



حریم خصوصی و امنیت

اینترنت

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری

مؤلف:

دکتر محمدعلی ترکمانی

سرشناسه : ترکمانی، محمدعلی، ۱۳۵۴ -

عنوان و نام پدیدآور : حریم خصوصی و امنیت اینترنت/مؤلف محمدعلی ترکمانی.

مشخصات نشر : مشهد: ارسطو، ۱۳۹۵

مشخصات ظاهری : ۲۰۲ ص. : مصور.

شابک : ۹۷۸-۶۰۰-۷۹۴۰-۹۲-۱

وضعیت فهرست‌نویسی : فیا

موضوع: اینترنت -- تدابیر ایمنی

موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی

موضوع: کامپیوترها -- ایمنی اطلاعات

موضوع: پایگاه‌های اطلاعاتی - امنیت

رده‌بندی کنگره: ۱۳۹۴ ح ۴/ت ۵۹/۵۱۰۵ TK۵۱

رده‌بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی : ۴۱۱۱۳۳۱

نام کتاب : حریم خصوصی و امنیت اینترنت

مؤلف : دکتر محمدعلی ترکمانی

ناشر : ارسطو (باهمکاری سامانه اطلاع‌رسانی چاپ و نشر ایران)

صفحه‌آرایی: محمدعلی ترکمانی

تنظیم و طرح جلد : محمدعلی ترکمانی و علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : چهارم - ۱۳۹۸

چاپ : مدیران

قیمت : ۳۶۰۰۰ تومان

تلفن‌های مرکز پخش : ۳۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۰۵۱ - ۰۹۱۷۷۱۶۴۹۴۰

وبسایت: www.chaponashr.ir/Torkamani

این اثر مشمول قانون حمایت از مولفان و مصنفان و هنرمندان است. هر کس تمام یا قسمتی از

این اثر را بدون اجازه مولف نشر یا پخش یا عرضه کند، مورد پیگرد قانونی قرار خواهد گرفت.

فهرست مطالب

فصل اول: مفاهیم و اصول امنیت اطلاعات ۱۵

- ۱-۱- امنیت اطلاعات چیست؟ ۱۵
- ۱-۱-۱- خصوصیات سیستم امن ۱۵
- ۱-۲- اصطلاحات امنیتی ۱۶
- ۱-۲-۱- آسیب پذیری ۱۶
- ۱-۲-۲- حمله ۱۶
- ۱-۲-۳- تهدید ۱۶
- ۱-۲-۴- مفهوم AAA در امنیت اطلاعات ۱۶
- ۱-۲-۵- عدم انکار (سندیت) ۱۸
- ۱-۳- نفوذ گر یا هکر ۱۸
- ۱-۴- دسته بندی کلی حملات ۱۸
- ۱-۴-۱- دسته بندی از نظر تغییر دادن اطلاعات ۱۸
- ۱-۴-۲- دسته بندی از نظر به چالش کشیدن اصول امنیت ۱۹
- ۱-۵- یک HACKER از چه راهی وارد سیستم می شود؟ ۲۰
- ۱-۶- سوالات تشریحی ۲۰

فصل دوم: انواع حملات در شبکه های کامپیوتری ۲۱

- ۲-۱- حمله تکرار یا استراق سمع یا شنود اطلاعات ۲۱
- ۲-۲- در پستی ۲۱
- ۲-۳- مصرف پهنای باند (حملات DOS) ۲۲
- ۲-۴- حمله مرد میانی ۲۲
- ۲-۵- ویروس ها و کرم ها ۲۳

۲۳ ۲-۶-اسب تروآ
۲۳ ۲-۷-جاسوس افزار
۲۴ ۲-۸-وبسایت های تقلبی(فیشینگ)
۲۴ ۲-۹-حمله با استفاده از نرم افزار های ثبت کننده کلید
۲۴ ۲-۱۰-حملات جهت یافتن کلمات عبور
۲۵ ۲-۱۱-هرزنامه
۲۶ ۲-۱۲-هرز تماس(SPIT) یا VOIP SPAM
۲۶ ۲-۱۳-SPOOFING
۲۷ ۲-۱۳-۱-IP Spoofing یا IP Forgery
۲۷ ۲-۱۳-۲-ARP Spoofing
۲۸ ۲-۱۳-۳-Email spoofing
۲۸ ۲-۱۴-BOTNET
۳۰ ۲-۱۵-سؤالات تشریحی

