امنیت اطلاعات

محمدتقی روغنی

تـــــوجـــــــه

خواننده گرامی

این PDF تنها شامل گزیده‌ای از کتاب "امنیت اطلاعات" است. در صورتیکه مطالب و نحوه نگارش را مفید ارزیابی کردید، برای خرید این کتاب به‌صورت کامل و در قالب چاپ کاغذی، می‌توانید انحصاراً از طریق لینک زیر اقدام نمایید:

نام کتاب: امنیت اطلاعات
مؤلف: محمدتقی روغنی
چاپ اول: زمستان ۱۳۹۳
۴۴۸ صفحه، وزیری
قیمت: ۲۵۰۰۰ تومان

لینک خرید:

حمد سزاوار خداوندیست

که نا بخشیدن، بر دارائی‌هایش نیافزاید؛

و اگر بخشش کند، بینوا نشود.

امام علی علیه‌السلام

امنیت اطلاعات

محمدتقی روغنی

مقدمه مؤلف:

خداوند حکیم را شاکرم که عنایت خویش را برای نگارش کتابی جدید شامل حال بنده نمود، تا بتوانم گام کوچک دیگری در راستای ارتقای علمی فناوری اطلاعات هموطنان عزیزم بردارم.

تعاملات بین مشتریان و سازمان‌ها از طریق سرویس‌های فناوری اطلاعات، روزبه‌روز بیشتر شده و سازمان‌ها را مجبور می‌نماید که برای رفع نیاز مشتریان، دیتای بیشتری را بر روی سرویس‌دهنده‌های خود قرار دهند. هرقدر فناوری اطلاعات در کسب‌وکار سازمان‌ها بیشتر وارد شده و باعث تسهیل امور می‌شود، در مقابل ریسک سازمان در حفاظت از دارایی‌های اطلاعاتی را بالا می‌برد. از طرف دیگر وابستگی ادامه حیات کسب‌وکار سازمان، بیشتر به سرویس‌های فناوری اطلاعات گره می‌خورد.

در این سیرِ رو به رشد استفاده از سرویس‌های فناوری اطلاعات، متأسفانه بحث امنیت بسیار مهجور و یا مغفول مانده است. مخصوصاً در بین شرکت‌ها و سازمان‌های ایرانی آن‌چنان‌که بایدوشاید به بحث امنیت توجه نمی‌شود.

بعضی از سازمان‌ها برای مباحث امنیتی ارزش خاصی قائل نشده و تا روز بروز مصیبت، هیچ قدمی در جهت محافظت از دارایی‌های اطلاعاتی سازمان خود برنمی‌دارند. بعضی دیگر، امنیت را به خرید چند محصول امنیتی مثل فایروال و آنتی‌ویروس، محدود کرده و تصور می‌کنند که باوجود این محصولات، امنیت را در سازمان خود برقرار نموده‌اند.

توجه داشته باشید که امنیت صرفاً با خرید چند محصول امنیتی، برقرار نمی‌شود. اگر امنیت را یک فرآیند در نظر بگیریم، محصولات امنیتی تنها بخشی از آن فرآیند خواهند بود. در این فرآیند امنیتی، طراحی و ایجاد سیاست‌های امنیتی در سطح مدیران ارشد سازمان، باید به‌عنوان یکی از مؤلفه‌های مهم در نظر گرفته شود.

پس از بحث مدیران ارشد، یکی دیگر از مشکلات در زمینه امنیت، ناآگاهی مدیران و کارشناسان IT نسبت به مفاهیم امنیت اطلاعات است. بسیاری از کارشناسان، پیکربندی تجهیزات را صرفاً به‌صورت تجربی و بدون اطلاع از نحوه عملکرد پروتکل‌ها انجام می‌دهند. لذا در اکثر مواقع پیکربندی درستی با توجه به نیازهای سازمان انجام نمی‌پذیرد.

در این کتاب سعی شده بجای یک محصول امنیتی خاص، به مفاهیم اساسی امنیت پرداخته شود. زمانی که یک مدیر یا کارشناس IT و امنیت، آگاهی درستی از مفاهیم امنیتی داشته باشد، توان تجزیه‌وتحلیل بهتری نسبت به فرآیندهای امنیتی پیداکرده و بالطبع در زمان طراحی سیاست‌های امنیتی و یا پیکربندی تجهیزات، عملکرد بهتری خواهد داشت.

مطالب این کتاب در چهار بخش تقسیم‌بندی شده است. در بخش اول به استاندارد سیستم مدیریت امنیت اطلاعات پرداخته‌شده است. قطعاً زمانی که وارد بحث امنیت اطلاعات می‌شویم، یکی از مهم‌ترین مواردی که باید در نظر گرفته شود، استانداردهای مربوطه است. اصلی‌ترین استاندارد درزمینه امنیت اطلاعات، استاندارد خانواده ISMS است. در فصل اول و دوم کتاب، استانداردهای ISO 27000، ISO 27001 و ISO 27002 به‌صورت اجمالی بررسی‌شده است.

در بخش دوم، به یکی از ارکان امنیت اطلاعات، یعنی رمزنگاری، پرداخته‌شده است. نحوه عملکرد الگوریتم‌های مهم رمزنگاری مثل DES، 3DES، AES، RSA و SHA شرح داده‌شده است. همچنین کاربرد این الگوریتم‌ها در برقراری سرویس‌های امنیتی مثل محرمانگی، احرازهویت، صحت، امضای دیجیتال و عدم انکار، تشریح شده است.

در بخش سوم این کتاب، مباحث امنیت شبکه مورد بررسی قرارگرفته است. با توجه به گسترش شبکه‌های ارتباطی، یکی از دغدغه‌های اصلی مدیران و کارشناسان، امنیت شبکه است. در فصول این بخش به مفاهیم امنیتی و تکنولوژی‌های مورداستفاده در امنیت شبکه ازجمله فایروال، IDS، IPS و هانی‌پات پرداخته شده است. در آخر این بخش نیز نحوه برقراری امنیت در ارتباطات شبکه‌ای با استفاده از IPsec و VPN، مورد بررسی قرار گرفته است.

در بخش چهارم، به امنیت سایر سرویس‌هایی که بیشتر مورداستفاده قرار می‌گیرند، پرداخته‌شده است. ازجمله تشریح پروتکل HTTPS برای امنیت وب، پروتکل PGP برای امنیت پست الکترونیک، بهترین شیوه‌های امنیت سیستم‌عامل و بررسی تهدیدات برتر دیتابیس و نحوه مقابله با آن‌ها، در فصول این بخش گنجانده شده است.

هرچند این کتاب توسط اساتید و کارشناسان امنیت مورد بازخوانی و رفع اشکال قرارگرفته، اما نمی‌توان آن را خالی از نقصان دانست. لذا خواهشمندم هرگونه انتقاد و پیشنهاد مدنظر خود را از طریق پست الکترونیک MTRoghani@Gmail.com، برای بنده ارسال نمایید.

در پایان امیدوارم که این کتاب بتواند نقشی هرچند کوچک، در افزایش آگاهی مدیران و کارشناسان IT و امنیت اطلاعات ایفا نماید. در ضمن از تمام اساتید و کارشناسان عزیزی که از راهنمایی‌های خود در نگارش این کتاب دریغ نکرده‌اند، صمیمانه سپاسگزاری می‌نمایم.

با احترام

محمدتقی روغنی

پاییز ۱۳۹۳

فهرست مطالب:

امنیت یک محصول نیست؛

بلکه فرآیندی است شامل سیاست‌گذاری، طراحی، مدیریت و اجرای صحیح تمام سرویس‌ها و محصولات فناوری اطلاعات.

و البته

نظارت مستدام بر عملکرد، به‌روزرسانی و ارتقاء آن‌ها.

بخش اول

استاندارد ISMS

فصل اول

مرور کلی استاندارد ISMS و الزامات آن

فصل دوم

دستورالعمل مدیریت امنیت اطلاعات

فصل اول

مرور کلی استاندارد ISMS و الزامات آن

مبحث اول

مرور استاندارد ISO/IEC 27000:2014

مبحث دوم

مرور استاندارد ISO/IEC 27001:2013

☑ مبحث اول

مرور استاندارد ISO/IEC 27000:2014

سازمان‌ها در هراندازه و هر نوع فعالیت علمی، سیاسی و اقتصادی که قرار داشته باشند، باید مقداری اطلاعات را جمع‌آوری، پردازش، نگهداری و ارسال نمایند. سازمان‌ها دارای مخاطبانی نیز هستند که ممکن است در صورت اعمال نکردن سیاست‌ها و کنترل‌های امنیتی مناسب، خواسته یا ناخواسته تأثیر نامطلوب یا مخرب بر روی سیستم بگذارند. همچنین اطلاعات سازمان می‌تواند همواره برای اشخاص دیگر جالب و موردتوجه باشد و بخواهند با استفاده از ضعف‌های امنیتی موجود در سیستم، به اطلاعات حساس و حیاتی سازمان دسترسی پیدا کنند. اما تهدیدات سازمان تنها به کاربران ناشی، ضعف سیستم و اشخاص خرابکار ختم نمی‌شود؛ بلکه بلایای طبیعی مثل سیل و زلزله یا اتفاقات پیش‌بینی‌نشده مثل آتش‌سوزی و حتی مخاطرات نوظهور نیز تهدید به‌حساب می‌آیند.

مدیران سازمان‌ها درصورتی‌که بخواهند سطح امنیت خود را افزایش داده و از اطلاعات خود محافظت کنند باید استانداردهای امنیتی جامعی را مورداستفاده قرار دهند که تمام ابعاد امنیت اطلاعات را موردتوجه قرار داده باشد. سپس استاندارد موردنظر را توسط افراد متخصص و باتجربه در سازمان خود پیاده‌سازی نموده و همواره برای تداوم عملکرد مناسب، بر آن نظارت داشته باشند.

سازمان استاندارد جهانی (ISO) با همکاری کمیسیون بین‌المللی الکتروتکنیک (IEC) جهت امنیت اطلاعات، اقدام به معرفی استانداردهای سری ISO/IEC 27000 نموده است. در این استانداردها که سیستم مدیریت امنیت اطلاعات (Information Security Management System) یا به‌اختصار ISMS، نامیده می‌شوند؛ سعی شده تا تمام مؤلفه‌های موردنیاز امنیت اطلاعات، از امنیت فیزیکی تا نحوه مدیریت، مدنظر قرار داده شود.

در سال ۱۳۸۷ سازمان استاندارد ملی ایران نیز بر اساس استانداردهای 27001 و 27002 اقدام به معرفی استاندارد ملی امنیت نموده است. شما می‌توانید استاندارد ملی ایران را از طریق وب‌سایت این سازمان به آدرس www.isiri.org دانلود نمایید.

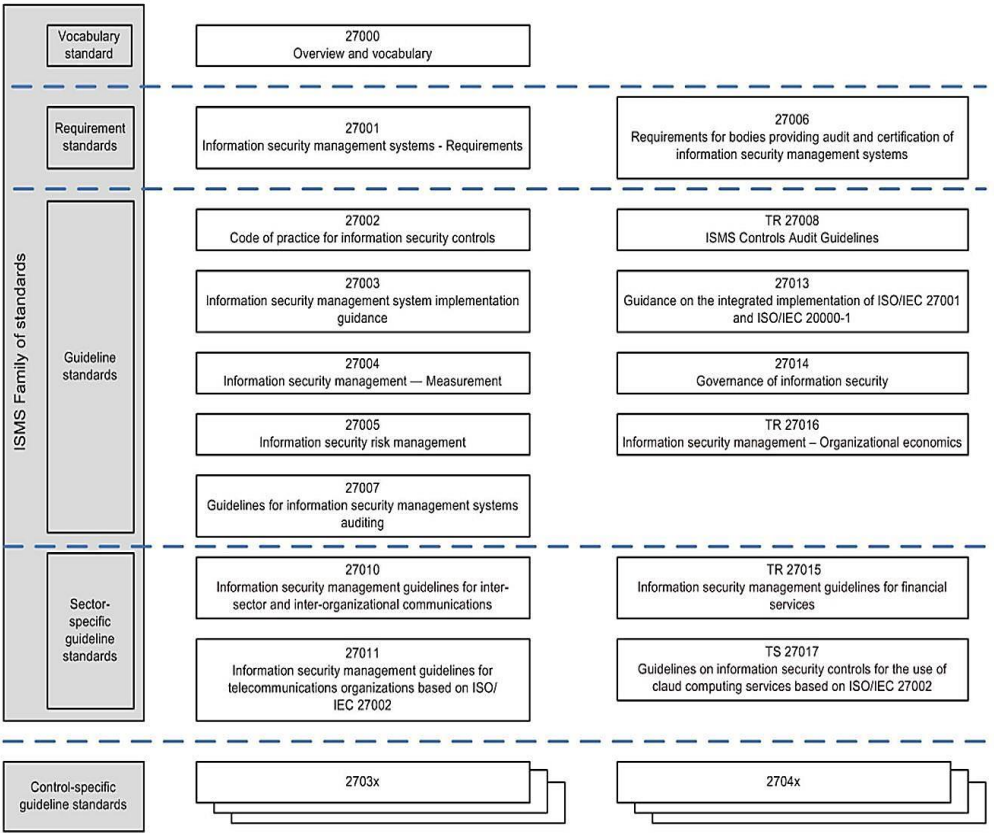
اما آخرین نسخه ارائه‌شده این استاندارد، ISO/IEC 27000:2014 است که در این مبحث به شرح مختصری از آن، که دربرگیرنده اصطلاحات و مرور کلی استانداردهای خانواده ISMS است، می‌پردازیم.

استانداردهای خانواده ISMS

خانواده ISMS متشکل از استانداردهای مرتبط باهم است که بعضی از آن‌ها در حال تدوین بوده و هنوز منتشرنشده و بعضی دیگر نیز منتشر گردیده است. این استانداردها دارای تعدادی مؤلفه مهم ساختاری می‌باشند که بر استانداردهای اصلی تمرکز دارند. استانداردهای اصلی شامل توصیف‌کننده الزامات ISMS (استاندارد ISO/IEC 27001) و الزامات مرکز صدور گواهینامه[1] (ISO/IEC 27006) جهت صادر کردن گواهی انطباق با ISO/IEC 27001 می‌باشند.

استانداردهای دیگر نیز فراهم‌کننده راهنما[2] برای جنبه‌های اجرایی مختلف ISMS، فرآیند عمومی، دستورالعمل‌های مربوط به کنترل و همچنین راهنمای یک بخش خاص می‌باشند.

تصویر زیر نشان‌دهنده ارتباطات درون خانواده استاندارد ISMS است.



[1] Certification
[2] Guidance

مروری بر استانداردهای خانواده ISMS

برای آشنایی با محتویات استانداردهای خانواده ISMS که در تصویر فوق نیز به آن‌ها اشاره گردیده است، به شرح مختصری از آن‌ها می‌پردازیم:

۱- **استاندارد ISO/IEC 27000 (همین استاندارد)**

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی[1]- سیستم مدیریت امنیت اطلاعات- مرور کلی و واژگان

حوزه کاربرد: این استاندارد بین‌المللی به افراد و سازمان‌ها در زمینه‌های زیر کمک می‌کند:

i. بررسی اجمالی استانداردهای خانواده ISMS
ii. مقدمه‌ای بر سیستم مدیریت امنیت اطلاعات (ISMS)
iii. شرح مختصری بر فرآیند PDCA
iv. آشنایی با اصطلاحات و تعاریف استفاده‌شده در استانداردهای خانواده ISMS

هدف: استاندارد ISO/IEC 27000 به توصیف مبانی ISMS و اصطلاحات به‌کاررفته در این سری استاندارد می‌پردازد.

۲- **استاندارد ISO/IEC 27001**

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- سیستم مدیریت امنیت اطلاعات- الزامات[2]

حوزه کاربرد: این استاندارد بین‌المللی الزامات ایجاد، پیاده‌سازی، راه‌اندازی، نظارت، بررسی، نگهداری و بهبود رسمی سیستم مدیریت امنیت اطلاعات (ISMS) را درزمینه مخاطرات کلی کسب‌وکار سازمان تعیین می‌نماید. همچنین این استاندارد مشخص‌کننده الزامات پیاده‌سازی کنترل‌های امنیتی سفارشی‌شده موردنیاز سازمان‌های مختلف و یا بخش‌های وابسته به آن‌ها است. این استاندارد بین‌المللی تمام انواع سازمان‌ها (به‌عنوان‌مثال شرکت‌های تجاری، سازمان‌های دولتی و سازمان‌های غیرانتفاعی) را دربر می‌گیرد.

