ویراست پنجم - ۲۰۱۴

مبانی امنیت شبکه

(کاربردها و استانداردها)

تألیف:

ویلیام استالینگز

ترجمه:

عین‌الله جعفرنژاد قمی

علوم رایانه

سرشناسه	: استالینگز، ویلیام Stallings, William
عنوان و نام پدیدآور	: مبانی امنیت شبکه (کاربردها و استانداردها) / ویلیام استالینگز؛ ترجمه عین‌الله جعفرنژادقمی.
مشخصات نشر	: بابل: علوم رایانه، ۱۳۹۳.
مشخصات ظاهری	: ۴۸۸ ص.: مصور، جدول.
شابک	: ۹۷۸-۶۰۰-۲۰۵-۰۷۰-۰
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: عنوان اصلی: Network security essentials: applications and standards, [fifth edition, 2014]
یادداشت	: واژه‌نامه
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: کامپیوترها -- ایمنی اطلاعات
شناسه افزوده	: جعفرنژاد قمی، عین‌الله، ۱۳۳۹ - ، مترجم.
رده‌بندی کنگره	: ۱۳۹۳ ۶ الف ۴۶ الف / ۵۹ / ۵۱۰۵ TK
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۳۵۷۹۳۴۰

علوم رایانه

www.olomrayaneh.net

بابل، صندوق پستی ۸۹۱-۴۷۱۳۵

تلفن : ۳۲۳۶۰۷۷۲ – ۰۱۱

مبانی امنیت شبکه (کاربردها و استانداردها)

تألیف: ویلیام استالینگز

ترجمه: عین‌الله جعفرنژاد قمی

چاپ اول

تابستان ۱۳۹۳

شمارگان: ۱۰۰۰ نسخه

قیمت: ۲۸۰۰۰ تومان

چاپ و صحافی: فرنگار رنگ

شابک : ۹۷۸-۶۰۰-۲۰۵-۰۷۰-۰

نشانی: بابل، خیابان شریعتی، مجتمع میلاد، واحد ۱۷

حروفچینی و صفحه‌آرایی : علوم رایانه

تهران، خیابان انقلاب، خیابان اردیبهشت، نبش وحید نظری ، شماره ۱۴۲ - تلفکس : ۶۶۴۰۰۲۲۰ – ۶۶۴۰۰۱۴۴

فهرست مطالب

پیش‌گفتار

"یک کتاب وجود دارد، بازرس. من آن را در اختیار شما گذاشتم، و نمی‌توانید شک داشته باشید که حاوی توضیحات کامل است".
- ماجراجویی از یال شیر، سر آرتور کانن دویل

در عصر حاضر از اتصال الکترونیک جهانی، از ویروس‌ها و هکرها، از استراق سمع الکترونیک و کلاهبرداری الکترونیک، امنیت بدون فوت وقت، یک موضوع مهم است. دو گرایش در کنار هم، موضوع این کتاب را از منافع حیاتی مطرح کرده‌اند. اول این‌که رشد انفجاری در سیستم‌های کامپیوتری و ارتباط آن‌ها از طریق شبکه‌ها، وابستگی سازمان‌ها و افراد بر اطلاعات ذخیره‌شده را افزایش داد. این موضوع به نوبه‌ی خود منجر به نیاز مبرم به حفاظت از داده‌ها و منابع در مقابل افشاشدن گردید، تا اصالت داده‌ها و پیام‌ها تضمین شود و سیستم‌ها در مقابل حملات مبتنی بر شبکه حفاظت شوند. دوم این‌که، نظام‌های رمزنگاری و امنیت شبکه بالغ شدند، که منجر به توسعه‌ی برنامه‌های کاربردی عملی برای اعمال امنیت شبکه گردید.

اهداف

هدف این کتاب، ارائه‌ی یک بررسی عملی از استانداردها و برنامه‌های کاربردی امنیت شبکه است. بر روی برنامه‌های کاربردی‌ای که به طور گسترده در اینترنت و شبکه‌های شرکت استفاده می‌شوند، و بر روی استانداردهایی (مخصوصاً استانداردهای اینترنت) که به طور گسترده مستقر شده‌اند، تأکید می‌شود.

