

۱۶۳۵۲۴۱

مبانی امنیت سیستم‌های کامپیوتری

مؤلف: علی امیری، حسن مختاری



**NAGHOOS
PUBLICATION**

سرشناسه

عنوان و نام پدیدآور

مشخصات نشر

مشخصات ظاهری

شابک

وضعیت فهرست نویسی : فیا

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

شناسه امروزه

رده بندی کنگره

رده بندی دیویی

شماره کتابشناسی

امیری، علی، ۱۳۶۶ -

مبانی امنیت سیستم های کامپیوتری / مولفین: علی امیری، حسن مختاری

تهران: انتشارات ناقوس، ۱۳۹۵.

۳۱۰ص: مصور، جدول.

۹-۸۸۵-۳۷۷-۹۶۴-۹۷۸ بها: ۲۲۰۰۰۰ ریال

شبکه های کامپیوتری - تدابیر ایمنی

Computer networks—Security measures

کامپیوترها - ایمنی اطلاعات

Computer security

شبکه های کامپیوتری - کنترل دستیابی

Computer networks—Access control

مختاری، حسن، ۱۳۵۶ -

TK۵۱۰/۵۹/الف۸۱۲/۵

۸/۱۰۰

۲۲۱۱



برای خرید به آدرس زیر مراجعه کنید:

www.naghpospress.ir

انتشارات ناقوس

نام کتاب	مبانی امنیت سیستم های کامپیوتری
ناشر	انتشارات ناقوس
مولفین	علی امیری، حسن مختاری
چاپ اول	۱۳۹۵
تیراژ	۲۰۰ جلد
چاپ و صحافی	نارنجستان
ناظر چاپ	یاسمن تجملی محدث
سرپرست صفحه آرا	ربابه موسوی خواه
قیمت	۲۲۰۰۰۰ ریال
شابک	۹-۸۸۵-۳۷۷-۹۶۴-۹۷۸
ISBN	978-964-377-885-9

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۳

«این کتاب چاپ اول از دستگاه چاپ دیجیتال استفاده شده است»

کلیه حقوق این کتاب محفوظ است.

تکثیر تمامی یا قسمتی از این اثر به صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناقوس

۱- خیابان انقلاب-خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن بست حقیقت- پلاک ۴

تلفن و فاکس: ۶۶۳۷۸۹۵۷-۶۶۳۷۸۹۵۸

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان: ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

فهرست مطالب

۱۹	 مقدمه
۲۱	 فصل ۱: تعاریف پایه
۲۱	 ۱، ۱- امنیت چیست؟
۲۲	 ۲، ۱- خواص امنیتی یا سرویس‌های امنیتی
۲۲	 ۱، ۲، ۱- محرمانگی
۲۳	 ۲، ۱- پایداری
۲۳	 ۱، ۲، ۱- دسترسی پذیری
۲۴	 ۴، ۲، ۱- عدم انکار
۲۴	 ۵، ۲، ۱- گمنامی
۲۴	 ۶، ۲، ۱- عدالت
۲۵	 ۷، ۲، ۱- اعتماد
۲۶	 ۳، ۱- سیاست‌های امنیتی
۲۶	 ۴، ۱- مکانیزم‌های امنیتی
۲۶	 ۱، ۴، ۱- رمزنگاری
۲۷	 ۲، ۴، ۱- سیستم تشخیص نفوذ
۲۷	 ۳، ۴، ۱- آنتی ویروس
۲۷	 ۴، ۴، ۱- هویت شناسی
۲۷	 ۵، ۴، ۱- کنترل دسترسی
۲۷	 ۶، ۴، ۱- امنیت فیزیکی
۲۷	 ۷، ۴، ۱- آموزش
۲۸	 ۸، ۴، ۱- روال‌های سازمانی
۲۸	 ۹، ۴، ۱- حسابرسی
۲۸	 ۱۰، ۴، ۱- پوشیده نگاری
۲۸	 ۱۱، ۴، ۱- فریب
۳۰	 ۵، ۱- نا امنی
۳۰	 ۱، ۵، ۱- آسیب پذیری
۳۰	 ۲، ۵، ۱- تهدید