هدف: استاندارد ISO/IEC 27001 الزامات اصلی توسعه و راه‌اندازی ISMS را ارائه می‌نماید. این الزامات شامل مجموعه‌ای از کنترل‌ها برای مهار و کاهش خطرات مربوط به دارایی‌های اطلاعاتی بوده که سازمان می‌خواهد از طریق عملیاتی کردن ISMS از آن‌ها محافظت نماید.

۳- **استاندارد ISO/IEC 27006**

---

[1] Security Techniques
[2] Requirements

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- الزامات نهادهای ارائه‌دهنده خدمات ممیزی[1] و صدور گواهینامه ISMS

حوزه کاربرد: این استاندارد بین‌المللی علاوه بر الزامات موجود در ISO/IEC 17021، الزامات دیگری نیز مشخص نموده و راهنمایی‌هایی را برای نهادهای ارائه‌کننده ممیزی و صدور گواهینامه ISMS، طبق استاندارد 27001 فراهم می‌نماید. درواقع این استاندارد برای پشتیبانی از تائید صلاحیت نهادهایی است که بر اساس استاندارد 27001 اقدام به صدور گواهینامه ISMS می‌نمایند.

هدف: استاندارد ISO/IEC 27006 مکمل[2] استاندارد 17021 در جهت مشخص نمودن الزاماتی است که باید توسط نهادهایی که قصد ارائه خدمات ممیزی یا صدور گواهی‌نامه دارند، رعایت گردد؛ تا امکان ممیزی یا صدور گواهی انطباق با استاندارد 27001 توسط آن‌ها فراهم گردد.

۴- استاندارد ISO/IEC 27002

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- دستورالعمل[3] مدیریت امنیت اطلاعات

حوزه کاربرد: این استاندارد بین‌المللی لیستی از اهداف کنترلی پذیرفته‌شده و بهترین شیوه‌های[4] کنترلی، فراهم آورده تا جهت راهنمایی در زمان انتخاب و پیاده‌سازی کنترل‌ها برای دست‌یابی به امنیت اطلاعات، مورداستفاده قرار گیرند.

هدف: استاندارد ISO/IEC 27002 فراهم‌کننده راهنما جهت پیاده‌سازی کنترل‌های امنیت اطلاعات است. بندهای ۵ تا ۱۵ این استاندارد به‌طور خاص به مشاوره و راهنمایی پیاده‌سازی بر اساس بهترین شیوه‌ها در خصوص کنترل‌های موجود در بندهای A.5 تا A.15 استاندارد ISO/IEC 27001 است.

۵- استاندارد ISO/IEC 27003

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی ISMS

حوزه کاربرد: این استاندارد بین‌المللی ضمن فراهم‌سازی راهنمای پیاده‌سازی عملی، اطلاعات بیشتری را نیز برای برقراری، پیاده‌سازی، راه‌اندازی، نظارت، بررسی، نگهداری و بهبود ISMS طبق استاندارد 27001 ارائه می‌نماید.

هدف: استاندارد ISO/IEC 27003 رویکردی فرآیندگرا جهت اجرای موفقیت‌آمیز ISMS مطابق با استاندارد 27001 فراهم می‌آورد.

---

[1] Audit
[2] Supplement
[3] Code of practice
[4] Best practice

۶- **استاندارد ISO/IEC 27004**

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- سنجش[1]

حوزه کاربرد: این استاندارد بین‌المللی راهنمایی و مشاوره برای توسعه و نحوه سنجش را به‌منظور ارزیابی اثربخشی ISMS، اهداف کنترلی و کنترل‌های استفاده‌شده برای پیاده‌سازی و مدیریت امنیت اطلاعات طبق استاندارد 27001، فراهم می‌نماید.

هدف: استاندارد ISO/IEC 27004 با ارائه چارچوب مشخصی برای سنجش، امکان ارزیابی تأثیرگذاری ISMS را مطابق با استاندارد 27001 فراهم می‌آورد.

۷- **استاندارد ISO/IEC 27005**

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- مدیریت ریسک امنیت اطلاعات

حوزه کاربرد: استاندارد بین‌المللی 27005 راهنمایی‌هایی را جهت مدیریت ریسک امنیت اطلاعات ارائه می‌نماید. روش‌های تشریح شده در این استاندارد بین‌المللی، از مفاهیم کلی مشخص‌شده در استاندارد 27001، پشتیبانی می‌کنند.

هدف: استاندارد ISO/IEC 27005 ارائه‌دهنده راهنمایی‌هایی جهت پیاده‌سازی رضایت‌بخش یک مدیریت ریسک فرآیندگرا و همچنین تحقق الزامات مدیریت ریسک امنیت اطلاعات بر اساس استاندارد 27001 است.

۸- **استاندارد ISO/IEC 27007**

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- راهنمای ممیزی ISMS

حوزه کاربرد: این استاندارد بین‌المللی علاوه بر شرایط موجود در استاندارد ISO 19011، شامل راهنمای طریقه انجام ممیزی ISMS و همچنین نحوه احراز صلاحیت بازرسان سیستم مدیریت امنیت اطلاعات، نیز است.

هدف: استاندارد ISO/IEC 27007 به ارائه راهنمایی برای سازمان‌هایی می‌پردازد که نیاز به انجام بازرسی داخلی یا خارجی ISMS داشته و یا برنامه ممیزی ISMS را جهت اجرای الزامات مشخص‌شده در استاندارد 27001 مدیریت می‌کنند.

۹- **استاندارد ISO/IEC TR 27008**[2]

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- راهنمای بازرسان بر روی کنترل‌های امنیت اطلاعات

---

[1] Measurement

[2] منظور از TR در این استاندارد، گزارش فنی یا Technical Report است.

حوزه کاربرد: این گزارش فنی، راهنمای نحوه بررسی پیاده‌سازی و بهره‌برداری از کنترل‌ها، شامل بررسی انطباق فنی کنترل‌های سیستم اطلاعات با استانداردهای امنیت اطلاعات سازمان را ارائه می‌دهد.

هدف: تمرکز این گزارش فنی بر روی بررسی کنترل‌های امنیت اطلاعات، ازجمله بررسی تطابق فنی با استاندارد امنیت اطلاعات که توسط سازمان پیاده‌سازی شده، می‌باشد. این استاندارد قصد ارائه راهنمایی خاصی جهت بررسی انطباق در مورد سنجش، ارزیابی ریسک یا ممیزی ISMS که در استانداردهای ISO/IEC 27004، ISO/IEC 27005 یا ISO/IEC 27007 مشخص گردیده را ندارد. این گزارش فنی برای سیستم‌های مدیریت ممیزی، نیز در نظر گرفته نشده است.

۱۰- استاندارد ISO/IEC 27013

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- راهنمای اجرای یکپارچه ISO/IEC 27001 و ISO/IEC 20000-1

حوزه کاربرد: این استاندارد بین‌المللی فراهم آورنده راهنمای اجرای یکپارچه ISO/IEC 27001 و ISO/IEC 20000-1، برای سازمان‌هایی است که قصد انجام یکی از کارهای زیر را دارند:

i. پیاده‌سازی ISO/IEC 27001 درزمانی که ISO/IEC 20000-1 قبلاً پذیرفته‌شده باشد؛ و بالعکس.
ii. پیاده‌سازی هر دو استاندارد ISO/IEC 27001 و ISO/IEC 20000-1 باهم.
iii. هم‌راستا نمودن مدیریت پیاده‌سازی سیستم‌های ISO/IEC 27001 و ISO/IEC 20000-1 موجود.

هدف: این استاندارد به‌منظور فراهم کردن درک بهتری برای سازمان، درباره ویژگی‌ها، شباهت‌ها و تفاوت‌های ISO/IEC 27001 و ISO/IEC 20000-1، ارائه شده است؛ تا کمکی در جهت برنامه‌ریزی یک سیستم مدیریت یکپارچه منطبق با هر دو استاندارد بین‌المللی، باشد.

۱۱- استاندارد ISO/IEC 27014

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- اداره امور امنیت اطلاعات

حوزه کاربرد: این استاندارد بین‌المللی فراهم آورنده راهنمای اصول و فرآیندهایی جهت اداره امور امنیت اطلاعات است؛ که از طریق آن، سازمان می‌تواند ارزیابی، هدایت و نظارت مدیریت امنیت اطلاعات را انجام دهد.

هدف: امنیت اطلاعات به یک موضوع کلیدی برای سازمان‌ها تبدیل‌شده و شکست اقدامات امنیت اطلاعات، می‌تواند به‌صورت مستقیم بر روی شهرت سازمان تأثیرگذار

باشد. بنابراین برای اطمینان از حصول اهداف سازمان، همواره باید بر امنیت اطلاعات نظارت گردد.

۱۲- استاندارد ISO/IEC TR 27016

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصاد سازمانی

حوزه کاربرد: این گزارش فنی روشی را ارائه می‌دهد که سازمان بتواند ازلحاظ اقتصادی درک بهتری از دارایی‌های اطلاعاتی خود داشته باشد. در این صورت سازمان با دقت بیشتری دارایی‌های اطلاعاتی خود را شناسایی نموده، خطرات بالقوه آن دارایی‌های اطلاعاتی را سنجیده، کنترل‌های حفاظت اطلاعات برای آن دارایی‌ها را تشخیص داده، و سطح بهینه منابعی که باید برای تأمین امنیت آن‌ها استفاده شود را تعیین می‌نماید.

هدف: این گزارش فنی مکمل استانداردهای خانواده ISMS است که با جمع‌آوری نقطه نظرات اقتصادی در حفاظت از دارایی‌های اطلاعاتی سازمان، از طریق مدل‌ها و نمونه‌ها، یک راهنمای اقتصاد سازمانی را ازلحاظ امنیت اطلاعات فراهم می‌آورد.

۱۳- استاندارد ISO/IEC 27010

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات برای ارتباطات بین بخشی و درون‌سازمانی

حوزه کاربرد: این استاندارد بین‌المللی، علاوه بر راهنمایی‌های ارائه‌شده در خانواده استاندارد ISO/IEC 27000، دستورالعملی را برای اجرای مدیریت امنیت اطلاعات در محل‌های اشتراک‌گذاری اطلاعات، ارائه نموده و همچنین کنترل‌ها و راهنمایی‌های ویژه مربوط به شروع، اجرا، نگهداری و بهبود امنیت اطلاعات در ارتباطات بین بخشی و درون‌سازمانی را فراهم می‌کند.

هدف: این استاندارد بین‌المللی، قابل‌اجرا برای تمام اشکال تبادل و اشتراک‌گذاری اطلاعات حساس، در هر دو حالت عمومی و خصوصی، ملی و بین‌المللی، در همان بخش کاری و یا بین بخشی، است. به‌طور خاص این استاندارد می‌تواند قابل‌اجرا برای اشتراک‌گذاری یا تبادل اطلاعات مربوط به تأمین، نگهداری و محافظت از زیرساخت‌های حیاتی ملی و یا سازمانی، باشد.

۱۴- استاندارد ISO/IEC 27011

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- راهنمای مدیریت امنیت اطلاعات بر اساس استاندارد ISO/IEC 27002 برای سازمان‌های مخابراتی[1]

[1] Telecommunication

حوزه کاربرد: این استاندارد بین‌المللی شامل دستورالعمل نحوه پیاده‌سازی مدیریت امنیت اطلاعات (ISM) در سازمان‌های مخابراتی است.

هدف: استاندارد ISO/IEC 27011 علاوه بر الزامات موجود در ضمیمه A استاندارد 27001، دستورالعمل خاصی را با اقتباس از استاندارد 27002 برای سازمان‌های مخابراتی فراهم نموده است.

۱۵- استاندارد ISO/IEC TR 27015

طبقه‌بندی: فناوری اطلاعات- فنون امنیتی- دستورالعمل مدیریت امنیت اطلاعات برای خدمات مالی[1]

حوزه کاربرد: این گزارش فنی، علاوه بر دستورالعمل‌های ارائه‌شده در خانواده استاندارد ISO/IEC 27000، دستورالعملی را برای شروع، اجرا، نگهداری و بهبود امنیت اطلاعات در سازمان‌های ارائه‌دهنده خدمات مالی، ارائه می‌نماید.

هدف: این گزارش فنی یک مکمل تخصصی برای ISO/IEC 27001 و ISO/IEC 27002، جهت استفاده توسط سازمان‌های ارائه‌دهنده خدمات مالی است، تا آن‌ها را در موارد زیر حمایت نماید:

i. شروع، اجرا، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات بر اساس استاندارد بین‌المللی ISO/IEC 27001:2005.

ii. طراحی و پیاده‌سازی کنترل‌های تعریف‌شده در ISO/IEC 27002:2005، یا در این استاندارد بین‌المللی.

۱۶- استاندارد ISO/IEC 27799

طبقه‌بندی: انفورماتیک بهداشت[2]- مدیریت امنیت اطلاعات در بهداشت بر اساس استاندارد 27002

حوزه عملکرد: این استاندارد بین‌المللی دستورالعمل پیاده‌سازی مدیریت امنیت اطلاعات (ISM) را در سازمان‌های بهداشت و درمان ارائه می‌نماید.

هدف: استاندارد ISO/IEC 27799 علاوه بر الزامات موجود در ضمیمه A استاندارد 27001، دستورالعمل خاصی را با اقتباس از استاندارد 27002 برای سازمان‌های بهداشت و درمان ارائه نموده است.

---

[1] Financial Services
[2] Health

اصطلاحات و تعاریف[1]

- **کنترل دسترسی (Access Control)**

اطمینان از دسترسی به دارایی‌ها به‌صورت مجاز و محدودشده بر اساس الزامات امنیتی و کسب‌وکار.

- **مسئولیت‌پذیری و پاسخ‌گویی (Accountability)**

مسئولیت‌پذیری یک نهاد در ازای تصمیمات و اقدامات خود.

- **دارایی (Asset)**

هر چیزی که برای سازمان ارزشمند باشد دارایی محسوب می‌گردد. دارایی می‌تواند شامل طیف گسترده‌ای از قبیل اطلاعات، برنامه‌های کاربردی، تجهیزات سخت‌افزاری، افراد و غیره باشد.

- **حمله (Attack)**

تلاش برای تخریب[2]، افشا[3]، تغییر[4]، غیرفعال کردن، سرقت[5] و دسترسی یا استفاده غیرمجاز[6] از یک دارایی را حمله می‌نامند.

- **احراز هویت (Authentication)**

ارائه تضمین، جهت درست بودن مشخصات ادعاشده.

- **اصالت (Authenticity)**

بررسی اینکه ارائه‌دهنده مشخصات، همان است که ادعا می‌کند.

- **دسترس‌پذیری (Availability)**

دارایی‌ها باید برای تقاضاهای مجاز همواره در دسترس و قابل‌استفاده باشد.

- **تداوم کسب‌وکار (Business Continuity)**

حصول اطمینان تداوم عملیات کسب‌وکار از طریق فرآیندها و رویه‌ها.

- **محرمانگی (Confidentiality)**

غیرقابل‌دسترس بودن یا آشکار نبودن اطلاعات برای افراد و فرآیندهای غیرمجاز را محرمانگی می‌گویند.

- **دارایی اطلاعاتی (Information Asset)**

---

[1] Terms and Definitions
[2] Destroy
[3] Expose
[4] Alter
[5] Steal
[6] Unauthorized

دانش یا دیتای دارای ارزش برای سازمان را دارایی‌های اطلاعاتی گویند.

- **امنیت اطلاعات (Information Security)**

منظور از امنیت اطلاعات حفظ محرمانگی، درستی و دسترس‌پذیری اطلاعات است.
البته امنیت اطلاعات علاوه بر موارد فوق می‌تواند شامل مواردی نظیر صحت، پاسخگویی[1]، انکارناپذیری و قابلیت اطمینان بودن اطلاعات نیز باشد.

- **رویداد امنیت اطلاعات (Information Security Event)**

یک رویداد امنیت اطلاعات می‌تواند شامل وقوع حالت شناخته‌شده‌ای در سیستم، شبکه یا سرویس باشد که نشان‌دهنده نقص احتمالی در امنیت اطلاعات، خط‌مشی یا مشکل در کنترل‌ها است. همچنین ممکن است رویداد شامل وضعیت ناشناخته‌ای باشد که به امنیت اطلاعات مربوط است.

- **حادثه امنیت اطلاعات (Information Security Incident)**

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا غیرمنتظره که به‌احتمال‌زیاد عملیات کسب‌وکار را به خطر انداخته و تهدیدی برای امنیت اطلاعات محسوب می‌گردد.