فصل سوم: انتخاب و مدیریت کلمه عبور ۳۱

۳۱ ۳-۱-مقدمه
۳۱ ۳-۲-برخی قوانین ساده و اولیه
۳۲ ۳-۳-هک کردن کلمات عبور شما
۳۳ ۳-۴-کلمه عبور خوب
۳۶ ۳-۸-نرم افزار های مدیریت رمز عبور
۳۶ ۳-۸-۱-Efficient Password Manager Pro
۳۶ ۳-۸-۲-Sticky Password Premium
۳۶ ۳-۸-۳-LastPass Password Manager
۳۷ ۳-۸-۴-Agilebits 1Password
۳۷ ۳-۸-۵-Password Door

- ۳۷ ۳-۸-۶- برخی دیگر از نرم‌افزارهای مدیریت رمز عبور.....
- ۳۸ COMFORT ON-SCREEN KEYBOARD PRO-۳-۹
- ۳۸ ۳-۱۰-سوالات تشریحی.....

فصل چهارم: امنیت در خرید اینترنتی ۳۹

- ۳۹ ۴-۱-مقدمه.....
- ۳۹ ۴-۲-نکات خرید آنلاین.....
- ۴۳ ۴-۳- بررسی فروشگاه.....
- ۴۵ ۴-۴- راه‌های مقابله با سرقت حساب.....
- ۴۷ ۴-۵- مرورگر خود را تنظیم کنید.....
- ۵۰ ۴-۶-توصیه‌هایی برای امنیت و جلوگیری از سرقت هویت.....
- ۵۲ ۴-۷-سوالات تشریحی.....

فصل پنجم: تورنت ۵۳

- ۵۳ ۵-۱-تورنت (TORRENT) چیست؟.....
- ۵۳ ۵-۲-فایل‌های تورنت و پروتکل BITTORRENT.....
- ۵۴ ۵-۳-آیا دانلود از تورنت قانونی است؟.....
- ۵۴ ۵-۴-آیا دانلود از تورنت امن است؟.....
- ۵۵ ۵-۵-چگونه می‌توان از تورنت دانلود کرد؟.....
- ۵۵ ۵-۶-اصطلاحات BITTORRENT.....
- ۵۹ ۵-۷-BITTORRENT چگونه کار می‌کند؟.....
- ۶۰ ۵-۸-نرم‌افزارهای دانلود از تورنت.....
- ۶۰ ۵-۸-۱- aTorrent PRO – Torrent App.....
- ۶۱ ۵-۹-سوالات تشریحی.....

فصل ششم: ایمیل ناشناس و گمنامی ایمیل ۶۳

- ۶۳ ۶-۱-ریمیلر چیست؟.....

- ۶-۲- انواع ریمیلرها ۶۴
- ۶-۳- دسته‌بندی دیگر ریمیلرها ۶۵
- ۶-۴- WEB BASED MAILER ۶۶
- ۶-۵- چرا ریمیلرها توسط دولت‌ها بلاک می‌شوند؟ ۶۶
- ۶-۶- نرم‌افزارهای ریمیلر ۶۶
- ۶-۷- سوالات تشریحی ۶۷

فصل هفتم: امنیت فیزیکی و محیطی ۶۹

- ۷-۱- مقدمه ۶۹
- ۷-۲- جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و توقف فعالیت‌های سازمان ... ۶۹
 - ۷-۲-۱- حصار امنیت فیزیکی ۶۹
 - ۷-۲-۲- کنترل تردد فیزیکی (ورود و خروج) ۶۹
 - ۷-۲-۳- ایمن‌سازی دفاتر اتاق‌ها و تأسیسات ۷۰
 - ۷-۲-۴- کار در محیط امن ۷۰
 - ۷-۲-۵- محافظت در مقابل تهدیدات محیطی و خارج ۷۱
 - ۷-۲-۶- جداسازی فضاهای دسترسی عمومی تخلیه، بارگیری و ارسال و دریافت ۷۱
- ۷-۳- پیشگیری از صدمه، خسارت، دزدی، یا لو رفتن دارایی‌های سازمان و توقف در فعالیت‌های سازمان ۷۲
 - ۷-۳-۱- تجهیزات ۷۲
 - ۷-۳-۱-۱- میز کار ۷۲
 - ۷-۳-۱-۲- ابزارهای قابل‌حمل (Portabe) ۷۲
 - ۷-۳-۲- امکانات پشتیبانی (منابع تغذیه) ۷۳
 - ۷-۳-۳- امنیت کابل‌کشی ۷۴
 - ۷-۳-۴- نگهداری از تجهیزات ۷۵
 - ۷-۳-۵- راه‌های خروج تجهیزات از سازمان ۷۵

