



امنیت در

# تجارت الکترونیک

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری برای رشته‌های کامپیوتر و فناوری

اطلاعات

مؤلف:

دکتر محمد علی ترکمانی

سرشناسه	: ترکمانی، محمدعلی، ۱۳۵۴ -
عنوان و نام پدیدآور	: امنیت در تجارت الکترونیک [کتاب] / مولف محمدعلی ترکمانی.
مشخصات نشر	: مشهد: ارسطو، ۱۳۹۶.
مشخصات ظاهری	: ۲۳۱ ص.: مصور، جدول، نمودار.
شابک	: 978-600-432-180-8
وضعیت فهرست نویسی	: قیبا
یادداشت	: کتابنامه: ص. ۲۲۰ - ۲۲۱.
موضوع	: بازرگانی الکترونیکی -- تدابیر ایمنی
موضوع	: Electronic commerce -- Security measures
موضوع	: بازرگانی الکترونیکی -- الگوهای ریاضی
موضوع	: Electronic commerce -- Mathematical models
موضوع	: رمزگذاری داده‌ها
موضوع	: Data encryption (Computer science)
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: Computer networks -- Security measures
رده بندی کنگره	: HF۵۵۴۸/۳۲/ت۴۴الف۸ ۱۳۹۶
رده بندی دیویی	: ۶۵۸/۸۴
شماره کتابشناسی ملی	: ۴۸۱۷۷۷۶

نام کتاب : امنیت در تجارت الکترونیک

مولف : دکتر محمد علی ترکمانی

موضوع: امنیت شبکه های کامپیوتری.

ناشر : ارسطو ( با همکاری سامانه اطلاع رسانی چاپ و نشر ایران )

صفحه آرای، تنظیم و طرح جلد : علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : دوم - ۱۳۹۸

تعداد صفحات: ۲۳۸ ص

چاپ : مدیران

قیمت : ۴۶۰۰۰ تومان

تلفن های مرکز پخش : ۳۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۰۵۱ - ۰۹۱۷۷۱۶۴۹۴۰

وب سایت: [www.chaponashr.ir/Torkamani](http://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 ..... ۱۷

- ۱-۱- امنیت اطلاعات چیست؟ ..... ۱۷
- ۱-۱-۱- خصوصیات سیستم امن ..... ۱۸
- ۱-۲- اصطلاحات امنیتی ..... ۱۸
- ۱-۲-۱- آسیب پذیری ..... ۱۸
- ۱-۲-۲- حمله ..... ۱۹
- ۱-۲-۳- تهدید ..... ۱۹
- ۱-۲-۴- مفهوم AAA در امنیت اطلاعات ..... ۱۹
- ۱-۲-۵- عدم انکار (سندیت) ..... ۲۱
- ۱-۳- نفوذگر یا هکر ..... ۲۱
- ۱-۳-۱- نفوذگران کلاه سفید ..... ۲۱
- ۱-۳-۲- نفوذگران کلاه سیاه ..... ۲۱
- ۱-۳-۳- نفوذگران کلاه خاکستری ..... ۲۲
- ۱-۳-۴- نفوذگران کلاه صورتی ..... ۲۲
- ۱-۴- دسته بندی کلی حملات ..... ۲۲
- ۱-۴-۱- دسته بندی از نظر تغییر دادن اطلاعات ..... ۲۲
- ۱-۴-۲- دسته بندی از نظر به چالش کشیدن اصول امنیت ..... ۲۳
- ۱-۸- سئوالات تشریحی ..... ۲۴
- ۱-۵- سئوالات چهارگزینه ای ..... ۲۵
- پاسخنامه: ..... ۲۶