- **مدیریت حوادث امنیت اطلاعات (Information Security Incident Management)**

به مجموع فرآیندهایی که برای آشکارسازی[2]، گزارش دهی[3]، ارزیابی[4]، پاسخ‌دهی به[5]، رسیدگی به[6] و یادگیری حوادث امنیت اطلاعات مورداستفاده قرار می‌گیرد، مدیریت حوادث امنیت اطلاعات می‌گویند.

- **سیستم مدیریت امنیت اطلاعات (Information Security Management System)**

سیستم مدیریت امنیت اطلاعات یا ISMS، بخشی از سیستم کلان مدیریتی است که اساس آن بر رویکرد مخاطره کسب‌وکار بوده و شامل برقراری[7]، پیاده‌سازی، عملیات، نظارت، بررسی، نگهداری و بهبود امنیت اطلاعات است.

- **ریسک امنیت اطلاعات (Information Security Risk)**

توانایی بالقوه یک تهدید در بهره‌برداری از آسیب‌پذیری یک یا گروهی از دارایی‌ها که درنهایت منجر به آسیب رسیدن به سازمان می‌گردد.

---

[1] Accountability
[2] Detecting
[3] Reporting
[4] Assessing
[5] Responding to
[6] Dealing with
[7] Establish

- **درستی** [۱] **(Integrity)**

خاصیت حفاظت از صحت [۲] و تمامیت [۳] دارایی‌ها.

- **خط‌مشی (Policy)**

خط‌مشی یا سیاست، عبارت است از قصد و جهت‌دهی کلی سازمان که به‌صورت رسمی توسط مدیریت تبیین شده است.

- **فرآیند (Process)**

مجموعه فعالیت‌های مرتبط باهم که باعث تبدیل ورودی به خروجی می‌گردد.

- **رویه (Procedure)**

راه و روش مشخص‌شده برای انجام یک فعالیت یا فرآیند را رویه می‌گویند.

- **تهدید (Threat)**

عامل بالقوه حادثه‌ای ناخواسته که ممکن است منجر به آسیب یک سازمان یا سیستم گردد.

- **آسیب‌پذیری (Vulnerability)**

ضعف موجود در یک دارایی یا کنترل که می‌تواند توسط یک تهدید مورد سوءاستفاده قرار گیرد را آسیب‌پذیری می‌گویند.

مروری بر ISMS

سیستم مدیریت امنیت اطلاعات یا ISMS، مدلی را برای برقراری، پیاده‌سازی، راه‌اندازی [۴]، نظارت [۵]، بررسی [۶]، حفظ و نگهداری [۷]، و بهبود حفاظت از دارایی‌های اطلاعاتی به‌منظور تحقق اهداف کسب‌وکار فراهم می‌نماید. طراحی این مدل بر اساس ارزیابی ریسک و سطح پذیرش آن توسط سازمان انجام‌گرفته تا مدیریت و رفع ریسک به‌صورت مؤثر انجام پذیرد.

تجزیه‌وتحلیل الزامات حفاظت از دارایی‌های اطلاعاتی و اعمال کنترل‌های مناسب جهت حصول اطمینان از حفاظت آن‌ها، به پیاده‌سازی موفق ISMS کمک می‌نماید.

---

[۱] عبارت Integrity دارای معانی بسیاری ازجمله درستی، صحت، یکپارچگی و تمامیت است. اما به نظر بنده معنی قابل‌قبول در جملات این بخش، درستی است.

[2] Accuracy
[3] Completeness
[4] Operating
[5] Monitoring
[6] Reviewing
[7] Maintaining

اصول اساسی زیر می‌تواند کمک شایانی در جهت اجرای موفقیت‌آمیز ISMS باشد:

- آگاهی از ضرورت نیاز به امنیت اطلاعات.
- تخصیص مسئولیت برای امنیت اطلاعات.
- ترکیب تعهد مدیریتی و منافع ذینفعان.
- افزایش ارزش‌های اجتماعی.
- ارزیابی ریسک جهت تعیین کنترل‌های مناسب برای دستیابی به سطح قابل‌قبول ریسک.
- گنجاندن امنیت به‌عنوان یک عنصر ضروری در سیستم‌ها و شبکه‌های اطلاعاتی.
- پیشگیری و تشخیص فعال حوادث امنیت اطلاعات.
- حصول اطمینان از یک رویکرد جامع برای مدیریت امنیت اطلاعات.
- ارزیابی مستمر امنیت اطلاعات و ایجاد تغییرات مناسب.

دستیابی به امنیت اطلاعات نیازمند مدیریت مخاطرات ناشی از تهدیدات فیزیکی، انسانی و فناوری‌های مربوط به اطلاعات در تمام اشکال مورداستفاده سازمان است. لذا همواره بخشی از ISMS هر سازمان را مخاطرات مرتبط با دارایی‌های اطلاعاتی تشکیل می‌دهد.

انتظار می‌رود پیاده‌سازی ISMS در سازمان به‌عنوان یک تصمیم استراتژیک موردپذیرش قرار گیرد. این تصمیم لازم است مطابق با نیازهای سازمان کاملاً یکپارچه، متناسب و به‌روز باشد.

طراحی و پیاده‌سازی ISMS، تحت تأثیر نیازها، اهداف سازمانی، الزامات امنیتی، فرآیندهای کسب‌وکار، وسعت و ساختار آن سازمان خواهد بود. توجه داشته باشید که منافع و امنیت اطلاعات موردنیاز همه ذینفعان ازجمله مشتریان، تأمین‌کنندگان[1]، شرکای تجاری، سهامداران[2] و سایر اشخاص ثالث[3] باید در طراحی و راه‌اندازی ISMS منعکس گردد.

سیستم مدیریت امنیت اطلاعات(ISMS) برای کسب‌وکار هر دو بخش خصوصی و عمومی مهم است. این سیستم که برای فعالیت‌های مدیریت ریسک نیز ضروری است، هر صنعتی را قادر می‌سازد تا از کسب‌وکار الکترونیکی پشتیبانی نماید. زمانی که یک سازمان اقدام به اتخاذ استانداردهای خانواده ISMS می‌نماید، توانایی خود را در اعمال اصول امنیت اطلاعات متقابل و پایدار در برابر شرکای تجاری و سایر طرف‌های ذینفع نشان می‌دهد.

با همه این اوصاف در برخی موارد هنگام طراحی و توسعه سیستم‌های اطلاعات، ممکن است امنیت اطلاعات موردتوجه قرار نگیرد. علاوه بر این امنیت اطلاعات اغلب به‌عنوان یک راه‌حل فنی

[1] Suppliers
[2] Shareholders
[3] Third parties

در نظر گرفته می‌شود؛ **ولی امنیتی که از راه‌های فنی به دست می‌آید محدود بوده و حتی ممکن است بدون پشتیبانی توسط مدیریت و فقدان روش‌های اجرایی مناسب، بی‌تأثیر باشد.** همچنین گنجاندن امنیت داخل یک سیستم اطلاعاتی پس از پیاده‌سازی آن می‌تواند پرهزینه و پرزحمت باشد. در مقابل سیستم ISMS شامل تمام کنترل‌ها بوده و نیازمند برنامه‌ریزی دقیق و توجه به تمام جزئیات است. به‌عنوان‌مثال کنترل‌های دسترسی که ممکن است فنی (منطقی)، فیزیکی، اداری (مدیریتی) و یا ترکیبی از این‌ها باشد؛ ابزارهایی فراهم می‌آورد تا از دسترسی مجاز و محدودشده به دارایی‌های اطلاعاتی اطمینان حاصل شود.

امنیت اطلاعات با اجرای مجموعه‌ای از کنترل‌هایی به دست می‌آید که از طریق فرآیند مدیریت ریسک انتخاب و توسط ISMS مدیریت می‌شوند. این کنترل‌ها شامل سیاست‌ها (خط‌مشی‌ها)، فرآیندها، روش‌های اجرایی، ساختار سازمانی، نرم‌افزار و سخت‌افزارهایی است که در جهت حفاظت از دارایی‌های اطلاعاتی شناسایی‌شده است. برای حصول اطمینان از دستیابی به اهداف موردنظر امنیتی و کسب‌وکار سازمان، نیاز است که این کنترل‌ها مشخص، پیاده‌سازی، نظارت و بررسی گردیده و در صورت لزوم بهبود یابند. این انتظار وجود دارد که همواره کنترل‌های امنیت اطلاعات با فرآیندهای کسب‌وکار سازمان یکپارچه‌شده باشند.

اصول PDCA

استانداردهای سیستم مدیریتیISO دارای اصول بهره‌برداری مصوب بانامPDCA می‌باشند که این اصول در استانداردهای خانواده ISMS نیز مورداستفاده قرار می‌گیرد. منظور از PDCA، فرآیندهای Plan، Do، Check و Act است که در ادامه به تشریح آن‌ها می‌پردازیم:

۱- **برنامه (Plan)**

تعیین اهداف و ایجاد برنامه‌ها (تجزیه‌وتحلیل وضعیت سازمان، تعیین اهداف کلی و زیرمجموعه‌ها و درنهایت توسعه برنامه جهت دستیابی به آن‌ها).

۲- **اجرا (Do)**

اجرای برنامه‌ها (انجام کارهایی که در برنامه مشخص‌شده‌اند).

۳- **بررسی (Check)**

سنجش نتایج به‌دست‌آمده (سنجش و نظارت بر دستاوردها، تا مشخص شود چه حد به اهداف موردنظر نزدیک شده‌ایم).

۴- **اقدام (Act)**

اصلاح و بهبود فعالیت‌ها (به قول خودمون شکست پلی است برای پیروزی! درس گرفتن از اشتباهات گذشته به‌منظور بهبود فعالیت‌ها در دستیابی به نتایج بهتر).

برقراری، نظارت، نگهداری و بهبود عملکرد ISMS

یک سازمان جهت برقراری، نظارت، نگهداری و بهبود عملکرد ISMS، نیازمند تعهد به انجام مراحل زیر است:

۱- شناسایی دارایی‌های اطلاعاتی و الزامات امنیتی مربوط به آن‌ها.
۲- ارزیابی مخاطرات امنیت اطلاعات.
۳- انتخاب و پیاده‌سازی کنترل‌های مربوطه برای مدیریت مخاطرات غیرقابل‌قبول.
۴- نظارت، نگهداری و بهبود اثربخشی کنترل‌های امنیتی مرتبط با دارایی‌های اطلاعاتی سازمان.

برای اطمینان از عملکرد مؤثرISMS در محافظت از دارایی‌های اطلاعاتی سازمان، لازم است تا موارد فوق به‌صورت مداوم جهت شناسایی تغییرات ایجادشده در مخاطرات، راهبردهای سازمان و یا اهداف کسب‌وکار تکرار شوند.

فصل دوم

دستورالعمل
مدیریت امنیت اطلاعات

مبحث اول

مرور استاندارد ISO/IEC 27002:2013

بخش دوم

رمزنگاری

فصل سوم

مفاهیم رمزنگاری

فصل چهارم

الگوریتم‌های رمزنگاری متقارن

فصل پنجم

الگوریتم‌های رمزنگاری نامتقارن

فصل ششم

توابع درهم‌سازی و کاربردها

فصل سوم

مفاهیم رمزنگاری

مبحث اول

مفاهیم و اصطلاحات رمزنگاری

مبحث دوم

مفاهیم رمزنگاری متقارن

مبحث سوم

مفاهیم رمزنگاری نامتقارن

مبحث چهارم

مفاهیم توابع درهم سازی

☑ مبحث سوم

مفاهیم رمزنگاری نامتقارن

رمزنگاری نامتقارن (Asymmetric) یا کلیدعمومی (Public Key)، نوعی رمزنگاری است که در آن، رمزگذاری و رمزگشایی با دو کلید متفاوت انجام می‌پذیرد. این دو کلید بانام‌های کلیدخصوصی (Private Key) و کلیدعمومی (Public Key) شناخته می‌شوند.

یکی از مهم‌ترین دلایل پیدایش رمزنگاری نامتقارن یا کلید عمومی، مشکل تبادل کلید در الگوریتم‌های رمزنگاری متقارن بود. برخلاف رمزنگاری متقارن که رمزگذاری و رمزگشایی با یک کلید یکسان انجام می‌گرفت؛ در رمزنگاری نامتقارن، رمزگذاری با یک کلید و رمزگشایی با کلید دیگری انجام می‌پذیرد.

الگوریتم‌های کلیدعمومی به‌جای Permutation و Substitution، بر اساس توابع ریاضی ایجاد شده‌اند. همچنین استفاده از دو کلید مجزا برای رمزگذاری و رمزگشایی، باعث نتایج بهتری درزمینه محرمانگی، احرازهویت و تبادل کلید گردیده است.

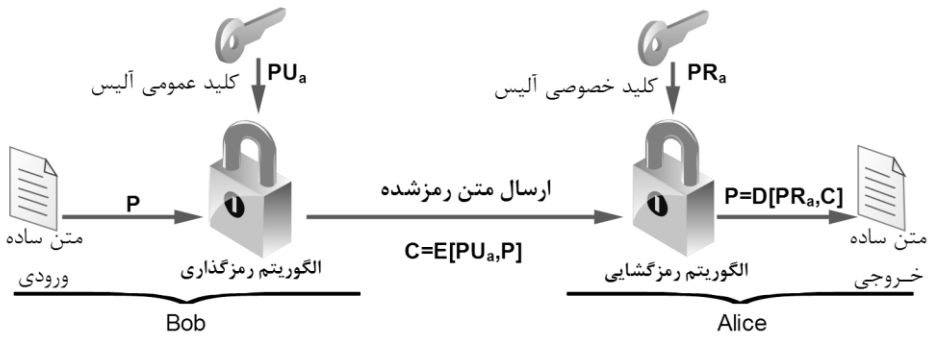
در مقایسه رمزنگاری نامتقارن یا کلیدعمومی با رمزنگاری متقارن، تصورات نادرستی وجود دارد که باید به آن‌ها پاسخ داده شود. اول آنکه تصور عمومی بر آن است که رمزنگاری کلیدعمومی از رمزنگاری متقارن امن‌تر است. ولی در اصل هیچ دلیلی وجود ندارد که بتوان یکی را از دیگری امن‌تر و در مقابل حملات مقاوم‌تر دانست؛ بلکه قدرت هر الگوریتم رمزنگاری به طول کلید و محاسبات انجام‌شده است.

تصور غلط دوم این است که باوجود رمزنگاری نامتقارن، رمزنگاری متقارن منسوخ‌شده یا به‌زودی منسوخ خواهد شد. اما به دلیل سربار محاسباتی کلیدعمومی، هیچ احتمال قابل پیش‌بینی برای کنار گذاشتن رمزنگاری متقارن وجود ندارد.

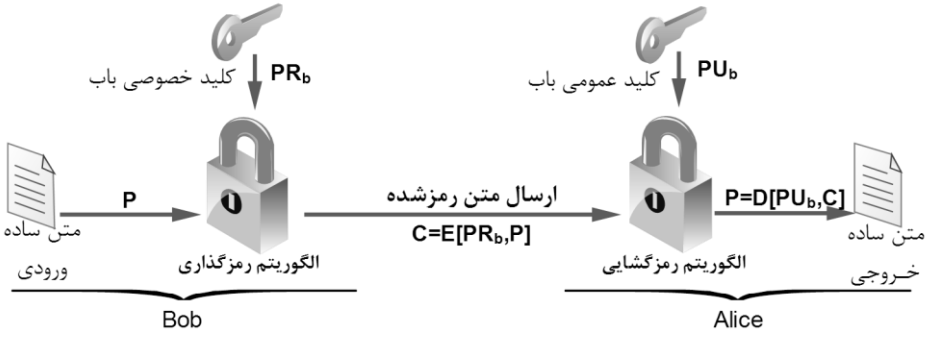
در رمزنگاری نامتقارن، رمزگذاری هم می‌تواند توسط کلید عمومی انجام شود و هم توسط کلید خصوصی. برای محرمانگی، رمزگذاری باید با کلیدعمومی گیرنده و برای احراز هویت، رمزگذاری باید با کلید خصوصی فرستنده انجام گیرد.

در الگوریتم رمز نامتقارن از هر دو کلیدخصوصی و عمومی، یکی برای رمزگذاری و دیگری برای رمزگشایی استفاده می‌شود؛ پس بالطبع هر دو کلید خصوصی و عمومی می‌توانند هم در رمزگذاری و هم در رمزگشایی مورداستفاده قرار گیرند. تصویر زیر نحوه استفاده از کلیدخصوصی و کلیدعمومی در رمزنگاری نامتقارن را به‌صورت ساده نمایش می‌دهد.