۳۱	 حمله ۳،۵،۱
۳۱	 ریسک ۴،۵،۱
۳۱	 دارایی ۵،۵،۱

فصل ۲: آسیب پذیری سیستم های کامپیوتری ۳۵

۳۵	 ۱،۲- آسیب پذیری چیست؟
۳۶	 ۱،۱،۲- خطا
۳۷	 ۲،۱،۲- رخنه
۳۷	 ۳،۱،۲- آسیب پذیری
۳۸	 ۴،۱،۲- سوء استفاده
۳۸	 ۲،۲- انواع آسیب پذیری
۳۸	 ۱،۲،۲- نقص کتبی دسترسی
۳۸	 ۲،۲،۲- نقص در مدیریت پیرامون
۳۹	 ۳،۲،۲- حفاظت ناقص از داده ها
۳۹	 ۱،۳،۲،۲- ذخیره سازی ناامن داده ها
۴۰	 ۲،۳،۲،۲- انتقال ناامن داده ها
۴۰	 ۴،۲،۲- اعتبار سنجی ناقص ورودی ها
۴۱	 ۱،۴،۲،۲- اعتبار سنجی ناقص ورودی های کاربر
۴۱	 ۲،۴،۲،۲- اعتبار سنجی ناقص ورودی های شده ای
۴۱	 ۵،۲،۲- شرط مسابقه
۴۲	 ۶،۲،۲- منع سرویس برنامه کاربردی
۴۲	 ۷،۲،۲- منع سرویس قفل
۴۳	 ۸،۲،۲- سرریز بافر
۴۴	 ۹،۲،۲- سرریز کپه
۴۴	 ۱۰،۲،۲- تزریق
۴۴	 ۱،۱۰،۲،۲- تزریق SQL
۴۵	 ۲،۱۰،۲،۲- تزریق HTML
۴۶	 ۳،۱۰،۲،۲- تزریق دستور
۴۶	 ۴،۱۰،۲،۲- تزریق XSS
۴۷	 ۱۱،۲،۲- واکنش نادرست به خطا
۴۹	 ۱۲،۲،۲- نقص در نظارت
۴۹	 ۱،۱۲،۲،۲- رویدادنگاری ضعیف
۴۹	 ۲،۱۲،۲،۲- تشخیص ضعیف:

- ۵۰..... ۱۳،۲،۲- نقص در پنهان سازی (رمزنگاری) اطلاعات
- ۵۰..... ۱،۱۳،۲،۲- نقص در الگوریتم های رمزنگاری
- ۵۰..... ۲،۱۳،۲،۲- نقص در مدیریت کلید
- ۵۰..... ۱۴،۲،۲- هویت سنجی ضعیف
- ۵۱..... ۱،۱۴،۲،۲- نقص در هویت سنجی کاربر
- ۵۲..... ۲،۱۴،۲،۲- نقص در مدیریت نشست
- ۵۲..... ۳،۲- تشخیص آسیب پذیری
- ۵۳..... ۱،۳،۲- تفاوت میان تشخیص آسیب پذیری و تست نفوذ
- ۵۵..... ۲،۳،۲- ابزار های تشخیص آسیب پذیری
- ۵۷..... ۱،۲،۲- کاوشگر امنیت Nessus
- ۵۷..... Axent Technologies NetRecon-۲،۱،۳،۲
- ۵۸..... ISS Internet Scanner-۳،۲،۳،۲
- ۵۸..... Nmap(Network Mapper)-۴،۲،۳،۲
- ۵۹..... ۴،۲- سوالات فصل دوم
- ۶۱..... فصل ۳: استفاده از آسیب پذیری در انجام حمله
- ۶۱..... ۱،۳- مقدمه
- ۶۴..... ۱،۱،۳- ویروس ها
- ۶۴..... ۲،۱،۳- کرم ها
- ۶۵..... ۳،۱،۳- تروجانها
- ۶۵..... ۲،۳- انواع حملات
- ۶۵..... ۱،۲،۳- حملات انکار سرویس یا خرابکاری
- ۶۶..... ۱،۱،۲،۳- حملات انکار سرویس توزیع شده یا DDos
- ۶۷..... ۲،۱،۲،۳- پینگ مرگبار
- ۶۹..... ۳،۱،۲،۳- طغیان UDP
- ۷۰..... ۴،۱،۲،۳- طغیان Sync
- ۷۱..... ۵،۱،۲،۳- قطع ارتباط از طریق ارسال RST
- ۷۲..... ۶،۱،۲،۳- حمله LAND
- ۷۳..... ۷،۱،۲،۳- حمله Smurf
- ۷۴..... ۸،۱،۲،۳- بمب های پست الکترونیکی
- ۷۵..... ۲،۲،۳- حملات استثماری
- ۷۵..... ۱،۲،۲،۳- دزدیدن اتصال لایه ۲

۷۵	 ۲،۲،۲،۳ - جنس زدن گنروازه
۷۶	 ۳،۲،۲،۳ - اسب تروا
۷۶	 ۴،۲،۲،۳ - سرریز بافر
۷۶	 ۵،۲،۲،۳ - حمله تزریق SQL
۷۷	 ۳،۲،۳ - حملات جمع آوری اطلاعات
۷۷	 ۱،۳،۲،۳ - پویش آدرس
۷۷	 ۲،۳،۲،۳ - پویش درگاه
۷۷	 ۳،۲،۳ - پویش آهسته:
۷۸	 ۴،۱،۲،۳ - جستجوی معماری
۷۸	 ۵،۲،۲،۳ - پروتکل انتقال ناحیه DNS
۷۸	 ۳،۲،۳ - Finger
۷۸	 ۷،۳،۲،۳ - پروتکل SMTP
۷۹	 ۴،۲،۳ - حملات اطلاعات عرب
۷۹	 ۱،۴،۲،۳ - آلوده کردن حافظه DNS
۷۹	 ۲،۴،۲،۳ - نامه‌های الکترونیکی جعلی
۸۰	 ۳،۳ - سوالات فصل سوم
۸۱	 فصل ۴: مراحل حمله و مدل سازی آن
۸۱	 ۱،۴ - مراحل اجرای عملیات حمله
۸۱	 ۱،۱،۴ - شناسایی مقدماتی
۸۲	 ۱،۱،۱،۴ - شناسایی مقدماتی شبکه بدون استفاده از هیچ گونه ابزار فنی
۸۲	 ۱،۱،۱،۴ - شناسایی به وسیله روش‌های روانشناختی (مهندسی اجتماعی)
۸۲	 ۲،۱،۱،۴ - دسترسی مستقیم و ورود بی‌واسطه به شبکه
۸۳	 ۲،۱،۱،۴ - جستجو در وب به دنبال اطلاعات شبکه هدف
۸۴	 ۳،۱،۱،۴ - جستجو در بانک اطلاعاتی Whois
۸۵	 ۴،۱،۱،۴ - جستجو از طریق سرویس دهنده‌ی DNS
۸۷	 ۲،۱،۴ - شناسایی اجزاء شبکه
۸۷	 ۱،۲،۱،۴ - جستجوی مودم شبکه
۸۸	 ۲،۲،۱،۴ - نقشه برداری از شبکه:
۸۹	 ۳،۲،۱،۴ - تعیین پورت‌های باز روی یک ماشین
۸۹	 ۱،۳،۲،۱،۴ - زمانبندی مناسب برای پویش پورت‌های باز
۸۹	 ۴،۲،۱،۴ - تعیین سیستم عامل ماشین هدف
۹۰	 ۵،۲،۱،۴ - جستجوی حفاظ

