

سرشناسه: استالینگر، ویلیام
Stallings, William

عنوان و نام پدیدآور: اصول و مبانی امنیت شبکه (کاربردها و استانداردها)/ویلیام استالینگر؛ ترجمه آرش حبیبی، نسرین بدیع، فرناز توحیدی، وضعیت ویراست: [ویراست ۲].

مشخصات نشر: تهران: انتشارات علوم ایران، ۱۳۹۶.

مشخصات ظاهری: ۸۰ ص.؛ مصور، جدول.

شابک: ۹۷۸-۹۶۴-۲۷۵۰-۶۰۰-۳

وضعیت فهرست نویسی: فیبا

یادداشت: عنوان اصلی: . [2014], 5th ed, Network security essentials : applications and standards

یادداشت: کتاب حاضر نخستین بار تحت عنوان "اصول امنیت شبکه‌های کامپیوتری: کاربردها و استانداردها" با ترجمه مسعود موحد در سال ۱۳۸۵ توسط انتشارات پیام‌سان منتشر شده است.

عنوان دیگر: اصول امنیت شبکه‌های کامپیوتری: کاربردها و استانداردها.

موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی

موضوع: Computer networks -- Security measures

موضوع: کامپیوترها -- ایمنی اطلاعات

موضوع: Computer security

شناسه افزوده: حبیبی‌لشکری، آرش، ۱۳۵۳ - مترجم

شناسه افزوده: بدیع، نسرین، ۱۳۶۱ - مترجم

شناسه افزوده: توحیدی، فرناز، ۱۳۵۴ - مترجم

رده بندی کنگره: ۶ ۱۳۹۶ الف۴۶الف/۵۹/TK ۵۱۰۵

رده بندی دیویی: ۰۰۵/۸۱

شماره کتابشناسی ملی: ۴۸۶۴۲۵۷



انتشارات علوم ایران

www.olomiran.net

انتشارات علوم ایران

تهران - تلفن ۰۹۱۲۵۳۶۷۶۲۱ و ۶۶۸۷۵۴۴۹

صندوق پستی: تهران ۳۵۳ - ۱۳۱۴۵

نام کتاب: اصول و مبانی امنیت شبکه (کاربردها و استانداردها) - ویلیام استالینگر [ویراست پنجم]

ترجمه: دکتر آرش حبیبی لشکری - مهندس نسرین بدیع - مهندس فرناز توحیدی

ناشر: علوم ایران شابک: ۳ - ۶۰ - ۲۷۵۰ - ۹۶۴ - ۹۷۸

تیراژ: ۵۰ نسخه نوبت و سال چاپ: چهارم - ۱۴۰۱



انتشارات علوم ایران

۴۲۰ هزار تومان

مرکز پخش:

کتاب کوشا - میدان انقلاب، ابتدای کارگر جنوبی، کوچه رشتچی، بن بست یکم، پلاک ۴

طبقه دوم واحد ۴ تلفن همراه: ۰۹۱۲۳۰۳۳۰۵۸

تلفن: ۶۶۹۴۱۱۶۷ و ۶۶۹۴۱۰۳۴ فکس: ۶۶۹۲۱۶۸۵

خرید آنلاین: ketabmail.com

هرگونه کپی‌برداری و یا تکثیر و یا انتشار و یا شبیه‌سازی هر قسمتی از این کتاب به هر شکلی و در هر مکانی بدون اجازه ناشر، با توجه به قانون حمایت از مؤلفین و مصنفان و هنرمندان مصوب ۱۳۴۸، پیگرد قانونی دارد.