رمزگذاری با استفاده از کلید عمومی



رمزگذاری با استفاده از کلید خصوصی



رمزنگاری نامتقارن برای رمزگذاری و رمزگشایی از دو کلید متفاوت استفاده می‌نماید؛ به‌عبارت‌دیگر امکان رمزگشایی با همان کلید مورداستفاده در رمزگذاری، وجود ندارد. درصورتی‌که رمزگذاری با کلید عمومی گیرنده انجام‌شده باشد، برای رمزگشایی حتماً باید از کلید خصوصی گیرنده استفاده شود؛ و اگر برای رمزگذاری از کلید خصوصی فرستنده استفاده شده باشد، فقط با کلید عمومی فرستنده قابل رمزگشایی خواهد بود.

کلید خصوصی و کلیدعمومی همزمان برای یک شخص ایجاد می‌گردد؛ به‌طوری‌که این دو کلید مستقل ولی مرتبط با یکدیگر می‌باشند. کلید عمومی ایجادشده به‌صورت عمومی در اختیار همه طرف‌های ارتباط قرار می‌گیرد. اما کلید خصوصی فقط باید نزد صاحب کلید و به‌صورت کاملاً محرمانه نگهداری و محافظت گردد.

ویژگی‌های الگوریتم رمزنگاری نامتقارن

الگوریتم رمزنگاری نامتقارن دارای ویژگی‌های زیر است:

- حتی در صورت اطلاع از الگوریتم رمزنگاری و کلید رمزگذاری مورداستفاده، امکان محاسبه کلید رمزگشایی وجود ندارد.
- هریک از دو کلید عمومی و خصوصی می‌توانند برای رمزگذاری و کلید دیگر برای رمزگشایی مورداستفاده قرار گیرد.
- درصورتی‌که پیام با کلید عمومی گیرنده رمز شود، فراهم آورنده محرمانگی و اگر با کلید خصوصی فرستنده رمز شود، فراهم آورنده احرازهویت است.
- هر کاربر می‌تواند یک دسته‌کلید از کلیدهای عمومی کاربران مختلف را در اختیار داشته باشد؛ چراکه کلید عمومی برای هر درخواست‌کننده‌ای ارسال می‌شود.
- اگر پیامی با کلید عمومی یک کاربر (مثلاً آلیس) رمز شده باشد، رمزگشایی آن فقط برای آلیس امکان‌پذیر است؛ به دلیل اینکه شخص دیگری از کلید خصوصی آلیس اطلاع ندارد و البته نباید داشته باشد.
- اگر پیامی فقط با کلید خصوصی فرستنده رمز شده باشد، رمزگشایی آن برای هر کاربری که از کلید عمومی فرستنده اطلاع داشته باشد، امکان‌پذیر خواهد بود.
- هرزمانی که کاربر احساس نیاز کند، می‌تواند برای خود یک جفت کلید خصوصی و عمومی جدید ایجاد نماید. کلید خصوصی را به‌صورت امن نزد خود نگه‌داشته و کلید عمومی را نیز در یک محل عمومی برای دسترسی درخواست‌کنندگان قرار دهد.
- در هر فرآیند رمزگذاری و رمزگشایی، باید از یک جفت کلید مربوط به هم استفاده شود. مثلاً نمی‌توان پیام را با کلید خصوصی باب رمزگذاری کرد ولی با کلید عمومی آلیس رمزگشایی نمود!
- کلیدهای عمومی به‌طورمعمول در یک مکان عمومی قرار می‌گیرند تا هر کاربری که نیاز داشته باشد به‌راحتی بتواند به آن‌ها دسترسی پیدا کند.
- تبادل کلیدهای عمومی به‌راحتی می‌تواند بر روی بستر ارتباطی ناامن انجام پذیرد.
- پیام‌های رمزشده در رمزنگاری نامتقارن، بر روی بستر ارتباطی عمومی و ناامن انتقال می‌یابند.
- لغو[1] کلید خصوصی و عمومی توسط مالک کلید، امکان‌پذیر است.
- در صورت افشا شدن کلید خصوصی، باید سریعاً زوج کلید مربوطه لغو شوند.

[1] Revoke

مقایسه رمزنگاری متقارن با رمزنگاری نامتقارن

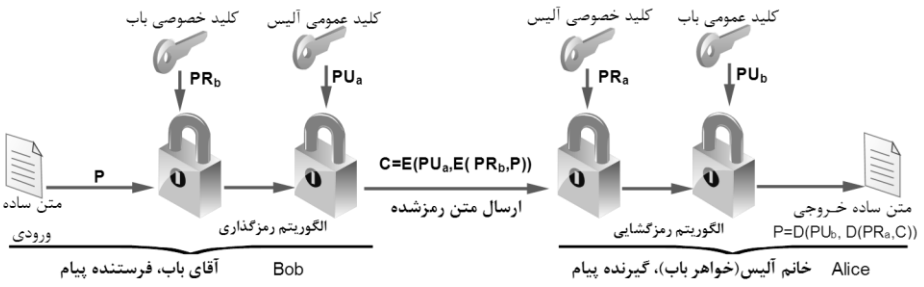
جدول زیر شامل مقایسه بین الگوریتم‌های رمزنگاری متقارن و الگوریتم‌های رمزنگاری نامتقارن است:

	رمزنگاری متقارن	رمزنگاری نامتقارن
نیازهای عملیاتی	۱. برای رمزگذاری و رمزگشایی از یک کلید و الگوریتم مشابه استفاده می‌شود. ۲. فرستنده و گیرنده باید الگوریتم و کلید مورداستفاده را باهم به اشتراک‌گذارند. ۳. برای اشتراک‌گذاری کلید، نیاز به یک کانال انتقال امن است.	۱. برای رمزگذاری و رمزگشایی از یک الگوریتم مشابه ولی دو کلید متفاوت استفاده می‌شود؛ یک کلید برای رمزگذاری و یک کلید برای رمزگشایی. ۲. فرستنده و گیرنده هرکدام باید یکی از کلیدها را در اختیار داشته باشند. (نیازی به یکسان بودن کلیدها نیست) ۳. کلید عمومی را می‌توان از طریق کانال ناامن انتقال داد.
نیازهای امنیتی	۱. کلید باید به‌صورت امن نگهداری شود. ۲. کشف پیام بدون داشتن سایر اطلاعات امکان‌پذیر نباشد. ۳. دانستن الگوریتم به‌علاوه داشتن چند نمونه متن رمزشده نباید منجر به کشف کلید شود.	۱. فقط یکی از دو کلید (کلید خصوصی) باید به‌صورت امن نگهداری شود. ۲. کشف پیام بدون داشتن سایر اطلاعات امکان‌پذیر نباشد. ۳. دانستن الگوریتم به‌علاوه یکی از کلیدها به همراه داشتن چند نمونه متن رمزشده، نباید منجر به کشف کلید شود.

محرمانگی و احرازهویت

همان‌طور که گفته شد، درصورتی‌که فرستنده، پیام را با کلید خصوصی خود رمز نماید، فراهم‌کننده احراز هویت و درصورتی‌که پیام را با کلید عمومی گیرنده رمز نماید، فراهم آورنده محرمانگی است. اما درصورتی‌که پیام صرفاً با کلید خصوصی فرستنده رمز شده باشد، هر کاربری که کلید عمومی فرستنده را در اختیار داشته باشد، قادر به رمزگشایی پیام خواهد بود.

اگر بخواهیم که احراز هویت و محرمانگی را همزمان باهم در اختیار داشته باشیم، باید فرستنده پس از رمزگذاری پیام با کلید خصوصی خود، مجدداً پیام را با کلید عمومی گیرنده نیز رمز نماید. در این صورت هیچ کاربری غیر از گیرنده موردنظر نمی‌تواند رمزگشایی مرحله اول که نیاز به کلید خصوصی گیرنده دارد را انجام دهد. اما گیرنده پس‌ازآنکه در مرحله اول پیام را با کلید خصوصی خود رمزگشایی نمود، در مرحله دوم رمزگشایی را با کلید عمومی فرستنده انجام می‌دهد. این عمل که در تصویر زیر نمایش داده‌شده است، باعث می‌گردد همزمان محرمانگی و احراز هویت را در اختیار داشته باشیم.



فرآیند احراز هویت در تصویر بالا به این صورت است که کلید خصوصی را هیچ‌کس جز مالک کلید در اختیار ندارد، از طرف دیگر وقتی رمزگذاری با کلید خصوصی انجام می‌شود، عملیات رمزگشایی فقط با کلید عمومی امکان‌پذیر است. پس وقتی آلیس می‌تواند با کلید عمومی باب، متن را رمزگشایی نماید، مطمئن می‌شود که فرستنده پیام نمی‌تواند کسی جز باب باشد.

کاربردهای سیستم رمزنگاری کلیدعمومی

بسته به کاربرد موردنظر، فرستنده می‌تواند از کلید خصوصی خود، کلید عمومی گیرنده و یا هر دو آن‌ها برای رمزگذاری استفاده نماید. اگر بخواهیم کاربردهای رمزنگاری نامتقارن را تقسیم‌بندی کنیم، سه گروه به‌صورت زیر خواهیم داشت:

- **رمزگذاری / رمزگشایی**

ارسال‌کننده، پیام را با کلید عمومی گیرنده رمزگذاری می‌نماید.

- **امضای دیجیتال**[1]

فرستنده، پیام را با کلیدخصوصی خود امضاء می‌نماید. معمولاً امضاء با اعمال الگوریتم رمزگذاری با کلیدخصوصی بر یک بلوک کوچک از دیتا انجام می‌پذیرد.

[1] Digital Signature

- تبادل کلید[1]

دو طرف باید کلید جلسه[2] را با یکدیگر تبادل نمایند.

بعضی از الگوریتم‌های رمزنگاری هر سه کاربرد فوق را می‌توانند فراهم آورند؛ و البته بعضی دیگر فقط می‌توانند یک یا دو کاربرد از موارد ذکرشده را پشتیبانی نمایند. جدول زیر نمایش‌دهنده این موضوع است:

الگوریتم	رمزگذاری/رمزگشایی	امضای دیجیتال	تبادل کلید
RSA	بلی	بلی	بلی
Elliptic Curve	بلی	بلی	بلی
Diffie-Hellman	خیر	خیر	بلی
DSS	خیر	بلی	خیر

الزامات رمزنگاری نامتقارن[3]

برای داشتن یک سیستم رمزنگاری نامتقارن، الزامات زیر باید فراهم باشد:

۱. محاسبات تولید یک جفت کلید (کلید عمومی و خصوصی) برای طرف B آسان باشد.

۲. برای فرستنده (A)، محاسبه متن رمزشده متناظر با کلید عمومی گیرنده و پیام (M)، آسان باشد. $C = \mathrm{E}(PUb, M)$

۳. برای دریافت‌کننده(B) محاسبه رمزگشایی(D) متن رمزشده(C) بر اساس کلید خصوصی خودش، آسان باشد.

$$M = \mathrm{D}(PRb, C) = \mathrm{D}[PRb, \mathrm{E}(PUb, M)]$$

۴. برای مهاجم، محاسبه کلیدخصوصی گیرنده (PR_b)، حتی با در اختیار داشتن کلید عمومی گیرنده(PU_b)، امکان‌پذیر نباشد.

۵. به دست آوردن پیام اصلی، حتی با داشتن متن رمزشده و کلیدعمومی گیرنده، برای مهاجم امکان‌پذیر نباشد.

۶. از هر دو کلید بتوان هم برای رمزگذاری و هم برای رمزگشایی استفاده نمود.

$$M = \mathrm{D}[PUb, \mathrm{E}(PRb, M)] = \mathrm{D}[PRb, \mathrm{E}(PUb, M)]$$

---

[1] Key Exchange

[2] Session Key

[3] همان‌طور که گفتم، برای رمزنگاری نامتقارن از عبارت کلیدعمومی نیز استفاده می‌شود. من در این کتاب نسبت به جمله جاری، به‌صورت متناوب از هر دو عبارت فوق استفاده کرده‌ام.

فصل چهارم

الگوریتم‌های رمزنگاری متقارن

مبحث اول

الگوریتم DES

مبحث دوم

الگوریتم AES

مبحث سوم

الگوریتم Triple DES

مبحث چهارم

روش‌های عملیاتی رمزنگاری بلوکی

☑ مبحث اول

الگوریتم DES

الگوریتم Data Encryption Standard(DES)، یک الگوریتم رمزنگاری متقارن است و در گروه رمزنگاری مدرن قرار می‌گیرد. الگوریتم DES عملیات رمزنگاری خود را به‌صورت بلوکی و بر اساس کلید محرمانه انجام می‌دهد.

الگوریتم DES در دهه 1970 میلادی در امریکا مطرح شد و تا سال 1999 به‌عنوان استاندارد مورداستفاده قرار می‌گرفت. در سال 1999 الگوریتم رمزنگاری DES شکسته شد و به همین دلیل جای خود را به یک الگوریتم قدرتمندتر واگذار نمود.

هرچند که امروزه از این الگوریتم کمتر استفاده می‌شود، ولی به دلیل اینکه فرآیند عملکرد این الگوریتم مبنایی برای بعضی استانداردهای رمزنگاری دیگر است، لذا در این مبحث به شرح آن می‌پردازیم.

الگوریتم DES نام استاندارد برای الگوریتم Lucifer است که برمبنای الگوریتم فایستل توسعه داده‌شده است. این الگوریتم یک بلوک مشخصی از دیتا را گرفته و با استفاده از کلید، آن را رمزگذاری می‌نماید. خروجی الگوریتم نیز یک بلوک دیتا به‌اندازه بلوک ورودی خواهد بود.

در این مبحث ابتدا به تشریح الگوریتم فایستل و سپس به شرح الگوریتم DES می‌پردازیم.

الگوریتم فایستل

فایستل یک الگوریتم رمزنگاری بلوکی است که توسط آقای Horst Feistel ارائه گردیده است. این الگوریتم بعدها مبنای ایجاد بسیاری از الگوریتم‌های رمزنگاری متقارن قرار گرفت.

به‌طور خاص فایستل پیشنهاد رمز کردن بر اساس جایگزینی و جابجایی متناوب در متن اصلی را مطرح نموده است. درواقع فایستل با ارائه این دو روش خواسته که برای شروط شانون، یک راهکار عملی ارائه نماید.

۱. **جایگزینی (Substitution)**

هر عنصر یا گروهی از عناصر متن‌ساده، منحصراً با عنصر یا گروهی از عناصر متناظر در متن رمزشده، جایگزین شوند.

۲. **جایگشت (Permutation)**

طی فرآیند جایگشت، رشته‌ای[1] از عناصر متن ساده، با یکدیگر جابجا می‌شوند. در این جابجایی هیچ‌یک از عناصر داخلی موجود در آن رشته نباید اضافه، حذف و یا جابجا شوند؛ بلکه قصد این است که توالی خود رشته از بین برود و نه عناصر موجود در آن.

رمزگذاری و رمزگشایی در فایستل

فایستل یک الگوریتم Block Cipher است، لذا دیتای ورودی این الگوریتم نیز باید به‌صورت بلوکی باشد. پس باید در ورودی یک بلوک از دیتای مربوط به متن ساده همراه با کلید موردنظر قرار گیرد. در ابتدا فایستل بلوک دریافتی را به دو قسمت مساوی راست (R) و چپ (L) تقسیم می‌نماید. ❶ سپس هر دونیمه را تحویل دور (Round) اول می‌دهد. ❷ با توجه به تعدد دورها، خروجی هر دور به‌عنوان ورودی دور بعد خواهد بود. در هر دور نیاز به یک کلید مخصوص هم داریم که این کلید از کلید اصلی مشتق گردیده است. ❸

در الگوریتم فایستل تعیین تعداد دورها (Round) بر عهده استفاده‌کننده است. فقط باید توجه داشته باشید که کلیدهای محرمانه هر دور باید متفاوت و برگرفته از کلید اصلی باشند.

