آشنایی با
مبانی امنیت شبکه(امنیت اطلاعات)

تالیف:

مهندس رمضان عباس‌نژادورزی
مهندس آتنا فرجی

فن‌آوری نوین

سرشناسه	: عباس‌نژادورزی، رمضان، ۱۳٤۸-
عنوان و نام پدیدآور	: آشنایی با مبانی امنیت شبکه(امنیت اطلاعات) / تالیف رمضان عباس‌نژادورزی، آتنا فرجی
مشخصات نشر	: بابل:فن‌آوری نوین، ۱۳۸۹
مشخصات ظاهری	: ۱۹۲ ص. مصور ، جدول.
شابک	: ۶۰۰۰۰ ریال:۹۷۸٦۰۰۹۱٤۱۳۸۸
وضعیت فهرست نویسی	: فیپا
یاداشت	: کتابنامه
موضوع	: شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع	: کامپیوترها—ایمنی اطلاعات
شناسه افزوده	: فرجی، آتنا، ۱۳٦۱-
رده بندی کنگره	: ۱۳۸۹ ٥ آ۲ع/TK٥۱۰٥/٥۹
رده بندی دیویی	: ۰۰٥/۸
شماره کتابشناسی ملی	: ۲۱۸۴۶۶۸

فن‌آوری نوین www.fanavarienovin.net
بابل، کدپستی ٤۷۱٦۷-۷۳٤٤۸ تلفن: ۲۲۵٦٦۸۷-۰۱۱۱

آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)

تألیف: مهندس رمضان عباس‌نژادورزی – مهندس آتنا فرجی

نوبت چاپ: چاپ اول

سال چاپ: زمستان ۱۳۸۹

شمارگان: ۱۰۰۰ جلد

قیمت: ٦۰۰۰ تومان

نام چاپخانه و صحافی: فرنگاررنگ

شابک: ۸- ۸- ۹۱٤۱۳ - ٦۰۰ - ۹۷۸

نشانی ناشر: بابل، چهارراه نواب، کاظم‌بیگی، جنب حسینیه منصور کاظم‌بیگی، طبقه همکف

طراح جلد: کانون آگهی و تبلیغات آبان (احمد فرجی)

تهران، خ اردیبهشت، نبش وحید نظری، پلاک ۱٤۲ تلفکس: ٦٦٤۰۰۲۲۰-٦٦٤۰۰۱٤٤

فهرست مطالب

فصل پنجم: بد افزار

فصل ششم: فایروال

فصل هفتم: امنیت در تجارت الکترونیک

فصل هشتم: سرویس‌ها و برنامه‌های کاربردی امنیت اطلاعات

مقدمه

امروزه اینترنت و یکی از مهم‌ترین مدل‌های ارتباطی در آن، یعنی شبکه جهانی وب (World Wide Web)، تغییرات اساسی در زندگی و روابط بین انسان‌ها ایجاد کرده است. به طوری که در عصر اطلاعات، فعالیت‌هایی از قبیل اطلاع رسانی، کسب و کار و تجارت، مدیریت و غیره به صورت مجازی انجام می‌شوند. فضای مجازی، در معرض چالش‌ها، آسیب‌ها و تهدیدهای مختلفی از قبیل تخریب اطلاعات، جاسوسی، خراب‌کاری، نقض حریم خصوصی، حملات انکار سرویس و دسترسی غیرمجاز می‌باشد. از طرف دیگر، کلیه کاربردهای فناوری اطلاعات مانند دولت الکترونیک، کسب‌وکار الکترونیک، تجارت الکترونیک، بانکداری الکترونیک، سلامت الکترونیک و دیگر کاربردها نیاز به زیرساخت اینترنت و شبکه‌های کامپیوتری دارند.

بی‌شک هیچ یک از این کاربردها بدون وجود امنیت نمی‌توانند مورد استفاده قرار گیرند. ایجاد امنیت در شبکه‌های کامپیوتری و اینترنت به امر خطیری تبدیل شده است، به طوری که در رشته‌های فناوری اطلاعات (IT) و فناوری اطلاعات و ارتباطات (ICT) درسی به نام **آشنایی با مبانی امنیت شبکه** تدوین شده است.

کتاب حاضر براساس سال‌ها تجربه در زمینه تالیف کتب دانشگاهی و تدریس طراحی گردید. این کتاب براساس سر فصل جدید وزارت علوم، تحقیقات و فناوری اطلاعات برای درس‌های آشنایی با مبانی امنیت شبکه، امنیت اطلاعات و امنیت شبکه در رشته‌های IT و ICT تدوین شده است.