## فصل دوم: انواع حملات در شبکه‌های کامپیوتری..... ۲۷

- ۲-۱- حملات مبتنی بر پوشش پورت ..... ۲۷
- ۲-۲- SPOOFING ..... ۲۸
- ۲-۲-۱- IP Spoofing یا IP Forgery ..... ۲۸
- ۲-۲-۲- ARP Spoofing ..... ۲۸
- ۲-۳- مصرف پهنای باند (حملات DOS) ..... ۲۹
- ۲-۳-۱- SYN flood ..... ۳۰
- ۲-۳-۲- UDP flood ..... ۳۰
- ۲-۳-۳- ICMP flood ..... ۳۰
- ۲-۳-۴- حمله Mix ..... ۳۱
- ۲-۳-۵- Reset (RST) ..... ۳۱
- ۲-۳-۶- Land Attack ..... ۳۱
- ۲-۳-۷- Smurfing یا Smurf Attack ..... ۳۲
- ۲-۳-۸- حمله Fraggle ..... ۳۲
- ۲-۳-۹- حمله Lttierra ..... ۳۲
- ۲-۳-۱۰- حمله Ping of Death ..... ۳۲
- ۲-۳-۱۱- حمله Jolt ..... ۳۲
- ۲-۳-۱۲- حمله Teardrop ..... ۳۳
- ۲-۴- حمله تکرار یا استراق سمع یا شنود اطلاعات ..... ۳۳
- ۲-۵- مهندسی اجتماعی ..... ۳۴
- ۲-۶- درپشتی ..... ۳۴
- ۲-۷- حمله مرد میانی ..... ۳۴
- ۲-۸- سرقت TCP/IP ..... ۳۵

۳۶	..... DNS POISONING-۲-۹
۳۶	..... ۲-۱۰- ویروس‌ها و کرم‌ها
۳۷	..... ۲-۱۱- اسب تروا
۳۷	..... ۲-۱۲- جاسوس افزار
۳۸	..... ۲-۱۳- وب سایت‌های تقلبی (فیشینگ)
۳۸	..... ۲-۱۴- حمله با استفاده از نرم‌افزارهای ثبت‌کننده کلید
۳۸	..... ۲-۱۵- حملات جهت یافتن کلمات عبور
۳۹	..... ۲-۱۶- بهره برداری از نرم‌افزار
۳۹	..... ۲-۱۷- شمارمگیر جنگی
۴۰	..... ۲-۱۸- سرریز بافر
۴۰	..... ۲-۱۹- حملات تزریق SQL
۴۰	..... ۲-۲۰- هرزنامه
۴۱	..... ۲-۲۱- هرز تماس (SPIT) یا VOIP SPAM
۴۱	..... ۲-۲۲- EMAIL SPOOFING
۴۲	..... ۲-۲۳- حمله XSS
۴۲	..... ۲-۲۴- BOTNET
۴۴	..... ۲-۲۴-۱- حمله DDOS با استفاده از BOTNET
۴۵	..... ۲-۲۵- سئوالات تشریحی
۴۶	..... ۲-۲۶- سئوالات چهارگزینه‌ای
۵۰	..... پاسخنامه:

## فصل سوم: کاربردهای رمزنگاری در امنیت شبکه ..... ۵۱

۵۱	..... ۳-۱- مفاهیم و اصطلاحات رمزنگاری
۵۲	..... ۳-۲- سیستم‌های رمزنگاری
۵۳	..... ۳-۲-۱- رمزنگاری متقارن
۵۳	..... ۳-۲-۲- رمزنگاری نامتقارن
۵۳	..... ۳-۳- تکنیک‌های رمزگذاری

۵۴	۳-۳-۱-رمزنگاری سزار
۵۵	۳-۳-۲-رمزنگاری ورنام
۵۶	۳-۳-۳-ترکیب جایگشتی و جایگزینی
۵۶	۳-۳-۴-تکنیک‌های رمزنگاری متقارن
۵۶	۳-۳-۴-۱-رمز رشته‌ای یا دنباله‌ای
۵۷	۳-۳-۴-۲-رمز بلاکی
۵۷	۳-۴-رمزنگاری DES
۵۹	۳-۵-الگوریتم 2DES
۵۹	۳-۶-الگوریتم 3DES
۶۰	۳-۷-امنیت DES
۶۱	۳-۸-رمزنگاری با کلید عمومی
۶۲	۳-۹-الگوریتم RSA
۶۲	۳-۹-۱-انتخاب کلید
۶۳	۳-۹-۲-روش رمزگذاری و رمزگشایی
۶۴	۳-۱۰-تبادل کلید نشست با استفاده از رمزنگاری RSA
۶۶	۳-۱۰-۱-پروتکل توزیع کلید متقارن با استفاده از کلید عمومی
۶۷	۳-۱۱-صحت پیام با استفاده از MAC
۶۹	۳-۱۲-الگوریتم‌های MAC
۷۱	۳-۱۳-امضای دیجیتال
۷۲	۳-۱۴-گواهینامه
۷۳	۳-۱۵-سئوالات تشریحی
۷۴	۳-۱۶-سئوالات چهارگزینه‌ای
۷۹	پاسخنامه:

## فصل چهارم: امنیت پست الکترونیکی ..... ۸۱

۸۱	۴-۱-تامین محرمانگی، تایید هویت و صحت پیام در ایمیل امن
----	--

۸۱	۴-۱-۱-سیستم اول
۸۲	۴-۱-۲-سیستم دوم
۸۳	۴-۱-۳-سیستم سوم
۸۴	۴-۲-استاندارد PGP
۸۵	۴-۳-پست الکترونیکی چند منظوره امن S/MIME
۸۷	۴-۴-سئوالات تشریحی
۸۷	۴-۵-سئوالات چهارگزینه‌ای
۸۸	پاسخنامه:

## ۸۹ فصل پنجم: امنیت IP

۸۹	۵-۱-مقدمه
۸۹	۵-۲-معماری IPSEC
۹۰	۵-۳-سرویس‌های IPSEC
۹۰	۵-۴-مدهای کاری IPSEC
۹۲	۵-۵-مزایای IPSEC VPN
۹۳	۵-۶-پروتکل‌های IPSEC
۹۴	۵-۶-۱-پروتکل AH
۹۴	۵-۶-۲-پروتکل ESP
۹۵	۵-۷-ترکیب مد و پروتکل IPSEC
۹۷	۵-۸-مجمع امنیتی (SA) و سیاست امنیتی (SP)
۹۸	۵-۹-پروتکل تبادل کلید در اینترنت (IKE)
۹۹	۵-۱۰-سئوالات تشریحی
۹۹	۵-۱۱-سئوالات چهارگزینه‌ای
۱۰۲	پاسخنامه:

## ۱۰۳ فصل ششم: امنیت وب

۱۰۳	۶-۱-مقدمه
-----	-----------

- ۱۰۴ ..... ۶-۲- محل قرار گرفتن SSL
- ۱۰۴ ..... ۶-۳- پروتکل SSL
- ۱۰۵ ..... ۶-۴- پروتکل TLS
- ۱۰۵ ..... ۶-۵- نحوه عملکرد SSL
- ۱۰۸ ..... ۶-۵-۱- صحت پیام SSL در هم ساز
- ۱۰۸ ..... ۶-۶- اثبات هویت سرویس دهنده
- ۱۰۹ ..... ۶-۷- حملات
- ۱۱۰ ..... ۶-۸- نتیجه گیری
- ۱۱۰ ..... ۶-۹- سئوالات تشریحی
- ۱۱۰ ..... ۶-۱۰- سئوالات چهارگزینه‌ای
- ۱۱۲ ..... پاسخنامه:

## فصل هفتم: امنیت تجارت الکترونیک ..... ۱۱۳

- ۱۱۳ ..... ۷-۱- مقدمه
- ۱۱۳ ..... ۷-۲- تراکنش الکترونیکی امن (SET)
- ۱۱۶ ..... ۷-۲-۱- مراحل تراکنش مالی توسط SET
- ۱۱۷ ..... ۷-۲-۲- پردازش پرداخت در SET
- ۱۱۷ ..... ۷-۲-۲-۱- درخواست خرید
- ۱۱۸ ..... ۷-۲-۲-۲- اجازه پرداخت
- ۱۲۱ ..... ۷-۲-۲-۳- اخذ پرداختی
- ۱۲۱ ..... ۷-۳- تجارت الکترونیک امن
- ۱۲۲ ..... ۷-۳-۱- مراجع صدور گواهی
- ۱۲۲ ..... ۷-۳-۲- کارت‌های هوشمند
- ۱۲۳ ..... ۷-۴- اعتماد به وب
- ۱۲۳ ..... ۷-۵- پول الکترونیکی
- ۱۲۴ ..... ۷-۶- امنیت مرورگر وب
- ۱۲۵ ..... ۷-۷- امنیت اسکریپت



- ۱۲۶ ..... ۷-۸-امنیت پروتکل وب
- ۱۲۷ ..... ۷-۹-سئوالات چهارگزینه‌ای
- ۱۲۷ ..... ۷-۱۰-سئوالات چهارگزینه‌ای
- پاسخنامه: ۱۲۹