- ۹۰ ۳، ۱، ۴ - جستجوی نقاط آسیب‌پذیر
- ۹۲ ۴، ۱، ۴ - نفوذ از طریق آسیب‌پذیری‌های یاد شده
- ۹۲ ۱، ۴، ۱، ۴ - استراق سمع در سطح لایه‌ی شبکه
- ۹۲ ۱، ۱، ۴، ۱، ۴ - استراق سمع
- ۹۳ ۲، ۱، ۴، ۱، ۴ - استراق سمع از هاب:
- ۹۴ ۳، ۱، ۴، ۱، ۴ - استراق سمع از سونیچ:
- ۹۵ ۲، ۴، ۱، ۴ - مقابله با استراق سمع
- ۹۵ ۳، ۴، ۱، ۴ - ربودن نشست
- ۹۶ ۵، ۱، ۴ - گم کردن و مخفی ماندن
- ۹۶ ۱، ۱، ۴ - سنککاری فایل‌های ثبت رخداد
- ۹۶ ۱، ۱، ۴، ۱، ۴ - جگونگی محافظت از فایل‌های رویدادنگار
- ۹۷ ۲، ۵، ۱، ۴ - اپ - فایل‌های پنهان روی ماشین قربانی
- ۹۷ ۳، ۵، ۱، ۴ - کد های مخفی در شبکه
- ۹۸ ۴، ۵، ۱، ۴ - فریب دادن ماشین‌ها با آدرس‌های IP جعلی
- ۹۸ ۲، ۴ - تکنیک‌های مدلسازی حمله
- ۹۹ ۱، ۲، ۴ - روش درخت حمله
- ۱۰۱ ۲، ۲، ۴ - گراف حمله
- ۱۰۲ ۱، ۲، ۲، ۴ - گراف حمله White board
- ۱۰۴ ۲، ۲، ۲، ۴ - گراف حمله Cunningham
- ۱۰۴ ۳، ۲، ۲، ۴ - گراف حمله Swiler
- ۱۰۶ ۳، ۴ - سوالات فصل چهارم
- ۱۰۷ فصل ۵: رمزنگاری و کاربردهای آن
- ۱۰۷ ۱، ۱، ۵ - مفاهیم رمزنگاری
- ۱۰۸ ۲، ۱، ۵ - رمزنگاری متقارن
- ۱۰۹ ۳، ۱، ۵ - رمزنگاری نامتقارن
- ۱۱۱ ۴، ۱، ۵ - توابع درهم ساز
- ۱۱۲ ۲، ۵ - استفاده از رمزنگاری در تامین خواص امنیتی
- ۱۱۳ ۱، ۲، ۵ - تامین جامعیت پیام با استفاده از کلید مشترک
- ۱۱۴ ۲، ۲، ۵ - تامین جامعیت و محرمانگی پیام با استفاده از کلید مشترک
- ۱۱۵ ۳، ۲، ۵ - امضاء دیجیتال و عدم انکار
- ۱۱۶ ۴، ۲، ۵ - ایجاد کلید نشست