سخن ناشر

وز خوردن آدمی زمین سیر نشد

بر چرخ فلک هیچ کسی چیر نشد

تعجیل مکن هم بخورد دیر نشد

مغرور بدانی که نخورده‌ست ترا

انتشارات علوم ایران در تلاش است تا کتبی را به دست خوانندگان برساند که توسط آنها حداقل گوشه‌ای از نیازهای علمی کشور برآورده شود. لذا از اساتید و مدرسین و اعضاء هیئت علمی دانشگاه‌ها و دانشجویان در مقاطع و رشته‌های مختلف تحصیلی و تمامی افرادی که می‌خواهند کتابی را ترجمه و یا تألیف نمایند، دعوت می‌کنیم تا جهت همکاری، با ما تماس بگیرند. برای ارتباط با انتشارات علوم ایران می‌توانید با شماره تلفن همراه ۰۹۱۲۵۳۶۷۶۲۱ تماس گرفته و یا به پست الکترونیکی olomiran@hotmail.com و یا به آدرس: تهران- صندوق پستی ۳۵۳ - ۱۳۱۴۵ پیشنهادات خود را ارسال نمایید. آدرس سایت انتشارات علوم ایران www.olomiran.net می‌باشد.

با تشکر

مهندس محمدتقی فرامرزی

مدیر انتشارات علوم ایران

پیش‌گفتار

سخن مترجمین

امروزه اهمیت و جایگاه امنیت شبکه‌های رایانه‌ای و حفاظت از اطلاعات داخل آنها نه تنها برای متخصصین علوم رایانه بلکه بر عموم محققین و متخصصین در سایر علوم نیز پوشیده نیست. چراکه، بی شک بدون داشتن شبکه‌های رایانه‌ای امروز مطمئن هیچ ارتباط و انتقال اطلاعاتی قابل انجام نبوده و شاید بتوان بخش بزرگی از پیشرفت‌های امروز بشر را مدیون ساختار دهکده جهانی آن هم بر پایه شبکه‌های رایانه‌ای ایمن و مطمئن دانست.

کتاب حاضر ترجمه ویرایش پنجم کتاب "اصول و مبانی امنیت شبکه‌ها: کاربردها و استانداردها" بقلم ویلیام استالینگر دانشگاه MIT به همراه پاسخ تشریحی مجموعه پرسش‌های دوره‌ای و مسائل کتاب برای هر فصل می‌باشد. در هر فصل کتاب ابتدا تعدادی پرسش دوره‌ای که مربوط به تئوری‌ها و مفاهیم پایه آن فصل بوده، مطرح گردیده و سپس مسائلی از آن فصل نیز ارائه شده است.

مزیت عمده این کتاب نسبت به سایر کتب مشابه این است که در این کتاب نویسنده در سه بخش به بررسی کامل و جامع امنیت و استانداردهای آن در شبکه‌های رایانه‌ای پرداخته است. در بخش اول موضوع و مفهوم رمزنگاری در غالب رمزگذاری و رمزگشایی در سه مدل متقارن، نامتقارن و درهم‌سازی مورد بررسی قرار گرفته و سپس در بخش دوم، به بررسی امنیت شبکه و موارد اصلی آن مانند طراحی و توزیع کلیدها، کنترل دسترسی در شبکه‌ها، امنیت شبکه‌های بی‌سیم امنیت پست‌های الکترونیکی پرداخته شده است. در بخش سوم و پایانی کتاب نیز به امنیت یک رایانه که همان بررسی کامل حملات معروف و عمومی یعنی نرم‌افزارهای بداندیش و روش‌های نفوذ آنها است، پرداخته و در انتها با بررسی دیوارهای آتش در واقع نحوه مقابله با آنها را مورد کندوکاو قرار داده است.

در هر فصل برای درک بهتر و عمیقتر مفاهیم کتاب و سایر مطالب مشابه در زمینه امنیت شبکه‌ها به زبان انگلیسی بخش با عنوان کلمات کلیدی و اختصارها در نظر گرفته شده و همچنین یکسری پرسش‌ها و مسائل مرتبط با هر فصل نیز گردآوری شده که پاسخ تشریحی این پرسش‌های دوره‌ای و مسائل در ضمیمه انتهایی کتاب ارائه شده است.