## فصل هشتم: فایروال ..... ۱۳۱

- ۱۳۱ ..... ۸-۱-مقدمه
- ۱۳۲ ..... ۸-۲-چرا از فایروال استفاده می‌کنیم؟
- ۱۳۲ ..... ۸-۳-نواحی امنیتی
- ۱۳۴ ..... ۸-۴-فایروال‌ها چگونه کار می‌کنند؟
- ۱۳۴ ..... ۸-۵-ویژگی‌های فایروال
- ۱۳۵ ..... ۸-۶-محدودیت‌های فایروال
- ۱۳۶ ..... ۸-۷-مشخصات فایروال قوی
- ۱۳۷ ..... ۸-۸-محل قرار گرفتن فایروال
- ۱۳۸ ..... ۸-۹-انواع فایروال
- ۱۳۹ ..... ۸-۹-۱-مسیریاب فیلتر بسته
- ۱۴۰ ..... ۸-۹-۲-دروازه سطح کاربرد
- ۱۴۳ ..... ۸-۹-۳-دروازه سطح مدار
- ۱۴۳ ..... ۸-۱۰-فایروال‌های شخصی
- ۱۴۴ ..... ۸-۱۱-امکانات فایروال برای مدیران شبکه
- ۱۴۴ ..... ۸-۱۲-سئوالات تشریحی
- ۱۴۵ ..... ۸-۱۳-سئوالات چهارگزینه‌ای
- ۱۴۶ ..... پاسخنامه:

## فصل نهم: رویدادنگاری و تشخیص نفوذگران ..... ۱۴۷

- ۱۴۷ ..... ۹-۱-مقدمه
- ۱۴۸ ..... ۹-۲-قابلیت‌های رویدادنگاری

- ۹-۳-۹-سیستم‌های تشخیص نفوذ (IDS) ..... ۱۴۹
- ۹-۳-۱-روش‌های مورد استفاده توسط سیستم تشخیص نفوذ ..... ۱۵۰
- ۹-۳-۲-تقسیم بندی IDS ها بر اساس منابع اطلاعاتی ..... ۱۵۱
- ۹-۳-۲-۱-N-IDS ..... ۱۵۱
- ۹-۳-۲-۱-۱-مزایای N-IDS ..... ۱۵۱
- ۹-۳-۲-۱-۲-معایب N-IDS ..... ۱۵۲
- ۹-۳-۲-۲-H-IDS ..... ۱۵۲
- ۹-۳-۲-۲-۱-مزایای H-IDS ..... ۱۵۲
- ۹-۳-۲-۲-۲-معایب H-IDS ..... ۱۵۳
- ۹-۳-۲-۳-A-IDS ..... ۱۵۳
- ۹-۳-۲-۳-۱-مزایای A-IDS ..... ۱۵۳
- ۹-۳-۲-۳-۲-معایب A-IDS ..... ۱۵۳
- ۹-۳-۳-آنالیز IDS ..... ۱۵۴
- ۹-۳-۳-۱-تشخیص سوء استفاده ..... ۱۵۴
- ۹-۳-۳-۱-۱-مزایای تشخیص سوء استفاده ..... ۱۵۴
- ۹-۳-۳-۱-۲-معایب تشخیص سوء استفاده ..... ۱۵۴
- ۹-۳-۳-۲-تشخیص بی قاعدگی ..... ۱۵۴
- ۹-۳-۳-۲-۱-تکنیک‌های استفاده شده در تشخیص بی قاعدگی ..... ۱۵۵
- ۹-۳-۳-۲-۲-مزایای تشخیص بی قاعدگی ..... ۱۵۵
- ۹-۳-۳-۲-۳-معایب تشخیص بی قاعدگی ..... ۱۵۵
- ۹-۳-۴-پاسخ‌های IDS ..... ۱۵۶
- ۹-۳-۴-۱-پاسخ‌های فعال ..... ۱۵۶
- ۹-۳-۴-۱-۱-جمع‌آوری اطلاعات اضافی ..... ۱۵۶
- ۹-۳-۴-۱-۲-تغییر محیط ..... ۱۵۶
- ۹-۳-۴-۱-۳-عمل در برابر کسانی که بدون اجازه وارد می‌شوند ..... ۱۵۶
- ۹-۳-۴-۲-پاسخ‌های غیر فعال ..... ۱۵۷
- ۹-۴-IDS های تشخیص نفوذ روی یک ماشین ..... ۱۵۷
- ۹-۴-۱-سیستم خبره تشخیص نفوذ (IDES) ..... ۱۵۷