ساختار تمام‌دورها شبیه به هم است؛ یعنی عملیاتی که در هر دور اتفاق می‌افتد یکسان است. در هر دور، عمل جایگزینی (Substitution) بر روی نیمه چپ دیتا اتفاق می‌افتد؛ به همین دلیل یک کپی از نیمه سمت راست به‌عنوان نیمه سمت چپ دیتا تحویل دور بعدی می‌گردد. ❹ از طرف دیگر، پس‌ازآنکه تابع F بر اساس کلید بر روی نیمه راست دیتا اعمال شد، خروجی تابع با نیمه چپ دیتا XOR گردیده و به‌عنوان نیمه راست دیتا به دور بعد تحویل داده می‌شود. ❺

دور بعد دونیمه راست و چپ را تحویل گرفته و فارغ از عملیات انجام‌شده بر روی دیتا، همان مراحل دور قبل را البته با کلید جدید، اعمال می‌نماید. ❻

اما پس از انجام دور پایانی، نیمه راست و چپ به‌دست‌آمده بدون انجام هیچ کار خاصی بر روی دیتا، با یکدیگر جابجا می‌شوند. ❼ این جابجایی پس از آخرین مرحله جهت ویژگی Permutation یا جایگشت می‌باشد که بر اساس پیشنهاد شانون انجام‌شده است.

همان‌طور که قبلاً گفته شد، عملیات رمزگشایی دقیقاً عکس عملیات رمزگذاری اتفاق می‌افتد. در الگوریتم فایستل نیز رمزگشایی به تعداد دورهای انجام‌شده در عملیات رمزگذاری تکرار می‌شود؛ اما این بار به‌صورت معکوس. ❽ توجه داشته باشید که ترتیب کلیدها در رمزگشایی نیز باید به‌صورت عکس رمزگذاری (یعنی آخر به اول)، مورداستفاده قرار گیرد. ❾

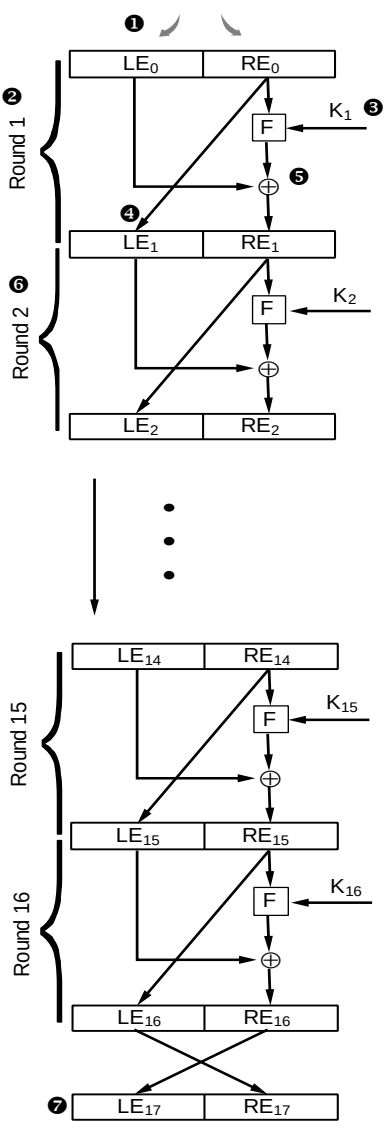
برای فهم بهتر الگوریتم فایستل، مراحل رمزگذاری و رمزگشایی که بر اساس ۱۶ دور ترسیم گردیده را در صفحه بعد ملاحظه بفرمائید.

[1] Sequence

مراحـل رمزگذاری فایستل
Encryption

ورودی (متن ساده)
Input

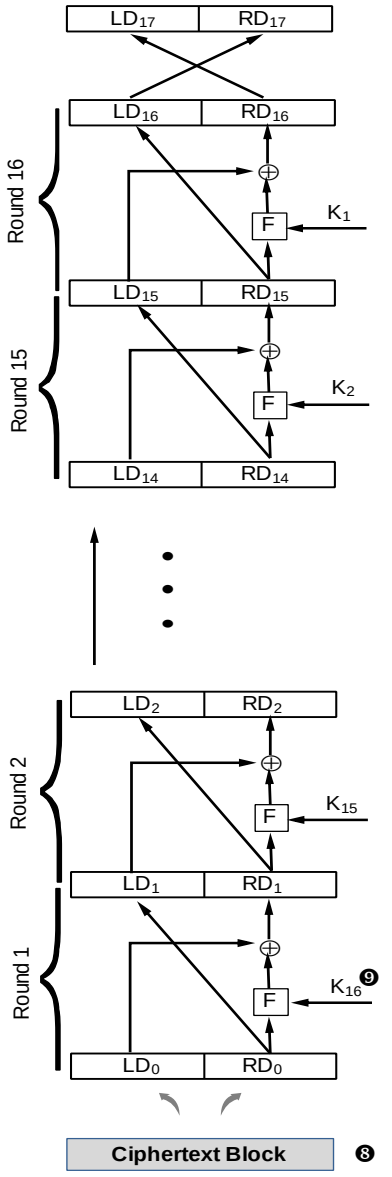
Plaintext Block



خـروجی (متن رمزشده)
Ciphertext

مراحـل رمزگشایی فایستل
Decryption

خروجی (متن ساده)
Output



Ciphertext Block ❽

ورودی (متن رمزشده)
Input

فصل پنجم

الگوریتم‌های رمزنگاری نامتقارن

مبحث اول

الگوریتم RSA

مبحث دوم

الگوریتم دیفی‌هلمن

☑ مبحث اول

الگوریتـم RSA

مشهورترین الگوریتم رمزنگاری نامتقارن، الگوریتم RSA است. تکنیک‌های اولیه آن در سال 1973 توسط آقای Clifford Cocks ایجاد گردید؛ ولی الگوریتم به‌صورت ساختاریافته و عملیاتی، در سال 1977 توسط سه دانش‌آموخته دانشگاه MIT، آقایان Ron Rivest، Adam Shamir و Len Adleman ارائه شد. نام الگوریتم RSA نیز برگرفته از حروف اول نام خانوادگی سه مخترع خود، یعنی Rivest-Shamir-Adleman (RSA) است.

الگوریتمRSA، یک الگوریتم رمزنگاری بلوکی نامتقارن (کلید عمومی) است. این الگوریتم از دو کلید با نام‌های کلیدخصوصی و کلیدعمومی، برای رمزگذاری و رمزگشایی استفاده می‌نماید. به دلیل خاصیت کلیدهای خصوصی و عمومی، این الگوریتم توانایی ارائه ویژگی‌هایی مثل احرازهویت و محرمانگی را نیز دارد. همچنین درصورتی‌که به همراه توابع درهم‌سازی مورد استفاده قرار گیرد، ویژگی‌هایی مثل امضای دیجیتال و سرویس عدم‌انکار را نیز فراهم می‌آورد.

الگوریتم RSA برای محاسبات کلید خود از ویژگی عدد اول استفاده نموده است. به‌طوری‌که بعداً در تشریح فرمول خواهید دید، برای قدرتمند کردن الگوریتم، نیاز به محاسبات اعداد اول بزرگ خواهیم داشت. الگوریتم RSA در طول سال‌هایی که از اختراع آن می‌گذرد، بدون تغییر و همواره به‌عنوان یک الگوریتم قابل‌اطمینان مورداستفاده قرارگرفته است. اما با توجه به تحولات سخت‌افزاری و پیشرفت قابل‌ملاحظه پردازشگرها، آن چیزی که این الگوریتم را در برابر شکست مصون نگه می‌دارد، مؤلفه‌های قدرتمندی است که باید بر اساس عدد اول، انتخاب‌شده و در محاسبات مورداستفاده قرار گیرند.

با توجه به اهمیت عدد اول ، مطالب زیر را جهت یادآوری عرض می‌کنم:

- **عدد اول یا Prime، عددی طبیعی و بزرگ‌تر از یک است که جز بر خودش و عدد ۱، بر هیچ عدد دیگری بخش‌پذیر نمی‌باشد.**
- **چونP عدد اول است، بنابراین تنها دو مقسوم‌علیه متمایز دارد.**
- **بینهایت عدد اول وجود دارد.**
- **هر عدد طبیعی بزرگ‌تر از یک را می‌توان به شکل حاصل‌ضربی از اعداد اول نوشت.**

تشریح الگوریتم RSA

الگوریتم RSA با استفاده از تابع‌نمایی بیان می‌گردد. در RSA متن ساده در قالب بلوک رمز می‌شود؛ به‌طوری‌که هر بلوک دارای یک **مقدار** باینری کوچک‌تر از n است. به این معنا که **سایز** بلوک باید کمتر یا مساوی با $log_2(n)+1$ باشد؛ در عمل سایز بلوک i بیت است که در آن $2^i < n \leq 2^{i+1}$ است.

رمزگذاری و رمزگشایی در RSA طبق فرمول‌های زیر انجام می‌پذیرد: (در این فرمول، متن ساده با M و متن رمزشده با C نمایش داده‌شده است.)

$$C = M^e mod\ n$$

$$M = C^d\ mod\ n = (M^e)^d\ mod\ n = M^{ed}\ mod\ n$$

هر دو طرف فرستنده و گیرنده باید از مقدار n مطلع باشند. ارسال‌کننده مقدار e را می‌داند، اما فقط دریافت‌کننده باید مقدار d را بداند. بنابراین مقدار کلید خصوصی شامل $PR = \{d, n\}$ و کلیدعمومی شامل $PU = \{e, n\}$ خواهد بود.

محاسبه کلید عمومی و خصوصی در RSA

برای محاسبه کلید عمومی و خصوصی باید مراحل زیر انجام پذیرد:

۱. دو عدد اول به نام‌های p و q انتخاب می‌کنیم؛ به‌طوری‌که مساوی هم نباشند. هرچه این اعداد اول انتخابی بزرگ‌تر باشند، قدرت رمزنگاری بیشتر خواهد شد.

عدد اول = p و عدد اول = q

درصورتی‌که $p \neq q$

۲. عددی به نام n که حاصل‌ضرب p و q است را محاسبه می‌کنیم:

$$n = p \times q$$

۳. محاسبه m را به‌صورت زیر انجام می‌دهیم:

$$m = \varphi(n) = (p-1)(q-1)$$

۴. عدد e را طوری انتخاب می‌کنیم که از m کوچک‌تر و نسبت به آن، اول باشد. تأکید می‌کنم که e باید نسبت به m اول باشد؛ یا به‌عبارتی‌دیگر، باید بزرگ‌ترین مقسوم‌علیه مشترک m و e، برابر یک باشد.

$$gcd\ (m, e) = 1; \quad 1 < e < m$$

۵. عدد d را طوری انتخاب می‌کنیم که باقیمانده حاصلضرب $d \times e$ تقسیم‌بر m برابر با یک باشد، که به زبان ریاضی می‌شود:

$$(d \times e) mod\ m = 1$$

اگر e را داشته باشیم و بخواهیم d را محاسبه نماییم، می‌توانیم از فرمول زیر بهره ببریم:

$$d \equiv e^{-1}\ (mod\ \varphi(n))$$

پس از انجام مراحل فوق، کلیدخصوصی و کلیدعمومی مشخص می‌شوند. کلیدخصوصی نزد صاحب کلید نگهداری شده و کلیدعمومی نیز در اختیار هرکسی که می‌خواهد با صاحب کلید ارتباط برقرار کند، گذاشته می‌شود.

مثال محاسبه کلید خصوصی و عمومی

برای اینکه نحوه ایجاد و استفاده از کلیدهای خصوصی و عمومی را بهتر درک کنید، یک مثال ساده به‌صورت زیر حل می‌نماییم.

طرف گیرنده که در اینجا آلیس است، قصد ایجاد کلیدعمومی و خصوصی دارد. پس از ایجاد کلید قرار است کلیدعمومی خود را در اختیار برادر گرامی(آقای باب) قرار دهد تا تبادل اطلاعات بین آن‌ها به‌صورت رمزشده انجام پذیرد.

پس در ابتدا آلیس باید مراحل زیر را جهت ایجاد کلید عمومی و خصوصی خود انجام دهد:

۱. انتخاب دو عدد اول:

$$p = 17 \qquad q = 11$$

۲. برای محاسبه n باید دو عدد اول مشخص‌شده را با یکدیگر ضرب نمود:

$$n = p \times q = 17 \times 11 = 187$$

۳. محاسبه $\varphi(n)$ که ما آن را m می‌نامیم:

$$m = (p-1)(q-1) = 16 \times 10 = 160$$

۴. حالا باید آلیس عددی را به‌عنوان e انتخاب نماید که نسبت به m اول باشد.

آلیس عدد 7 را انتخاب می‌نماید. چراکه عدد 7 نسبت به 160 اول است؛ یعنی بزرگ‌ترین مقسوم‌علیه مشترک 7 و 160 برابر با 1 است. $e = 7$

۵. در این مرحله آلیس باید عددی را به‌عنوان d مشخص نماید که کوچک‌تر از m بوده و همچنین باقیمانده حاصل‌ضرب آن در e ، تقسیم‌بر m برابر 1 باشد.
آلیس عدد 23 را انتخاب نموده است: $d = 23$
عدد 23 شرط اول را دارد: یعنی $160 > 23$
همچنین حائز شرط دوم نیز هست، یعنی:

$$(d \times e) mod\ m = 1$$
$$(23 \times 7) mod\ 160 = 1$$

پس از انجام مراحل فوق، مؤلفه‌های موردنیاز جهت کلیدعمومی و کلیدخصوصی به‌دست می‌آید. با توجه به محاسبات انجام‌گرفته، کلیدخصوصی برابر با $PR = \{d, n\} = \{23,187\}$ و کلید عمومی برابر با $PU = \{e, n\} = \{7,187\}$ می‌باشد.

حالا آلیس باید کلید عمومی خود را برای باب ارسال نماید. ارسال کلید می‌تواند به‌راحتی از طریق یک کانال ناامن انجام پذیرد و اصلاً اشکالی ندارد که هرکسی از آن اطلاع پیدا کند. اما آلیس باید از کلیدخصوصی خود به‌دقت محافظت نماید.

پس از تبادل کلیدعمومی، فرستنده می‌تواند متن موردنظر خود را طبق فرمول، رمز کرده و برای گیرنده ارسال نماید. متنی که توسط کلید عمومی رمزشده، تنها با کلید خصوصی مربوطه قابل رمزگشایی است؛ به همین دلیل به‌راحتی می‌تواند از طریق یک کانال ناامن برای گیرنده ارسال شود.

در این مثال فرض می‌کنیم که باب می‌خواهد یک پیام برای آلیس ارسال نماید. توجه داشته باشید که پیام باید کوچک‌تر از n باشد. اگر متن‌ساده موردنظر را 88 در نظر بگیریم، طبق فرمول رمزگذاری و کلیدعمومی، محاسبات زیر باید توسط باب بر روی متن ساده انجام پذیرد:

i. فرمول رمزگذاری در RSA به‌صورت زیر است:

$$C = M^e mod\ n$$

ii. مقدار متن‌ساده نیز به‌صورت زیر است:

$$M = 88$$

iii. کلید عمومی که آلیس در اختیار باب قرار داده نیز به‌صورت زیر است:

$$PU = \{e, n\} = \{7,187\}$$

همان‌طور که ملاحظه می‌کنید، مقدار n نیز در کلیدعمومی مشخص شده است.

iv. با توجه به موارد فوق، باب تمام مؤلفه‌های موردنیاز برای رمزگذاری را در اختیار دارد. لذا طبق فرمول رمزگذاری محاسبات زیر باید انجام پذیرد:

$$C = M^e mod\ n$$

$$C = 88^7 mod\ 187 = 11$$

پس از اعمال فرمول رمزگذاری بر روی متن‌ساده، متن رمزشده به دست می‌آید؛ که در اینجا برابر با ۱۱ می‌باشد. پس از محاسبه متن رمزشده، باب می‌تواند آن را از طریق کانال ناامن برای آلیس ارسال نماید.

پس‌ازآنکه آلیس متن رمزشده را دریافت نمود، باید از طریق فرمول رمزگشایی و با استفاده از کلیدخصوصی خود، آن را رمزگشایی نماید.