- ۷۶-۳-۶- امنیت تجهیزات خارج از محل‌های اصلی ۷۶
- ۷۶-۳-۷- اسقاط یا استفاده مجدد از تجهیزات ۷۶
- ۷۶-۳-۷- ۱- خطمشی اسقاط یا استفاده مجدد از تجهیزات ۷۶
- ۷۷-۳-۸- تجهیزات رهاسده و بدون مراقبت توسط کاربر ۷۷
- ۷۷-۳-۹- سیاست نمایشگر پاک و میز پاک ۷۷
- ۷۸-۳-۹-۱- خطمشی نمایشگر پاک ۷۸
- ۷۸-۴- سوالات تشریحی ۷۸

۷۹ فصل هشتم: امنیت در شبکه بی‌سیم

- ۷۹-۸-۱- امنیت بی‌سیم ۷۹
- ۸۰-۸-۱-۱- تهدیدهای شبکه بی‌سیم ۸۰
- ۸۲-۸-۱-۲- اقدامات امنیتی بی‌سیم ۸۲
- ۸۴-۸-۲- امنیت دستگاه سیار ۸۴
- ۹۰-۸-۳- سوالات تشریحی ۹۰

۹۲ فصل نهم: حریم خصوصی

- ۹۲-۹-۱- حفاظت از حریم و قانون ۹۲
- ۹۳-۹-۲- تعریف حریم در اساسنامه ایالات متحده ۹۳
- ۹۳-۹-۳- حریم اطلاعاتی ۹۳
- ۹۳-۹-۴- قوانین حریم، کاربردها و احکام دادگاه ۹۳
- ۹۴-۹-۴-۱- داده‌های مالی ۹۴
- ۹۴-۹-۴-۱-۱- قانون گزارش دهی اعتبار منصفانه (سال ۱۹۷۰) ۹۴
- ۹۴-۹-۴-۱-۲- قانون Gramm-Leach-Bliley (GLBA) ۹۴
- ۹۶-۹-۴-۲- اطلاعات سلامت ۹۶
- ۹۶-۹-۴-۲-۱- قانون پاسخگویی و قابلیت انتقال بیمه سلامت سال ۱۹۹۶ (HIPAA) ۹۶
- ۹۷-۹-۴-۳- داده‌های شخصی کودکان ۹۷

- ۹۷-۳-۱-۹-۴- قانون حفاظت حریم آنلاین کودکان (سال ۱۹۹۸) ۹۷
- ۹۷-۴-۹- نظارت الکترونیکی ۹۷
- ۹۷-۴-۱-۹-۴- قانون ارتباطات سال ۱۹۳۴ ۹۷
- ۹۸-۴-۲-۹-۴- قانون نظارت اطلاعات خارجی (سال ۱۹۷۸) ۹۸
- ۹۸-۴-۳-۹-۴- قانون اصلاحیات اطلاعات خارجی (سال ۲۰۰۸) ۹۸
- ۹۹-۴-۴-۹-۴- قانون USA PATRIOT (سال ۲۰۰۱) ۹۹
- ۹۹-۴-۵-۹-۴- صدور داده‌های شخصی ۹۹
- ۹۹-۴-۵-۱-۹-۴- سازمان همکاری اقتصادی و توسعه عملیات اطلاعات منصفانه (سال ۱۹۸۰) ۹۹
- ۱۰۰-۴-۵-۲-۹-۴- دستورالعمل حفاظت داده‌های اتحادیه اروپا (سال ۱۹۹۸) ۱۰۰
- ۱۰۱-۴-۵-۳-۹-۴- TRUSTe و BBBONLINE ۱۰۱
- ۱۰۲-۴-۶-۹-۴- دسترسی به رکوردهای دولت ۱۰۲
- ۱۰۲-۴-۶-۱-۹-۴- قانون آزادی اطلاعات (FOIA) سال ۱۹۶۶ در سال ۱۹۷۴ اصلاح شد ۱۰۲
- ۱۰۲-۴-۶-۲-۹-۴- قانون حریم سال ۱۹۷۴ ۱۰۲
- ۱۰۳-۵-۹-۵- مسائل کلیدی حریم و ناشناسی ۱۰۳
- ۱۰۳-۵-۱-۹-۵- سرقت هویت ۱۰۳
- ۱۰۳-۵-۱-۱-۹-۵- رخنه به داده‌ها ۱۰۳
- ۱۰۳-۵-۱-۲-۹-۵- خریداری داده‌های شخصی ۱۰۳
- ۱۰۴-۵-۱-۳-۹-۵- فیشینگ ۱۰۴
- ۱۰۵-۵-۱-۴-۹-۵- Spyware (نرم‌افزار جاسوسی) ۱۰۵
- ۱۰۵-۵-۲-۹-۵- حریم مصرف‌کننده در تجارت الکترونیک ۱۰۵
- ۱۰۵-۵-۲-۱-۹-۵- جمع‌آوری اطلاعات مصرف‌کننده ۱۰۵
- ۱۰۵-۵-۲-۲-۹-۵- حریم داده‌های مصرف‌کننده ۱۰۵
- ۱۰۶-۵-۲-۳-۹-۵- رفتار مسئولانه با داده‌های مصرف‌کننده ۱۰۶
- ۱۰۶-۵-۲-۴-۹-۵- نظارت بر محل کار ۱۰۶
- ۱۰۷-۶-۹-۵- سوالات تشریحی ۱۰۷