در پایان امیدواریم این اثر نیز مورد توجه اساتید و دانشجویان عزیز قرار گیرد.

از تمامی عزیزانی که در جمع‌آوری این اثر ما را یاری نمودند، صمیمانه تشکر می‌کنیم.

بابل، زمستان۱۳۸۹

مولفین

دیگر آثار مولف			
نام کتاب	انتشارات	نام کتاب	انتشارات
حل مسائل C (مرجع کامل)	فن آوری نوین	آموزش گام به گام Crystal Report	علوم رایانه
حل مسائل C++ (مرجع کامل)	فن آوری نوین	آشنایی با شبکه GSM	علوم رایانه
آموزش گام به گام برنامه نویسی بانک اطلاعات با C# (مرجع کامل)	فن آوری نوین	آموزش گام به گام سیستم عامل لینوکس	علوم رایانه
حل مسائل C# (مرجع کامل)	فن آوری نوین	خود آموز اکسس	علوم رایانه
حل مسائل پاسکال (مرجع کامل)	فن آوری نوین	آموزش گام به گام Word	علوم رایانه
آموزش گام به گام برنامه نویسی بانک اطلاعات با ویژوال بیسیک‌نت (مرجع کامل)	فن آوری نوین	آموزش گام به گام اکسل	علوم رایانه
آموزش گام به گام برنامه نویسی LINQ با C# (مرجع کامل)	فن آوری نوین	ICDL مهارت ۱: مفاهیم پایه اطلاعات	علوم رایانه
تجارت الکترونیکی	فن آوری نوین	ICDL مهارت۲: به کارگیری کامپیوتر و مدیریت	علوم رایانه
آموزش گام به گام برنامه ویژوال بیسیک	علوم رایانه	ICDL مهارت۳: واژه پردازی به کمک کامپیوتر	علوم رایانه
آموزش گام به گام برنامه ویژوال بیسیک‌نت	علوم رایانه	ICDL مهارت٤: صفحات گسترده	علوم رایانه
برنامه نویسی به زبان اسمبلی	علوم رایانه	ICDL مهارت٥: پایگاه داده	علوم رایانه
برنامه نویسی با دلفی	علوم رایانه	ICDL مهارت٦: ارائه مطلب	علوم رایانه
آموزش گام به گام دلفی‌نت	علوم رایانه	ICDL مهارت۷: اطلاعات و ارتباطات	علوم رایانه
آموزش گام به گام C#.NET	علوم رایانه	آموزش گام به گام FLASH MX	علوم رایانه
آموزش گام به گام VisualC++.NET	علوم رایانه	درس و کنکور برنامه‌نویسی به زبان C	علوم رایانه
آموزش گام به گام برنامه نویسی با ویژوال C++	علوم رایانه	برنامه سازی سیستم	علوم رایانه
آموزش گام به گام J#.NET	علوم رایانه	پرسش‌های چهار گزینه‌ای پاسکال	علوم رایانه
آموزش گام به گام SQL Server	علوم رایانه	آموزش گام به گام VC++	علوم رایانه
آموزش گام به گام SQL	علوم رایانه	کارور رایانه ۱	علوم رایانه
رهیافت و پرسش‌های چهار گزینه‌ای C	علوم رایانه	کارور رایانه ۲	علوم رایانه
رهیافت و پرسش‌های چهار گزینه‌ای C++	علوم رایانه	مبانی فناوری اطلاعات	علوم رایانه
تست و پرسش‌های چهار گزینه‌ای C	علوم رایانه		

فصل ۱ 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 پست‌الکترونیک[1] به جای ارسال نامه‌ها از طریق اداره پست استفاده می‌کنند. پست‌الکترونیک 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 پست‌الکترونیک شبیه به پست نمودن نامه بدون پاکت است. بنابراین، اگر فردی بخواهد پیام شخصی یا اطلاعات محرمانه را از طریق پست‌الکترونیک 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 رمزشده (کدشده) به دست فرد دیگری (به جزگیرنده) برسد، آن فرد با خواندن پیام چیزی از اطلاعات آن نمی‌فهمد. با چگونگی رمزکردن[2] 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

---

[1].Email [2].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 نانوایی را در نظر بگیرید. نانوا، پس از خاتمه کار نانوایی، فقط درب نانوایی را می‌بندد (یعنی نیازی به گاوصندوق و سیستم ضد سرقت ندارد). بنابراین، همان‌طور، که بیان گردید، سطوح امنیتی که برای طلا فروشی ایجاد می‌کنیم، خیلی قوی‌تر و پیچیده‌تر از یک نانوایی 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 برروی کامپیوتر شرکت نگهداری

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.