مطالب جدید در ویراست پنجم

چهار سال پس از ویراست چهارم این کتاب، این حوزه شامل نوآوری‌ها و بهبودهایی بوده است. در این ویراست جدید، سعی می‌کنم این تغییرات را بررسی کنم و در عین حال کل این حوزه را به طور جامع پوشش دهم. برای شروع این فرآیند بازبینی، ویراست چهارم این کتاب به طور جامع توسط تعدادی از اساتید که در این حوزه تدریس و کار می‌کنند بررسی شده است. نتیجه این‌است‌که، در بسیاری از موارد، مطالب دقیق‌تر و روشن‌تر بیان شده‌اند، و توضیحات نیز بهبود پیدا کردند. فراتر از پالایش‌های انجام‌شده برای بهبود تعلیم و کاربرپسندی، تغییرات اساسی در سراسر کتاب حاصل شده است. مطالب بسیاری از فصل‌ها تحت همان عناوین قبلی، شدیداً بازبینی و مطالب جدیدی اضافه شدند. عمده‌ترین تغییرات به شرح ذیل است:

- **کنترل دسترسی به شبکه:** فصل جدیدی به "کنترل دسترسی به شبکه" می‌پردازد که حاوی مرور کلی به اضافه‌ی بحث درباره‌ی پروتکل احراز اصالت توسعه‌پذیر و IEEE 802.1X است.
- **امنیت بد:** بخش جدیدی که به موضوعات امنیت مرتبط با حوزه‌ی جدید رایانش ابری می‌پردازد.
- **SHA-3 :** یک فصل آنلاین، استاندارد جدید درهم‌سازی رمزنگاری، یعنی SHA-3 را پوشش می‌دهد، که در سال ۲۰۱۲ پذیرفته شد.
- **امنیت دستگاه سیار:** امنیت دستگاه سیار به عنوان جنبه‌ی مهمی از امنیت شبکه‌ی سازمان محسوب می‌شود. بخش جدیدی به این موضوع مهم می‌پردازد.

- **نرم‌افزار مغرض (بدافزار):** این فصل بر موضوعاتی غیر از ویراست چهارم تأکید دارد. به طور فزاینده‌ای مشاهده می‌شود که بدافزار نوع در پشتی و روت‌کیت توسط حملات مهندسی اجتماعی نصب می‌شوند (به جای آلودگی مستقیم ویروس و کرم کلاسیک). فیشینگ نیز بیش از گذشته مطرح است. این گرایش‌ها در این فصل منعکس شده‌اند.
- **برنامه‌ی درسی نمونه:** این کتاب حاوی مطالبی بیش از یک ترم تحصیلی است. بر این اساس، چندین نمونه از برنامه‌ی درسی نمونه برای اساتید فراهم شد که استفاده از کتاب را در زمان محدود (۱۶ یا ۱۲ هفته) امکان‌پذیر می‌سازد. این نمونه‌ها بر اساس تجربه‌ی واقعی اساتید در ویراست اول تهیه شده است.
- **اهداف آموزشی:** هر فصل با لیستی از اهداف آموزشی آغاز می‌گردد.

