

" Intrusion Detection "

تشخیص نفوذ (Intrusion Detection) عبارت است از پروسه تشخیص تلاشهایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می شوند. در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام حملات پیدا کرد. سپس بنابر درک بدست آمده، روشی دو مرحله ای را برای متوقف کردن حملات برگزید. اول این که مطمئن شوید که الگوی عمومی فعالیتهای خطرناک تشخیص داده شده است. دوم این که اطمینان حاصل کنید که با حوادث مشخصی که در طبقه بندی مشترک حملات نمی گنجد، به سرعت رفتار می شود. به همین دلیل است که بیشتر سیستم های تشخیص نفوذ (Intrusion Detection System) بر مکانیزمهایی جهت بروزرسانی نرم افزارشان متکی هستند که جهت جلوگیری از تهدیدات شبکه به اندازه کافی سریع هستند. البته تشخیص نفوذ به تنهایی کافی نیست و باید مسیر حمله را تا هکر دنبال کرد تا بتوان به شیوه مناسبی با وی نیز برخورد کرد.

انواع حملات شبکه ای با توجه به طریقه حمله:

یک نفوذ به شبکه معمولاً یک حمله قلمداد می شود. حملات شبکه ای را می توان بسته به چگونگی انجام آن به دو گروه اصلی تقسیم کرد. یک حمله شبکه ای را می توان با هدف نفوذگر از حمله توصیف و مشخص کرد. این اهداف معمولاً از کار انداختن سرویس (Denial of Service یا DOS) یا دسترسی غیرمجاز به منابع شبکه است.

۱. حملات از کار انداختن سرویس:

در این نوع حملات، هکر استفاده از سرویس ارائه شده توسط ارائه کننده خدمات برای کاربران را مختل می کند. در این حملات حجم بالایی از درخواست ارائه خدمات به سرور فرستاده می شود تا امکان خدمات رسانی را از آن بگیرد. در واقع سرور به پاسخگویی به درخواستهای بی شمار هکر مشغول می شود و از پاسخگویی به کاربران واقعی باز می ماند.

۲. حملات دسترسی به شبکه:

در این نوع از حملات، نفوذگر امکان دسترسی غیرمجاز به منابع شبکه را پیدا می کند و از این امکان برای انجام فعالیتهای غیرمجاز و حتی غیرقانونی استفاده می کند. برای مثال از شبکه به عنوان مبدا حملات DOS خود استفاده می کند تا در صورت شناسایی مبدا، خود گرفتار نشود. دسترسی به شبکه را می توان به دو گروه تقسیم کرد.

☑ **دسترسی به داده :** در این نوع دسترسی ، نفوذگر به داده موجود بر روی اجزاء شبکه دسترسی غیرمجاز پیدا می کند. حمله کننده می تواند یک کاربر داخلی یا یک فرد خارج از مجموعه باشد. داده های ممتاز و مهم معمولاً تنها در اختیار بعضی کاربران شبکه قرار می گیرد و سایرین حق دسترسی به آنها را ندارند. در واقع سایرین امتیاز کافی را جهت دسترسی به اطلاعات محرمانه ندارند، اما می توان با افزایش امتیاز به شکل غیر مجاز به اطلاعات محرمانه دسترسی پیدا کرد. این روش به تعدیل امتیاز یا **Privilege Escalation** مشهور است.

☑ **دسترسی به سیستم :** این نوع حمله خطرناکتر و بدتر است و طی آن حمله کننده به منابع سیستم و دستگاهها دسترسی پیدا می کند. این دسترسی می تواند شامل اجرای برنامه ها بر روی سیستم و به کار گیری منابع آن در جهت اجرای دستورات حمله کننده باشد. همچنین حمله کننده می تواند به تجهیزات شبکه مانند دوربینها ، پرینترها و وسایل ذخیره سازی دسترسی پیدا کند. حملات **Brute Force** ، **Trojan** و یا استفاده از ابزارهایی جهت تشخیص نقاط ضعف یک نرم افزار نصب شده بر روی سیستم از جمله نمونه های قابل ذکر از این نوع حملات هستند.

فعالیت مهمی که معمولاً پیش از حملات **DoS** و دسترسی به شبکه انجام می شود، شناسایی یا **Reconnaissance** است. یک حمله کننده از این فاز جهت یافتن حفره های امنیتی و نقاط ضعف شبکه استفاده می کند. این کار می تواند به کمک بعضی ابزارها آماده انجام پذیرد که به بررسی پورتهای رایانه های موجود بر روی شبکه می پردازند و آمادگی آنها را جهت انجام حملات مختلف بر روی آنها بررسی می کنند.