- ۵,۲,۵- تبادل گواهی دیجیتال ۱۱۶
- ۳,۵- سوالات فصل پنجم ۱۱۹
- ۶: هویت شناسی ۱۲۳
- ۱,۶- قراردادهای احراز هویت ۱۲۳
- ۱,۱,۶- کاربردها و اهداف تعیین هویت ۱۲۳
- ۲,۱,۶- خصوصیات قراردادهای تعیین هویت ۱۲۴
- ۲,۶- روش‌های مبتنی بر دانستن چیزی ۱۲۵
- ۱,۲,۶- پروازها (احراز اصالت ضعیف) ۱۲۵
- ۱,۱,۱,۶- فایده‌های گذرواژه‌ی ذخیره شده به صورت ساده ۱۲۵
- ۲,۱,۲,۶- بایگ گذرگاه «رمز شده» ۱۲۶
- ۲,۲,۶- روش‌های تقویت پروازها ۱۲۷
- ۱,۲,۲,۶- قوانین گذرواژه ۱۲۷
- ۲,۲,۲,۶- کند کردن نگاشت گذرگاه ۱۲۷
- ۳,۲,۲,۶- گذرواژه‌های نمک ۱۲۷
- ۴,۲,۲,۶- عبارت گذر ۱۲۸
- ۳,۲,۶- انواع حملات به مدل‌های گذرواژه ۱۲۸
- ۱,۳,۲,۶- تکرار گذرواژه‌های ثابت ۱۲۸
- ۲,۳,۲,۶- جستجوی فضای حالت گذرواژه ۱۲۹
- ۳,۳,۲,۶- حملات واژنامه و حدس زدن گذرواژه ۱۳۰
- ۳,۶- روش‌های مبتنی بر داشتن چیزی ۱۳۱
- ۱,۳,۶- PIN ها و گذر کلیدها ۱۳۱
- ۱,۱,۳,۶- PIN ها ۱۳۱
- ۲,۱,۳,۶- گذرواژه‌های یکبار مصرف ۱۳۲
- ۳,۱,۳,۶- گذرواژه‌های یکبار مصرف مبتنی بر توابع یکطرفه (S/Key) ۱۳۳
- ۲,۳,۶- تعیین هویت چالش‌پاسخ (احراز هویت قوی) ۱۳۳
- ۳,۳,۶- قراردادهای تعیین هویت فاقد دانش خاص ۱۳۳
- ۱,۳,۳,۶- تعریف خصوصیت فاقد دانش ۱۳۵
- ۴,۳,۶- انواع حملات به قراردادهای تعیین هویت ۱۳۶
- ۴,۶- مقدمه‌ای بر معیارهای زیستی ۱۳۶
- ۱,۴,۶- مزایا و فرصت‌های تعیین هویت ۱۳۷
- ۲,۴,۶- روشهای تعیین هویت ۱۳۸

۱۳۹	۳، ۴، ۶- معیارهای زیستی
۱۳۹	۱، ۳، ۴، ۶- صوت
۱۴۱	۲، ۳، ۴، ۶- دما، نگاشت مادون قرمز صورت و رگهای دست
۱۴۱	۳، ۳، ۴، ۶- اثر انگشت
۱۴۲	۴، ۳، ۴، ۶- چهره
۱۴۲	۵، ۳، ۴، ۶- عنبیه
۱۴۳	۶، ۳، ۴، ۶- نحوه گام برداشتن
۱۴۳	۷، ۳، ۴، ۶- دینامیک ضربه‌ی کلید
۱۴۴	۸، ۲، ۴، ۶- DNA
۱۴۴	۹، ۱، ۴، ۶- امضاء و اصوات تولید شده
۱۴۵	۱۰، ۳، ۴، ۶- اسکن شبکیه
۱۴۶	۱۱، ۳، ۴، ۶- بدنه دست و انگشت
۱۴۶	۴، ۴، ۶- مقایسه فناوری‌های معیارهای زیستی
۱۴۹	۵، ۶- سوالات فصل ششم
۱۵۱	فصل ۷: دیوار آتش
۱۵۱	۱، ۷- مقدمه
۱۵۲	۲، ۷- دیواره آتش چیست؟
۱۵۲	۳، ۷- کارکردهای مدل جامع دیواره‌ی آتش
۱۵۴	۴، ۷- مشکلات استفاده از دیواره‌ی آتش
۱۵۴	۵، ۷- انواع دیواره‌ی آتش
۱۵۵	۱، ۵، ۷- فیلتر کردن بسته‌های اطلاعاتی
۱۵۶	۲، ۵، ۷- بررسی حالت‌مند بسته‌های اطلاعاتی
۱۵۶	۳، ۵، ۷- درگاه‌های کاربردی
۱۵۷	۶، ۷- زمینه‌های تحقیقاتی دیواره‌ی آتش
۱۵۸	۷، ۷- سوالات فصل هفتم
۱۶۱	فصل ۸: کنترل دسترسی
۱۶۱	۱، ۸- مدل‌های کنترل دسترسی
۱۶۲	۱، ۱، ۸- کنترل دسترسی اختیاری و الزامی
۱۶۳	۲، ۱، ۸- مدل بی ال پی

