

بسمه تعالی

امنیت اطلاعات

مؤلف: محمد علی ترکمانی

www.ketab.ir

سرشناسه : ترکمانی، محمد علی، ۱۳۵۴ -

عنوان و نام پدیدآور : امنیت اطلاعات : مرجعی برای دروس مبانی امنیت در ارتباطات...

مشخصات نشر : مشهد: ارسطو، ۱۳۹۳.

مشخصات ظاهری : ۱۶۵ ص.: مصور، جدول، ۲۴×۱۷ س.م.

شابک : 978-600-7558-32-4

وضعیت فهرست نویسی : فیبای مختصر

یادداشت : این مدرک در آدرس <http://opac.nliai.ir> قابل دسترسی است.

شماره کتابشناسی ملی : ۳۷۶۵۳۰۶

نام کتاب : امنیت اطلاعات

مولف : محمد علی ترکمانی

ناشر : ارسطو

نوبت چاپ : اول - ۱۳۹۴

چاپ : مدیران

قیمت : ۱۴۰۰۰ تومان

شابک : 978-600-7558-32-4

تلفن مرکز بخش : ۰۹۱۵۹۲۲۴۳۲۰

فهرست مطالب

فصل اول: مفاهیم و اصول امنیت اطلاعات ۱۲

- ۱-۱- امنیت اطلاعات چیست؟ ۱۲
- ۱-۱-۱- خصوصیات سیستم امن ۱۳
- ۱-۲- اصطلاحات امنیتی ۱۳
- ۱-۲-۱- آسیب‌پذیری ۱۳
- ۱-۱-۲- حمله ۱۴
- ۱-۱-۳- تهدید ۱۴
- ۱-۱-۴- تأیید هویت و اجازه ۱۴
- ۱-۲- مفهوم MOM در حملات ۱۵
- ۱-۲-۱- روش ۱۵
- ۱-۲-۲- فرصت ۱۵
- ۱-۲-۳- انگیزه ۱۶
- ۱-۳- نفوذگر یا هکر ۱۶
- ۱-۳-۱- گروه نفوذگران کلاه سفید ۱۶
- ۱-۳-۲- گروه نفوذگران کلاه سیاه ۱۶
- ۱-۳-۳- گروه نفوذگران کلاه خاکستری ۱۷
- ۱-۴- دسته‌بندی کلی حملات ۱۷
- ۱-۵- روش‌های دفاعی در مقابل حملات ۱۹
- ۱-۶- انواع حملات در شبکه‌های ۲۰

۲۰	 حملات مبتنی بر پویش پورت ۱-۷-۱
۲۱	 Spoofing-۲-۷-۱
۲۱	 IP Spoofing یا IP Forgery-۱-۲-۷-۱
۲۱	 ARP Spoofing-۲-۲-۷-۱
۲۲	 مصرف پهنای باند ۳-۷-۱
۲۳	 SYN flood-۱-۳-۷-۱
۲۳	 UDP flood-۲-۳-۷-۱
۲۳	 ICMP flood-۳-۳-۷-۱
۲۴	 Mix حمله ۴-۳-۷-۱
۲۴	 Reset (RST)-۵-۳-۷-۱
۲۴	 Land Attack-۶-۳-۷-۱
۲۵	 Smurf Attack یا Smurfing-۷-۳-۷-۱
۲۵	 Fraggie حمله ۸-۳-۷-۱
۲۵	 Lttierra حمله ۹-۳-۷-۱
۲۵	 Ping of Death حمله ۱۰-۳-۷-۱
۲۵	 Jolt حمله ۱۱-۳-۷-۱
۲۶	 Teardrop حمله ۱۲-۳-۷-۱
۲۶	 ۴-۷-۱- استراق سمع یا شنود اطلاعات
۲۷	 ۵-۷-۱- مهندسی اجتماعی
۲۷	 ۶-۷-۱- دزد پستی
۲۷	 ۷-۷-۱- حمله مرد میانی
۲۸	 ۸-۷-۱- حمله تکرار
۲۸	 ۹-۷-۱- سرقت TCP/IP
۲۹	 ۱۰-۷-۱- DNS Poisoning
۲۹	 ۱۱-۷-۱- ویروس‌ها و کرم‌ها
۳۰	 ۱۲-۷-۱- اسب تروا