مراحلی که سمت آلیس برای رمزگشایی انجام می‌شود به‌صورت زیر خواهد بود:

i. فرمول رمزگشایی الگوریتمRSA به‌صورت زیر است:

$$M = C^d\ mod\ n$$

ii. مقدار متن رمزشده که به دست آلیس رسیده است:

$$C = 11$$

iii. کلید خصوصی آلیس که خودش آن را محاسبه کرده:

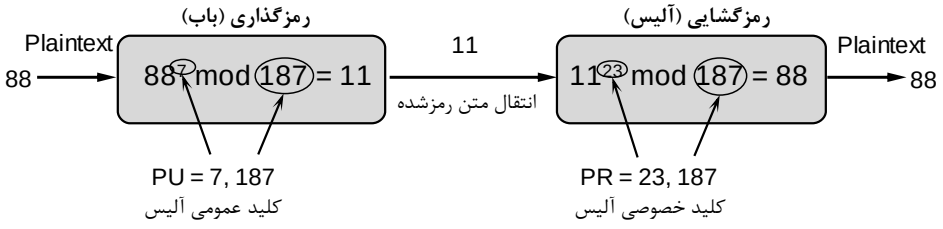
$$PR = \{d, n\} = \{23,187\}$$

iv. با توجه به موارد فوق، آلیس تمام مؤلفه‌های موردنیاز جهت جایگزینی در فرمول رمزگشایی را در اختیار دارد؛ لذا باید محاسبات زیر را انجام دهد:

$$M = C^d\ mod\ n$$

$$M = 11^{23}\ mod\ 187 = 88$$

همان‌طور که ملاحظه کردید، پس از جاگذاری مؤلفه‌ها در فرمول رمزگشایی، متن ساده اولیه به‌دست‌آمد. تصویر زیر فرآیند رمزگذاری و رمزگشایی در RSA را نمایش می‌دهد:



فصل هشتم

توابع درهم‌سازی و کاربردها

مبحث اول

تصدیق پیام

مبحث دوم

امضای دیجیتال

مبحث سوم

الگوریتم SHA

☑ مبحث اول

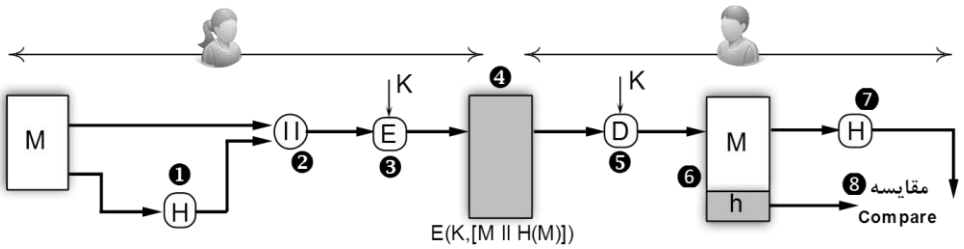
تصدیق پیام

توابع درهم‌سازی به‌تنهایی و همچنین در کنار الگوریتم‌های رمزنگاری متقارن می‌توانند امکان تصدیق پیام (Message Authentication) را فراهم آورند. با تصدیق پیام، گیرنده اطمینان حاصل می‌نماید که پیام دریافت شده دقیقاً همان چیزی است که ارسال‌شده؛ و در مسیر تبادل از خطراتی مثل تغییرات[1]، حذف[2]، درج[3] و بازپخش[4] مصون مانده است.

بسته به نوع و نحوه استفاده از الگوریتم رمزنگاری و نیازهای مدیر امنیت اطلاعات درزمینه محرمانگی و صحت، روش‌های اجرایی تصدیق پیام می‌تواند متفاوت باشد. در ادامه به تشریح چهار روش آن می‌پردازیم:

روش اول؛ تصدیق پیام به‌علاوه محرمانگی

درصورتی‌که بخواهیم ضمن تصدیق پیام، محرمانگی پیام نیز فراهم گردد، می‌توانیم از الگوریتم‌های رمزنگاری متقارن در کنار توابع درهم‌سازی به شکل زیر استفاده نماییم. اگر آلیس را ارسال‌کننده و باب را دریافت‌کننده در نظر بگیریم، مراحل به‌صورت زیر خواهد بود:



آلیس از پیام Hash گرفته❶ و آن را به متن اصلی الصاق می‌نماید.❷ سپس توسط یک الگوریتم رمزنگاری متقارن و بر اساس کلید توافق شده، متن ساده و Hash الصاقی را رمزگذاری نموده❸ و آن را برای باب ارسال می‌نماید.❹

---

[1] Modification
[2] Deletion
[3] Insertion
[4] Replay

بخش سوم

امنیت شبکه

فصل هفتم

مفاهیم امنیت شبکه

فصل هشتم

تکنولوژی‌ها و ابزارهای امنیتی

فصل نهم

ارتباطات امن شبکه

فصل هفتم

مفاهیم امنیت شبکه

مبحث اول

مفاهیم امنیتی

مبحث دوم

انواع تهدیدات

مبحث سوم

انواع حملات

مبحث چهارم

سرویس‌ها و مکانیسم‌های امنیتی

☑ مبحث اول

مفاهیم امنیتی

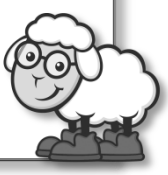
هر سازمانی در هر زمینه و ابعاد کاری، دارای اطلاعات مهمی است که ادامه حیات کسب‌وکار خود را وابسته به آن‌ها می‌داند. قطعاً دارایی‌های اطلاعاتی سازمان‌ها نسبت به نوع کار، اندازه، تعداد کارکنان، پراکندگی و گستردگی فیزیکی ساختمان‌ها، با یکدیگر متفاوت بوده و در درجه‌های مختلف امنیتی قرار می‌گیرند.

در ابعاد بزرگ، برخی از دارایی‌های اطلاعاتی ممکن حیات یک کشور و یا دولت را تحت تأثیر قرار دهد. در ابعاد میانی این اطلاعات می‌تواند باعث افشای یک تکنولوژی یا دستاورد جدید گردد. در ابعاد کوچک نیز ممکن است افشای اطلاعات یک شرکت تجاری مثل اطلاعات مشتری و یا بازرگانی، کسب‌وکار شرکت را دچار اختلال سازد.

به‌هرحال دارایی‌های اطلاعاتی هر سازمان کوچک و بزرگی، ازنظر خودش دارای اهمیت بالایی است و باید به‌دقت از آن‌ها محافظت شود. اهمیت محافظت از اطلاعات وقتی بیشتر می‌شود که سازمان دارای شبکه گسترده بوده و یا مجبور است شبکه خود را با شبکه دیگری که مدیریت آن مستقل است، مثل سازمان‌های دیگر و یا اینترنت، مرتبط سازد.

یک راه امنیتی این است که کامپیوتر خود را درون یک گاوصندوق (البته ضدآب) گذاشته و آن را به اعماق اقیانوس بفرستید! در این صورت کامپیوتری نخواهید داشت که نگرانش باشید. تعجب نکنید! متأسفانه قطع کامل ارتباط، به اولین راهکار مورداستفاده برخی از سازمان‌ها با هر سطحی از ارزش اطلاعات، تبدیل شده است. در دنیای امروز که تمام ابعاد زندگی انسان وابسته به ارتباطات دیتا گردیده، قطع ارتباط برای پاک کردن صورت‌مسئله، کاری غیرقابل‌قبول و تقریباً غیرممکن است.

البته در مقابل گروه حساس فوق، بسیارند کسانی که حداقل‌های امنیتی را هم رعایت نکرده و امیدوارند که هیچ حمله‌ای به آن‌ها صورت نگیرد.



و اما گروه اعجاب‌انگیز دیگری نیز هستند که علیرغم علم به ارزش بالای اطلاعات سازمان، به‌واسطه قدرت و توان بالای مدیریتی که در خود سراغ دارند! بدون انجام هیچ‌گونه اقدام پیشگیرانه‌ای، منتظر می‌مانند به سازمان حمله صورت پذیرد، تا بتوانند آن را مدیریت نمایند. :)

همان‌طور که در بخش اول کتاب گفته شد، امنیت باید در لایه‌های مختلف از امنیت فیزیکی تا دستورالعمل‌های مدیریتی، صورت پذیرد. اما آنچه در بخش سوم کتاب بر روی آن تمرکز داریم، امنیت شبکه و ارتباطات خواهد بود. نوع حملات به شبکه بسیار گسترده‌تر، پیچیده‌تر و خاص‌تر از حملات دیگر مثل دسترسی فیزیکی است؛ و بالطبع آسیب‌پذیری‌ها و اقدامات پیشگیرانه آن نیز وسیع‌تر از سایر ابعاد امنیتی خواهد بود.

امنیت شبکه نه‌تنها برای شبکه، بلکه برای سرویس‌های دیگر نیز دارای اهمیت فراوان است. حتی بسیاری از آسیب‌پذیری‌های دیگر که ممکن است بر روی سایر سرویس‌ها، مثل سیستم‌عامل و یا دیتابیس وجود داشته باشند را می‌توان با طراحی و پیکربندی مناسب شبکه، به حداقل رساند.

با توجه به وسعت مفاهیم امنیت شبکه، وقتی صحبت از امنیت شبکه می‌شود، بالطبع امنیت سرویس‌ها و سیستم‌های دیگر نیز در این عرصه وارد شده و مباحث پیرامونی آن نیز گسترده‌تر می‌شود و باید به‌صورت جامع مطرح شوند. لذا مباحثی که در این فصل مطرح‌شده غالباً جنبه عمومی داشته و علاوه بر امنیت شبکه، ممکن است شامل امنیت سایر سرویس‌ها و سیستم‌ها نیز گردد.

یک مدیر یا مشاور امنیت توانمند و باتجربه، باید یک طراحی مناسب و قابل‌قبول برای حفظ امنیت شبکه و سیستم‌ها ارائه نماید. طراحی درست و منطقی باید با توجه به میزان اهمیت اطلاعات سازمان، میزان ریسک قابل‌قبول و توان مالی سازمان انجام‌گرفته و بین آن‌ها تعادل برقرار نمود. به این معنی که نه آن‌قدر بی‌خیال که تا بروز یک اتفاق وحشتناک دارایی‌های اطلاعاتی را رها کند؛ و نه آن‌قدر سخت‌گیر و محتاط که هم روال کار را مختل کرده و هم باعث شود هزینه‌های سازمان برای حفاظت از اطلاعات، بیش از ارزش خود اطلاعات شود.

آگاهی از اصول امنیت، شناسایی راهکارها، تقسیم‌بندی دارایی‌های اطلاعاتی سازمان بر اساس درجه اهمیت و بررسی الزامات سازمانی، ازجمله مواردی است که در زمان طراحی امنیت اطلاعات، باید توسط طراح در نظر گرفته شوند.

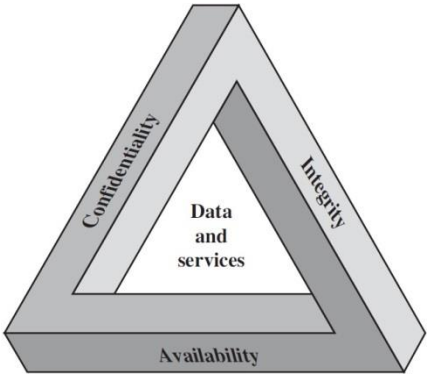
مدیر امنیت پس از فراهم کردن یک طرح امنیتی بر اساس بهترین شیوه‌ها (Best Practice)، باید آن را در سراسر سازمان اجرا نماید.

نکته مهمی که یک مدیر باید در نظر داشته باشد، نظارت همیشگی بر اجرای صحیح طرح امنیتی است. صرف اجرای یک طرح خوب نمی‌تواند برای مدت زیادی تضمین‌کننده امنیت باشد؛ بلکه نظارت بر اجرای صحیح طرح و همچنین به‌روزرسانی نرم‌افزارها و تجهیزات امنیتی، از الزامات ادامه روند وضعیت امن در فناوری اطلاعات است.

مثلث امنیت اطلاعات

امنیت صرفاً جلوگیری از افشای اطلاعات نیست. بلکه در دسترس نبودن اطلاعات در زمان موردنیاز و تغییر اطلاعات در مسیر تبادل نیز باعث از دست دادن امنیت می‌گردد.

امنیت اطلاعات دارای سه مفهوم اصلی Confidentiality، Integrity و Availability است که به دلیل حروف اول این سه کلمه، بانام مثلث CIA مشهور گردیده است.



- **محرمانگی (Confidentiality)**

محرمانه بودن یعنی فقط افراد یا سیستم‌های مجاز بتوانند به اطلاعات موردنظر دسترسی داشته باشند. به‌عبارت‌دیگر افراد غیرمجاز نباید امکان دسترسی به اطلاعات را داشته باشند.

دو نوع دیتا وجود دارد. اول، دیتای در حال حرکت بر روی شبکه. دوم، دیتای ذخیره‌شده بر روی تجهیزات مثل سیستم‌ها، سرورها، Storageها و Cloud.

برای امنیت دیتای در حال حرکت باید از روش‌های رمزنگاری استفاده نمود؛ یعنی ابتدا دیتا رمزشده، و سپس اقدام به ارسال آن نماییم. راه دیگر، ایجاد کانال‌های ارتباطی امن برای تبادل دیتا بین فرستنده و گیرنده است. راهکارهای امنیت دیتای در حال حرکت در این بخش از کتاب موردبحث قرار می‌گیرند.

برای امنیت دیتای ذخیره‌شده نیز باید مکانیسم‌های کنترل دسترسی فراهم گردد. البته در کنار مکانیسم کنترل دسترسی، می‌توان از رمزنگاری نیز بهره برد. درباره مکانیسم کنترل دسترسی بر روی سیستم‌عامل و دیتابیس، در بخش چهارم همین کتاب توضیحاتی ارائه شده است.

- **صحت و تمامیت (Integrity)**

صحت یعنی فقط افراد یا سیستم‌های مجاز، امکان تغییر و اصلاح دیتا را داشته باشد. در امنیت شبکه منظور از صحت این است که دیتای دریافتی دقیقاً همان چیزی باشد که فرستنده ارسال کرده است.

در بخش دوم کتاب، نحوه استفاده از توابع درهم‌ساز برای بررسی صحت پیام تشریح شد. البته از توابع درهم‌ساز می‌توان هم برای بررسی صحت اطلاعات ذخیره‌شده و هم برای بررسی صحت اطلاعات در حال حرکت بهره برد.

- **دسترس‌پذیری (Availability)**

افراد مجاز در زمان مجاز باید به دیتای موردنظر دسترسی داشته باشند.

اصلی‌ترین مباحث بر سر موضوع دسترس‌پذیری در بخش امنیت شبکه است. البته امنیت فیزیکی نیز در دسترس‌پذیری از اهمیت ویژه‌ای برخوردار است؛ اما اگر بحث حملات و هکرها را در نظر بگیریم، امنیت شبکه نسبت به امنیت فیزیکی و افزونگی، به‌صورت پویاتری با دسترس‌پذیری در ارتباط است.

در همین بخش از کتاب، حملاتی که باعث اختلال در دسترس‌پذیری می‌شوند، بررسی خواهند شد.

موسسه NIST، مثلث CIA را طی استاندارد FIPS 199 در جهت اجرای طرح دولت الکترونیک در ایالات‌متحده، برای سازمان‌های دولتی تعریف نموده است.[1] در این استاندارد تأثیرات بالقوه از دست دادن هریک از سه اصل فوق را در سه گروه و به‌صورت زیر تقسیم‌بندی کرده است:

- **تأثیرات بالقوه کم (Low)**

انتظار می‌رود از دست دادن محرمانگی، صحت و یا دسترس‌پذیر بودن، عوارض جانبی محدودی بر روی عملیات سازمانی، دارایی‌های سازمانی و افراد داشته باشد.

- **تأثیرات بالقوه متوسط (Moderate)**

انتظار می‌رود از دست دادن محرمانگی، صحت و یا دسترس‌پذیر بودن، باعث عوارض جانبی جدی بر روی عملیات سازمانی، دارایی‌های سازمانی و افراد داشته باشد. مثلاً ممکن است باعث تخریب قابل‌توجه مأموریت‌های سازمان گردیده و یا منجر به زیان مالی بزرگی شود.

- **تأثیرات بالقوه زیاد (High)**

انتظار می‌رود از دست دادن محرمانگی، صحت و یا دسترس‌پذیر بودن، باعث عوارض جانبی فاجعه‌باری بر روی عملیات سازمانی، دارایی‌های سازمانی و افراد داشته باشد. فاجعه‌بار به این معناست که ادامه حیات سازمان به خطر خواهد افتاد.

[1] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

فصل هشتم

تکنولوژی‌ها و ابزارهای امنیتی

مبحث اول

کنترل دسترسی

مبحث دوم

فایروال

مبحث سوم

IDS/IPS

مبحث چهارم

هانی‌پات

☑ مبحث اول

کنترل دسترسی

کنترل دسترسی جزء اولین اقدامات امنیتی است که باید جهت محافظت از منابع، مورد استفاده قرار گیرد. کنترل دسترسی مشخص می‌کند هر کاربر یا سیستم به کدام منابع و در چه سطحی می‌تواند دسترسی داشته باشد.