۱۵۸	MIDAS-۹-۴-۲
۱۶۰	Haystack-۹-۴-۳
۱۶۱	۹-۵-برخی از IDS های تشخیص نفوذ شبکه
۱۶۲	۹-۵-۱-سیستم دیدبانی امنیت شبکه (NSM)
۱۶۳	۹-۵-۲-سیستم تشخیص نفوذ توزیع شده (DIDS)
۱۶۴	۹-۵-۳-سیستم NADIR
۱۶۴	۹-۵-۴-سیستم CSM
۱۶۵	۹-۶-نظارت و قانون
۱۶۵	۹-۷-سئوالات تشریحی
۱۶۶	۹-۸-سئوالات چهارگزینه‌ای
۱۶۸	پاسخنامه:

## فصل دهم: سیستم جلوگیری از نفوذ ۱۷۱

۱۷۱	۱۰-۱-تعریف
۱۷۱	۱۰-۲-چرا دیواره آتش به تنهایی کافی نیست؟
۱۷۲	۱۰-۳-وظایف IPS
۱۷۲	۱۰-۴-روش کار IPS
۱۷۳	۱۰-۵-انواع IPS
۱۷۳	۱۰-۶-انواع IPS های شرکت سیسکو
۱۷۴	۱۰-۷-معماری IPS
۱۷۴	۱۰-۷-۱-محل نصب
۱۷۴	۱۰-۷-۲-پایگاه داده
۱۷۴	۱۰-۸-پروتکل های IPS
۱۷۴	۱۰-۹-روش های IPS در تحلیل ترافیک
۱۷۶	۱۰-۱۰-روش های دور زدن IPS و دفاع در مقابل آنها
۱۷۷	۱۰-۱۱-تفاوت IDS و IPS

- ۱۷۸ ..... ۱۰-۱۲-سئوالات تشریحی
- ۱۷۹ ..... ۱۰-۱۳-سئوالات چهارگزینه ای
- ۱۸۰ ..... پاسخنامه

## فصل یازدهم: HONEY POT ..... ۱۸۱

- ۱۸۱ ..... ۱۱-۱-مقدمه
- ۱۸۱ ..... ۱۱-۲-اصول کاری هانی پات ها
- ۱۸۲ ..... ۱۱-۳-نقاط ضعف و معایب HONEY POT ها
- ۱۸۳ ..... ۱۱-۴-تعریف هانی پات
- ۱۸۳ ..... ۱۱-۵-انواع HONEY POTS
- ۱۸۴ ..... ۱۱-۶-معماری و ساختمان HONEYPOT
- ۱۸۴ ..... ۱۱-۷-مزایای هانی پات ها
- ۱۸۵ ..... ۱۱-۸-دسته بندی هانی پات ها از نظر واکنش
- ۱۸۵ ..... ۱۱-۸-۱- هانی پات های کم واکنش
- ۱۸۶ ..... ۱۱-۸-۲- هانی پات های پر واکنش
- ۱۸۷ ..... ۱۱-۸-۳- هانی پات های با واکنش یا تعامل متوسط
- ۱۸۸ ..... ۱۱-۹- هانی پات ها چگونه به سازمانها کمک می کنند
- ۱۹۰ ..... ۱۱-۱۰-مقایسه کاربرد فایروال، IDS و هانی پات
- ۱۹۱ ..... ۱۱-۱۱-سئوالات تشریحی
- ۱۹۱ ..... ۱۱-۱۲-سئوالات چهارگزینه ای
- ۱۹۳ ..... پاسخنامه:

## فصل دوازدهم: ملاحظات امنیتی کاربران در تجارت

### الکترونیک ..... ۱۹۵

- ۱۹۵ ..... ۱۲-۱-مقدمه
- ۱۹۶ ..... ۱۲-۲-نکات خرید آنلاین

- ۲۰۰ ..... ۱۲-۳- بررسی فروشگاه
- ۲۰۲ ..... ۱۲-۴- راه‌های مقابله با سرقت حساب
- ۲۰۴ ..... ۱۲-۵- مرورگر خود را تنظیم کنید
- ۲۰۷ ..... ۱۲-۶- توصیه‌هایی برای امنیت و جلوگیری از سرقت هویت
- ۲۱۰ ..... ۱۲-۷- سوالات تشریحی
- ۲۱۱ ..... ۱۲-۸- سوالات چهارگزینه‌ای
- ۲۱۲ ..... پاسخنامه