- ۳۰-۱۳-۷-۱ جاسوس افزار
- ۳۰-۱۴-۷-۱ وب سایت های تقلبی (فیشینگ)
- ۳۰-۱۵-۷-۱ حمله با استفاده از نرم افزارهای ثبت کننده کلید
- ۳۱-۱۶-۷-۱ حمله روز تولد
- ۳۲-۱۷-۷-۱ حملات جهت یافتن کلمات عبور
- ۳۲-۱۸-۷-۱ بهره برداری از نرم افزار
- ۳۲-۱۹-۷-۱ شماره گیر جنگی
- ۳۳-۲۰-۷-۱ سرریز بافر
- ۳۳-۲۱-۷-۱ حملات تزریق SQL
- ۳۳-۲۲-۷-۱ هرزنامه
- ۳۴-۲۳-۷-۱ VoIP Spam یا SPIT
- ۳۵-۲۴-۷-۱ Email spoofing
- ۳۵-۲۵-۷-۱ BOTNET
- ۳۷-۱-۲۵-۷-۱ حمله DDOS با استفاده از BOTNET
- ۳۹-۸-۱ سرویس های امنیتی
- ۳۹-۸-۱ سرویس های امنیتی X.800
- ۴۱-۹-۱ مکانیزم های امنیتی
- ۴۳-۱۰-۱ سیاست های امنیتی
- ۴۴-۱-۱۰-۱ سیاست های کلمه عبور
- ۴۴-۲-۱۰-۱ سیاست های اینترنتی
- ۴۴-۳-۱۰-۱ پشتیبان گیری و احیای اطلاعات
- ۴۵-۱۱-۱ ۱۱-۱ سئوالات چهارگزینه ای فصل اول

۵۲ پاسخنامه سئوالات چهارگزینه‌ای فصل اول

فصل دوم: مروری بر مفاهیم ریاضی مورد نیاز ۵۳

۵۳ ۱-۲- بخش پذیری

۵۴ ۱-۲- قضیه

۵۵ ۱-۲-۳- تابع کف و تابع سقف

۵۵ ۱-۲-۴- قضیه تقسیم

۵۵ ۱-۲-۵- بزرگترین مقسوم علیه مشترک

۵۶ ۱-۲-۵-۱- الگوریتم اقلیدسی

۵۶ ۱-۲-۵-۱- قضیه

۵۷ ۱-۲-۵-۲- نکات مهم

۵۷ ۱-۲-۵-۲- الگوریتم اقلیدسی توسعه یافته

۵۸ ۲-۲- اعداد اول

۵۸ ۱-۲-۲- تعریف

۵۸ ۲-۲-۲- لم

۵۸ ۱-۲-۲- نتیجه

۵۸ ۲-۲-۳- قضیه اساسی حساب اعداد

۵۸ ۲-۲-۴- مسئله تجزیه اعداد

۵۹ ۲-۲-۵- هم نهستی

۵۹ ۲-۲-۵-۱- قضیه

۶۰ ۲-۲-۵-۲- نکته

۶۱ ۲-۲- الگوریتم توان رسانی سریع

۶۳ ۲-۳-۱- شبه کد توان رسانی سریع

۶۴ ۲-۴- ماتریس ها

- ۶۵..... ۱-۴-۲ - جمع دو ماتریس
- ۶۵..... ۲-۴-۲ - ضرب یک عدد در یک ماتریس
- ۶۵..... ۳-۴-۲ - ضرب ماتریسها
- ۶۶..... ۴-۴-۲ - محاسبات دترمینان ماتریس 2×2
- ۶۶..... ۵-۴-۲ - محاسبه دترمینان ماتریس 3×3
- ۶۷..... ۵-۴-۲ - ۱- روش ساروس برای محاسبه دترمینان
- ۶۷..... ۶-۴-۲ - ماتریس وارون
- ۶۹..... ۵-۲ - سئوالات چهارگزینه‌ای
- ۷۲..... پاسخنامه