نحوه کنترل دسترسی بر اساس سیاست‌گذاری‌ها، برنامه‌ها و تکنولوژی‌ها مشخص می‌شود. کنترل دسترسی باید هم به‌صورت فیزیکی و هم به‌صورت منطقی مورداستفاده قرار گیرد. کنترل دسترسی‌ها می‌توانند به سه صورت اجباری، اختیاری و غیر اختیاری باشند.[۱]

۱. کنترل دسترسی اجباری (Mandatory Access Controls)

کنترل دسترسی اجباری که به‌اختصار MAC نامیده می‌شود، از طرح طبقه‌بندی داده‌ها[۲] برای اعطای دسترسی استفاده می‌کند؛ که در آن کاربران و مالک[۳]داده، کنترل محدودشده‌ای برای اعطای دسترسی به منابع اطلاعاتی را دارند. به‌عبارت‌دیگر نحوه و سطح دسترسی‌ها توسط سیستم و بر اساس سیاست‌های امنیتی مشخص می‌شود و حتی مالک داده نمی‌تواند به‌راحتی، اقدام به اعطای مجوز به سایر کاربران نماید.

در طرح طبقه‌بندی داده‌ها، مجموعه‌های اطلاعاتی را رتبه‌بندی می‌کنند؛ از طرفی به هر کاربر نیز امتیازی تعلق می‌گیرد که مشخص‌کننده سطح دسترسی او به اطلاعات رتبه‌بندی شده است. تعیین این امتیازات بر اساس میزان حساسیت، انجام‌گرفته و نشان‌دهنده سطح محرمانگی اطلاعات است.

MAC دارای یک ماتریس کنترل دسترسی است که در آن، نحوه ارتباط هر فاعل (Subject) را با هر مفعول (Object) مشخص می‌کند.

Subject\Object	File 1	File 2	Printer
MTR	Read\Write\Execute	Read\Write\Execute	Yes
Bob	Read	Read	No
Alice	-	Read\Write	Yes

[۱] در مبحث دوم فصل دوازدهم، سطوح امنیتی طی استاندارد DOD 85، به‌صورت مفصل تشریح شده است.

[2] Data Classification

[3] Owners

۲. **کنترل دسترسی غیراختیاری (Non-discretionary control)**

کنترل دسترسی غیراختیاری، یک نسخه "به‌شدت اجباری" از MAC است؛ که توسط یک قدرت مرکزی در سازمان، مدیریت‌شده و می‌تواند بر اساس نقش (Role-Based) یا بر اساس وظیفه (Task-Based)، وجود داشته باشد.

کنترل‌های مبتنی بر نقش (Role-Based)، به نقش یک کاربر در سازمان گره‌خورده و کنترل مبتنی بر وظیفه (Task-Based)، به وظیفه یا مسئولیت خاصی مرتبط است.

استفاده از کنترل‌های مبتنی بر نقش و وظیفه، مدیریت کنترل‌ها را آسان‌تر می‌نماید. در این صورت، مدیریت به‌جای اعطای جداگانه دسترسی به هر فرد، یک‌بار به هر نقشی دسترسی‌های موردنیاز را داده و ازآن‌پس افراد موردنظر را در آن نقش یا وظیفه قرار می‌دهد. با قرارگیری فرد در آن نقش یا وظیفه، تمام دسترسی‌های آن نقش به کاربر اعطا می‌شود و به‌محض خارج کردن کاربر از آن نقش یا وظیفه، تمام دسترسی‌های داده‌شده، باطل می‌شود. این کار مخصوصاً برای محیط‌هایی که جابجایی افراد زیاد است، می‌تواند تأثیرات خوبی داشته باشد.

۳. **کنترل دسترسی اختیاری (Discretionary Access Control)**

در کنترل دسترسی اختیاری که به‌اختصار DAC نامیده می‌شود؛ کاربر می‌تواند برای دیتای تحت مالکیت خود، اقدام به اعطای مجوز به سایر افراد نماید.

مکانیسم‌های کنترل دسترسی

به‌طورکلی، تمامی روش‌های کنترل دسترسی، بر اساس مکانیسم‌های زیر عمل می‌کنند:

۱. شناسایی (Identification)
۲. احرازهویت (Authentication)
۳. اختیارات یا مجوزدهی (Authorization)
۴. پاسخگویی (Accountability)

در ادامه هریک از چهار مکانیسم فوق تشریح می‌شوند:

شناسایی

مکانیسم شناسایی، به هر نهادی که قصد دسترسی به منابع را دارد، یک برچسب (Label) تخصیص می‌دهد تا از طرف سیستم قابل‌شناسایی باشد. برچسب داده‌شده به متقاضی را شناسه (Identifier) نامیده و به‌اختصار با ID نمایش می‌دهند. این ID باید به‌صورت منحصربه‌فرد و فقط به یک متقاضی اختصاص داده شود.

فصل نهم

ارتباطات امن شبکه

مبحث اول

IPsec

مبحث دوم

شبکه خصوصی مجازی

☑ مبحث اول

IPsec

برای برقراری امنیت، پروتکل‌ها و سرویس‌های مختلفی وجود دارد. برخی از این پروتکل‌ها تاکنون بررسی‌شده و به برخی دیگر نیز در فصول آینده پرداخته می‌شود. اما هر یک از این پروتکل‌ها، امنیت یک لایه یا سرویس را فراهم آورده و در یک لایه از مدل OSI کار می‌کنند. هرچه امنیت را در لایه‌های پایین‌تر OSI برقرار نماییم، بالطبع لایه‌های بالاتر نیز از امنیت بهره‌مند خواهند شد. حتی می‌توانند علاوه بر امنیت تأمین‌شده در لایه‌های پایین‌تر، در لایه مربوط به خود نیز از پروتکل‌ها و سرویس‌های امن استفاده نمایند.

یکی از مهم‌ترین پروتکل‌های امنیتی، IP Security است. این پروتکل که به‌اختصار IPsec نامیده می‌شود در لایه شبکه (لایه سوم) مدل OSI اقدام به برقراری امنیت می‌نماید. در این صورت لایه‌های بالاتر نیز از امنیت نسبی برخوردار خواهند شد.

اجرای پروتکل IPsec باعث فراهم شدن امنیت در سطح شبکه می‌شود. وقتی یک شبکه امن باشد، تبادل دیتا نیز بر روی بستر امن صورت گرفته و تا حد قابل قبولی از امنیت برخوردار خواهد بود. با اجرای IPsec، سازمان می‌تواند مطمئن باشد که نه‌تنها برای برنامه‌های کاربردی دارای مکانیسم امنیتی، بلکه برای برنامه‌های کاربردی فاقد هرگونه مکانیسم امنیتی نیز سطح خوبی از امنیت را فراهم آورده است.

امنیت در سطح IP شامل سه سطح کاربردی: احرازهویت، محرمانگی و مدیریت کلید است. مکانیسم احرازهویت، دریافت‌کننده را مطمئن می‌سازد که بسته دریافتی را فرستنده موردنظر ارسال کرده و در مسیر انتقال نیز دچار تغییر نشده است. محرمانگی نیز با استفاده از رمزنگاری باعث می‌شود در صورت استراق سمع بسته توسط شخص ثالث، از افشای اطلاعات جلوگیری شود. مکانیسم مدیریت کلید نیز تسهیل‌کننده تبادل امن کلیدهای مربوطه است.

سازمان IETF طی RFC 4301، اقدام به ارائه استاندارد معماری امنیت برای پروتکل اینترنت (IP) نموده است.[1] این استاندارد نحوه پیاده‌سازی امنیت برای پروتکل IP را تشریح کرده است. همان‌طور که در این RFC بیان‌شده است، امکان استفاده از IPsec در محیط هر دو پروتکل IPv4 و IPv6 وجود دارد. البته این سند ارائه‌دهنده یک معماری امنیتی کلی برای اینترنت نیست؛ بلکه امنیت ارائه‌شده در این سند، فقط برای فراهم کردن امنیت در لایه IP، از طریق ترکیب رمزنگاری

[1] https://www.ietf.org/rfc/rfc2401.txt

و مکانیسم‌های امنیتی دیگر است. استفاده از IPsec در پروتکل IPv4 به‌صورت اختیاری است؛ ولی IAB[1] استفاده از آن را در نسل بعدی IP، یعنی IPv6 به‌صورت اجباری اعلام کرده است.

کاربردهای IPsec

استفاده از پروتکل IPsec قابلیت برقراری امنیت در کانال‌های ارتباطی را فراهم می‌آورد. حفاظت از کانال‌های ارتباطی در سراسر شبکه LAN، سراسر شبکه‌های خصوصی و عمومی WAN، و سراسر اینترنت، را می‌توان با استفاده از IPsec برقرار نمود. نمونه‌هایی از استفاده IPsec به‌صورت زیر است:

- برقراری اتصال امن بین شعبه و سازمان، بر روی اینترنت.
شرکت می‌تواند یک شبکه خصوصی مجازی امن، بر روی اینترنت یا شبکه عمومی WAN، ایجاد نماید. این کار شرکت را قادر می‌سازد برای تسهیل کسب‌وکار خود از ظرفیت عظیم اینترنت بهره برده و هزینه مربوط به برپایی شبکه‌های خصوصی و سربار مدیریتی را کاهش دهد.
- دسترسی از راه دور امن بر روی اینترنت.
کاربر نهایی با استفاده از IPsec می‌تواند از طریق اینترنت یک ارتباط امن را با شبکه سازمان خود برقرار نماید. این کار باعث صرفه‌جویی در هزینه جابجایی کارمندان شده و باعث تسهیل دورکاری نیز می‌گردد.
- برقراری شبکه‌های داخلی[2] و خارجی[3] با شرکا.
جهت برقراری یک ارتباط امن با سایر سازمان‌ها و شرکا، می‌توان از IPsec بهره برد. با استفاده از IPsec هر دو طرف می‌توانند از احرازهویت، محرمانگی و مکانیسم تبادل کلید مطمئن باشند.
- افزایش امنیت تجارت الکترونیک[4].
اگرچه برخی برنامه‌های کاربردی وب و تجارت الکترونیک به‌صورت توکار[5] از پروتکل‌های امنیتی استفاده می‌نمایند؛ اما به‌کارگیری IPsec تضمین می‌کند که تمام ترافیک تبادل شده، تحت رمزنگاری و تصدیق هویت بوده و یک‌لایه امنیتی به هر آنچه توسط لایه کاربرد ارائه‌شده، اضافه گردیده است.

---

[1] Internet Architecture Board (IAB)
[2] Intranet
[3] Extranet
[4] Electronic Commerce
[5] Built-in

بخش چهارم

امنیت سیستم‌ها و سرویس‌ها

فصل دهم

امنیت وب

فصل یازدم

امنیت پست الکترونیک

فصل دوازدهم

امنیت سیستم‌عامل

فصل سیزدهم

امنیت دیتابیس

فصل دهم

امنیت وب

مبحث اول

پروتکل SSL/TLS

مبحث دوم

پروتکل HTTPS

☑ مبحث اول

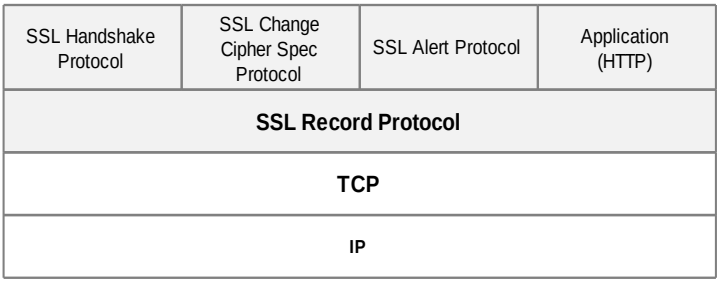
پروتکل SSL/TLS

شرکت Netscape برای برقراری امنیت در ارتباطات اینترنتی، اقدام به انتشار یک پروتکل امنیتی بانام Secure Socket Layer (SSL) نموده و از آن، در مرورگرهای خود پشتیبانی کرد. سازمان IETF به دلیل کاربرد وسیع و مناسب SSL، اقدام به انتشار این پروتکل در قالب استاندارد Transport Layer Security(TLS) و طی RFC 5246 نمود[۱]. پروتکل TLS بر اساس SSL v3.1 ارائه گردیده و از بسیاری جهات شبیه به یکدیگر می‌باشند. لذا در این مبحث پروتکل SSL v3 (ارائه‌شده در RFC 6101) تشریح خواهد گردید.

لازم به ذکر است، IETF در سال 2011 طی RFC 6176 استفاده از SSL v2 را به دلایلی مثل استفاده ازMD5 در احرازهویت، عملیات Handshake محافظت نشده، استفاده از کلید یکسان برای هر دو عملیات رمزنگاری و صحت، و همچنین آسیب‌پذیری در مقابل حملات مردمیانی، ممنوع اعلام کرده است.

معماری SSL

پروتکل SSL طوری طراحی‌شده که از TCP برای فراهم آوردن یک سرویس End-to-end امن و قابل‌اطمینان استفاده می‌نماید. همان‌طور که در تصویر زیر نشان داده‌شده، SSL یک پروتکل تنها نیست، بلکه شامل دو لایه از پروتکل‌ها است. به‌عبارت‌دیگر SSL، یک پروتکل لایه‌بندی شده است.



[۱] نسخه‌های اولیه این استاندارد عبارتند از RFC 3268، RFC 4346 و RFC 4366.

توجه داشته باشید که لایه‌بندی پروتکل SSL، برای تعریف بهتر و نحوه تعامل پروتکل‌ها با یکدیگر بوده و تأثیری در لایه‌های مدل OSI ندارد.

پروتکل SSL Record فراهم آورنده سرویس‌های امنیتی اساسی برای پروتکل‌های مختلف لایه‌های بالاتر است. به‌طور خاص، پروتکل HTTP که یک سرویس تعاملی کلاینت/سروری است، می‌تواند در بالای SSL مورداستفاده قرار گیرد.

پروتکل SSL، علاوه بر SSL Record Protocol، دارای سه پروتکل دیگر در لایه بالاتر است که عبارتند از: SSL Handshake Protocol، SSL Change Cipher Spec Protocol و SSL Alert Protocol؛ این پروتکل‌ها برای مدیریت تبادلات SSL مورداستفاده قرار می‌گیرند.

مفاهیم Session و Connection در SSL

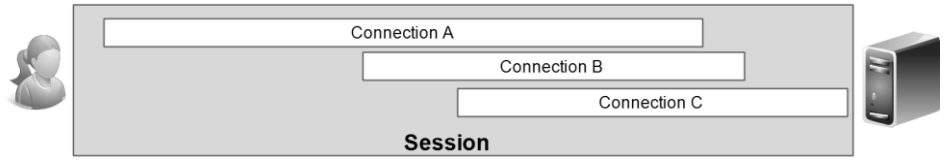
دو مفهوم مهم در SSL، عبارتند از Connection و Session، که تشریح آن‌ها به‌صورت زیر است:

- **Connection**

یک اتصال (Connection)، یک انتقال (لایه چهارم مدل OSI یا همان Transport) بوده، که نوع مناسبی از سرویس را فراهم می‌کند. برای SSL، این قبیل اتصال‌ها، ارتباط Peer-to-peer هستند.[۱] اتصال‌ها، زودگذر و موقتی هستند. هر Connection با یک Session در ارتباط است.

- **Session**

یک SSL Session، یک ارتباط بین کلاینت و سرور است؛ که توسط پروتکل Handshake ایجاد می‌گردد. نشست‌ها (Session) مجموعه‌ای از پارامترهای امنیتی رمزنگاری را تعریف می‌کنند که می‌توانند در میان اتصالات متعدد به اشتراک گذاشته شوند. نشست‌ها از انجام مذاکرات متعدد و پرهزینه که برای مشخص کردن پارامترهای امنیتی جدید در هر اتصال باید انجام شود، جلوگیری می‌کنند.



[۱] در ارتباطات Peer-to-peer، دو نقطه بدون نیاز به برقراری یک ساختار متمرکز و پرهزینه، اقدام به برقراری ارتباط با یکدیگر می‌نمایند.

فصل یازدهم

امنیت پست الکترونیک

مبحث اول

پروتکل PGP

مبحث دوم

پروتکل S/MIME

پست‌الکترونیک یکی از پرکاربردترین سرویس‌هایی است که امروزه توسط کاربران مورداستفاده قرار می‌گیرد. پست‌الکترونیک نه‌تنها بر روی اینترنت، بلکه در شبکه‌های داخلی نیز کاربرد فراوانی دارد. حتی برخی از مؤسسات از پست‌الکترونیک خدماتی شبیه اتوماسیون اداری دریافت می‌کنند! و یا اتوماسیون‌ها و روال‌های کاری در سازمان‌ها به پست الکترونیک وابسته شده است.