۱۰۸ فصل دهم: VPN

- ۱۰۸-۱-۱۰- مقدمه ۱۰۸

- ۱۰۹ ۱۰-۲-VPN چیست؟
- ۱۰۹ ۱۰-۳-چرا VPN؟
- ۱۰۹ ۱۰-۴-چه وقت از VPN استفاده می‌شود؟
- ۱۱۰ ۱۰-۵-تونلینگ (TUNNELING)
- ۱۱۰ ۱۰-۶-بررسی انواع VPN
- ۱۱۱ ۱۰-۷-بررسی امنیت VPN
- ۱۱۲ ۱۰-۸-سؤالات تشریحی

فصل یازدهم: حریم شخصی در مرورگرها ۱۱۴

- ۱۱۴ ۱۱-۱-مقدمه
- ۱۱۵ ۱۱-۲-مرورگر TOR
- ۱۱۵ ۱۱-۳-مرورگر EPIC
- ۱۱۶ ۱۱-۴-مرورگر PIRATE BROWSER
- ۱۱۷ ۱۱-۵-انتخاب مرورگر مناسب
- ۱۱۸ ۱۱-۶-سؤالات تشریحی

فصل دوازدهم: امکانات امنیتی سیستم عامل ویندوز .. ۱۲۰

- ۱۲۰ ۱۲-۱-مقدمه
- ۱۲۰ ۱۲-۲-صفحه‌کلید مجازی
- ۱۲۰ ۱۲-۳-فایروال سیستم عامل ویندوز
- ۱۲۳ ۱۲-۴-WINDOWS DEFENDER
- ۱۲۳ ۱۲-۵-رمزنگاری در ویندوز
- ۱۲۴ ۱۲-۵-۱-EFS
- ۱۲۷ ۱۲-۵-۲-Export نمودن گواهی با استفاده از wizard
- ۱۳۴ ۱۲-۵-۳-Cipher-دستور
- ۱۳۶ ۱۲-۵-۴-دسترسی به فایل‌های رمز شده
- ۱۴۰ ۱۲-۵-۵-موارد امنیتی EFS

- ۱۴۰ Encrypt شده ۱۲-۵-۶-تهیه Copy از فایل‌های
- ۱۴۱ CIPHER با دستور ۱۲-۵-۷-Export نمودن گواهی
- ۱۴۱ Import کردن گواهی ۱۲-۵-۸
- ۱۴۲ استفاده از داده‌های رمز شده توسط کاربران دیگر ۱۲-۵-۸-۱
- ۱۴۲ BIT LOCKER از ۱۲-۶-۱-رمزگذاری درایوها با استفاده از
- ۱۴۲ Bit locker چیست؟ ۱۲-۶-۱-۱
- ۱۴۳ BitLocker و EFS مقایسه ۱۲-۶-۲-۲
- ۱۴۳ فعال‌سازی BitLocker برای یک درایو ۱۲-۶-۳-۳
- ۱۵۱ دستورات BitLocker در خط فرمان (CMD) ۱۲-۶-۴-۴
- ۱۵۱ سوالات تشریحی ۱۲-۷-۱