- ۱۶۴..... Biba مدل ۳، ۱، ۸
- ۱۶۵..... مدل کلارک ویلسون ۴، ۱، ۸
- ۱۶۵..... مدل نقش مینا ۵، ۱، ۸
- ۱۶۶..... مدیریت مجوزها ۶، ۱، ۸
- ۱۶۶..... نقش‌های سلسله‌مراتبی ۱، ۶، ۱، ۸
- ۱۶۷..... کمترین امتیاز ۲، ۶، ۱، ۸
- ۱۶۷..... جداسازی مسئولیت‌ها ۳، ۶، ۱، ۸
- ۱۶۷..... مدل مدیریت اطلاعات پزشکی ۷، ۱، ۸
- ۱۶۷..... مدل دیوار چین ۱، ۱، ۸
- ۱۶۸..... پیاده‌سازی کنترل دسترسی ۲، ۸
- ۱۶۸..... ماتریس کنترل دسترسی ۱، ۲، ۸
- ۱۶۹..... قابلیت‌ها ۲، ۲، ۸
- ۱۷۱..... ۳، ۸ سوالات فصل هفتم
- ۱۷۳..... فصل ۹: سیستم‌های تشخیص نفوذ
- ۱۷۳..... ۱، ۹ مقدمه
- ۱۷۴..... ۲، ۹ معرفی سیستم تشخیص نفوذ
- ۱۷۷..... ۱، ۲، ۹ اهداف سیستم‌های تشخیص نفوذ
- ۱۷۸..... ۲، ۲، ۹ ویژگی‌های مطلوب در سیستم‌های تشخیص نفوذ
- ۱۷۹..... ۳، ۲، ۹ خطا در سیستم تشخیص نفوذ
- ۱۷۹..... ۴، ۲، ۹ چرا حفاظتها کافی نیستند؟
- ۱۸۰..... ۳، ۹ تاریخچه سیستم‌های تشخیص نفوذ
- ۱۸۱..... ۱، ۳، ۹ نسل اول: سیستم‌های تشخیص نفوذ مبتنی بر میزبان
- ۱۸۲..... ۲، ۳، ۹ نسل دوم: سیستم‌های تشخیص نفوذ مبتنی بر شبکه
- ۱۸۲..... ۳، ۳، ۹ نسل سوم: سیستم‌های تشخیص نفوذ مبتنی بر منابع ناهمگون
- ۱۸۳..... ۴، ۹ انواع سیستم‌های تشخیص نفوذ
- ۱۸۳..... ۱، ۴، ۹ انواع سیستم‌های تشخیص نفوذ در يك نگاه
- ۱۸۴..... ۲، ۴، ۹ منبع اطلاعات سیستم
- ۱۸۵..... ۱، ۲، ۴، ۹ نظارت مبتنی بر شبکه
- ۱۸۷..... ۲، ۲، ۴، ۹ نظارت مبتنی بر میزبان
- ۱۸۸..... ۳، ۲، ۴، ۹ نظارت مبتنی بر برنامه کاربردی

۱۸۹	 ۳، ۴، ۹ - انواع روش تحلیل
۱۸۹	 ۱، ۳، ۴، ۹ - تشخیص سوءاستفاده
۱۸۹	 ۱، ۱، ۳، ۴، ۹ - سیستم‌های خبره
۱۹۰	 ۲، ۱، ۳، ۴، ۹ - رویکردهای گذار حالت
۱۹۰	 ۲، ۳، ۴، ۹ - تشخیص ناهنجاری
۱۹۱	 ۱، ۲، ۳، ۴، ۹ - مدل پایه دینینگ
۱۹۱	 ۲، ۲، ۳، ۴، ۹ - تحلیل آماری
۱۹۲	 ۳، ۲، ۳، ۴، ۹ - تحلیل غیر پارامتری
۱۹۲	 ۴، ۲، ۳، ۴، ۹ - روش‌های مبتنی بر قاعده
۱۹۲	 ۵، ۳، ۴، ۹ - شبکه عصبی
۱۹۳	 ۶، ۲، ۱، ۴، ۹ - تشخیص مبتنی بر پردازش
۱۹۴	 ۱، ۲، ۱، ۴، ۹ - روش سیستم ایمنی
۱۹۴	 ۱، ۲، ۳، ۴، ۹ - کار
۱۹۵	 ۹، ۲، ۳، ۴، ۹ - تشخیص مبتنی بر عامل
۱۹۵	 ۱۰، ۲، ۳، ۴، ۹ - تشخیص با طوف فازی
۱۹۶	 ۴، ۴، ۹ - زمان تحلیل
۱۹۶	 ۱، ۴، ۴، ۹ - زمان‌گذاری تناوبی
۱۹۷	 ۲، ۴، ۴، ۹ - زمان‌گذاری بلادرنگ
۱۹۷	 ۵، ۴، ۹ - معماری سیستم
۱۹۷	 ۱، ۵، ۴، ۹ - معماری توزیع‌شده
۱۹۷	 ۲، ۵، ۴، ۹ - معماری سلسله مراتبی
۱۹۸	 ۳، ۵، ۴، ۹ - سیستم مبتنی بر عامل
۲۰۰	 ۴، ۵، ۴، ۹ - سیستم‌های مبتنی بر عامل متحرك
۲۰۲	 ۵، ۹ - سوالات فصل نهم
۲۰۳	 فصل ۱۰: سایر مکانیزم‌های امنیتی
۲۰۳	 ۱، ۱، ۱ - مقدمه
۲۰۳	 ۲، ۱، ۱ - امنیت فیزیکی
۲۰۵	 ۱، ۲، ۱، ۱ - نواحی امن
۲۰۵	 ۱، ۱، ۲، ۱، ۱ - محدوده امنیت فیزیکی
۲۰۶	 ۲، ۱، ۲، ۱، ۱ - کنترل‌هایی که در محلهای ورود اعمال می‌گردند
۲۰۶	 ۳، ۱، ۲، ۱، ۱ - ایمن‌سازی دفتر کار، اتاقها، و امکانات