٤. 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 فدورال 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.

٤. 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.

٦. بنابر تخمین شرکت سمانتیک 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 برروی 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 سمانتیک 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 براین 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، سیاست مداران، نرم‌افزارهای مخرب (ویروس‌ها)، و غیره می‌باشند. این مهاجمان ممکن است انگیزه‌هایی از قبیل جمع آوری هوشمندانه، دستبرد فکری، انکار سرویس (عدم پذیرش سرویس)، کشف کردن، سرگرمی، احساس غرور، مورد توجه واقع شدن، تخریب اطلاعات و غیره را داشته باشند.

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**[1]، 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**[2]، 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**[3]، 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**[4]، ضعف‌های موجود در نرم‌افزار، سیستم یا دیگر مکانیزم‌هایی که یک رخنه‌گر برای دسترسی به سیستم یا شبکه می‌تواند از آن بهره بگیرد.

☒ **ریسک**[5]، احتمال این که ضعف‌ها یا آسیب‌پذیری سیستم شناخته شده و از آن‌ها استفاده گردد.

☒ **افشا**[6]، 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 قابلیتی است که رفتار مورد انتظار را انجام می‌دهد. ولی، به آسانی در خطر کشف قرار می‌گیرد.

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

☒ **شبکه‌های بات**[7]، 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**[8] **هکر**[9]، 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 جانبی منفی را به دنبال داشته باشد.

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

---

1. Security
2. Threat
3. Attack
4. Vulnerability
5. Risk
6. Exposure
7. BotNet
8. Attacker
9. Hacker

☒ **بدافزار[1] 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[2]**، 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[3]، 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[4]**، در هنگام انتقال پیام بین فرستنده و گیرنده، فرد یا افراد غیر مجاز دیگری بتوانند پیام را بخوانند (شکل ۱- ۱). مکالمه تلفنی، سیستم پست‌الکترونیک و فایل در حال انتقال ممکن است شامل اطلاعات حساس محرمانه باشند. هدف جلوگیری از مطلع شدن معارضین (افراد غیر

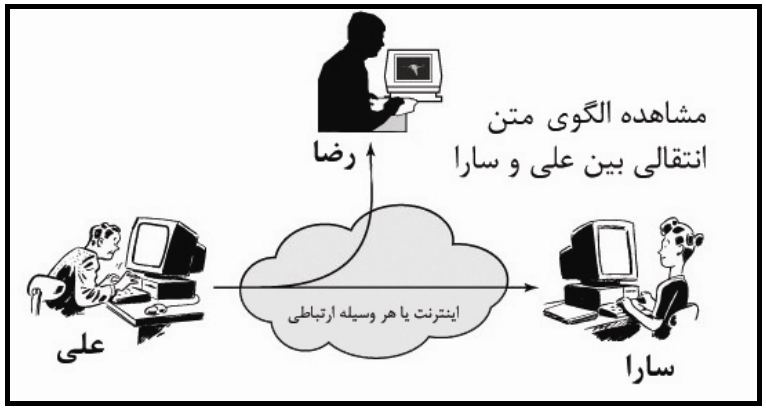
---

[1].MalWare [2].Trojan [3]. Passive Attack [4]. Release of Message

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 پیام‌اصلی 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 ۲ – ۱). 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 ۲ – ۱ حمله تحلیل ترافیک.

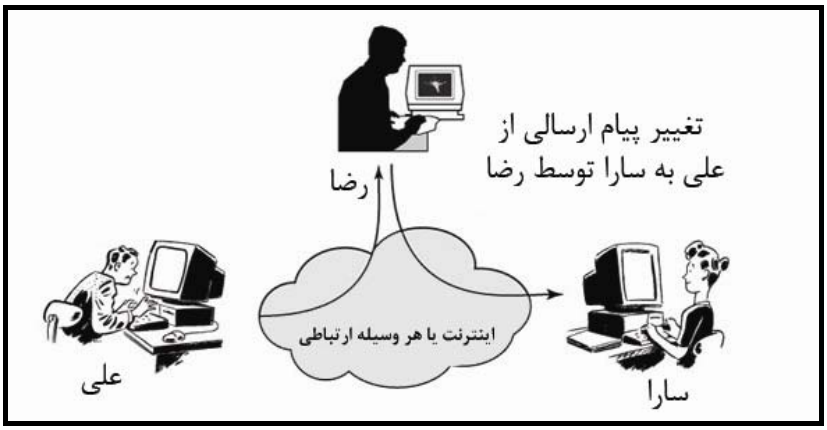
۲-۵-۱. حملات فعال

حملات فعال[1]، 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**[2]، 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**[3]، وقتی رخ می‌دهد که بخشی از یک پیام صحیح تغییر یابد یا پیام به تعویق افتاده و یا مجدداً ارسال شود (شکل ٤ – 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."