فصل سیزدهم: محافظت از IP ۱۵۲

- ۱۵۲ مقدمه ۱۳-۱-۱
- ۱۵۲ یافتن IP ۱۳-۲-۱
- ۱۵۲ Ping فرمان ۱۳-۲-۱-۱
- ۱۵۳ IP Config / All فرمان ۱۳-۲-۲-۲
- ۱۵۳ Net stat فرمان ۱۳-۲-۳-۳
- ۱۵۵ به دست آوردن IP هنگام استفاده از یاهو مسنجر ۱۳-۲-۴-۴
- ۱۵۶ نرم‌افزارهای محافظت از IP ۱۳-۳-۱-۳
- ۱۵۶ SafeIP ۱۳-۳-۱-۱
- ۱۵۶ Easy Hide IP ۱۳-۳-۲-۲
- ۱۵۷ Real Hide IP ۱۳-۳-۳-۳
- ۱۵۷ سوالات تشریحی ۱۳-۴-۱

فصل چهاردهم: فایروال‌ها و آنتی‌ویروس‌ها ۱۵۸

۱۵۸	۱۴-۱- مقدمه
۱۵۹	۱۴-۲- چرا از فایروال استفاده می‌کنیم؟
۱۵۹	۱۴-۳- فایروال‌ها چگونه کار می‌کنند؟
۱۶۰	۱۴-۴- بسته‌های امنیتی اینترنت و آنتی‌ویروس‌ها
۱۶۰	۱۴-۴-۱- ESET Smart Security
۱۶۰	۱۴-۴-۲- ESET NOD32 Antivirus
۱۶۰	۱۴-۴-۳- ESET Endpoint Security
۱۶۰	۱۴-۴-۴- Norton 360
۱۶۲	۱۴-۴-۵- Norton Internet Security
۱۶۲	۱۴-۴-۶- Bitdefender Total Security
۱۶۳	۱۴-۴-۷- Symantec Endpoint Protection
۱۶۴	۱۴-۴-۸- Panda Global Protection
۱۶۴	۱۴-۴-۹- Kaspersky Internet Security
۱۶۴	۱۴-۴-۱۱- ZoneAlarm Pro
۱۶۵	۱۴-۴-۱۲- NSasoft BlueAuditor
۱۶۵	۱۴-۵- سؤالات تشریحی

فصل پانزدهم: نرم‌افزارهای محافظت از اطلاعات ۱۶۶

۱۶۶	۱۵-۱- مقدمه
۱۶۶	۱۵-۲- DISK DRIVE ADMINISTRATOR
۱۶۶	۱۵-۳- FOLDER LOCK
۱۶۷	۱۵-۴- FOLDER GUARD حفاظت از پوشه‌ها
۱۶۸	۱۵-۵- O&O SAFEERASE PROFESSIONAL
۱۶۸	۱۵-۶- TENORSHARE DATA WIPE
۱۶۸	۱۵-۷- ACTIVE KILLDISK PROFESSIONAL SUITE

۱۶۹	COPY PROTECT-۱۵-۸
۱۶۹	GILISOFT PRIVACY PROTECTOR-۱۵-۹
۱۶۹	SECRET DISK-۱۵-۱۰
۱۷۰	HDD LOW LEVEL FORMAT-۱۵-۱۱
۱۷۰	TRACKS ERASER-۱۵-۱۲
۱۷۰	POINTSTONE TOTAL PRIVACY-۱۵-۱۳
۱۷۱	۱۵-۱۴-سؤالات تشریحی

فصل شانزدهم: مراقبت از فرزندان در فضای مجازی .. ۱۷۲

۱۷۲	۱۶-۱-مقدمه
.....	۱۶-۲-نرم افزار های فیلترینگ خانگی و نظارت بر عملکرد کودکان و کاربران ۱۷۲
۱۷۲	۱۶-۲-۱- kidlogger
۱۷۳	۱۶-۲-۲- I net
۱۷۳	۱۶-۲-۳- MM Guardian Parental Control
۱۷۳	۱۶-۲-۴- AppLock یا قفل کننده اپلیکیشن
۱۷۳	۱۶-۲-۵- safeld Child Control
۱۷۵	۱۶-۲-۶- Kids PC Time Administrator
۱۷۶	۱۶-۳-افزونه های فایرفاکس
۱۷۶	۱۶-۴-سیم کارت های کودک و نوجوان
۱۷۷	۱۶-۵-سؤالات تشریحی
۱۷۷	مراجع:

مقدمه:

امروزه با گسترش روزافزون اینترنت، تجارت الکترونیک و بانکداری مبتنی بر اینترنت، سازمان‌ها بسیاری از سرویس‌های خود را از طریق اینترنت ارائه می‌دهند. همچنین تعداد فروشگاه‌های اینترنتی نیز به شدت افزایش یافته است. اما وجود آسیب‌پذیری در سیستم‌های کامپیوتری باعث شده است که کاربران اینترنت با تهدیدهای زیادی روبرو باشند. نفوذ گران از بد ابزارها و مکانیزم‌های تهاجمی مختلفی برای نفوذ، آسیب‌رسانی یا سرقت اطلاعات استفاده می‌کنند. لذا همه کاربران اینترنت باید دانش موردنیاز در زمینه حریم خصوصی و امنیت اینترنت را کسب نمایند. با توجه به نیاز کاربران اینترنت به منبعی کاربردی و جامع این کتاب را تألیف نمودم. در این کتاب سعی شده است که مطالب با زبانی ساده ارائه گردد که تمامی مخاطبین بتوانند از آن استفاده نمایند. همچنین این کتاب سرفصل‌های وزارت علوم، تحقیقات و فناوری برای درس حریم خصوصی و امنیت اینترنت را پوشش می‌دهد. در پایان هر فصل نیز تعدادی سؤال تشریحی و چهارگزینه‌ای تألیفی وجود دارد تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌های پیش رو آماده نمایند. از مخاطبین گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشالله در ویرایش‌های بعدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدیدنظر قرار گیرد. در پایان وظیفه خود می‌دانم از زحمات همکار گرامی، آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین مدیریت انتشارات ارسطو جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.

محمدعلی ترکمانی

اسفند ۹۶

فصل اول

مفاهیم و اصول امنیت اطلاعات

۱-۱- امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل دسترسی‌های غیرمجاز، استفاده، افشاء، اختلال، اصلاح، مطالعه، بازرسی، ضبط یا تخریب، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات. سایر ویژگی‌های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می‌تواند مشمول این حفاظت باشند.

۱-۱-۱- خصوصیات سیستم امن

- **محرمانگی:** اطلاعات باید تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد. به‌عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند.
- **صحت:** داده‌ها نباید به‌صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند.

- **دسترسی پذیری:** هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به عبارت دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های موردنظر را ارائه دهد.

۲-۱- اصطلاحات امنیتی

۱-۲-۱- آسیب پذیری^۲

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است.

۱-۲-۲- حمله^۳

حمله عبارت است از بهره‌برداری از آسیب‌پذیری‌های یک سیستم.

۱-۲-۳- تهدید^۴

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

۴-۲-۱- مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات واژه مخفف AAA مخفف سه کلمه ذیل است:

- **Authentication:** تائید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر

^۱Availability

^۲Vulnerability

^۳Attack

^۴Threat

- موجودیت (مانند یک شخص یا یک سرویس‌دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلال‌گر ثالث است که خود را به‌جای طرف واقعی جا زده است.
- Authorization: اجازه مکانیزی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احراز شده، مجوز انجام چه کارها و عملیاتی را در سیستم دارد.
- Accounting: حسابداری مکانیزی است که مشخص می‌کند فرد موردنظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به‌عنوان مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهم‌ترین مرحله Authentication است که تأمین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به‌عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیدا کند، ما می‌خواهیم بدانیم آیا همان فرد موردنظر است یا خیر، تأیید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به‌عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تأیید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر کارکنان دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تأیید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تأیید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین Authorization نیز با موفقیت انجام می‌شود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۵-۲-۱-عدم انکار (سندیت)^۱

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

۳-۱-نفوذ گر یا هکر^۲

هکر در لغت به معنی نفوذ گر است. هکرها به ۴ گروه نفوذ گران کلاه سفید، نفوذ گران کلاه سیاه، نفوذ گران کلاه خاکستری و نفوذ گران کلاه صورتی تقسیم‌بندی می‌شوند که در ادامه هر یک از این موارد شرح داده می‌شود.