- ۲۰۷..... ۴،۱،۲،۱۰- کارکردن در نواحی امن
- ۲۰۸..... ۵،۱،۲،۱۰- نواحی انتقال و بارگیری مجزا
- ۲۰۸..... ۲،۲،۱۰- امنیت تجهیزات
- ۲۰۸..... ۱،۲،۲،۱۰- جای‌دهی تجهیزات و محافظت از آنها
- ۲۱۰..... ۲،۲،۲،۱۰- تامین کننده‌های جریان
- ۲۱۰..... ۳،۲،۲،۱۰- امنیت کابل‌کشی
- ۲۱۱..... ۴،۲،۲،۱۰- نگهداری تجهیزات
- ۲۱۱..... ۵،۲،۲،۱۰- امنیت تجهیزات مورد استفاده در بیرون سازمان
- ۲۱۲..... ۱،۲،۱،۱۰- امنیت در دورریختن تجهیزات یا استفاده مجدد از آنها
- ۲۱۲..... ۲،۱۰- کنترل‌ها، عمومی
- ۲۱۳..... ۱،۲،۲،۱۰- سیاست‌های نیز نمودن میزکار و صفحه نمایشگر
- ۲۱۳..... ۲،۳،۲،۱۰- سیاست‌های رایانه‌ای
- ۲۱۴..... ۳،۱۰- امنیت سازمانی
- ۲۱۴..... ۱،۳،۱۰- زیر ساخت امنیت اطلاعات
- ۲۱۴..... ۱،۱،۳،۱۰- کمیته مدیریت امنیت اطلاعات
- ۲۱۴..... ۲،۱،۳،۱۰- هماهنگی امنیت اطلاعات
- ۲۱۵..... ۳،۱،۳،۱۰- تخصیص مسئولیتهای امنیت اطلاعات
- ۲۱۶..... ۴،۱،۳،۱۰- فرایند اعطای مجوز برای تدریلات پردازش اطلاعات
- ۲۱۶..... ۵،۱،۳،۱۰- توصیه‌های تخصصی در زمینه امنیت اطلاعات
- ۲۱۷..... ۶،۱،۳،۱۰- هماهنگی بین سازمانها
- ۲۱۷..... ۲،۳،۱۰- امنیت دسترسی شخص ثالث
- ۲۱۷..... ۱،۲،۳،۱۰- شناسایی ریسکهای مربوط به دسترسی شخص ثالث
- ۲۱۷..... ۱،۱،۲،۳،۱۰- انواع دسترسی
- ۲۱۸..... ۲،۱،۲،۳،۱۰- دلایل دسترسی
- ۲۱۸..... ۳،۱،۲،۳،۱۰- پیمانکاران در محل
- ۲۱۸..... ۳،۳،۱۰- برون سپاری
- ۲۱۹..... ۱،۳،۳،۱۰- الزامات امنیتی در قراردادهای برون سپاری
- ۲۱۹..... ۴،۱۰- امنیت کارکنان
- ۲۱۹..... ۱،۴،۱۰- امنیت در تعریف شغل و تامین منابع انسانی
- ۲۲۰..... ۱،۱،۴،۱۰- گنجاندن امنیت در مسئولیت‌های شغل
- ۲۲۰..... ۲،۱،۴،۱۰- خط مشی و گزینش کارکنان
- ۲۲۱..... ۳،۱،۴،۱۰- توافقتنامه‌های محرمانگی

۲۲۱	 ۴، ۱، ۴، ۱۰ - شرایط و ضوابط استخدام
۲۲۱	 ۲، ۴، ۱۰ - آموزش کاربر
۲۲۱	 ۱، ۲، ۴، ۱۰ - آموزش امنیت اطلاعات
۲۲۲	 ۳، ۴، ۱۰ - واکنش به وقایع و خرابی های امنیتی
۲۲۲	 ۱، ۳، ۴، ۱۰ - گزارش دهی وقایع امنیتی
۲۲۲	 ۲، ۳، ۴، ۱۰ - گزارش دهی خرابیهای نرم افزاری
۲۲۳	 ۳، ۳، ۴، ۱۰ - فرآیند انضباطی
۲۲۳	 ۵، ۱۰ - مکاتیزمهای دیگر
۲۲۴	 ۶، ۱۰ - مکاتیزمهای فصل دهم
۲۲۵	 فصل ۱۱: امنیت در فرآیند تحلیل و طراحی نرم افزار
۲۲۵	 ۱، ۱۱ - مهندسی نیازمندی های امنیتی نرم افزار
۲۲۶	 ۱، ۱، ۱۱ - سابقه تحولات انجام شده در مهندسی نیازمندیهای امنیتی
۲۲۷	 ۲، ۱۱ - طراحی امن نرم افزار
۲۲۸	 ۱، ۲، ۱۱ - اصول طراحی امن نرم افزار
۲۳۲	 ۲، ۲، ۱۱ - مکاتیزمهای امنیتی در لراح
۲۳۲	 ۱، ۲، ۲، ۱۱ - هویت شناسی
۲۳۲	 ۲، ۲، ۲، ۱۱ - کنترل دسترسی و مجوزدهی
۲۳۳	 ۳، ۲، ۲، ۱۱ - مدیریت نشست
۲۳۳	 ۴، ۲، ۲، ۱۱ - رویدادنگاری و ممیزی
۲۳۵	 ۳، ۱۱ - سوالات فصل یازدهم
۲۳۷	 فصل ۱۲: امنیت در مراحل پیاده سازی، آزمون و استقرار
۲۳۷	 ۱، ۱۲ - کننویسی امن در تولید نرم افزار
۲۳۸	 ۱، ۱، ۱۲ - راهکارهای کلی برای پیاده سازی امن نرم افزار
۲۴۸	 ۲، ۱۲ - آزمون امنیتی نرم افزار
۲۴۹	 ۳، ۱۲ - نرم افزار در محیط عملیاتی
۲۵۱	 ۴، ۱۲ - سوالات فصل دوازدهم
۲۵۳	 فصل ۱۳: امنیت در فرآیند تولید نرم افزار
۲۵۳	 ۱، ۱۳ - مقدمه