🚩 انواع حملات شبکه ای با توجه به حمله کننده :

حملات شبکه ای را می توان با توجه به حمله کننده به چهار گروه تقسیم کرد :

☑ حملات انجام شده توسط کاربر مورد اعتماد (داخلی) : این حمله یکی از مهمترین و خطرناکترین نوع حملات است، چون از یک طرف کاربر به منابع مختلف شبکه دسترسی دارد و از طرف دیگر سیاستهای امنیتی معمولاً محدودیتهای کافی درباره این کاربران اعمال نمی کنند.

☑ حملات انجام شده توسط افراد غیر معتمد (خارجی) : این معمولترین نوع حمله است که یک کاربر خارجی که مورد اعتماد نیست شبکه را مورد حمله قرار می دهد. این افراد معمولاً سخت ترین راه را پیش رو دارند زیرا بیشتر سیاستهای امنیتی درباره این افراد تنظیم شده اند

☑ حملات انجام شده توسط هکرها بی تجربه : بسیاری از ابزارهای حمله و نفوذ بر روی اینترنت وجود دارند. در واقع بسیاری از افراد می توانند بدون تجربه خاصی و تنها با استفاده از ابزارهای آماده برای شبکه ایجاد مشکل کنند.

☑ حملات انجام شده توسط کاربران مجرب : هکرها با تجربه و حرفه ای در نوشتن انواع کدهای خطرناک متبحرند. آنها از شبکه و پروتکلها آن و همچنین از انواع سیستم های عمل آگاهی کامل دارند. معمولاً این افراد ابزارهایی تولید می کنند که توسط گروه اول به کار گرفته می شوند. آنها معمولاً پیش از هر حمله ، آگاهی کافی درباره قربانی خود کسب می کنند .

پر دازه تشخیص نفوذ :

تا بحال با انواع حملات آشنا شدیم. حال باید چگونگی شناسایی حملات و جلوگیری از آنها را بشناسیم. امروزه دو روش اصلی برای تشخیص نفوذ به شبکه ها مورد استفاده قرار می گیرد:

IDS مبتنی بر خلاف قاعده آماری

روش اول مبتنی بر تعیین آستانه انواع فعالیتها بر روی شبکه است، مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان (Host) اجرا می شود. لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت خلاف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه ای هستند که نمی توان براحتی و با کمک این روش آنها را تشخیص داد.

IDS مبتنی بر امضا یا تطبیق الگو

در واقع روشی که در بیشتر سیستمهای موفق تشخیص نفوذ به کار گرفته می شود، IDS مبتنی بر امضا یا تطبیق الگو است. منظور از امضا مجموعه قواعدی است که یک حمله در حال انجام را تشخیص می دهد. دستگاہی که قرار است نفوذ را تشخیص دهد با مجموعه ای از قواعد بارگذاری می شود. هر امضا دارای اطلاعاتی است که نشان می دهد در داده های در حال عبور باید به دنبال چه فعالیتهایی گشت. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می شود و مدیر شبکه را از وقوع یک نفوذ آگاه می کند. در بسیاری از موارد IDS علاوه بر آگاه کردن مدیر شبکه، اتصال با هکر را باز آغاز می کند و یا با کمک یک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می کند.

اما بهترین روش برای تشخیص نفوذ، استفاده ترکیبی از دو روش فوق است.