بپاس قدردانی از زحمات بی‌دریغ همه آموزگاران و معلمین این مرز و بوم که برای تربیت، آموزش و پرورش فرزندان این آب و خاک از هیچ کوششی فروگذار نبوده‌اند، این مجموعه را به این عزیزان تقدیم نموده و از خداوند منان سلامتی و توفیق روزافزون برای یکایکشان را خواستاریم.

در خاتمه، با سپاس فراوان از عزیزانی که با ارسال نظرات و پیشنهادها خود باعث تغییراتی جهت بهبود در چاپ دوم این کتاب شدند، درخواست ما از خوانندگان عزیز به ویژه همکاران، اساتید محترم و دانشجویان گرامی اینست که همچنان نظرات و پیشنهادها خود را از طریق ناشر این کتاب در ایران و یا از طریق سایت اینترنتی <http://www.ahlashkari.com> و آدرس پست الکترونیکی A.Habibi.L@gmail.com بطور مستقیم در اختیار ما قرار دهند.

با احترام

تهران - مرداد ۱۳۹۶

سخن مولف

در این عصر ارتباطات الکترونیکی جهانی، با وجود ویروس‌ها و هکرها، استراق سمع‌های الکترونیکی، حمله‌ها و کلاهبرداری‌های الکترونیکی، برآستی که دیگر زمانی برای عدم توجه به امنیت باقی نمانده است. در واقع دو موضوع باعث حیاتی بودن و اهمیت بالای این کتاب هستند. نخست آنکه رشد ناگهانی و بسیار سریع سیستم‌های رایانه‌ای و ارتباط آنها از طریق شبکه‌ها باعث افزایش نیازمندی و وابستگی افراد و شرکت‌ها به ذخیره اطلاعات و استفاده از سیستم‌های رایانه‌ای شده است. که این امر خود موجب افزایش نیاز به دانش بیشتر در مورد موضوعاتی چون حفاظت اطلاعات و منابع برای تضمین صحت اطلاعات و پیام‌های ارسالی و همچنین حفاظت سیستم‌ها از حملات مرتبط با شبکه‌های رایانه‌ای خواهد شد. دوم آنکه، رشد و تکامل رشته‌های علمی چون رمزنگاری و امنیت شبکه، برجستگی توسعه عملی و سهولت برنامه‌های کاربردی در دسترس باعث تاکید بیشتر بر امنیت شبکه‌ها گردیده است.

اهداف این کتاب:

هدف اصلی این کتاب مطالعه جامع و گسترده بصورت عملی روی استانداردها و کاربردهای امنیت شبکه است. تاکید بیشتر این کتاب روی کاربردهایی که بطور گسترده در اینترنت و شبکه‌های متحد بکار رفته و استانداردهایی که (بخصوص استانداردهای اینترنتی) در زمینه‌های مختلفی گسترش یافته‌اند، قرار دارد.

موارد جدید در ویرایش پنجم:

از چهار سال پیش که ویرایش چهارم این کتاب به چاپ رسیده است، پیشرفت‌ها و ابداعات همچنان در این حوزه با سرعت ادامه داشته است. در این ویرایش، سعی شده است تا این تغییرات و به روز رسانی‌ها بطور گسترده و همه جانبه پوشش داده شود. برای آغاز این پروسه به روز رسانی، پروفیسورها و استادان بسیاری از دانشگاه‌ها که مدرس موضوعات مشابه بوده‌اند و متخصصین زیادی که در این حوزه بصورت تخصصی فعالیت داشته‌اند به بررسی و بازنگری ویرایش چهارم پرداختند. نتیجه اینچنین بود که در بسیاری از موارد، موضوعات شفافتر شده و توضیحات بصورت مصور بهبود داده شدند. براساس این پالایش‌ها برای بهبود آموزش و درک بهتر کاربران، تغییرت زیادی در کتاب پدید آمد ولی ساختار کلی فصل‌ها حفظ شده و علاوه بر افزودن چند فصل جدید بیشتر اطلاعات و مطالب فصل‌های پیشین تغییر یافته و بروز شده‌اند. بیشترین تغییرات اساسی بشرح ذیل میباشند:

* **کنترل دسترسی شبکه:** یک فصل جدید برای پوشش کنترل دسترسی شبکه که شامل تصویر کلی موضوع و بحث درباره پروتکل اعتبارسنجی توسعه‌یافته و استاندارد IEEE 802.1X می‌باشد، به فصول پیشین اضافه شده است.

* **امنیت محاسبات ابری:** یک فصل جدید برای پوشش مشکلات امنیتی روی موضوع جدید محاسبات ابری به فصول پیشین افزوده شده است.

* **امنیت تلفن‌های همراه:** موضوع امنیت تلفن‌های همراه امروزه به یکی از جنبه‌های اساسی امنیت شبکه‌های سازمان‌ها و موسسه‌ها تبدیل شده است. یک بخش جدید این موضوع را نیز مورد بررسی قرار می‌دهد.

* **نرم‌افزار بداندیش:** این فصل نسبت به فصل موجود در ویرایش چهارم تغییرات بسیاری کرده است. بطور خاصی روی درب‌های پستی و روت‌کیت‌ها بعنوان بدافزارهای استفاده شده در حملات مهندسی اجتماعی نسبت به حملات مستقیم ویروس‌ها و کرم‌های کلاسیک بیشتر پرداخته شده است. همچنین حمله جعل صفحات بیشتر از بقیه موارد بررسی شده و بطور کلی این رویدادها پوشش داده شده‌اند.

* **سرفصل‌های ساده:** همیشه متن با اطلاعات بیشتر در صورت ساده بودن براحتی می‌تواند در یک ترم دانشگاهی پوشش داده شود. بنابراین، استادان سرفصل‌های بسیاری را بصورت ساده و با مثال‌های متنوع مهیا نموده‌اند که

فهرست مطالب

فصل اول: مقدمه / ۱۳

- ۱.۱ مفاهیم امنیت کامپیوتر / ۱۴
 - ۲.۱ معماری امنیتی OSI / ۱۸
 - ۳.۱ حملات امنیتی / ۱۹
 - ۴.۱ سرویس‌های امنیتی / ۲۱
 - ۵.۱ مکانیزم‌های امنیتی / ۲۴
 - ۶.۱ یک مدل برای امنیت شبکه / ۲۶
 - ۷.۱ استانداردها / ۲۸
 - ۸.۱ رئوس مطالب کتاب / ۲۹
 - ۹.۱ منابع توصیه شده / ۲۹
 - ۱۰.۱ اصطلاحات کلیدی و اختصارها / ۳۰
- پرسش‌ها و سوال‌های فصل اول

بخش اول: رمزنگاری

فصل دوم: رمزگذاری متقارن و محرمانگی پیغام / ۳۳

- ۱.۲ اصول رمزنگاری متقارن / ۳۳
 - ۲.۲ الگوریتم‌های رمزنگاری بلوکی متقارن / ۳۹
 - ۳.۲ اعداد تصادفی و شبه تصادفی / ۴۵
 - ۴.۲ رمزهای جریانی و RC4 / ۴۹
 - ۵.۲ حالت‌های عملیاتی رمزنگاری بلوکی / ۵۳
 - ۶.۲ منابع توصیه شده / ۵۹
 - ۷.۲ اصطلاحات کلیدی و اختصارها / ۵۹
- پرسش‌ها و سوال‌های فصل دوم