۲۵۵	۲، ۱۳- حوزه‌های فعلی دانش در امنیت نرم‌افزار
۲۵۶	۳، ۱۳- امنیت و مهندسی نرم‌افزار
۲۵۶	۱، ۳، ۱۳- بهترین روش‌ها در امنیت نرم‌افزار
۲۵۸	۲، ۳، ۱۳- فرایندها، استانداردها و روش‌های مهندسی امن نرم‌افزار
۲۶۲	۴، ۱۳- جمع‌بندی و جهت‌گیری‌های
۲۶۴	۱، ۴، ۱۳- جهت‌گیری‌های آتی در امنیت نرم‌افزار
۲۶۷	۵، ۱۳- سوالات فصل سیزدهم
۲۶۹	فصل ۴ : مدیریت و تحلیل مخاطره
۲۶۹	۱، ۱۴- مفاهیم پایه
۲۷۰	۱، ۱، ۱۴- دارایی
۲۷۰	۱، ۱، ۱، ۱۴- تعریف ارزش دارایی‌ها
۲۷۱	۲، ۱، ۱۴- تهدید
۲۷۳	۳، ۱، ۱۴- رخنه یا نقاط آسیب‌پذیر
۲۷۳	۴، ۱، ۱۴- حفاظتها
۲۷۴	۵، ۱، ۱۴- ریسک
۲۷۵	۱، ۵، ۱، ۱۴- تحلیل ریسک
۲۷۵	۶، ۱، ۱۴- مخاطرات باقی مانده
۲۷۶	۷، ۱، ۱۴- ارتباط بین مفاهیم در مدیریت امنیت اطلاعات
۲۷۷	۲، ۱۴- روش‌های مدیریت مخاطره
۲۷۸	۳، ۱۴- روش استاندارد تحلیل ریسک امنیت اطلاعات
۲۷۸	۱، ۳، ۱۴- روش‌های کمی تحلیل مخاطره
۲۷۹	۲، ۳، ۱۴- روش‌های کیفی تحلیل مخاطره
۲۷۹	۱، ۲، ۳، ۱۴- تحلیل ریسک کیفی ده‌گامی
۲۸۰	۲، ۲، ۳، ۱۴- روش دوم تحلیل ریسک کیفی
۲۸۰	۳، ۲، ۳، ۱۴- روش تحلیل ۳۰ دقیقه‌ای
۲۸۱	۴، ۲، ۳، ۱۴- روش تحلیل ریسک تسهیل شده
۲۸۱	۳، ۳، ۱۴- روشهای تحلیل ریسک مختلط
۲۸۲	۴، ۱۴- سوالات فصل چهاردهم
۲۸۳	فصل ۵ : استاندارد مدیریت امنیت اطلاعات

۲۸۳	۱،۱۵- مقدمه
۲۸۴	۲،۱۵- استاندارد ISO/IEC 17799 یا ISO 27002
۲۸۴	۱،۲،۱۵- ISO 17799 چیست؟
۲۸۵	۲،۲،۱۵- کنترل‌های موجود در این استاندارد
۲۸۵	۱،۲،۲،۱۵- سیاست امنیتی
۲۸۶	۲،۲،۲،۱۵- امنیت سازمانی
۲۸۶	۳،۲،۲،۱۵- کنترل و طبقه‌بندی دارایی‌ها
۲۸۷	۴،۲،۲،۱۵- امنیت پرسنل
۲۸۷	۵،۲،۲،۱۵- امنیت فیزیکی و محیطی
۲۸۸	۶،۲،۲،۱۵- مدیریت ارتباطات و عملیات
۲۸۹	۷،۲،۲،۱۵- کنترل دسترسی
۲۹۰	۸،۲،۲،۱۵- توسعه و نگهداری سیستم
۲۹۰	۹،۲،۲،۱۵- مدیریت اسرار و فعالیت‌های تجاری
۲۹۰	۱۰،۲،۲،۱۵- انطباق با قوانین
۲۹۱	۳،۲،۲،۱۵- فرایند
۲۹۱	۱،۳،۲،۱۵- اخذ حمایت مدیران سطح بالا
۲۹۱	۲،۳،۲،۱۵- تعریف حیطه امنیت
۲۹۲	۳،۳،۲،۱۵- تدوین سیاست امنیت اطلاعات
۲۹۲	۴،۳،۲،۱۵- ایجاد سیستم مدیریت امنیت اطلاعات
۲۹۲	۵،۳،۲،۱۵- اجرای ارزیابی مخاطره امنیتی
۲۹۲	۶،۳،۲،۱۵- انتخاب و پیاده‌سازی کنترل‌ها
۲۹۳	۷،۳،۲،۱۵- تدوین بیانیه کاربردی
۲۹۳	۸،۳،۲،۱۵- بازرسی
۲۹۳	۳،۱۵- استاندارد BS 7799
۲۹۳	۱،۳،۱۵- مقدمه
۲۹۴	۲،۳،۱۵- سیستم مدیریت امنیت
۲۹۶	۴،۱۵- جمع‌بندی
۲۹۷	۵،۱۵- سوالات فصل پانزدهم
۲۹۹	فصل ۱۶: استاندارد معیار مشترک
۲۹۹	۱،۱۶- مقدمه