رمز نگاری

۱- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنهای متمادی محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می شده، استفاده شده است تا پیغامهای آنها محرمانه بماند. هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می توانند از رمزنگاری استفاده کنند. اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخفها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی (که بعنوان *plaintext* شناخته می شود)، آنرا با استفاده از یک کلید (رشته ای محدود از بیتها) بصورت رمز در می آوریم تا کسی که دیتای حاصله را می خواند قادر به درک آن نباشد. دیتای رمز شده (که بعنوان *cipher text* شناخته می شود) بصورت یک سری بی معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می رسد. برای حصول متن اولیه دریافت کننده آنرا رمزگشایی می کند. یک شخص ثالث (مثلا یک هکر) می تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته (*cryptanalysis*) کند. بخاطر داشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی خود بی معنی است. رمزنگاری مدرن فرض می کند که الگوریتم شناخته شده است یا می تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده سازی تغییر می کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند. دیتای اولیه اغلب قبل از رمز شدن بازچینی می شود؛ این عمل عموماً بعنوان *scrambling* شناخته می شود. بصورت مشخص تر، *hash function* ها بلوکی از دیتا را (که می تواند هر اندازه ای داشته باشد) به طول از پیش مشخص شده کاهش می دهد. البته دیتای اولیه نمی تواند از *hashed value* بازسازی شود. *Hash function* ها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه ای از پیام (شامل مهم ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و *hash* می شود. یک چک تایید پیام (*Message Authentication Check*) یا *MAC* یک الگوریتم ثابت با تولید یک امضاء بر روی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می شود، منجر به ایجاد امضای دیجیتال (*digital signature*) می شود.

۲- الگوریتمها

طراحی الگوریتمهای رمزنگاری مقوله ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (*Shannon*) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پایه پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

۱-۲ سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد **data encryption algorithm** یا **DEA** است که بیشتر بعنوان **DES** شناخته می‌شود. **DES** یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای ۶۴ بیتی دیتا توسط یک کلید تنها که معمولا ۵۶ بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. **DES** از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری **DES** عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای **DES** ۴۰ بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶ بیتی عموما توسط سخت‌افزار یا شبکه‌های بخصوصی شکسته می‌شوند. رمزنگاری **DES** سه تایی عبارتیست از کدکردن دیتای اصلی با استفاده از الگوریتم **DES** که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر) مطابق شکل زیر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.

الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده‌اند. الگوریتمهایی مانند **Blowfish** و **IDEA** برای زمانی مورد استفاده قرار گرفته‌اند اما هیچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای **DES** برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (**AES**) الگوریتم **Rijndael** را برای جایگزینی **DES** بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم **Twofish** مشخصا برای پیاده‌سازی در پردازنده‌های توان-پایین مثلا در کارتهای هوشمند طراحی شد. در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها **Skipjack** و مبادله کلید را که در کارتهای **Fortezza** استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود.

برای رمزنگاری جریانی (**streaming encryption**) (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد بجای اینکه دیتای گذشته در یک فایل مجزا قرار گیرد) الگوریتم **RC4** سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. **RC4** که متعلق به امنیت دیتای **RSA** است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۲-۲ سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عمومی یا **public key**) منتشر شود در حالیکه دیگری (کلید اختصاصی یا **private key**) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند. عبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای بجز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولترین سیستم نامتقارن بعنوان **RSA** شناخته می‌شود (حروف اول پدیدآورندگان آن یعنی **Rivest**، **Shamir** و **Adleman** است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشان دادن اینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحاً امضاء نام دارد. **RSA** شامل دو تبدیل است که هرکدام احتیاج به بتوان رسانی ماجولار با توانهای خیلی طولانی دارد:

- امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛
- رمزگشایی عملیات مشابه‌ای روی متن رمز شده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمز شده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمز شده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم **RSA** این فرمول است: $X = Y^k \pmod{r}$

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزئیات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌های بایتی بخصوص روی ۸ بیتی‌ها که در کارتهای هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه **RSA** هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده می‌شود و برای نشان دادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

سایر سیستمهای کلید نامتقارن شامل سیستمهای لگاریتم گسسته می‌شوند مانند **Diffie-Hellman**، **EIGamal** و سایر طرحهای چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرحها عملکردهای یک-طرفه‌ای دارند که اجازه تایید هویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم **RPK** است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. **RPK** یک پروسه دو

مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین بخوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.

طولهای کلیدها برای این طرح‌های جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چپ‌کارتهای مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سده‌ها از این الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می‌رود.

کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده‌ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

۱- کلیدهای محرمانه (Secret keys)

الگوریتمهای متقارن مانند DES از کلیدهای محرمانه استفاده می‌کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود. چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می‌سازد. کارتهای هوشمند معمولاً برای ذخیره کلیدهای محرمانه استفاده می‌شوند. در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است: باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم نباید در مخاطره قرار گیرد.