فصل سوم: رمزنگاری کلید-عمومی و احراز هویت پیغام / ۶۷

- ۱.۳ خط‌مشی‌های احراز هویت پیام / ۶۷
 - ۲.۳ توابع امن درهم‌سازی / ۷۲
 - ۳.۳ کدهای احراز هویت پیام یا MAC / ۷۹
 - ۴.۳ اصول رمزنگاری کلید-عمومی / ۸۴
 - ۵.۳ الگوریتم‌های رمزنگاری کلید-عمومی / ۸۷
 - ۶.۳ امضاهای الکترونیکی / ۹۵
 - ۷.۳ منابع توصیه شده / ۹۶
 - ۸.۳ اصطلاحات کلیدی و اختصارها / ۹۶
- پرسش‌ها و سوال‌های فصل سوم

بخش دوم: کاربردهای امنیت شبکه

فصل چهارم: توزیع کلید و احراز هویت کاربر / ۱۰۷

- ۱.۴ توزیع کلید متقارن با استفاده از رمزگذاری متقارن / ۱۰۷۰
- ۲.۴ Kerberos / ۱۰۸
- ۳.۴ توزیع کلید با استفاده از رمزگذاری نامتقارن / ۱۲۲
- ۴.۴ گواهینامه‌های X.509 / ۱۲۴
- ۵.۴ زیرساختار کلید-عمومی / ۱۳۲
- ۶.۴ مدیریت هویت فدرال / ۱۳۴
- ۷.۴ منابع توصیه شده / ۱۴۰
- ۸.۴ اصطلاحات کلیدی و اختصارها / ۱۴۰

پرسش‌ها و سوال‌های فصل چهارم

فصل پنجم: کنترل دسترسی شبکه و امنیت محاسبات ابری / ۱۴۷

- ۱.۵ کنترل دسترسی شبکه / ۱۴۷
- ۲.۵ پروتکل احراز هویت توسعه یافته / ۱۵۰
- ۳.۵ کنترل دسترسی شبکه مبتنی بر گذرگاه IEEE 802.1X / ۱۵۴
- ۴.۵ محاسبات ابری / ۱۵۷
- ۵.۵ ریسک‌های امنیتی ابر و اقدامات متقابل / ۱۶۳
- ۶.۵ محافظت داده‌ها در ابر / ۱۶۵
- ۷.۵ امنیت ابر بعنوان یک سرویس / ۱۶۸
- ۸.۵ منابع توصیه شده / ۱۷۱
- ۹.۵ اصطلاحات کلیدی و اختصارها / ۱۷۲

پرسش‌ها و سوال‌های فصل پنجم

فصل ششم: امنیت لایه - انتقال / ۱۷۵

- ۱.۶ ملاحظات امنیت وب / ۱۷۵
- ۲.۶ لایه سوکت‌های امن یا SSL / ۱۷۸
- ۳.۶ امنیت لایه انتقال / ۱۹۱
- ۴.۶ پروتکل HTTPS / ۱۹۶
- ۵.۶ پوسته امن یا SSH / ۱۹۷
- ۶.۶ منابع توصیه شده / ۲۰۸
- ۷.۶ اصطلاحات کلیدی و اختصارها / ۲۰۸

پرسش‌ها و سوال‌های فصل ششم

فصل هفتم: امنیت شبکه‌های بی سیم / ۲۱۱

- ۱.۷ امنیت بی سیم / ۲۱۱
- ۲.۷ امنیت تجهیزات سیار / ۲۱۴
- ۳.۷ مروری بر شبکه‌های محلی بی سیم IEEE 802.11 / ۲۱۹
- ۴.۷ امنیت شبکه محلی بی سیم IEEE 802.11i / ۲۲۵