اهمیت و کاربرد پست الکترونیک، در حدی است که بسیاری از مکاتبات محرمانه سازمان‌ها نیز از این طریق انجام می‌پذیرد. فاکتورهای فروش، رسیدهای پرداخت، مکاتبات و دستورات محرمانه اداری، بخشنامه‌های اداری، درخواست‌ها و بسیاری از مضامین پراهمیت دیگر، از طریق پست الکترونیک ارسال و دریافت می‌گردد.

پست‌الکترونیک از پروتکل Simple Mail Transfer Protocol(SMTP) برای تبادل نامه‌های الکترونیکی استفاده می‌کند. متأسفانه SMTP هیچ‌گونه امنیتی را برای محتوای نامه الکترونیک فراهم نکرده و همچنان که از اسم آن نیز مشخص است، صرفاً فقط وظیفه تبادل ساده پیام‌ها را بر عهده دارد.

به دلیل کمبودها و ضعف‌های موجود در SMTP، سازمان IETF اقدام به ارائه یک پروتکل جدید بانام MIME برای پست الکترونیک نمود. هرچند که این پروتکل ازنظر ویژگی‌های پستی بهتر از SMTP است، اما بازهم امنیت قابل‌توجهی بر روی آن وجود ندارد.

با توجه به گسترش روزافزون استفاده از پست‌الکترونیک در تمام ابعاد کسب‌وکار سازمان‌ها، باید برای احرازهویت و محرمانگی نامه‌های الکترونیک، تمهیداتی اندیشه شود. برای این منظور دو پروتکل PGP و S/MIME برای برقراری امنیت در پست الکترونیک ارائه شدند.

پروتکل PGP برای برقراری امنیت در پست الکترونیک مبتنی بر SMTP و پروتکل S/MIME برای برقراری امنیت پست الکترونیک مبتنی بر MIME توسعه داده شده‌اند.

در مبحث اول این فصل به بررسی پروتکل PGP و نحوه عملکرد آن می‌پردازیم. با توجه به اینکه پروتکل S/MIME، نسخه استانداردشده پروتکل PGP بوده و ازنظر عملکرد، شبیه آن است؛ لذا در مبحث دوم نیز به بررسی پروتکل S/MIME می‌پردازیم.

☑ مبحث اول

پروتکل PGP

پروتکل Pretty Good Privacy (PGP)، یک پروتکل متن‌باز[۱] است که توسط آقای Phil Zimmermann، جهت امنیت پست الکترونیک ارائه گردیده است. البته پروتکل PGP در برقراری امنیت موارد دیگری مثل فایل‌ها و دیتای ذخیره‌شده نیز می‌تواند مورداستفاده قرار گیرد؛ اما شهرت آن به دلیل کاربرد این پروتکل در پست‌الکترونیک است.

پروتکلPGP فراهم آورنده سرویس‌های امنیتی احرازهویت و محرمانگی برای پست الکترونیک و ذخیره‌سازی فایل است. این پروتکل توسط IETF و طی RFC 4880 نیز منتشر گردیده است.

در اصل می‌توان گفت آقای زیمرمن برای به وجود آوردن پروتکل PGP، کارهای زیر را انجام داده است:

۱. انتخاب بهترین الگوریتم رمزنگاری موجود، برای ساخت بلوک‌ها دیتا.
۲. یکپارچه‌سازی الگوریتم انتخاب‌شده در یک برنامه کاربردی همه‌منظوره[۲]، که مستقل از سیستم‌عامل و پردازشگر است.
۳. ایجاد یک Package و مستندسازی آن شامل : کد منبع، در دسترس عموم قرار دادن آن از طریق اینترنت، درج آن در اعلانات و شبکه‌های تجاری مثل AOL[۳].
۴. دستیابی به توافق با یک شرکت، جهت فراهم آوردن یک نسخه تجاری کم‌هزینه و کاملاً سازگار از PGP.

رشد PGP به‌صورت انفجارگونه بوده و در حال حاضر به‌طور گسترده‌ای مورداستفاده قرار می‌گیرد. موارد زیر برخی از دلایلی است که می‌توان برای این رشد سریع عنوان کرد:

۱. به‌صورت رایگان در سراسر جهان در دسترس بوده و امکان اجرا بر روی انواع سیستم‌عامل‌ها ازجمله ویندوز، یونیکس و مکینتاش را دارد. علاوه بر این، نسخه تجاری برای کاربرانی که نیاز به پشتیبانی فروشنده دارند، نیز فراهم گردیده است.

---

[۱] منظور از Open Source یا متن‌باز، برنامه‌ای است که کد آن به‌صورت کامل در اختیار همگان قرارگرفته و استفاده از آن بدون پرداخت هزینه امکان‌پذیر است.

[2] General-purpose
[3] America On Line

۲. بر اساس الگوریتم‌هایی ایجادشده، که امنیت آن‌ها به‌صورت گسترده مورد تائید قرارگرفته است. به‌صورت خاص، این Package شامل RSA، DSS و دیفی‌هلمن برای رمزنگاری کلیدعمومی؛ و الگوریتم‌های CAST-128، IDEA و 3DES برای رمزنگاری متقارن؛ و الگوریتم SHA برای عملیات درهم‌سازی، است.
۳. کاربرد وسیعی برای شرکت‌هایی که مایل به انتخاب و اجرای یک طرح استاندارد رمزنگاری جهت فایل‌ها و پیام‌ها برای افرادی که می‌خواهند با آن‌ها از طریق اینترنت یا شبکه‌های دیگر ارتباط امن داشته باشند، دارد.
۴. این پروتکل توسط یک دولت یا سازمان استاندارد، توسعه‌نیافته و کنترل نمی‌شود؛ لذا برای کسانی که نسبت به دولت‌ها و سازمان‌ها بی‌اعتماد هستند، استفاده از PGP جذاب خواهد بود.
۵. در حال حاضر PGP از طریق استانداردهای اینترنت دنبال می‌شود[1]؛ اما بااین‌وجود، PGP همچنان غیر وابسته به هر سازمان یا دولتی می‌تواند مورداستفاده قرار گیرد.

نشانه‌گذاری

در کتاب آقای استالینگز[2]، برای تشریح PGP از نمادها و نشانه‌هایی استفاده‌شده است. البته ممکن است بعضی از این نشانه‌ها و نمادها در استانداردها یا مراجع دیگر، به‌صورت متفاوتی مورداستفاده قرارگرفته باشد. لذا قبل از شروع بررسی PGP، به تشریح نشانه‌های مورداستفاده می‌پردازیم:

K_S = کلید نشست که توسط رمزنگاری متقارن مورداستفاده قرار می‌گیرد.
PR_a = کلیدخصوصی طرف A، که توسط رمزنگاری کلیدعمومی (نامتقارن) مورداستفاده قرار می‌گیرد.
PU_a = کلیدعمومی طرف A، که توسط رمزنگاری کلیدعمومی مورداستفاده قرار می‌گیرد.
EP = عملیات رمزگذاری(Encryption) در الگوریتم رمزنگاری کلیدعمومی.
DP = عملیات رمزگشایی(Dycryption) در الگوریتم رمزنگاری کلیدعمومی.
EC = رمزگذاری در الگوریتم رمزنگاری متقارن.
DC = رمزگشایی در الگوریتم رمزنگاری متقارن.
H = تابع درهم‌سازی

[1] RFC 3156; MIME Security with OpenPGP
[2] Cryptography and Network Security Principles and Practice

|| = الصاق یا Concatenation

Z = فشرده‌سازی با استفاده از الگوریتم ZIP.

R64 = تبدیل به فرمت ASCII 64.

تشریح عملیات PGP

پروتکل PGP، چهار سرویس زیر را فراهم می‌آورد:

- احرازهویت (Authentication)
- محرمانگی (Confidentiality)
- فشرده‌سازی (Compression)
- سازگاری با پست الکترونیک (E-mail compatibility)

در جدول زیر، توضیح مختصری درباره هر چهار مورد فوق آورده شده است. البته در ادامه این مبحث، این موارد به‌صورت کامل نیز تشریح خواهند شد.

عملیات	الگوریتم مورداستفاده	توضیحات
امضای دیجیتال (احرازهویت)	DSS/SHA RSA/SHA	الگوریتم SHA چکیده پیام را تولید نموده و سپس چکیده توسط DSS یا RSA با کلیدخصوصی فرستنده امضا می‌شود.
رمزنگاری پیام (محرمانگی)	CAST or IDEA or 3DES 3DES با دیفی‌هلمن یا RSA	پیام توسط الگوریتم‌های CAST-128، IDEA یا 3DES رمزگذاری می‌شود. این رمزگذاری با استفاده از کلید نشست (Session key) یک‌بارمصرف تولیدشده توسط فرستنده انجام می‌شود. کلید نشست تولیدشده با استفاده از RSA یا دیفی‌هلمن و بر اساس کلیدعمومی گیرنده، تبادل می‌گردد.
فشرده‌سازی	ZIP	می‌توان پیام را قبل از ذخیره یا تبادل، توسط الگوریتم ZIP، فشرده‌سازی نمود.
سازگاری با پست الکترونیک	Radix-64 conversion	جهت فراهم آوردن شفافیت برای برنامه‌های پست الکترونیک، می‌توان پیام رمزشده را به کد ASCII تبدیل کرد.

فصل دوازدهم

امنیت سیستم‌عامل

مبحث اول

بهترین شیوه‌های مدیریت امن سیستم

مبحث دوم

سطوح امنیتی در سیستم‌عامل

مبحث سوم

بهترین شیوه‌های امنیت سیستم‌عامل

امنیت دیتابیس

فصل سیزدهم

مبحث اول

ده تهدید برتر دیتابیس

مبحث دوم

روش‌های مقابله با تهدیدات

منابع و معرفی کتاب

منابع:

[۱] روغنی، محمدتقی. شبکه؛ صفر تا صد. انتشارات ناقوس، ۱۳۹۲
[2] Stalling, William. *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE*. Fifth Edition.
[3] ISO/IEC 27000:2014
[4] ISO/IEC 27001:2013
[5] ISO/IEC 27002:2013
[6] NIST FIPS-197 (AES)
[7] NIST FIPS-198 (HMAC)
[8] IETF RFC 2104. *Keyed-Hashing for Message Authentication*.
[9] NIST FIPS-186 (DSS)
[10] NIST FIPS-180 (SHA)
[11] IETF RFC 3174. *Secure Hash Algorithm.*
[12] Barker, Keith. *CCNA Security 640-554 Official Cert Guide*. Cisco Press.
[13] Wilkins, Sean. *CCNP Security SECURE 642-637 Official Cert Guide*.
[14] NIST FIPS-199. *Standards for Security Categorization of Federal Information and Information Systems*.
[15] Whitman, Michael E. *Principles of Information Security*. Fourth Edition
[16] ITU X.800. *Security architecture for Open Systems Interconnection for CCITT applications.*
[17] IETF RFC 2828. *Internet Security Glossary*.
[18] IETF RFC 4962. *Guidance for Authentication, Authorization, and Accounting (AAA).*
[19] NIST SP 800-10.
[20] IETF RFC 2827. *Network Ingress Filtering.*
[21] NIST SP 800-94. *Guide to Intrusion Detection and Prevention Systems (IDPS).*
[22] IETF RFC 4301. *Security Architecture for the Internet Protocol*.
[23] IETF RFC 2637. *Point-to-Point Tunneling Protocol (PPTP).*
[24] IETF RFC 2661. *Layer Two Tunneling Protocol (L2TP).*

[25] NIST SP 800-113. *Guide to SSL VPNs*.
[26] IETF RFC 6101. *The Secure Sockets Layer (SSL) Protocol Version 3.0*.
[27] IETF RFC 2818. *HTTP Over TLS*.
[28] IETF RFC 4880. *OpenPGP Message Format*.
[29] IETF RFC 5322. *Internet Message Format*.
[30] IETF RFC 2045 – 2049. *Multipurpose Internet Mail Extensions (MIME)*.
[31] IETF RFC 2119. *Key words for use in RFCs to Indicate Requirement Levels*.
[32] IETF RFC 2315. *Cryptographic Message Syntax*.
[33] Setty, Harish. *System Administrator - Security Best Practices*. SANS Institute.
[34] NIST SP 800-123. *Guide to General Server Security*.
[35] Cole, Eric. *Security Best Practices*. Secure Anchor.
[36] Cui-Qing Yang. *Operating System Security and Secure Operating Systems*.
[37] DoD 5200.28-STD.*Trusted Computer System Evaluation Criteria*. TCSEC.
[38] NIST SP 800-40. *Guide to Enterprise Patch Management Technologies*.
[39] NIST SP 800-162. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.
[40] Basta, Alfred. *Database Security*. Course Technology.
[41] *Top Ten Database Threats*. imperva.com.
[42] http://www.ietf.org
[43] https://cve.mitre.org
[44] http://www.securityfocus.com
[45] https://www. Intrusion.com
[46] http://www.verizonenterprise.com
[47] http://www.idc.com
[48] https://www.otalliance.org
[49] http://www.pwc.com
[50] http://www.imperva.com
[51] http://iase.disa.mil/stigs


NAGHOOS PUBLICATION
0-100
شبکه
صفر تا صد
* سازمانهای توسعه دهنده شبکه و اینترنت
* مدلها، استانداردها، پروتکل‌ها و اصطلاحات شبکه
* شبکه های LAN و WAN بر اساس پروتکل های IPv4 و IPv6
* اجرای ۱۹ سناریوی عملیاتی بر اساس IPv4 و IPv6 در موضوعات سوئیچینگ و مسیریابی
* امنیت شبکه ضمن بررسی مدل امنیتی سیسکو و استاندارد سیستم مدیریت امنیت اطلاعات (ISMS)
* توصیه شده برای مدیران و مشاوران IT ، کارشناسان و علاقه‌مندان به شبکه
محمدتقی روغنی
MFP

کتاب: شبکه؛ صفر تا صد
مؤلف: محمدتقی روغنی

چاپ اول؛ تابستان ۱۳۹۲
۵۴۶ صفحه، وزیری
انتشارات ناقوس

در این کتاب سعی شده مطالب مربوط به شبکه از صفر تا صد به‌صورت علمی، عملیاتی و با نگارشی روان و قابل‌فهم ارائه گردد. همچنین با اجرای ۱۹ سناریو عملیاتی، ضمن ارائه مطالب علمی و فنی، پیکربندی تجهیزات را نیز آموزش داده تا خواننده پس از پایان این کتاب بتواند به‌عنوان یک کارشناس شبکه با توانایی انجام کار عملیاتی معرفی گردد.

ازآنجاکه خواست نگارنده بر آن بوده که این کتاب بتواند نیاز طیف وسیعی از علاقه‌مندان به شبکه را برآورده سازد؛ لذا مطالب در بخش‌ها، فصل‌ها و مباحث مختلفی طبقه‌بندی گردیده تا خواننده بتواند به‌راحتی به مطلب موردنظر دسترسی پیدا نماید.

شروع کتاب با معرفی سازمان‌های بین‌المللی و شرکت‌های پیشرو درزمینه شبکه شروع شده، سپس به پروتکل‌های اولیه و پایه موردنیاز در شبکه‌های کوچک پرداخته می‌شود. این روند به‌صورت تکاملی ادامه می‌یابد تا به شبکه‌های محلی بزرگ‌تر و پروتکل‌های مسیریابی در شبکه‌های گسترده می‌رسیم. بررسی پروتکل‌های شبکه‌های محلی و گسترده، هم بر اساس IPv4 و هم IPv6 انجام شده است. در بخش پایانی نیز به امنیت و استانداردهای مربوط به شبکه پرداخته شده است.

با توجه به مطالب ذکرشده، این کتاب برای مدیران و مشاوران IT، مدیران شبکه، کارشناسان و علاقه‌مندان به شبکه، با هر سطحی از دانش، پیشنهاد می‌گردد.

برای خرید یا دانلود این کتاب می توانید از طریق لینک زیر اقدام نمایید:
http://parscenter.com/networkgod/Product/112742

تـــــوجـــــــه

خواننده گرامی

این PDF تنها شامل گزیده‌ای از کتاب "امنیت اطلاعات" است. در صورتیکه مطالب و نحوه نگارش را مفید ارزیابی کردید، برای خرید این کتاب به‌صورت کامل و در قالب چاپ کاغذی، می‌توانید انحصاراً از طریق لینک زیر اقدام نمایید:

نام کتاب: امنیت اطلاعات
مؤلف: محمدتقی روغنی
چاپ اول: زمستان ۱۳۹۳
۴۴۸ صفحه، وزیری
قیمت: ۲۵۰۰۰ تومان

لینک خرید: