



مبانی امنیت اطلاعات

دکتر علی شکیبا

«عضو هیئت علمی دانشگاه ولی عصر رفسنجان»

محمد تاری

منصوره عشوریون

امروزه کتاب‌خوانی و علم‌آموزی، نه تنها یک وظیفه ملی، که یک واجب دینی است.^۱

مقام معظم رهبری

در عصر حاضر یکی از شاخصه‌های ارزیابی رشد، توسعه و پیشرفت فرهنگی هر کشوری میزان تولید کتاب، مطالعه و کتاب‌خوانی مردم آن مرز و بوم است. ایران اسلامی نیز از دیرباز تاکنون با داشتن تمدنی چندهزارساله و مراکز متعدد علمی، فرهنگی، کتابخانه‌های معتبر، علما و دانشمندان بزرگ با آثار ارزشمند تاریخی، سرآمد دولت‌ها و ملت‌های دیگر بوده و در عرصه فرهنگ و تمدن جهانی به‌سان خورشیدی تابناک همچنان می‌درخشد و با فرزندان نیک‌نهاد خویش هنرنمایی می‌کند. چه کسی است که در دنیا با دانشمندان فرزانه و نام‌آور ایرانی همچون ابوعلی سینا، ابوریحان بیرونی، فارابی، خوارزمی و ... همچنین شاعران برجسته‌ای نظیر فردوسی، سعدی، مولوی، حافظ و ... آشنا نباشد و در مقابل عظمت آنها سر تعظیم فرود نیاورد. تمامی این افتخارات ارزشمند، برگرفته از میزان عشق و علاقه فراوان ملت ما به فراگیری علم و دانش از طریق خواندن و مطالعه منابع و کتاب‌های گوناگون است. به شکرانه الهی، تاریخ و گذشته ما، همیشه درخشان و پر بار است. ولی اکنون در این زمینه در چه جایگاهی قرار داریم؟ آمار و ارقام ارائه‌شده از سوی مجامع و سازمان‌های فرهنگی در مورد سرانه مطالعه هر ایرانی، برایمان چندان امیدوارکننده نمی‌باشد.

کتاب، دروازه‌ای به سوی گستره دانش و معرفت است و کتاب خوب، یکی از بهترین ابزارهای کمال بشری است. همه دستاوردهای بشر در سراسر عمر جهان، تا آنجا که قابل کتابت بوده است، در میان دست‌نوشته‌هایی است که انسان‌ها پدید آورده و می‌آورند. در این مجموعه بی‌نظیر، تعالیم الهی، درس‌های پیامبران به بشر، و همچنین علوم مختلفی است که سعادت بشر بدون آگاهی از آنها امکان‌پذیر نیست. کسی که با دنیای زیبا و زندگی‌بخش کتاب ارتباط ندارد بی‌شک از مهم‌ترین دستاورد انسانی و نیز از بیشترین معارف الهی و بشری محروم است. با این دیدگاه، به‌روشنی می‌توان ارزش و مفهوم رمزی عمیق در این حقیقت تاریخی را دریافت که اولین خطاب خداوند متعال به پیامبر گرامی اسلام (ص) این است که «بخوان!» و در اولین

۱. پیام مقام معظم رهبری به مناسبت آغاز هفته کتاب ۷۲/۱۰/۴

سوره‌ای که بر آن فرستاده عظیم‌الشان خداوند، فرود آمده، نام «قلم» به تجلیل یاد شده‌است: «إِقْرَأْ وَ رَبُّكَ الْأَكْرَمُ. الَّذِي عَلَّمَ بِالْقَلَمِ» در اهمیت عنصر کتاب برای تکامل جامعه انسانی، همین بس که تمامی ادیان آسمانی و رجال بزرگ تاریخ بشری، از طریق کتاب جاودانه مانده‌اند.

دانشگاه پیام‌نور با گستره جغرافیایی ایران‌شمول خود با هدف آموزش برای همه، همه‌جا و همه‌وقت، به‌عنوان دانشگاهی کتاب‌محور در نظام آموزش عالی کشورمان، افتخار دارد جایگاه اندیشه‌سازی و خردورزی بخش عظیمی از جوانان جویای علم این مرز و بوم باشد. تلاش فراوانی در ایام طولانی فعالیت این دانشگاه انجام پذیرفته تا با بهره‌گیری از تجربه‌های گرانقدر استادان و صاحب‌نظران برجسته کشورمان، کتاب‌ها و منابع آموزشی درسی شاخص و خودآموز تولید شود. در آینده هم، این مهم با هدف ارتقای سطح علمی، روزآمدی و توجه بیشتر به نیازهای مخاطبان دانشگاه پیام‌نور با جدیت ادامه خواهد داشت. به‌طور قطع استفاده از نظرات استادان، صاحب‌نظران و دانشجویان محترم، ما را در انجام این وظیفه مهم و خطیر یاری‌رسان خواهد بود. پیشاپیش از تمامی عزیزانی که با نقد، تصحیح و پیشنهادهای خود ما را در انجام این وظیفه خطیر یاری می‌رسانند، سپاسگزاری می‌نماییم. لازم است از تمامی اندیشمندانی که تاکنون دانشگاه پیام‌نور را منزلگاه اندیشه‌سازی خود دانسته و ما را در تولید کتاب و محتوای آموزشی درسی یاری نموده‌اند، صمیمانه قدردانی گردد. موفقیت و بهروزی تمامی دانشجویان و دانش‌پژوهان عزیز آرزوی همیشگی ما است.

دانشگاه پیام‌نور

فهرست مطالب

پانزده	پیشگفتار
۱	فصل اول: مقدمه‌ای بر مبانی امنیت اطلاعات
۱	هدف کلی
۱	هدف‌های یادگیری
۱	مقدمه
۴	۱-۱ مثلث C.I.A.
۸	۲-۱ استانداردها
۹	۳-۱ مفاهیم پایه در امنیت
۹	۱-۳-۱ حمله امنیتی
۱۲	۲-۳-۱ خدمات امنیتی
۱۳	۳-۳-۱ سازوکارهای امنیتی
۱۹	خلاصه فصل اول
۲۰	برای مطالعه بیشتر
۲۰	خودآزمایی چهارگزینه‌ای فصل اول
۲۱	خودآزمایی تشریحی فصل اول
۲۳	فصل دوم: کنترل دسترسی
۲۳	هدف کلی
۲۳	هدف‌های یادگیری
۲۳	مقدمه
۲۸	۱-۲ کنترل‌های دسترسی در سامانه عامل
۳۳	۲-۲ گروه‌ها و نقش‌ها

۳۴	۳-۲ فهرست‌های کنترل دسترسی
۳۶	۴-۲ کنترل دسترسی به پایگاه داده
۳۶	۱-۴-۲ مدل کنترل دسترسی مبتنی بر نقش (RBAC)
۳۶	۲-۴-۲ خانواده مدل‌های مبتنی بر نقش
۳۹	۵-۲ کنترل دسترسی به مراکز داده
۴۰	۱-۵-۲ استانداردهای زیرساختی مراکز داده
۴۱	۲-۵-۲ مروری بر کنترل‌های استاندارد TIA942
۴۴	۳-۵-۲ طبقه‌بندی کلاس مرکز داده براساس سطح
۴۶	۶-۲ جعبه شنی
۴۷	خلاصه فصل دوم
۴۷	برای مطالعه بیشتر
۴۸	خودآزمایی چهارگزینه‌ای فصل دوم
۴۸	خودآزمایی تشریحی فصل دوم
۵۱	فصل سوم: امنیت داده و برنامه
۵۱	هدف کلی
۵۱	هدف‌های یادگیری
۵۱	مقدمه
۵۳	۱-۳ ویروس‌ها
۵۵	۲-۳ کرم‌ها
۵۶	۳-۳ اسب‌های تروا
۵۶	۴-۳ هرزنامه‌ها
۵۶	۵-۳ باج‌افزارها
۵۷	۶-۳ زامبی‌ها
۵۷	۷-۳ جاسوس‌افزارها

۵۷	۳-۸ رخنه‌افزارها
۵۷	۳-۹ مقابله با بدافزارها
۵۸	۳-۱۰ حملات سرریزبافر
۶۷	۳-۱۱ امنیت در لایه سامانه عامل
۷۰	۳-۱۲ امنیت مجازی‌سازی
۷۳	۳-۱۳ امنیت ابر
۷۸	۳-۱۴ امنیت اینترنت اشیاء
۷۹	۳-۱۵ امنیت پایگاه داده
۸۱	خلاصه فصل سوم
۸۱	برای مطالعه بیشتر
۸۲	خودآزمایی چهارگزینه‌ای فصل سوم
۸۳	خودآزمایی تشریحی فصل سوم
۸۵	فصل چهارم: الگوریتم‌های رمزنگاری با کلید متقارن
۸۵	هدف کلی
۸۵	هدف‌های یادگیری
۸۵	مقدمه
۸۶	۴-۱ مدل رمزنگاری با کلید متقارن
۹۰	۴-۲ رمزهای کلاسیک
۹۰	۴-۲-۱ رمزهای جانشانی
۹۴	۴-۲-۲ رمزهای جابجایی
۹۴	۴-۳ رمزهای جریانی و رمزهای قطعه‌ای
۹۵	۴-۴ رمز با کلید یک‌بار مصرف
۹۶	۴-۵ آشفته‌سازی و پراکنش
۹۹	۴-۶ استاندارد رمزگذاری داده (DES)

۱۰۰	۴-۶-۱ الگوریتم رمزگذاری
۱۰۴	۴-۶-۲ زمانبندی کلید
۱۰۵	۴-۶-۳ الگوریتم رمزگشایی
۱۰۵	۴-۶-۴ امنیت رمز
۱۰۷	۴-۶-۵ رمز 3DES
۱۰۸	۴-۶-۶ حمله ملاقات در وسط
۱۰۹	۴-۶-۷ رمز DESX
۱۱۰	۴-۷ استاندارد رمزگذاری پیشرفته (AES)
۱۱۰	۴-۷-۱ الگوریتم رمزگذاری
۱۱۵	۴-۷-۲ زمانبندی کلید
۱۱۹	۴-۷-۳ الگوریتم رمزگشایی
۱۲۱	۴-۷-۴ امنیت رمز
۱۲۲	۴-۸ سبک‌های به‌کارگیری رمزهای قطعه‌ای
۱۲۳	۴-۸-۱ سبک کتابچه رمز (ECB)
۱۲۳	۴-۸-۲ سبک زنجیره‌ای قالب‌های رمز (CBC)
۱۲۴	۴-۸-۳ سبک پس‌خورد رمز (CFB)
۱۲۵	۴-۸-۴ سبک پس‌خورد خروجی (OFB)
۱۲۵	۴-۸-۵ سبک شمارنده (CTR)
۱۲۶	۴-۸-۶ سبک XTS-AES
۱۲۹	۴-۸-۷ مقایسه سبک‌های به‌کارگیری رمزهای قطعه‌ای
۱۳۰	۴-۹ تولید اعداد شبه‌تصادفی ایمن
۱۳۱	۴-۹-۱ روش BBS
۱۳۲	۴-۹-۲ روش مبتنی بر رمزهای قطعه‌ای
۱۳۳	خلاصه فصل چهارم

۱۳۳	برای مطالعه بیشتر
۱۳۴	خودآزمایی چهارگزینه‌ای فصل چهارم
۱۳۵	خودآزمایی تشریحی فصل چهارم
۱۴۱	فصل پنجم: الگوریتم‌های رمزنگاری با کلید نامتقارن
۱۴۱	هدف کلی
۱۴۱	هدف‌های یادگیری
۱۴۱	مقدمه
۱۴۲	۱-۵ مدل رمزنگاری با کلید نامتقارن
۱۴۳	۲-۵ الگوریتم تبادل کلید دیفی-هلمن
۱۴۵	۱-۲-۵ مسئله لگاریتم گسسته و امنیت الگوریتم تبادل کلید دیفی-هلمن
۱۴۶	۲-۲-۵ الگوریتم مجذور و ضرب
۱۴۷	۳-۵ الگوریتم رمزنگاری طاهرالجمال
۱۵۰	۱-۳-۵ امنیت الگوریتم
۱۵۰	۲-۳-۵ الگوریتم اقلیدس تعمیم‌یافته برای محاسبه معکوس ضربی
۱۵۲	۴-۵ الگوریتم رمزنگاری RSA
۱۵۳	۱-۴-۵ الگوریتم تولید کلید
۱۵۴	۲-۴-۵ الگوریتم‌های رمزگذاری و رمزگشایی
۱۵۴	۳-۴-۵ صحت
۱۵۶	۴-۴-۵ تحلیل امنیت
۱۵۸	۵-۴-۵ جنبه‌های محاسباتی
۱۶۲	۵-۵ الگوریتم رمزنگاری مبتنی بر خم بیضوی
۱۶۳	۱-۵-۵ مروری بر خم‌های بیضوی
۱۶۷	۲-۵-۵ الگوریتم تبادل کلید مبتنی بر خم بیضوی
۱۶۹	۳-۵-۵ تحلیل امنیت

۱۷۱	۵-۵-۴ الگوریتم رمزگذاری و رمزگشایی مبتنی بر خم بیضوی
۱۷۳	۵-۶ تولید اعداد تصادفی با استفاده از الگوریتم‌های رمزنگاری نامتقارن
۱۷۵	خلاصه فصل پنجم
۱۷۶	برای مطالعه بیشتر
۱۷۷	خودآزمایی چهارگزینه‌ای فصل پنجم
۱۷۸	خودآزمایی تشریحی فصل پنجم
۱۸۱	فصل ششم: الگوریتم‌های درهم‌سازی
۱۸۱	هدف کلی
۱۸۱	هدف‌های یادگیری
۱۸۱	مقدمه
۱۸۲	۶-۱ کاربردهای الگوریتم‌های درهم‌سازی
۱۸۳	۶-۲ تعریف توابع درهم‌ساز
۱۸۵	۶-۳ نیازمندی‌های امنیتی
۱۸۶	۶-۳-۱ یک‌طرفه‌بودن یا مقاومت در برابر پیش‌تصویر
۱۸۶	۶-۳-۲ مقاومت در برابر پیش‌تصویر دوم یا مقاومت در برابر برخورد ضعیف
۱۸۶	۶-۳-۳ مقاومت در برابر برخورد یا مقاومت در برابر برخورد قوی
۱۹۰	۶-۴ توابع درهم‌سازی مبتنی بر رمزهای قطعه‌ای
۱۹۳	۶-۵ خانواده SHA
۱۹۴	۶-۵-۱ ساختار اسفنج
۱۹۷	۶-۵-۲ تابع تکرار SHA-3
۲۰۱	۶-۶ کدهای احراز اصالت پیام (MAC)
۲۰۲	۶-۶-۱ کدهای احراز اصالت پیام مبتنی بر توابع درهم‌سازی: HMAC
۲۰۵	۶-۶-۲ ساختار CBC-MAC
۲۰۸	۶-۶-۳ رمزگذاری توأم با احراز اصالت CCM و GCM

۲۱۳	۶-۶-۴ سبک پوشش کلید
۲۱۵	۶-۷ سازوکار دنباله‌گذاری PKCS#1 نسخه ۲/۱
۲۱۶	۶-۸ درخت‌های مرکب
۲۱۹	خلاصه فصل ششم
۲۲۰	برای مطالعه بیشتر
۲۲۰	خودآزمایی چهارگزینه‌ای فصل ششم
۲۲۱	خودآزمایی تشریحی فصل ششم
۲۲۵	فصل هفتم: امضای دیجیتال
۲۲۵	هدف کلی
۲۲۵	هدف‌های یادگیری
۲۲۵	مقدمه
۲۲۶	۷-۱ تفاوت امضای دیجیتال و امضای الکترونیکی
۲۲۷	۷-۲ نیازمندی‌های امضای دیجیتال
۲۲۷	۷-۲-۱ زیرساخت‌های امضای دیجیتال
۲۲۸	۷-۲-۲ ساختار امضای دیجیتال
۲۲۹	۷-۲-۳ کاربردهای امضای دیجیتال
۲۳۰	۷-۳ امضای دیجیتال مبتنی بر رمز نامتقارن طاهرالجمال
۲۳۱	۷-۴ طرح مبتنی بر خم‌های بیضوی (ECDSA)
۲۳۲	۷-۵ طرح RSA-PSS
۲۳۲	۷-۶ مقایسه سه استاندارد امضای دیجیتال
۲۳۴	خلاصه فصل هفتم
۲۳۴	برای مطالعه بیشتر
۲۳۵	خودآزمایی چهارگزینه‌ای فصل هفتم
۲۳۵	خودآزمایی تشریحی فصل هفتم

۲۳۷	فصل هشتم: مدیریت و توزیع کلید
۲۳۷	هدف کلی
۲۳۷	هدف‌های یادگیری
۲۳۷	مقدمه
۲۳۸	۸-۱ مسئله مدیریت و توزیع کلید
۲۴۱	۸-۲ توزیع کلید با استفاده از رمزهای با کلید متقارن
۲۴۷	۸-۳ توزیع کلید با استفاده از رمزهای با کلید نامتقارن
۲۵۱	۸-۴ توزیع کلیدهای عمومی
۲۵۷	خلاصه فصل هشتم
۲۵۷	برای مطالعه بیشتر
۲۵۷	خودآزمایی چهارگزینه‌ای فصل هشتم
۲۵۸	خودآزمایی تشریحی فصل هشتم
۲۶۱	فصل نهم: احراز هویت
۲۶۱	هدف کلی
۲۶۱	هدف‌های یادگیری
۲۶۱	مقدمه
۲۶۳	۹-۱ احراز هویت
۲۶۳	۹-۲ احراز هویت با استفاده از گذرواژه
۲۶۴	۹-۳ احراز هویت با استفاده از توکن
۲۶۴	۹-۴ احراز هویت با استفاده از بیومتریک
۲۶۶	۹-۵ احراز هویت با رمزهای متقارن
۲۷۱	۹-۶ روش کربراس
۲۷۳	۹-۷ احراز هویت با رمزهای نامتقارن
۲۷۶	خلاصه فصل نهم

۲۷۷	برای مطالعه بیشتر
۲۷۷	خودآزمایی چهارگزینه‌ای فصل نهم
۲۷۸	خودآزمایی تشریحی فصل نهم
۲۷۹	فصل دهم: تهدیدات، حملات و آسیب‌پذیری‌ها
۲۷۹	هدف کلی
۲۷۹	هدف‌های یادگیری
۲۷۹	مقدمه
۲۸۰	۱-۱۰ حملات منع خدمت
۲۸۷	۲-۱۰ تشخیص نفوذ
۲۹۳	۳-۱۰ دیواره‌های آتش
۲۹۶	۴-۱۰ تله ظرف غسل
۲۹۸	۵-۱۰ مدیریت یکپارچه تهدیدات
۳۰۰	خلاصه فصل دهم
۳۰۰	برای مطالعه بیشتر
۳۰۱	خودآزمایی چهارگزینه‌ای فصل دهم
۳۰۲	خودآزمایی تشریحی فصل دهم
۳۰۵	فصل یازدهم: مباحث تکمیلی
۳۰۵	هدف کلی
۳۰۵	هدف‌های یادگیری
۳۰۵	مقدمه
۳۰۶	۱-۱۱ ارزش‌های دیجیتالی و زنجیره بلوکی
۳۲۶	۲-۱۱ راهنمایی بر تمرین‌های عملی با CrypTool 2.0
۳۳۲	خلاصه فصل یازدهم

۳۳۲	برای مطالعه بیشتر
۳۳۲	خودآزمایی چهارگزینه‌ای فصل یازدهم
۳۳۳	خودآزمایی تشریحی فصل یازدهم
۳۳۵	پاسخنامه
۳۳۷	منابع

پیشگفتار

هدف از تدوین کتاب حاضر، آشنایی دانشجویان با مبانی امنیت اطلاعات و مسائل کلیدی آن است. هر چند کتاب‌هایی بسیار در این موضوع توسط بزرگان علم امنیت اطلاعات به رشته تحریر درآمده است، اما در این کتاب هدف این بوده است که با نگارشی روان و درعین حال غنی، مطالب به گونه‌ای ارائه گردند که مخاطبین بتوانند مطالب را مطالعه نموده و درک نمایند. مطالب این کتاب در یازده فصل ارائه شده‌اند: در فصل اول، به تعریف امنیت و الزامات پیاده‌سازی آن در سامانه‌های نرم‌افزاری و سخت‌افزاری پرداخته می‌شود. فصل دوم به مسئله کنترل دسترسی خواهد پرداخت و این مسئله را در لایه‌های مختلف مورد بررسی قرار می‌دهد. فصل سوم به‌طور خاص به امنیت در لایه نرم‌افزار می‌پردازد و به‌صورت خلاصه، سازوکارهای برنامه‌نویسی ایمن را ارائه می‌نماید. در فصل‌های چهارم و پنجم، دو سنگ‌بنای علم رمزنگاری، یعنی رمزهای با کلید متقارن و رمزهای با کلید نامتقارن، ارائه می‌شوند. در فصل ششم، الگوریتم‌های درهم‌سازی به‌عنوان یکی دیگر از پایه‌های علم رمزنگاری مورد بررسی قرار گرفته‌اند. فصل‌های هفتم، هشتم و نهم به کاربردهای الگوریتم‌های پایه در طراحی خدمات‌های امنیتی مانند امضای دیجیتال، مدیریت و توزیع کلید و احراز هویت پرداخته‌اند. در فصل دهم، تهدیدات، حملات و آسیب‌پذیری‌ها در دنیای واقعی مورد بررسی قرار گرفته‌اند و راهکارهایی برای جلوگیری یا مقابله با آن‌ها ارائه شده‌اند. در فصل یازدهم، علاوه بر ارائه راهنمایی کوچک برای استفاده از ابزار CrypTool 2.0، به مسئله زنجیره بلوکی و کاربردهای آن در ایجاد رمزارزها مانند بیت‌کوین پرداخته شده‌است.

برای همگان واضح است که موضوعات بسیار جذاب، بدیع و کاربردی در امنیت اطلاعات وجود دارند که حتی نام‌بردن از آن‌ها در یک نوشتار چند صد صفحه‌ای غیرممکن است. نویسندگان اثر حاضر، تلاش داشته‌اند تا مطالبی را در نوشتار حاضر درج نمایند که مخاطب علاقه‌مند بتواند پس از مطالعه و درک آن‌ها، سفر خود را در دنیای

علوم امنیت داده آغاز نماید. علاوه بر متن حاضر، صفحه‌ای در شبکه جهانی اینترنت به آدرس <http://infosecbook.ir> فراهم شده است تا زمینه ارتباط بین مؤلفین و مخاطبین را ایجاد نماید. علاوه بر این، در این صفحه، به مرور، محتوای کمک درسی نیز برای نوشتار حاضر قرار خواهد گرفت. هر یک از مؤلفین بنا به تخصص، علاقه و تجربه خود، نگارش بخشی از این کتاب را به عهده داشته‌اند. نگارش فصل‌های اول، سوم تا ششم، هشتم، دهم و یازدهم توسط نویسندۀ اول و فصل‌های دوم، هفتم و نهم به صورت مشترک توسط نویسندگان دوم و سوم انجام شده است.

گرچه نگارندگان اثر حاضر تلاش داشته‌اند تا اثری با حداقل ایرادات و کاستی‌ها فراهم آورند، اما خود معترف‌اند که هیچ اثری زمینی بدون عیب نیست. بنابراین، مؤلفان کتاب امیدوارند خوانندگان این اثر، ایرادات، نظرات و پیشنهادهای خود را به نویسندگان ارسال نمایند تا در فرصت‌های آتی برای رفع آن‌ها اقدام شود.

دکتر علی شکیبا، دانشگاه ولی عصر (عج) رفسنجان

منصوره عشوریون، دانشگاه پیام‌نور

محمد تاری، دانشگاه پیام‌نور

تابستان ۱۳۹۸ بهار ۱۴۰۰

فصل اول

مقدمه‌ای بر مبانی امنیت اطلاعات

هدف کلی

آشنایی با تعاریف، تهدیدها، حملات و استانداردهای رایج در امنیت اطلاعات

هدف‌های یادگیری

انتظار می‌رود پس از خواندن این فصل بتوانید:

۱. مفاهیم اساسی در امنیت را تشریح نمایید.
۲. معماری امنیتی X.800 را توصیف نمایید.
۳. انواع تهدیدات و حملات را شرح دهید.
۴. اصول اساسی یک طراحی ایمن را شرح دهید.
۵. سازوکارهای امنیتی را شرح دهید.

مقدمه

امنیت، موضوع اصلی کتاب حاضر است و در این کتاب به موضوعات مختلفی از حوزه امنیت داده^۱، امنیت رایانه^۲ و امنیت شبکه^۳ خواهیم پرداخت. مجموعه‌ای از روش‌ها که برای حفظ امنیت داده، فارغ از شکل آن، به کار می‌روند، روش‌های امنیت داده نام دارند.

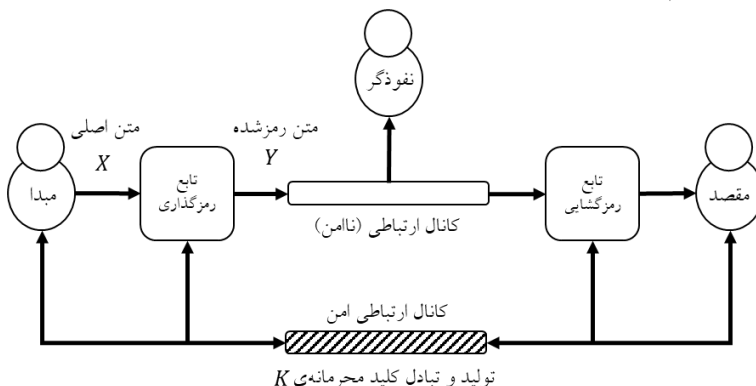
1. Data security
2. Computer security
3. Network security

به عبارت دیگر، روش‌های برقراری امنیت داده، به داده دیجیتال و غیر دیجیتال قابل تعمیم هستند. در امنیت رایانه، به دنبال برقراری یک دستگاه رایانه، مانند رایانه‌های شخصی، خادم‌ها، ابررایانه‌ها و حتی گوشی‌های تلفن همراه، هستیم. این دستگاه ممکن است به شبکه متصل باشد یا اتصالی به شبکه نداشته باشد. در امنیت شبکه، به تأمین امنیت مجموعه‌ای از دستگاه‌های رایانه‌ای که به هم متصل هستند به همراه ادوات شبکه‌ای می‌پردازیم. با این تفکیک اولیه، مباحث این کتاب در سه بخش قابل دسته‌بندی هستند: (۱) الگوریتم‌های رمزنگاری، (۲) قراردادهای ارتباطی و (۳) ابزارهای تأمین امنیت.

الگوریتم‌های رمزنگاری سنگ بنای امنیت هستند و در بخش امنیت داده مورد بررسی قرار می‌گیرند. این الگوریتم‌ها در سه زمینه کلی قابل دسته‌بندی هستند: (۱) رمزنگاری‌های با کلید متقارن، (۲) رمزنگاری‌های با کلید نامتقارن، و (۳) الگوریتم‌های بررسی جامعیت داده. ساختار این الگوریتم‌ها به شدت وابسته به علوم ریاضی، مانند نظریه اعداد، جبر و هندسه، و پیچیدگی محاسباتی هستند.

الگوریتم‌های رمزنگاری با کلید متقارن از پنج قسمت شامل (۱) کلید، (۲) الگوریتم رمزگذاری، (۳) الگوریتم رمزگشایی و (۴) متن اصلی و (۵) متن رمز شده تشکیل شده‌اند و برای یک متن اصلی، متن رمز شده معادل را تولید می‌کنند. شمای کلی این الگوریتم‌ها در شکل ۱-۱ آمده است. از این جهت که کلید مورد استفاده برای رمزگشایی و رمزگذاری یکسان است، به این نوع الگوریتم‌ها، الگوریتم‌های رمزنگاری با کلید متقارن گفته می‌شود. به عنوان نمونه‌ای از این الگوریتم‌ها، فرض کنید پیام X را در قطعه‌ای کاغذ نوشته شده است. به منظور رمزگذاری، آن پیام را در یک صندوق غیرقابل نفوذ قرار می‌دهیم و درب آن صندوق را قفل می‌کنیم. فرض کنید که تنها راه دسترسی به پیام قرار گرفته درون صندوق، استفاده از کلید و بازکردن درب صندوق باشد. حال صندوق را به مقصد ارسال می‌کنیم. در مقصد، دریافت کننده از کلید استفاده کرده و درب صندوق را باز می‌کند. سپس، وی می‌تواند به محتوای پیام دسترسی پیدا کند. در اینجا چند نکته

قابل توجه است: (۱) لازم است تا کلید مورد استفاده برای صندوق، هم در مبدأ و هم در مقصد وجود داشته باشد. (۲) محرمانگی پیام وابسته به نفوذ ناپذیری صندوق و محرمانه بودن کلید است. به منظور تبادل کلید، لازم است تا طرفین ارتباط از یک کانال ارتباطی امن استفاده کنند. در فصل چهارم در مورد این الگوریتم‌ها بیشتر خواهید آموخت و در فصل هشتم، مسئله تبادل کلید به صورت دقیق بررسی خواهد شد.



شکل ۱-۱. طرح کلی یک الگوریتم رمزنگاری با کلید متقارن

علاوه بر الگوریتم‌های رمزنگاری با کلید متقارن، الگوریتم‌های رمزنگاری با کلید نامتقارن نیز وجود دارند. در این الگوریتم‌ها، از یک کلید برای رمزگذاری و از کلیدی دیگر برای رمزگشایی استفاده می‌شود. به دلیل تفاوت کلیدهای رمزگذاری و رمزگشایی، به این الگوریتم‌ها، الگوریتم‌های رمزنگاری با کلید نامتقارن^۱ نیز گفته می‌شود. برای نمونه، فرض کنید جعبه‌هایی نفوذناپذیر در اختیار داریم که درب آن‌ها توسط یک کلید قفل می‌شود و از کلید دیگری برای بازکردن قفل آن استفاده می‌شود. به عبارت دیگر، از کلید قفل کننده نمی‌توان برای بازکردن قفل جعبه استفاده کرد و از کلید بازکننده نیز نمی‌توان

۱. به الگوریتم‌های رمزنگاری با کلید نامتقارن، الگوریتم‌های کلید عمومی (Public-key) نیز گفته می‌شود. دقت داشته باشید که کلید رمزگذاری می‌تواند در کاربردهای امضای دیجیتال (فصل هفتم) به عنوان کلید خصوصی یا محرمانه در نظر گرفته شود و کلید رمزگشایی را به عنوان کلید عمومی در اختیار عموم قرار داد. در صورتی که در کاربرد حفظ محرمانگی، فصل پنجم، کلید رمزگذاری کلیدی عمومی است و کلید رمزگشایی یک کلید خصوصی محسوب می‌شود.

برای قفل کردن جعبه استفاده کرد. حال فرض کنید طرف A قصد دارد تا دیگران بتوانند برای وی پیامی را ارسال کنند. بنابراین جعبه‌های مربوط به خود را تولید می‌کند، کلید رمزگشایی را برای خود به صورت محرمانه نگهداری کرده و جعبه و کلید رمزگذاری را به صورت عمومی، در اختیار سایرین قرار می‌دهد. حال هر طرفی که بخواهد به طرف A پیامی را به صورت محرمانه ارسال کند، کافی است جعبه طرف A را یافته و سپس پیام خود را در آن قرار دهد. سپس، با استفاده از کلید رمزگذاری، جعبه را قفل نماید و جعبه را ارسال کند. تنها کسی که می‌تواند قفل جعبه را باز کند، فردی است که کلید رمزگشا را در اختیار دارد. بنابراین، طرف A می‌تواند جعبه را بازگشایی نموده و محتوای پیام را دریافت کند. در مورد این الگوریتم‌ها در فصل پنجم بیشتر خواهید آموخت. البته این الگوریتم‌ها کاربردهایی اساسی در سایر مسائل مهم دنیای واقعی امنیت اطلاعات دارند که در فصل‌های هفتم تا نهم به تفصیل به آن‌ها پرداخته خواهد شد.

سومین دسته از الگوریتم‌های رمزنگاری، الگوریتم‌های جامعیت داده هستند. پایه‌ای‌ترین جزء در این الگوریتم‌ها، الگوریتم‌های درهم‌سازی¹ هستند. به صورت شهودی، این الگوریتم‌ها را می‌توان به دستگاه‌های آبمیوه‌گیری تشبیه کرد که چکیده‌ای از ورودی خود را تولید می‌کنند، به طوری که (۱) در صورتی که ورودی حتی به میزان یک بیت تغییر کند، خروجی بسیار متفاوت باشد، و (۲) با استفاده از چکیده نتوان ورودی را تشخیص داد. البته ویژگی‌های دیگری نیز برای این توابع مطرح است که در فصل ششم به صورت دقیق بررسی خواهند شد.

با ترکیب سه ساختار الگوریتم‌های رمزنگاری با کلید متقارن، الگوریتم‌های رمزنگاری با کلید نامتقارن، و الگوریتم‌های بررسی جامعیت داده می‌توان قراردادهای امنیت را ایجاد و از آن‌ها برای ایجاد ابزارهای تأمین امنیت داده استفاده نمود.

۱-۱ مثلث C.I.A.