---

[1].Active Attack [2] . Masquerade [3] .Message Modification

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)**[1]، از استفاده نرمال منابع ارتباطی و امکانات جلوگیری می‌کند (شکل ۵ – ۱).

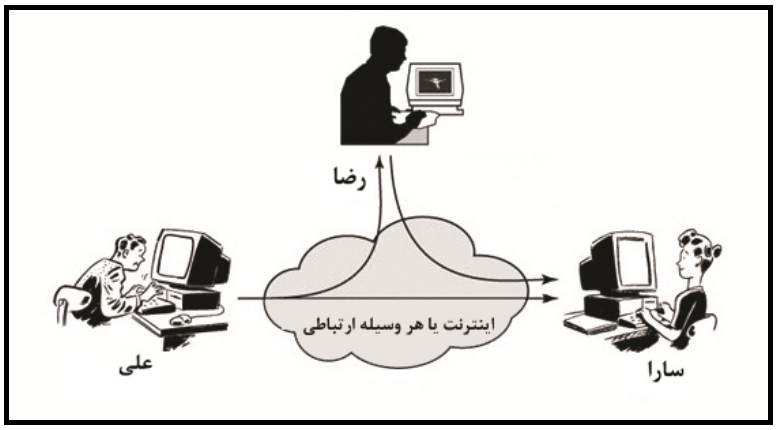
شکل ۵ – ۱ حمله انکار سرویس.

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[2] 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**[3]، به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند (شکل ٦ –۱).

---

[1].Dinal of Service [2]. Server [3].Replay



شکل ۶ – ۱ حمله تکرار.

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. 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 پست‌الکترونیک 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 عبارت‌انداز:

☒ 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[1]، 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[2]، 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[3] (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.

---

[1].Access Control [2].Confidentiality [3].Data Integrity

۵.عدم انکار[1] **(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.دسترس‌پذیری[2] **(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 دسترسی‌پذیری 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 مکانیزیم‌های امنیتی عبارت‌اند از:

۱. **رمزکردن**[3]، استفاده از الگوریتم‌های ریاضی برای انتقال داده به فرمی که توسط افراد غیر مجاز قابل خواندن (قابل فهم) نباشد.

۲. **امضای دیجیتال**[4]، 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**[5]، 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[6]، کنترل دستیابی مبتنی بر نقش[7]، کنترل دستیابی اجباری[8] و کنترل دستیابی مبتنی بر HTTP وجود دارند.

٤. **کنترل مسیر**[9]، مسیریابی امن فیزیکی مقدار مشخصی از داده را ممکن ساخته و تغییرات مسیریابی را وقتی شکاف امنیتی رخ می‌دهد، مجاز می‌سازد.

۵. **کنترل ترافیک**[10]، بیت‌هایی در جاهای خالی داده (شکاف‌های داده) جاگذاری کرده تا تلاش تحلیل ترافیک را خنثی نماید.

٦. **تعویض هویت**[11]، مکانیزمی که به تشخیص موجودیت توسط تعویض هویت کمک می‌کند.

۷. **گواهی**[12]، 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

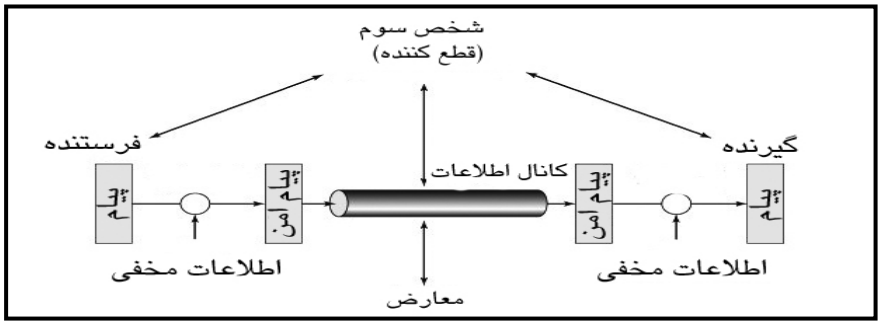
جدول ۱ – ۱ ارتباط بین سیاست‌های امنیتی و مکانیزم‌های امنیتی.