۲- کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستمهای کلید نامتقارن این است که آنها اجازه می‌دهند که یک کلید (کلید اختصاصی) با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر (کلید عمومی) می‌تواند منتشر شود. کلیدهای عمومی می‌توانند همراه پیامها فرستاده شوند یا در فهرستها لیست شوند (شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام‌رسانی الکترونیکی ITU X.500 وجود دارد)، و از یک شخص به شخص بعدی داده شوند. مکانیسم توزیع کلیدهای عمومی می‌تواند رسمی (یک مرکز توزیع کلید) یا غیررسمی باشد.

محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد. کلیدهای اختصاصی نباید هرگز بصورت رمز نشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند. در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمانهای بزرگ معمولاً نباید در یک کارت ذخیره شود.

۳- کلیدهای اصلی و کلیدهای مشتق شده (keys Master keys and derived)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می‌شوند. در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق شده استفاده می‌شود که بعداً برای رمزنگاری استفاده می‌گردد. برای مثال، اگر یک صادر کننده با تعداد زیادی

کارت سروکار دارد، می‌تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق شده حاصل می‌شود و به آن کارت اختصاص داده می‌شود.

شکل دیگری از کلیدهای مشتق شده با استفاده از **token**ها که محاسبه‌گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می‌شوند. آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یک **PIN** وارد شده توسط کاربر و تاریخ و زمان استفاده کنند. خود **token** شامل الگوریتم و یک کلید اصلی است. چینی **token**هایی اغلب برای دسترسی به سیستمهای کامپیوتری امن استفاده می‌شوند.

۴- کلیدهای رمزکننده کلید (Key-encrypting keys)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می‌رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمز شده منطقی بنظر می‌رسد. کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری (یا کارت هوشمند) ارسال نمی‌شوند و بنابراین می‌توانند آسانتر محافظت شوند تا آنهایی که ارسال می‌شوند. اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می‌شود، مورد استفاده قرار می‌گیرد.

از مفهوم دامنه کلید (**domain key**) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه‌شان استفاده می‌کنیم. معمولاً یک دامنه، یک سیستم کامپیوتری خواهد بود که می‌تواند بصورت فیزیکی و منطقی محافظت گردد. کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده کلید محلی ذخیره می‌شوند. هنگامی که کلیدها می‌خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می‌شوند که اغلب بعنوان کلید کنترل ناحیه (**key zone control**) شناخته می‌شوند. با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می‌شوند. بنابراین کلیدهایی که در دامنه‌های یک ناحیه قرار دارند از دامنه‌ای به دامنه دیگر بصورتی که بیان گردید منتقل می‌شوند.

۵- کلیدهای نشست (Session keys)

برای محدود کردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می‌شود. این کلید ممکن است یک عدد تصادفی تولید شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد. اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می‌تواند با استفاده از کلید عمومی کارت رمز شود.

بخشی از تراکنش که در آن کلید منتقل می‌شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرف نظر است. چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است. (توضیح اینکه روشهای رمز متقارن از نامتقارن بمراتب سریعتر هستند بنابراین می‌توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد.)

شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستم‌های پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می‌شود. بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می‌شود و این کلید برای تراکنش بعدی مورد استفاده قرار می‌گیرد.

شکستن کلیدها در رمزنگاری

چه طول کلیدی در رمزنگاری مناسب است؟

امنیت هر الگوریتم مستقیماً به پیچیده بودن اصولی مربوط است که الگوریتم بر اساس آن بنا شده است. امنیت رمزنگاری بر اساس پنهان ماندن کلید است نه الگوریتم مورد استفاده. در حقیقت، با فرض اینکه که الگوریتم از قدرت کافی برخوردار است (یعنی که ضعف شناخته‌شده‌ای که بتوان برای نفوذ به الگوریتم استفاده کرد، وجود نداشته باشد) تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است. در بیشتر انواع حمله، حمله‌کننده تمام کلیدهای ممکن را تولید و روی متن رمز شده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتم‌های رمزنگاری در برابر این نوع حمله آسیب‌پذیر هستند، اما با استفاده از کلیدهای طولانی‌تر، می‌توان کار را برای حمله‌کننده مشکل‌تر کرد. هزینه امتحان کردن تمام کلیدهای ممکن با تعداد بیت‌های استفاده شده در کلید بصورت نمایی اضافه می‌شود، و این در حالیکه انجام عملیات رمزنگاری و رمزگشایی بسیار کمتر افزایش می‌یابد.