فصل سوم: تکنیک‌ها و الگوریتم‌های رمزنگاری ۷۳

- ۷۳..... ۱-۳ - مفاهیم و اصطلاحات رمزنگاری
- ۷۵..... ۲-۳ - سیستم‌های رمزنگاری
- ۷۶..... ۱-۲-۳ - رمزنگاری متقارن
- ۷۶..... ۲-۲-۳ - رمزنگاری نامتقارن
- ۷۷..... ۳-۳ - علم تحلیل رمز یا شکستن رمز
- ۷۸..... ۴-۳ - تکنیک‌های رمزگذاری
- ۷۸..... ۱-۴-۳ - رمزنگاری سزار
- ۸۰..... ۲-۴-۳ - رمزنگاری ورنام
- ۸۰..... ۳-۴-۳ - رمزنگاری جابجایی ستونی
- ۸۱..... ۴-۴-۳ - ترکیب جایگشتی و جایگزینی
- ۸۲..... ۵-۴-۳ - تکنیک‌های رمزنگاری متقارن
- ۸۲..... ۱-۵-۴-۳ - رمز رشته‌ای یا دنباله‌ای

- ۸۲..... ۲-۴-۲- رمز بلاکی
- ۸۳..... ۶-۴-۲- جایگزینی و جایگشتی بلاکی
- ۸۳..... ۱-۶-۴-۲- جایگزینی بلاکی (S-BOX)
- ۸۴..... ۲-۶-۴-۲- جابجایی بلاکی (جایگشتی) یا P-BOX
- ۸۵..... ۱-۲-۶-۴-۲- P-BOX حمله به
- ۸۶..... ۵-۳- رمزنگاری Hill
- ۹۲..... ۶-۳- رمزنگاری DES
- ۹۴..... ۱-۶-۳- جزئیات تابع $F_{Ri} - 1, Ki$
- ۱۰۰..... ۲-۶-۳- روش استخراج کلیدهای فرعی از کلید اصلی یا شاه کلید
- ۱۰۲..... ۳-۶-۳- رمزگشایی DES
- ۱۰۳..... ۴-۶-۳- خاصیت بهمنی DES
- ۱۰۳..... ۵-۶-۳- نکات مهم الگوریتم DES
- ۱۰۳..... ۶-۶-۳- 2DES الگوریتم
- ۱۰۴..... ۷-۶-۳- 3DES الگوریتم
- ۱۰۵..... ۸-۶-۳- امنیت DES
- ۱۰۵..... ۷-۳- الگوریتم AES
- ۱۰۸..... ۸-۳- رمزنگاری با کلید عمومی
- ۱۰۹..... ۹-۳- الگوریتم RSA
- ۱۱۰..... ۱-۹-۳- انتخاب کلید
- ۱۱۱..... ۲-۹-۳- روش رمزگذاری و رمزگشایی
- ۱۱۵..... ۱۰-۳- مقایسه رمزنگاری متقارن و نامتقارن
- ۱۱۵..... ۱۱-۳- تبادل کلید با استفاده از رمزنگاری RSA
- ۱۱۶..... ۱-۱۱-۳- پروتکل توزیع کلید متقارن با استفاده از کلید عمومی

- ۱۱۸-۱۲-۳ رمزنگاری کلید عمومی الجمال و روش مبادله کلید دیفی-هلمن ۱۱۸
- ۱۱۹-۱۳-۳-اختفاء کامل ۱۱۹
- ۱۲۱-۱۴-۳ رمزشکنی و تحلیل متن ۱۲۱
- ۱۲۱-۱۴-۳-۱ انواع حملات تحلیل رمز ۱۲۱
- ۱۲۳-۱-۱۴-۳-۱ الگوریتم رمزگذاری و رمزگشایی امن ۱۲۳
- ۱۲۳-۲-۱۴-۳ رمزشکنی DES ۱۲۳
- ۱۲۳-۱-۲-۱۴-۳ رمزشکنی تفاضلی ۱۲۳
- ۱۲۴-۲-۲-۱۴-۳ رمزشکنی خطی ۱۲۴
- ۱۲۴-۳-۱۴-۳ حمله به RSA ۱۲۴
- ۱۲۶-۱۵-۳ سخت افزارهای رمزکننده ۱۲۶
- ۱۲۸-۱۶-۳-سئوالات چهارگزینه‌ای ۱۲۸
- ۱۳۹-پاسخنامه سئوالات چهارجوابی فصل سوم ۱۳۹