- ۳۰۰..... ۲، ۱۶- مفاهیم اولیه CC
- ۳۰۱..... ۱، ۲، ۱۶- ساختار استاندارد CC
- ۳۰۲..... ۲، ۲، ۱۶- نیازمندی‌های امنیتی
- ۳۰۲..... ۱، ۲، ۲، ۱۶- نیازمندی‌های عملیاتی
- ۳۰۳..... ۲، ۲، ۲، ۱۶- نیازمندی‌های اطمینان بخشی
- ۳۰۳..... ۳، ۲، ۱۶- سطوح ارزیابی اطمینان بخشی
- ۳۰۵..... ۴، ۲، ۱۶- کاربرد
- ۳۰۵..... ۱، ۴، ۱۶- مشخصات PP
- ۳۰۶..... ۲، ۱، ۲، ۱۶- مشخصات ST
- ۳۰۶..... ۵، ۲، ۱۶- مراحل ارزیابی امنیتی
- ۳۰۷..... ۳، ۱۶- جمع‌بندی
- ۳۰۸..... ۴، ۱۶- سوالات فضا سازد م

مقدمه

رایانه‌ها، شبکه‌های کامپیوتری و اینترنت روز به روز در دنیا در حال گسترش می‌باشند. با توجه به این گستردگی و ارتباطات ما بین رایانه‌ها از طریق شبکه‌ها نیاز به امن کردن این ارتباطات و اطلاعاتی که در این ارتباطات مبادله می‌شوند، روز به روز بیشتر احساس می‌گردد. از آنجا که روز به روز بر مخاطراتی که شبکه‌های کامپیوتری و رایانه‌ها را تهدید می‌نماید، افزوده می‌شود به همان میزان نیز باید بر امنیت شبکه‌های کامپیوتری و رایانه‌ها افزوده شود. با گسترش شبکه‌های کامپیوتری نیاز به امنیت در این شبکه‌ها به نیازی اساسی تبدیل شده است.

هدف این کتاب آشنایی با یک تصویر کلی از مهندسی امنیت اطلاعات و ارتباطات برای خوانندگان می‌باشد. در این کتاب، خوانندگان المانهای مختلف مهندسی امنیت و ارتباط آنها با یکدیگر را درک خواهند نمود. از آنجا که امنیت اطلاعات و ارتباطات تنها یک بحث فنی نیست، برای آرایه یک تصویر کامل از مهندسی امنیت اطلاعات، ارتباطات با ایستای خواننده این کتاب با مباحث مدیریتی این بحث نیز آشنا شود. به همین دلیل قسمتهایی از این کتاب به این مساله اختصاص یافته است. مطالب این درس به گونه‌ای کنار هم چیده شده است که خواننده کتاب بتواند درک علمی و عملی از تهدیدات و مخاطرات موجود در سیستم‌های رایانه‌ای پیدا نموده و همچنین توانایی تحلیل امنیت یک سیستم را با توجه به اصول مدیریتی و مهندسی داشته باشد.

ما در این کتاب قصد داریم که اصول و مبانی امنیت را که نیاز مقدماتی و ضروری تمام متخصصان آی تی و شبکه و کامپیوتر می‌باشد به قلم تحریر کرده و در اختیار شما قرار دهیم. در این کتاب با اصول و مبانی امنیت آشنا شده و در صورت نیاز می‌توانید برای یادگیری تخصص امنیت کتابهای دیگری که به طور تخصصی یک شاخه از امنیت را مورد بررسی قرار داده‌اند مراجعه کنید. این کتاب مرجع مناسبی برای تمام دانشجویان کامپیوتر و آی تی و همچنین برای تمام کسانی که علاقه دارند به مسائل امنیتی می‌باشند، می‌باشد. با توجه به اینکه مطمئناً هیچ کاری بدون نقص نمی‌باشد از تمام دوستان و دانشجویان گرامی تقاضا می‌کنیم که نظرات و پیشنهادات خود را برای بهبود کیفیت و مطالب این کتاب با نویسندگان آن از طریق آدرس‌ها الکترونیکی زیر در میان بگذارند تا به توسعه و بهبود کیفیت مطالب این کتاب کمک نمایند.