	مکانیزم‌ها							
سرویس		امضای دیجیتال	کنترل دسترسی	صحت داده	تغییر سندیت	پیمایش ترافیک	کنترل مسیریاب	گواهی
تصدیق‌موجودیت همتا	Y	Y			Y			
تصدیق‌داده‌های اصلی	Y	Y						
کنترل‌دسترسی			Y					
قابلیت اعتماد	Y						Y	
قابلیت‌اعتماد جریان داده	Y					Y	Y	
صحت داده	Y	Y		Y				
رد انکار		Y		Y				Y
دسترس‌پذیری				Y	Y			

۷–۱. یک مدل امنیت شبکه

یک مدل امنیت شبکه که اغلب مورد بحث قرار می‌گیرد، در شکل ۷ – ۱ نشان داده شده است.

در این شکل، پیام از شخص توسط کانالی مانند اینترنت ارسال می‌شود. دو شخص که مسئولان این انتقال هستند باید جهت تغییرات همکاری کنند. کانال اطلاعات محلی با تعریف یک مسیر مانند اینترنت توسط پروتکل‌هایی مانند TCP و IP توسط دو مسئول ساخته می‌شوند.



شکل ۷ – ۱ یک مدل امنیت شبکه.

امنیت اطلاعات به این بستگی دارد که اطلاعات انتقالی از دست معارض در امان بماند. تکنیک‌های مورد استفاده برای برقراری امنیت دارای دو قسمت هستند:

۱. تبدیل امنیت روی انتقال اطلاعات.

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 می‌شود.

این مدل چهار نکته مهم پایه‌ای را در طراحی سرویس امنیتی نشان می‌دهد که عبارت‌اند از:

۱. الگوریتمی برای اجرای امنیت طراحی می‌شود. الگوریتم باید به صورتی طراحی شود که معارض نتواند به هدف خود برسد.

۲. با استفاده از الگوریتم، اطلاعات سرّی تولید می‌شوند.

۳. روش‌هایی برای تولید و به اشتراک گذاری اطلاعات سرّی ایجاد می‌شوند.

٤. پروتکلی برای استفاده دو مسئول تعریف می‌شود که کاربرد الگوریتم امنیتی و اطلاعات سرّی برای دستیابی به سرویس امنیتی ویژه را ایجاد می‌کند.

فصل ۲ 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).

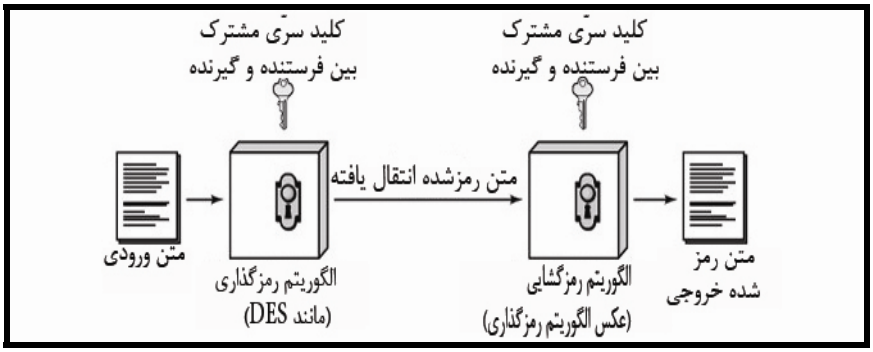
۱ –۲. مدل رمزگذاری متقارن

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 سرّی[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.



شکل ۱ – ۲ مدل ساده شده رمزگذاری مرسوم.

[1].PlianText [2].Encryption Algorithm [3]. Secret Key [4].CipherText [5].Decryption Algorithm

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

☒ **متن رمزشده:** پیامی غیر قابل فهم که خروجی الگوریتم رمزگذاری می‌باشد. غیر قابل فهم بودن این متن، به طول کلید سرّی و قدرت الگوریتم رمزگذاری وابسته است.

☒ **الگوریتم رمزگشایی:** در حقیقت این الگوریتم معکوس الگوریتم رمزگذاری است. این الگوریتم متن رمز شده و کلید سرّی 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[1] نتواند متن رمزشده را رمزگشایی کند یا کلید را کشف کند.

۲. فرستنده و گیرنده باید کپی کلید سرّی 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.

فرض می‌کنیم دانش الگوریتم رمزگذاری/ رمزگشایی مشخص باشد، با این حال رمزگشایی پیام رمزشده، 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 برروی 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 ($X = [x_1,x_2,\ldots x_n]$) می‌باشد. N، تعداد حروف الفبای متناهی است (الفبای لاتین از ۲۶ حرف تشکیل شده است).