## فصل سیزدهم: مهندسی نرم افزار امن و مقایسه آن با

### امنیت شبکه ..... ۲۱۳

- ۲۱۳ ..... ۱۳-۱- مقدمه
- ۲۱۳ ..... ۱۳-۲- مسئله امنیت
- ۲۱۴ ..... ۱۳-۳- مهندسی نرم افزار امن
- ۲۱۵ ..... ۱۳-۴- امنیت برنامه‌های کاربردی در مقایسه امنیت نرم افزار
- ۲۱۶ ..... ۱۳-۴-۱- ابزارهای آزمون امنیت برنامه کاربردی
- ۲۱۷ ..... ۱۳-۵- مشکلات یا ابعاد سه‌گانه مسئله امنیت نرم افزار
- ۲۲۰ ..... ۱۳-۶- حل مسئله امنیت نرم افزار
- ۲۲۰ ..... ۱۳-۷- مشکلات امنیتی در نرم افزار
- ۲۲۰ ..... ۱۳-۷-۱- نقص (Defect)
- ۲۲۰ ..... ۱۳-۷-۱-۱- اشکال یا خطا (Bug)
- ۲۲۱ ..... ۱۳-۷-۱-۲- عیب (Flaw)
- ۲۲۲ ..... ۱۳-۷-۲- ریسک
- ۲۲۲ ..... ۱۳-۷-۳- محدوده نواقص (defects)
- ۲۲۳ ..... ۱۳-۸- سوالات تشریحی

## فصل چهاردهم: چرخه توسعه امنیت (SDL) مایکروسافت ۲۲۵

۲۲۵	.....	۱۴-۱-مقدمه
۲۲۶	.....	۱۴-۲-اصول راهنما برای SD3+C
۲۲۹	.....	۱۴-۳-اصول راهنما برای PD3+C
۲۳۰	.....	۱۴-۴-مرور چرخه مایکروسافت
۲۳۳	.....	۱۴-۵-مقایسه SDL با چرخه مک گرا؟
۲۳۳	.....	۱۴-۶-برخی از ابزارهای ارائه شده SDL
۲۳۳	.....	۱۴-۶-۱-ابزار Attack Surface Analyzer
۲۳۴	.....	۱۴-۶-۲-ابزار SDL Threat Modeling Tool
۲۳۴	.....	۱۴-۶-۳-ابزار فاز تست پایه فایل MiniFuzz
۲۳۴	.....	۱۴-۶-۴-ابزار فاز تست Regex
۲۳۶	.....	۱۴-۷-سوالات تشریحی
۲۳۷	.....	مراجع:

## مقدمه:

امروزه کسب و کارهای مبتنی بر وب و تجارت الکترونیکی با تهدیدهای زیادی روبرو هستند. نفوذگران از بد ابزارها و مکانیزم‌های تهاجمی مختلفی برای نفوذ، آسیب رسانی یا سرقت اطلاعات استفاده می‌کنند. لذا متخصصان تجارت الکترونیک باید دانش مورد نیاز در زمینه امنیت شبکه را کسب نمایند. به همین علت درس امنیت در تجارت الکترونیکی در برنامه درسی رشته‌های مهندسی IT گرایش تجارت الکترونیک قرار گرفته است. علیرغم اینکه این درس یکی از دروس اصلی این رشته‌ها محسوب می‌شود، اما مرجع مناسبی برای آن وجود ندارد. حجم مراجع معرفی شده برای این درس بسیار زیاد است و تدریس این مطالب در یک نیم سال تحصیلی دشوار است. در این کتاب سعی شده است که مطالب با زبانی ساده ارائه گردد. در انتهای هر فصل مجموعه سئوالات تشریحی و چهارگزینه‌ای به همراه حل آنها آورده شده است تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده نمایند. از آنجا که تاکید این کتاب بر روی اصول و مفاهیم رمزنگاری نیست، مباحث مربوط به رمزنگاری بسیار مختصر و مفید و در حدی که خوانندگان برای فهم مباحث مربوط به امنیت شبکه و بررسی کاربردهای رمزنگاری در امنیت شبکه به آن نیاز دارند، بیان شده است. علاقه مندان به مباحث رمزنگاری و دانشجویان درس رمزنگاری می‌توانند برای مطالعه مباحث مقدماتی تا پیشرفته این علم به کتاب رمزنگاری از همین مولف مراجعه نمایند. امید است این اثر مورد توجه همکاران و دانشجویان گرامی قرار گیرد. از اساتید و دانشجویان گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل [m.a.torkamani@gmail.com](mailto:m.a.torkamani@gmail.com) با اینجانب در میان بگذارند تا انشالله در ویرایش‌های بعدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدید نظر 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 تشکر و قدردانی نمایم.