فصل یازدهم: نفوذگران / ۳۵۹

۱.۱۱ نفوذگران / ۳۶۰

۲.۱۱ کشف نفوذ / ۳۶۴

۳.۱۱ مدیریت رمزعبور / ۳۷۹

۴.۱۱ منابع توصیه شده / ۳۹۰

۵.۱۱ اصطلاحات کلیدی و اختصارها / ۳۹۰

پرسش‌ها و سوال‌های فصل یازدهم

فصل دوازدهم: دیوارهای آتش / ۳۹۵

۱.۱۲ نیاز به دیوارهای آتش / ۳۹۵

۲.۱۲ خصوصیات دیوار آتش / ۳۹۶

۳.۱۲ انواع دیوارهای آتش / ۳۹۸

۴.۱۲ دیوار آتش مینا / ۴۰۴

۵.۱۲ تنظیمات و محل استقرار دیوار آتش / ۴۰۶

۶.۱۲ منابع توصیه شده / ۴۱۱

۷.۱۲ اصطلاحات کلیدی و اختصارها / ۴۱۱

پرسش‌ها و سوال‌های فصل دوازدهم

ضمایم / ۴۱۹

ضمیمه الف: اعداد تصادفی و شبه تصادفی / ۴۲۰

ضمیمه ب: رمز جابجایی مضاعف / ۴۲۲

ضمیمه پ: لیست رمزهای عبور کرم موریس / ۴۲۴

ضمیمه ت: پاسخ تشریحی پرسش‌ها و مسائل / ۴۲۶

۵.۷ منابع توصیه شده / ۲۴۰

۶.۷ اصطلاحات کلیدی و اختصارها / ۲۴۱

پرسش‌ها و سوال‌های فصل هفتم

فصل هشتم: امنیت پست الکترونیکی / ۲۴۵

۱.۸ حریم خصوصی مناسب / ۲۴۵

۲.۸ S/MIME / ۲۵۲

۳.۸ دامنه‌های کلیدی پست الکترونیکی شناخته شده / ۲۷۰

۴.۸ منابع توصیه شده / ۲۷۸

۵.۸ اصطلاحات کلیدی و اختصارها / ۲۷۸

پرسش‌ها و سوال‌های فصل هشتم

فصل نهم: امنیت IP / ۲۸۱

۱.۹ بازیگری امنیت IP / ۲۸۲

۲.۹ سیاست امنیت IP / ۲۸۵

۳.۹ کپسوله کردن بار مفید امنیتی / ۲۹۳

۴.۹ ترکیب اجتماعات امنیتی / ۳۰۱

۵.۹ تبادل کلید اینترنتی / ۳۰۴

۶.۹ مجموعه روش‌های رمزگذاری / ۳۱۲

۷.۹ منابع توصیه شده / ۳۱۴

۸.۹ اصطلاحات کلیدی و اختصارها / ۳۱۵

پرسش‌ها و سوال‌های فصل نهم

بخش سوم: امنیت سیستم

فصل دهم: نرم‌افزار بد اندیش / ۳۱۹

۱.۱۰ انواع نرم‌افزارهای بداندیش (بدافزار) / ۳۲۰

۲.۱۰ ویروس‌ها - محتوای آلوده شده - انتشار / ۳۲۲

۳.۱۰ کرم‌ها - استفاده از آسیب‌پذیری - انتشار / ۳۲۸

۴.۱۰ تروجان‌ها و اسپیم‌ها - مهندسی اجتماعی - انتشار / ۳۳۳

۵.۱۰ ظرفیت - خرابی سیستم / ۳۳۵

۶.۱۰ ظرفیت - عامل حمله - بات‌ها و زامبی / ۳۳۷

۷.۱۰ ظرفیت - دزدی اطلاعات - ثبت کلیدها، جعل صفحات، جاسوس‌افزار / ۳۳۹

۸.۱۰ ظرفیت - سرقت - روت‌کیت و درب‌های مخفی / ۳۴۰

۹.۱۰ اقدامات متقابل / ۳۴۲

۱۰.۱۰ حملات محرومیت - از - خدمات گسترش یافته / ۳۴۹

۱۱.۱۰ منابع توصیه شده / ۳۵۴

۱۲.۱۰ اصطلاحات کلیدی و اختصارها / ۳۵۵

پرسش‌ها و سوال‌های فصل دهم