علاوه بر تعریف ارائه شده در ابتدای فصل از امنیت رایانه، تعریف دقیق تری نیز توسط مؤسسه ملی استاندارد و فناوری آمریکا^۱ ارائه شده است: «منظور از امنیت رایانه، ابزارها و کنترل‌هایی است که از محرمانگی^۲، جامعیت^۳ و در دسترس بودن^۴ سامانه‌های اطلاعاتی شامل سخت‌افزار، میان‌افزار، نرم‌افزار، اطلاعات مورد پردازش، ذخیره و تبادل شده اطمینان حاصل می‌کند». در این تعریف، از سه هدف کلیدی که به مثلث C.I.A. نیز معروف است، نام برده شده است. در محرمانگی، دو هدف مهم وجود دارد: (۱) اطلاعات خصوصی و مهم تنها در اختیار موجودیت‌های مجاز قرار گیرد و محتوای این اطلاعات برای سایر موجودیت‌ها فاش نشود. (۲) موجودیت‌ها مدیریت اطلاعات مربوط به خود را در اختیار داشته باشند و بدانند که این اطلاعات توسط چه کسانی و چگونه جمع‌آوری می‌شود و در اختیار چه کسانی و به چه منظوری قرار می‌گیرد. هدف اول، محرمانگی داده و هدف دوم را حریم خصوصی^۵ گویند.

مثال ۱: برای نمونه فرض کنید طرف A قصد دارد تا پیام X را به طرف B ارسال نماید، به گونه‌ای که تنها B بتواند از محتوای آن مطلع شود. در اینجا طرف سوم نیز به عنوان نفوذگر وجود دارد که هدف وی، کسب اطلاع از محتوای پیام X است. به همین منظور، طرف A پیام خود را به صورتی محرمانه به طرف B منتقل می‌کند، به صورتی که تنها او به پیام دسترسی داشته باشد. البته بدیهی است ممکن است نفوذگر بتواند محتوای پیام را به تصادف حدس بزند. اما در صورتی که وی بتواند محتوای پیام رمز شده را بهتر از حدس زدن تشخیص دهد، محرمانگی خدشه دار شده است.

مثال ۲: فرض کنید طرف A از یک پایگاه اطلاع‌رسانی بازدید می‌کند. در طی بازدید، وی به مجموعه‌ای از اخبار علاقه نشان داده و علاقه خود را با کلیک بر روی

-
1. National Institute of Security and Technology (NIST)
 2. Confidentiality
 3. Integrity
 4. Availability
 5. Privacy

لینک‌ها و مطالعه اخبار پی می‌گیرد. ممکن است زمان حضور وی در هر صفحه و قسمت‌هایی که بیشترین توجه وی به آن معطوف بوده است نیز ثبت شود. علاوه بر این، آدرس IP او، ساعت ورود، مشخصات مرورگر و سامانه عامل وی نیز ممکن است مورد ثبت قرار گیرد. اما این اطلاعات چه می‌شود؟ مهم‌تر از آن، این اطلاعات چگونه و تحت چه معیارهای امنیتی ذخیره می‌شوند و قرار است از آن‌ها چه استفاده‌ای شود؟ در صورتی که اطلاعات به درستی ذخیره و نگهداری نشوند، ممکن است بر اثر نفوذ، این اطلاعات فاش شده و هویت کاربران را به خطر اندازند. همچنین ممکن است کاربری تمایل نداشته باشد تا این اطلاعات در مورد وی جمع‌آوری شوند. در صورتی که یک سامانه اقدام به جمع‌آوری و ذخیره‌سازی اطلاعات بدون اطلاع و اجازه کاربر نماید، آن سامانه دارای حریم خصوصی نیست. حتی اگر این اطلاعات با اطلاع و اجازه کاربر ذخیره شوند، اما سازمان یا مالک آن پایگاه در نگهداری اطلاعات دقت کافی به عمل نیاورد و منجر به افشای اطلاعات کاربر شود، حریم خصوصی خدشه‌دار می‌شود. لازم به ذکر است که تعریف‌های متعددی از حریم خصوصی و سازوکارهای رعایت آن ارائه شده‌اند که از مقبول‌ترین آن‌ها می‌توان به حریم خصوصی تفاضلی^۱ اشاره کرد.

در جامعیت نیز از دو مفهوم استفاده می‌شود: (۱) جامعیت داده و (۲) جامعیت سامانه. در جامعیت داده، هدف تشخیص هرگونه تغییر در داده توسط موجودیت‌های غیرمجاز یا به شیوه‌های غیرمجاز است. در جامعیت سامانه، هدف اطمینان از عملکرد صحیح سامانه بدون مداخله موجودیت‌های غیرمجاز است.

مثال ۳: فرض کنید طرف استاد درس مبانی امنیت اطلاعات، سرفصل درس را در ابتدای ترم منتشر می‌کند. نیاز نیست تا محرمانگی این اطلاعات حفظ شوند، اما ممکن است فردی قصد داشته باشد تا دانشجویان این استاد را با تغییر سرفصل منتشرشده همراه

۱. به صورت شهودی، حریم خصوصی تفاضلی (Differential Privacy) به این معنی است که در صورتی که داده یک کاربر در پایگاه داده باشد و پرس و جویی بر آن پایگاه داده اعمال شود، نتیجه تفاوت چندانی با حالتی که داده آن کاربر در پایگاه داده قرار ندارد، نداشته باشد. پرداختن به مدل‌های مختلف حریم خصوصی و روش‌های پیاده‌سازی آن‌ها موضوعی جذاب و داغ در صنعت و علم است که البته از حوصله متن حاضر خارج است.