امروزه از الفبای باینری $\{0 , 1\}$ استفاده می‌گردد. کلید به شکل $k = \{k_1, k_2,\ldots,k_j\}$ تولید می‌شود. بعد از تولید کلید، باید توسط کانالی 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 $y = [y_1,y_2,\ldots,y_n]$ را تولید می‌کند. یعنی:

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

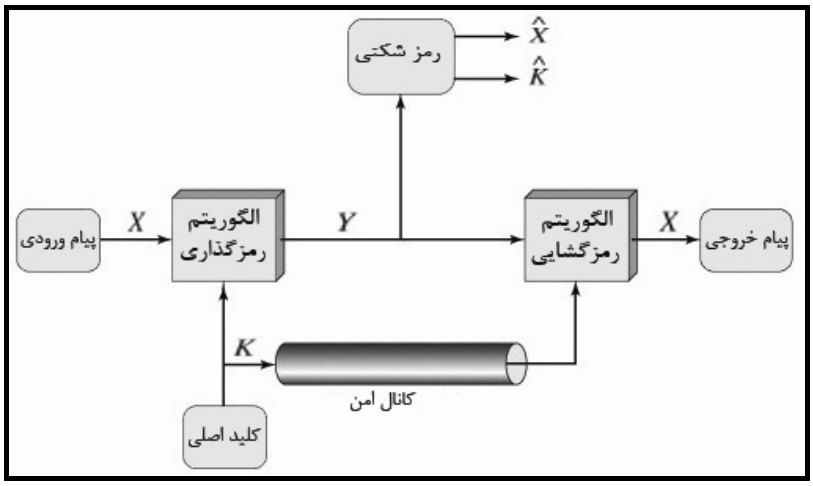
[1].opponent

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).



شکل ۲ – ۲ مدل سیستم رمزقراردادی.

۲-۲. رمز نویسی

سیستم‌های رمزنویسی[1] از سه بعد زیر با یکدیگر مقایسه می‌شوند:

۱. نوع عملیات استفاده شده برای تبدیل متن ساده به متن رمز، تمام الگوریتم‌های رمزگذاری براساس دو اصل کلی (جانشینی و جابجایی) بنا شده‌اند. **جانشینی**[2] یعنی، هر عنصر در متن، یک بیت، بایت، حرف، مجموعه‌ای از بیت‌ها یا حروف) با عنصر دیگر جایگزین می‌شود. **انتقال**[3] 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[4] در آمده‌اند، مراحل چندگانه جابه‌جایی و جانشینی را انجام می‌دهند (مانند الگوریتم DES).

---

[1] .Cryptography [2]. Substitution [3]. Transposition [4].Product Systems

۲. تعداد کلیدهای استفاده شده، اگر گیرنده و فرستنده از یک کلید مشترک استفاده کنند، سیستم به صورت متقارن (تک کلید یا کلید سرّی) 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[1] یا دنباله‌ای[2] باشد. در رمزکننده بلوکی، یک بلوک از عناصر به عنوان ورودی دریافت می‌شود، و بلوکی از عناصر رمز شده تولید می‌شود. ولی، رمز کننده 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. رمزشکنی خطی[3] **۲.** حمله جستجوی جامع[4]

۱ – ۳ – ۲. رمز شکنی خطی

حملات تحلیل رمز علاوه براین که به طبیعت الگوریتم بستگی دارد، ممکن است به دانش خصوصیات کلی متن نیز وابسته باشد.

این نوع حمله از خصوصیات الگوریتمی استفاده می‌کند که سعی دارد متن یا کلید را کاهش دهد.

جدول ۱ – ۲ انواع حملات به پیام‌های رمز شده.

نوع حمله	شناخته شده برای تحلیلگر متن
فقط متن رمز شده	الگوریتم رمزگذاری متن رمز شده
متن معلوم و آشکار	الگوریتم رمزگذاری متن رمز شده یک یا چند متن رمز شده یا ساده اجرا شده با کلید مخفی
متن اصلی انتخابی	الگوریتم رمزگذاری پیام متنی انتخاب شده توسط تحلیل‌گر به همراه متن رمزشده تطبیقی تولید شده با کلید سرّی
متن رمز شده انتخابی	الگوریتم رمزگذاری متن رمز شده متن رمز شده با معنی انتخاب شده توسط تحلیل‌گر، به همراه متن رمزگشایی شده تطبیق تولید شده با کلید سرّی

[1].Block [2].Stream [3].Cyptanalysis [4].Brute – Force Attack

۲ – ۳ – ۲. حمله جستجوی جامع

در این روش حمله‌کننده تمام کلیدهای ممکن که برای رمزگذاری استفاده می‌شوند را امتحان می‌کند تا متن اصلی را به دست آورد.

برای به دست آوردن متن اصلی، به طور متوسط نصف تمام کلیدهای ممکن باید آزمایش شوند.

جدول ۱ – ۲ انواع حملات تحلیل رمز که براساس مقدار اطلاعاتی که تحلیل‌گر رمز می‌داند، را به‌طور خلاصه نشان می‌دهد.

سخت‌ترین حالت وقتی است که همه چیز در متن، رمزشده باشد. در برخی حالات، حتی اگر الگوریتم رمزگذاری شناخته شده نباشد، می‌توان فرض کرد معارض الگوریتم مورد استفاده برای رمزگذاری را می‌داند. اگر کلید خیلی بزرگ باشد حمله جستجوی جامع پیچیده خواهد شد. بنابراین، معارض باید به تحلیل متن رمزشده اکتفا کرده، و آزمون‌های آماری متفاوت را به کار ببرد.

برای استفاده از این روش، معارض باید ساختار نوع متنی که مخفی شده است، از قبیل متن انگلیسی یا فرانسوی، فایل اجرایی، لیست برنامه جاوا، فایل حسابداری و غیره را داشته باشد.

حمله به متن رمزشده آسان‌ترین روش برای دفاع است. زیرا، معارض حداقل مقدار اطلاعات را برای کارکردن دارد. در اکثر حالات، تحلیل‌گر اطلاعات زیادی را در اختیار دارد.

شاید تحلیل‌گر بتواند یک یا چند پیام متنی را بهتر از رمزگذاری‌ها در اختیار بگیرد، یا ممکن است بداند الگوهای متنی مشخصی در متن ظاهر می‌شوند.

به عنوان مثال، فایلی در قالب پست الکترونیکی که انتقال وجه را انجام می‌دهد رمزگذاری نشده است. تمامی این نمونه‌ها برای متن، آشکار و معلوم هستند. با این دانش، تحلیل‌گر می‌تواند کلید را بر مبنای روشی که متن منتقل می‌شود به دست بیاورد.

اگر تحلیل‌گر بتواند به روشی منبع سیستم را به دست آورده و پیام انتخاب شده را به سیستم اضافه کند، حمله انتخابی امکان‌پذیر خواهد بود.

یک مثال از این سیاست، رمزشکنی تفاضلی[1] است. این نوع رمزشکنی را در ادامه می‌بینید.

در کل، اگر تحلیل‌گر بتواند پیام‌ها را برای رمزگذاری انتخاب کند، عمداً از الگوهایی استفاده می‌کند که برای آشکارسازی ساختار کلید مورد انتظار باشد.

در جدول ۱ – ۲ دو نوع حمله دیگر آمده است که عبارت‌اند از:

۱. متن رمزشده انتخابی **۲.** متن انتخابی

[1].differential cryptanalysis

به طور معمول این نوع حملات، کمتر به عنوان تکنیک‌های تحلیل رمز استفاده می‌شوند. اما، با این حال راه‌های ممکن حمله می‌باشند. فقط الگوریتم‌های نسبتاً ضعیف برای مقاومت در برابر حمله متن رمز شده شکست می‌خورند.

به طور کل، الگوریتم‌های رمزگذاری جهت مقاومت در برابر حملات متن معلوم و آشکار طراحی شده‌اند.

دو تعریف در این زمینه وجود دارند:

۱. الگوی رمزگذاری امن قطعی[1] است، اگر متن رمزشده تولید شده توسط الگو شامل اطلاعات کافی برای تعیین متن ساده نباشد، مهم نیست که چه مقدار متن رمزشده وجود دارد. یعنی، مهم نیست معارض چقدر زمان در اختیار دارد، چون امکان رمزگشایی متن رمز شده برای او وجود ندارد. به جز الگویی که به عنوان کلید یک بار مصرف معروف است، الگوریتم رمزگذاری وجود ندارد که امن قطعی باشد.

بنابراین، تمام کاربران الگوریتم رمزگذاری می‌توانند الگوریتمی را امتحان کنند که یک یا هر دو شرط زیر را داشته باشند:

- ☒ هزینه شکستن رمز از ارزش اطلاعات رمز گذاری شده بیشتر شود.
- ☒ زمان لازم برای شکستن رمز از طول عمر مفید اطلاعات بیشتر باشد.

۲. الگوی رمزگشایی، امن محاسباتی[2] است، اگر هر دو شرط فوق را داشته باشد. تخمین مقدار آزمایشات لازم برای موفقیت تحلیل رمز متن رمزشده بسیار مشکل است.

جدول ۲ – ۲ زمان متوسط مورد نیاز برای جستجوی کلید جامع.