فصل چهارم: صحت پیام، MAC، امضای دیجیتال و

گواهینامه ۱۴۰

- ۱۴۰-۱-۴ صحت پیام با استفاده از MAC ۱۴۰
- ۱۴۲-۲-۴ الگوریتم‌های MAC ۱۴۲
- ۱۴۲-۳-۴ امضای دیجیتال ۱۴۲
- ۱۴۴-۴-۴ گواهینامه ۱۴۴
- ۱۴۵-۵-۴ سئوالات چهارگزینه‌ای ۱۴۵
- ۱۴۷-پاسخنامه ۱۴۷

فصل پنجم: امنیت پست الکترونیکی ۱۴۸

- ۱۴۸-۱-۵-ایمیل امن ۱۴۸

۱۴۸ ۱-۱-۵ سیستم اول

۱۴۹ ۱-۲-۵ سیستم دوم

۱۵۰ ۱-۳-۵ سیستم سوم

۱۵۱ ۲-۵ استاندارد PGP

۱۵۲ ۳-۵ توسعه پست الکترونیکی چند منظوره امن S/MIME

۱۵۴ ۴-۵ سوالات چهارگزینه‌ای

۱۵۵ پاسخنامه

۱۵۶ پیوست‌ها

۱۵۶ پیوست ۱: نمونه سوالات تشریحی

۱۵۹ پیوست ۲: حل برخی از سوالات

۱۶۵ پیوست ۳: جدول کدهای اسکی

۱۶۶ مراجع

مقدمه مولف:

امروزه کاربران شبکه‌های کامپیوتری و اینترنت با تهدیدهای زیادی روبرو هستند. نفوذگران از بد ابزارها و مکانیزم‌های تهاجمی مختلفی برای نفوذ، آسیب رسانی یا سرقت اطلاعات استفاده می‌کنند. لذا دانشجویان رشته‌های مهندسی کامپیوتر، IT، ICT باید دانش مورد نیاز در زمینه امنیت شبکه و رمزنگاری را کسب نمایند. به همین علت دروس رمزنگاری، مبانی امنیت در ارتباطات، امنیت شبکه و امنیت در تجارت الکترونیک در برنامه درسی رشته‌های کامپیوتر، IT و ICT قرار گرفته است. علیرغم اهمیت این دروس، مرجع مناسبی برای آنها وجود ندارد. حجم مراجع معرفی شده برای این دروس بسیار زیاد است و تدریس این مطالب در یک نیم‌سال تحصیلی دشوار است. این کتاب به منظور سهولت کار اساتید و دانشجویان گرامی و همچنین افزایش کیفیت آموزشی دروس اصول و مفاهیم رمزنگاری و مبانی امنیت در ارتباطات تدوین گردیده است. همچنین این کتاب می‌تواند به عنوان مرجعی برای سایر دروس مرتبط نظیر امنیت در تجارت الکترونیک و امنیت شبکه مورد استفاده قرار گیرد. اساتید گرامی این دو درس می‌توانند با توجه به امکانات دانشگاه و سطح علمی دانشجویان، مباحث عملی مورد نظر خود را در کنار مباحث تئوری موجود در کتاب، آموزش دهند. در این کتاب سعی شده است که مطالب با زبانی ساده و به همراه مثال‌های متنوعی ارائه گردد. در انتهای هر فصل مجموعه سئوالات تستی به همراه حل آنها آورده شده است. در پایان کتاب نیز تعدادی تشریحی به همراه پاسخ آنها ارائه شده است تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده 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 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 آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین مدیریت انتشارات ارسطو جناب آقای حسین قنبری تشکر و قدردانی نمایم.