۴-۱-دسته‌بندی کلی حملات

۴-۱-۱-دسته‌بندی از نظر تغییر دادن اطلاعات

حملات را می‌توان به دودسته کلی فعال^۳ و غیرفعال^۴ تقسیم نمود. در حمله غیرفعال مهاجم صرفاً پیام‌های ارسالی را بازبینی و استراق سمع می‌نماید. حمله فعال زمانی رخ می‌دهد که حمله‌کننده علاوه بر استراق سمع یا دریافت پیام، آن را تغییر داده و برای گیرنده ارسال نماید. از آنجاکه در حمله غیرفعال تغییری در داده‌ها رخ نمی‌دهد، تشخیص آن‌ها خیلی مشکل است.

^۱Non-repudiation

hacker

^۳Active Attack

^۴Passive Attack

۲-۴-۱- دسته‌بندی از نظر به چالش کشیدن اصول امنیت

- افشای پیام^۱ یا سرقت اطلاعات: خواندن یک ایمیل محرمانه یا شنود یک ارتباط تلفنی نمونه‌ای از این نوع حمله است. واضح است که این حمله عدم محرمانگی را فراهم می‌کند. (محرمانگی را به چالش می‌کشد).
- قطع ارتباط^۲: عدم دسترسی‌پذیری را فراهم می‌کند.
- تغییر اطلاعات^۳: صحت را به هم می‌زند.
- جعل اطلاعات^۴: عدم صحت اطلاعات و عدم اعتبار را فراهم می‌کند.
- انکار سرویس (رد درخواست)^۵: عدم دسترسی را فراهم می‌کند. سیستم را از سرویس خارج می‌کند.
- حمله تکرار^۶: به عمل دریافت داده در بین راه و ارسال مجدد آن باهدف دستیابی غیرمجاز، تکرار گویند. محرمانگی را به چالش می‌کشد.
- نقاب زنی یا بدل^۷: حمله‌ای است که در آن حمله‌کننده خودش را جای فرد دیگری جا می‌زند. درواقع حمله‌کننده هویت فرد دیگری را سرقت می‌نماید. این حمله نوعی جعل اطلاعات است و عدم صحت را به دنبال دارد. اما چون مهاجم موفق شده خودش را به جای قربانی جا بزند، در ادامه می‌تواند اطلاعات محرمانه قربانی را خوانده (عدم محرمانگی) و یا با ارسال بسته‌های زیاد قابلیت دسترسی را به چالش بکشد.

Release of Message

Interception

Interruption

Modification

Fabrication

Denial of Service

Reply

Masquerade

۵-۱- یک Hacker از چه راهی وارد سیستم می شود؟

برخی از روش‌هایی که ممکن است کامپیوتر شما از طریق آن هک یا ویروسی شود

- هکر می‌تواند در موارد ذیل IP کامپیوتر شما را به دست آورده و پورت‌های باز کامپیوتر شما را شناسایی نماید:
- زمانی که روی یک لینک کلیک می‌کنید.
- وارد یک سایت می‌شوید .
- با مسنجر در حال چت کردن هستید.
- هکر می‌تواند برای شما یک بدافزار را در قالب یک تصویر یا فایل اجرایی ایمیل کند و شما به محض باز کردن آن فایل هک می‌شوید.
- نهایتاً هکرها می‌توانند به حساب بانکی و پسوردهای شما دسترسی پیدا کند و یا اینکه خسارت‌های جبران‌ناپذیری به شما وارد کند

۶-۱- سوالات تشریحی

۱- اصطلاحات زیر را توضیح دهید؟

الف- Confidentiality ب- Reply Attack

۲- شش مورد از نیازمندی‌های امنیتی یک سیستم را نام‌برده و توضیح دهید.

۳- در هر یک از موارد زیر مشخص کنید کدامیک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟

الف- جواد تمرین‌های مریم را کپی کرد.

ب- علی سیستم مهسا را از کار انداخت.

ج- فریدون مقدار موجودی حساب زهرا را از ۱۰۰ دلار به ۱۰۰۰ دلار تغییر داد.

د- داریوش امضای خودش را به جای امضای رضا گذاشت.

ه- بهرام یک دامنه بانام Yahoo.com ثبت کرد و با استفاده از آن جلوی سرورس Yahoo Buy را گرفت.