طول کلید (بیت)	تعداد کلیدهای جایگزین	زمان مورد نیاز در یک رمز گشایی برحسب میلی ثانیه	زمان مورد نیاز در 10^6 رمزگشایی برحسب میلی ثانیه
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s$ =35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s$ =1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s$ =5.4×10^{24}	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s$ =5.9×10^{36}years	5.9×10^{30} years
26Characters (permutation)	$26! = 4 \times 10^{26}$	$2\times 10^{26}\ \mu s$ =6.4×10^{12} Years	6.4×10^{6} years

[1].Unconditionally secure [2]. Computationally Secure

تمام گونه‌های رمزشکنی خطی الگوهای رمزگذاری متقارن از این جهت طراحی شده‌اند که در برابر این واقعیت که مراحل ساختار یا الگو در متن ممکن است الگوریتم را نجات داده و در متن رمز شده قابل تشخیص باشند، مقاومت کنند. وقتی الگوریتم رمزگذاری متقارنی را آزمایش می‌کنیم، مطالب بیان شده کاملاً قابل درک خواهند شد.

در حمله جستجوی جامع، هر کلید ممکن آنقدر امتحان می‌شود، تا معنی قابل درکی از متن رمزشده به دست آید. بطور متوسط نیمی از کلیدهای ممکن باید برای حصول موفقیت امتحان شوند. جدول ۲ – ۲ زمان لازم برای پیدا کردن کلیدهای مختلف را نشان می‌دهد.

۴ –۲. روش‌های کلاسیک رمزگذاری متقارن

در این بخش چند نمونه از رمزگذاری کلاسیک را می‌بینید.

با مطالعه این تکنیک‌ها می‌توانید روش‌های اولیه رمزگذاری متقارن و انواع حملات تحلیل رمز را بشناسید. روش‌های کلاسیک رمزگذاری متقارن به دو نوع رمزگذاری جانشینی و جابه‌جایی، تقسیم می‌شوند.

۱ – ۴ – ۲. روش‌های جانشینی

همان‌طور که بیان شد، تکنیک جانشینی تکنیکی است که حروف متن در آن با حروف‌های دیگر و یا با اعداد و نشانه‌های دیگر جایگزین می‌شوند. اگر متن مورد نظر به عنوان رشته‌ای از بیت‌ها باشد، آن‌گاه جانشینی با تعویض الگوهای بیتی متن با الگوهای بیتی متن رمزشده این کار را انجام می‌دهد.

وقتی که از موارد زیر استفاده نمایید، حروف پیچیده‌تر می‌گردند:

- ☒ متن اصلی همیشه با حروف کوچک باشد.
- ☒ متن رمزشده با حروف بزرگ باشد.
- ☒ مقادیر کلید به صورت حروف کوچک مورب هستند.

رمز سزار

اولین بار رمزسزار[1] توسط امپراتور ژولیوس‌سزار برای ارسال پیام‌های نظامی به ارتش استفاده گردید. این امپراتور هر کاراکتر از الفبا را با سه حرف بعدی جایگزین کرد. حروف با این روش به صورت زیر جایگزین می‌شوند:

متن اصلی:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
متن رمزشده:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

[1].Caesar cipher

مثال ۱ – ۲: متن زیر را به روش سزار رمز کنید:

متن اصلی : meet me after the toga party

حل:

متن رمز شده: PHHW PH DIWHU WKH WRJD SDUWB

مثال ۲ – ۲: متن زیر را به روش سزار رمز نمایید:

متن اصلی : This Is a Private Message

حل:

متن رمزشده : WKLV LV D SULYDWH PHVVDJH

بنابراین معادل عددی برای هر حرف نیز به صورت زیر است:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

پس می‌توان الگوریتم را به صورت زیر بیان کرد:

$$C = E(3, P) = (P + 3) \bmod 26$$

این الگوریتم هر حرف متن ساده (P)را با حرف متن رمزشده (C) جایگزین می‌کند. درحالت کلی، الگوریتم سزار به صورت زیر بیان می‌گردد:

$$C = E(K, P) = (C, K) \bmod 26$$

یعنی، به جای ۳ می‌توان از K (بین ۱ تا ۲۵) استفاده کرد.

اگر نوع رمزگذاری مشخص و سزار باشد، آن‌گاه با رمزشکنی خطی جستجوی جامع به راحتی می‌توان از متن رمزشده متن ساده کلید را به دست آورد. شکل ۳ – ۲ نتایج اجرای استراتژی را برای متن نمونه نشان می‌دهد. در این حالت متن اصلی در خط سوم رمزگشایی می‌گردد.

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

شکل ۳ – ۲ رمزشکنی خطی رمزسزار.