.
Simple boundary
This is implicitly typed plain ASCII text.
It does NOT end with a linebreak.
Simple boundary

```

²²MIME-version ².Content-type ³.Content-Transfer-Encoding
⁴.Content-ID ⁵.Content-Description



آشنایی با مبانی امنیت شبکه



Content-type : text / plain: Charest = us-ascii
This is explicitly typed plain ASCII text.
It Does end with linebreak.
Simple boundary
This is the epilogue. It is also to be ignored.

جدول ۳-۸. محتوی استفاده شده در MIME

توصیف	زیرنوع	نوع
متن قالببندی نشده، که ممکن است اسکی یا ISO8859 باشد.	Plain	Text
العطاف‌پذیری بیشتری برای قالببندی فراهم می‌شود.	Enriched	
قسمت‌های متفاوت مستقل هستند، اما با هم عبور داده می‌شوند. این قسمت‌ها باید با همان ترتیب اولیه به گیرنده تحویل داده شوند.	Mixed	Multipart
تنها تفاوت آن با mixed این است که ترتیب در دریافت بخش‌های پیام رعایت نمی‌شود.	Parallel	
قسمت‌های مختلف نسخه‌های دیگر از همان اطلاعات هستند و طوری مرتب شده‌اند که مثل همان حالت اولیه بوده و باید به بهترین نسخه به گیرنده نشان داده شوند.	Alternative	
همانند mixed است. اما، نوع / زیر نوع پیش فرض هر بخش از پیام RFC822 است.	Digest	Message
بدنه آن به صورت پیامی است که در بسته‌ای قرار داده شده است که با RFC822 مطابقت دارد.	RFC822	
جهت صدور اجازه قطعه شدن پست‌های بزرگ به صورتی که برای گیرنده شفاف باشد.	Partial	
از اشاره‌گری به یک شیء که در محل دیگری قرار دارد، تشکیل شده است.	External body	Image
تصویر یا قالببندی JPEG و کدگذاری JFIF است.	jpeg	
تصویری با قالببندی GIF است.	gif	
قالب MPEG است.	Mpeg	Video
کانال ۸ بیتی ISDN که با قانون M با نرخ نمونه‌برداری 8KHZ رمزگذاری شده است.	Basic	Audio
Adobe PostScript	Postscript	Application
داده‌های دودویی عمومی شامل بایت‌های A بیتی است.	Octet-Stream	



آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)



مدرس: علی رضا تاجی



منابع

۱. عباس نژادورزی، رمضان، عباس نژادورزی، یوسف، "تجارت الکترونیکی" (چاپ اول)، فناوری نوین، ۱۳۸۹.
۲. علاءالدین، حمیده، "امنیت در یادگیری الکترونیکی" (چاپ اول)، دانشگاه علوم کشاورزی و منابع طبیعی گرگان، ۱۳۸۸.
۳. بختیاری، شهرام، قاضی مغری، سعید، "اصول امنیت سیستم‌ها و شبکه‌های رایانه‌ای"، موسسه انتشارات علمی، (چاپ اول)، ۱۳۸۵.
۴. صفایی کوچکسرای، فاطمه، اکبری، احمد، "تبعات هرزتماس‌ها و ضرورت استفاده از مکانیزم‌های ضد هرزتماس در سیستم‌های صوتی اینترنت"، اولین کنفرانس دانشجویی فناوری اطلاعات ایران دانشگاه کردستان، ۱۳۸۹.

5. William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall, 2005.
6. Vense Hassler, "Security Fundamentals For E-Commerce ",Atrech House".
7. Efraim Turban, Divid king, judy mckay / peter marshall, jae lee, Dennis Viehland, "Electronic commerce a Managerial Perspective 2008, Prentice Hall".
8. William Stallings , "Cryptography and network Security principles and practices", Fifth Edition, prantice Hall, 2008.
9. Chris McNab " Network Security Assessment", O'Reilly, 2004.
10. Fred Piper and Sean Murphy . "Cryptography: A Very Short Introduction", Oxford University Press.2002.
11. JoAnn Ward, "Caesar Ciphers: An Introduction to Cryptography", Purdue University GK-12, 2006-07.
12. Matt Bishop, "Computer Security: Art and Science", Addison Wesley, 2002.
13. WWW. Purde.edu/df/gk12/downloads/Cryptography.pdf
14. WWW.Math.Cudenver.edu
15. WWW.CS.berkeley.edu
16. WWW.CS.Trinconn.edu