محمد علی ترکمانی

پاییز ۱۳۹۴





# فصل اول

## مفاهیم و اصول امنیت اطلاعات

### ۱-۱- امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل دسترسی های غیر مجاز، استفاده، افشاء، اختلال، اصلاح، مطالعه، بازرسی، ضبط یا تخریب، همچنین علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس پذیری اطلاعات. سایر ویژگی های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می تواند مشمول این حفاظت باشند.

یک سیستم درست سیستمی است که اگر ورودی خوب و درست به آن داده شود خروجی درست به ما می دهد.

اما سیستم امن سیستمی است که اگر حمله کننده به آن ورودی بد بدهد، سیستم خراب نشود. به طور کلی طراحی امکانات بیشتر در یک سیستم از نظر امنیت اطلاعات در دسر ساز است. زیرا باید کنترل روی ورودی ها بیشتر باشد.

در امنیت اطلاعات به دنبال ساده بودن و مینیمم بودن سیستم هستیم. در صورتی که در یک سیستم خوب همیشه به دنبال امکانات بیشتر هستیم. در کل هدف ما این است که یک سیستمی داشته باشیم که هم درست و هم امن باشد.

## ۱-۱-۱- خصوصیات سیستم امن

- **محرمانگی:** اطلاعات باید تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد. به عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند.
- **صحت:** داده‌ها نباید به صورت 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 مورد نظر را ارائه دهد.

## ۱-۲- اصطلاحات امنیتی

### ۱-۲-۱- آسیب پذیری<sup>۴</sup>

- آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند در یکی از موارد زیر باشد:
- طراحی سیستم: در این حالت پروتکل یا الگوریتم ایراد دارد. به عنوان مثال طراحی پروتکل TCP/IP درست انجام نشده و بسته‌های TCP/IP به صورت متن ساده (رمز نشده) هستند. این یک ایراد طراحی است که یک آسیب‌پذیری را برای این پروتکل به وجود آورده است و باعث شده است که اگر یک نفر گوش کند، بتواند محتوای بسته‌های IP را ببیند.

---

√Confidentiality

√Integrity

√Availability

√Vulnerability

ΔClear Text

- پیاده‌سازی: به عنوان مثال فرض کنید در برنامه نویسی یک پروتکل، مواردی ( نظیر اصول یا استانداردهای کدنویسی امن) را رعایت نکرده‌ایم، یا اشتباهاتی داریم. علاوه بر
- این، در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است. برای رفع این مورد باید از نسخه‌های جدیدتر این زبان و یا زبان جاوا استفاده کرد.
- عملیات سیستم ایراد دارد: فرآیندها درست انجام نمی‌شود. به عنوان مثال یک فرم پر شده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آنرا ببیند.

### ۲-۲-۱-حمله<sup>۱</sup>

حمله عبارتست از بهره برداری از آسیب‌پذیری‌های یک سیستم.

### ۳-۲-۱-تهدید<sup>۲</sup>

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 به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- **Authentication:** تأیید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت (مانند یک شخص یا یک سرویس دهنده بانکی) بررسی می‌کند که آیا

---

<sup>۱</sup>Attack

<sup>۲</sup>Threat

شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلاص‌گر ثالث است که خود را به جای 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 مورد نظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به عنوان مثال اعتبار کافی دارد یا خیر.

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

به عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیدا کند، ما می‌خواهیم بدانیم آیا همان فرد مورد نظر است یا خیر، تایید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تایید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر پرسنل دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تایید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد. در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تایید 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)<sup>۱</sup>

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-نفوذگر یا هکر<sup>۲</sup>

هکر در لغت به معنی نفوذگر است. هکرها به ۴ گروه نفوذگران کلاه سفید، نفوذگران کلاه سیاه، نفوذگران کلاه خاکستری و نفوذگران کلاه صورتی تقسیم بندی می‌شوند که در ادامه هر یک از این موارد شرح داده می‌شود.