الگوریتم‌های متقارن

DES که یک الگوریتم کلید متقارن است معمولاً از کلیدهای ۶۴ بیتی برای رمزنگاری و رمزگشایی استفاده می‌کند. الگوریتم متن اولیه را به بلوک‌های ۶۴ بیتی می‌شکند و آنها را یکی یکی رمز می‌کند. DES^۳ الگوریتم پیشرفته‌تر است و در آن الگوریتم DES سه بار اعمال می‌شود (در مقاله رمزنگاری به آن اشاره شده است). نسخه دیگری از این الگوریتم (پایدارتر از قبلیها) از کلیدهای ۵۶ بیتی و با فضای کلید موثر ۱۶۸ بیت استفاده می‌کند و سه بار عملیات رمزنگاری را انجام می‌دهد. جدول زیر زمان لازم برای یافتن کلید در الگوریتم DES را نشان می‌دهد.

طول کلید	تعداد کلیدهای ممکن	زمان مورد نیاز برای رمزگشایی در هر میلی‌ثانیه	زمان مورد نیاز برای زمان مورد نیاز برای
۳۲ بیت	$2^{32} = 4/3 \times 10^9$	۳۵/۸ دقیقه = 2^{31} میلی‌ثانیه	۲/۱۵ میلی‌ثانیه
۵۶ بیت	$2^{56} = 7/2 \times 10^{16}$	۱۱۴۲ سال = 2^{55} میلی‌ثانیه	۱۰ ساعت
۱۲۸ بیت	$2^{128} = 3/4 \times 10^{38}$	$5/4 \times 10^{24}$ سال = 2^{127} میلی‌ثانیه	$5/4 \times 10^{18}$ سال
۱۶۸ بیت	$2^{168} = 3/7 \times 10^{50}$	$5/9 \times 10^{36}$ سال = 2^{167} میلی‌ثانیه	$5/9 \times 10^{30}$ سال

ستون سوم مربوط به کامپیوترهایی است که می‌توانند در هر میلی‌ثانیه یک رمزگشایی را انجام دهند که برای کامپیوترهای امروزی توان محاسباتی معقولی محسوب می‌شود. ستون آخر برای سیستمهای بسیار بزرگ محاسباتی است بطوریکه قدرت پردازش یک میلیون برابر زیاد شده باشد.

بدون در نظر گرفتن طول کلید، الگوریتمهای متقارن قوی نیز نمی‌توانند امنیت الگوریتمهای نامتقارن را داشته باشند، زیرا کلید باید بین دو طرف ارتباط مبادله شود.

الگوریتمهای نامتقارن

عموماً سیستمی امن محسوب می‌شود که هزینه شکستن آن بیشتر از ارزش دیتایی باشد که نگهداری می‌کند. اما در ذهن داشته باشید که با افزایش قدرت محاسباتی، سیستمهای رمزنگاری، آسانتر توسط روشهای سعی و خطا مورد حمله قرار خواهند گرفت.

برای مثال، طبق گزارشی از سایت **RSA**، تخمین زده می‌شود که یک کلید ۲۱۵ بیتی می‌تواند با هزینه‌ای کمتر از ۱ میلیون دلار و یک تلاش ۸ ماهه شکسته شود. **RSA** توصیه میکند که کلیدهای ۲۱۵ بیتی در حال حاضر امنیت کافی ایجاد نمی‌کنند و باید بنفع کلیدهای ۸۶۷ بیتی برای استفاده‌های شخصی کنار بروند! به همین ترتیب برای استفاده شرکتها کلیدهای ۱۰۲۴ بیتی و از ۲۰۴۸ بیت برای کلیدهای فوق العاده ارزشمند استفاده شود. البته پیش بینی شده بود که این مقادیر تا حداقل سال ۲۰۰۴ معتبر است.

جدول زیر نشاندهنده افراد یا گروههایی است که توانایی شکستن کلیدها با طولهای متفاوت را دارند.

نفوذگران بالقوه	طول کلید
افراد عادی	۲۵۶ بیتی
گروههای تحقیق دانشگاهی و شرکتها	۳۸۴ بیتی
گروههای دولتی با تمام امکانات	۵۱۲ بیتی
امن برای کوتاه مدت	۷۶۸ بیتی
امن تا آینده نزدیک	۱۰۲۴ بیتی
امن احتمالاً تا چند ده سال!	۲۰۴۸