#### ۱-۳-۱- نفوذگران کلاه سفید<sup>۳</sup>

هدف این گونه از هکرها نشان دادن ضعف سیستم‌های امنیتی و شبکه‌های کامپیوتری می‌باشد. این گروه به نام هکرها خوب معروف هستند. این دسته نه تنها به سیستم آسیب نمی‌رسانند، بلکه در تحکیم دیواره حفاظتی شبکه‌ها نقش اساسی دارند. کلاه سفیدها دارای خلاقیت عجیبی هستند و هر بار با روش جدیدی از دیواره امنیتی عبور می‌کنند.

#### ۲-۳-۱-نفوذگران کلاه سیاه<sup>۴</sup>

نام دیگر این گروه Cracker است. کراکرها خرابکارانه ترین نوع هکرها هستند. این گروه به طور کاملا پنهانی اقدام به عملیات خرابکارانه می‌کنند. کلاه سیاه‌ها اولین چیزی که به فکرشان

---

<sup>۱</sup>Non-repudiation

<sup>۲</sup>hacker

<sup>۳</sup>White hat Hacker Group

<sup>۴</sup>Black Hat Hacker Group

می‌رسد نفوذ به سیستم قربانی است. کلاه سیاه‌ها می‌توانند با ارسال ویروسی که خودشان تهیه نموده‌اند، کنترل سیستم قربانی را در دست بگیرند. همیشه هویت اصلی کلاه سیاه‌ها پنهان است.

### ۳-۳-۱- نفوذگران کلاه خاکستری<sup>۱</sup>

نام دیگر این گروه Whacker است. هدف اصلی واگرها استفاده از اطلاعات سایر کامپیوترها می‌باشد و صدمه‌ای به کامپیوترها وارد نمی‌کنند. این گروه کدهای ورودی به سیستم‌های امنیتی را پیدا کرده و به داخل آن نفوذ می‌کنند، اما سرقت و خرابکاری جزء کارهای کلاه خاکستری‌ها نیست. آنها معمولا اطلاعات فنی را در اختیار عموم مردم قرار می‌دهند.

### ۳-۳-۲- نفوذگران کلاه صورتی<sup>۲</sup>

نام دیگر این گروه Booter می‌باشد. بوترها افراد بی سواد هستند که فقط قادرند در سیستم‌ها اختلال به وجود آورند و یا مزاحم سایر کاربران در اتاق‌های چت شوند. کلاه صورتی‌ها اغلب از نرم‌افزارهای دیگران استفاده می‌کنند و خود سواد برنامه‌نویسی ندارند. البته در بعضی مواقع همین هکرهای کم سواد می‌توانند خطرهای جدی برای امنیت باشند.

### ۴-۱- دسته‌بندی کلی حملات

#### ۴-۱-۱- دسته بندی از نظر تغییر دادن اطلاعات

حملات را می‌توان به دو دسته کلی فعال<sup>۳</sup> و غیر فعال<sup>۴</sup> تقسیم نمود. در حمله غیر فعال مهاجم صرفاً پیام‌های ارسالی را بازبینی و استراق سمع می‌نماید. حمله فعال زمانی رخ می‌دهد

---

<sup>۱</sup>Gray Hat Hacker Group

<sup>۲</sup>Pink Hat Hacker Group

<sup>۳</sup>Active Attack

<sup>۴</sup>Passive Attack

که حمله کننده علاوه بر استراق سمع یا دریافت پیام، آنرا تغییر داده و برای گیرنده ارسال نماید. از آنجا که در حمله غیر فعال تغییری در داده‌ها رخ نمی‌دهد، تشخیص آنها خیلی مشکل است.

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

- افشای پیام<sup>۱</sup> 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<sup>۲</sup>: عدم دسترسی پذیری را فراهم می‌کند.
- تغییر اطلاعات<sup>۳</sup>: صحت را به هم می‌زند.
- جعل اطلاعات<sup>۴</sup>: عدم صحت اطلاعات و عدم اعتبار را فراهم می‌کند.
- انکار سرویس (رد درخواست)<sup>۵</sup>: عدم دسترسی را فراهم می‌کند. سیستم را از سرویس خارج می‌کند.
- حمله تکرار<sup>۶</sup>: به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند. محرمانگی را به چالش می‌کشد.
- نقاب‌زنی یا بدل<sup>۷</sup>: حمله‌ای است که در آن حمله کننده خودش را جای فرد دیگری جا می‌زند. در واقع حمله کننده 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

---

Release of Message

Interception

Interruption

Modification

Fabrication

Denial of Service

Reply

Masquerade