پشتیبانی از برنامه‌های درسی علوم کامپیوتر ACM/IEEE در ۲۰۱۳

این کتاب برای مخاطبان دانشگاهی و حرفه‌ای‌ها تهیه شده است. به عنوان یک کتاب درسی، هدف آن یک ترم درس رمزنگاری و امنیت شبکه برای رشته‌های علوم کامپیوتر، مهندسی کامپیوتر، و مهندسی الکترونیک است. هدف از تغییرات این کتاب پشتیبانی از نسخه‌های پیش‌نویس فعلی ACM/IEEE از ۲۰۱۳ است (CS2013). CS2013 امنیت و تضمین اطلاعات (IAS) را به پیشنهاد برنامه‌ی درسی، به عنوان حوزه‌های دانش در "بدنه‌ی علوم کامپیوتر از دانش" اضافه می‌کند. این سند می‌گوید که IAS اکنون به عنوان بخشی از پیشنهاد برنامه‌ی درسی است، زیرا IAS نقش حیاتی در آموزش علوم کامپیوتر دارد. CS2013 کل کار درس را به سه طبقه تقسیم می‌کند: "Core-Tier 1" (کل موضوعات باید در برنامه‌ی درسی باشند)، "Core-Tier 2" (تمام یا تقریباً تمام موضوعات باید گنجانده شوند)، و انتخابی (برای تأمین وسعت و عمق مطالب). در حوزه‌ی ISA، دوره‌ی CS2013 موضوعاتی درباره‌ی مفاهیم اساسی و امنیت شبکه در "Tier 1" و "Tier 2" و موضوعات رمزنگاری به عنوان موضوعات انتخابی پیشنهاد می‌کند. این کتاب درسی تقریباً تمام موضوعات لیست‌شده توسط CS2013 در این سه طبقه را دربردارد. این کتاب منبع خوبی برای مطالعه‌ی شخصی نیز هست.

طرح این کتاب

این کتاب در سه بخش تنظیم شده است:

- **بخش اول. رمزنگاری:** بررسی مختصر الگوریتم‌های رمزنگاری و پروتکل‌های مربوط به برنامه‌های کاربردی امنیت شبکه، از جمله رمزگذاری، توابع درهم‌سازی، احراز اصالت پیام، و امضاهای دیجیتال.
- **بخش دوم. برنامه‌های کاربردی امنیت شبکه:** ابزارهای مهم امنیت شبکه و برنامه‌های کاربردی را در بر می‌گیرد، مثل توزیع کلید، کربروس، گواهی‌های X.509v3، پروتکل احراز اصالت توسعه‌پذیر، S/MIME، امنیت IP، SSL/TLS، امنیت IEEE 802.11i WiFi و امنیت ابر.
- **بخش سوم. امنیت سیستم:** مسائل امنیتی سطح سیستم را بررسی می‌کند، از جمله تهدیدها و اقدامات متقابل بدافزارها و نفوذگران، و استفاده از فایروال‌ها.

این کتاب شامل تعدادی ویژگی‌های برنامه‌ی درسی است، از جمله استفاده از شکل‌ها و جدول‌ها برای روشن‌کردن مباحث. هر فصل حاوی لیستی از واژه‌های کلیدی، پرسش‌های مرور درس، مسأله‌های تکلیف، و پیشنهاداتی برای خواندن بیشتر است. این کتاب همچنین حاوی واژه‌نامه‌ی وسیع، سرنام‌های متداول و لیستی از مراجع است. علاوه‌براین، یک بانک آزمون برای اساتید مهیا است.

راهنمای پشتیبان استاد

هدف اصلی این کتاب، تبدیل آن به یک ابزار تدریس موثر برای این موضوع مهیج است. این هدف، هم در ساختار این کتاب و هم در مطالب پشتیبانی منعکس شده است. مطالب تکمیلی زیر به استاد کمک می‌کند:

- **راهنمای حل مسأله‌ها:** تمام پرسش‌های مرور درس و مسأله‌ها را حل می‌کند.
- **راهنمای پروژه‌ها:** تکالیف پروژه‌ی پیشنهادی برای تمام پروژه‌های مطرح‌شده در زیر.
- **اسلایدهای پاورپوینت:** مجموعه‌ای از اسلایدها که کل فصل‌ها را دربرمی‌گیرد و برای تدریس مناسب است.
- **بانک آزمون:** مجموعه‌ای از سوالات فصل به فصل در فایل‌های مجزا از پاسخ‌ها.
- **برنامه‌ی درسی نمونه:** مطالب کتاب بیش از حدّی است که بتوان آن را در یک ترم ارائه کرد. بر این اساس، چند نمونه از برنامه‌ی درسی ارائه شد که امکان استفاده از کتاب را در مدت زمان محدود فراهم می‌سازد. این نمونه‌ها بر اساس تجربه‌ی واقعی اساتید در ویراست دوم تهیه شده‌اند.

در تمام این مطالب پشتیبان در مرکز منابع استاد (IRC) برای این کتاب، وجود دارند، که از طریق وب‌سایت ناشر کتاب (اصلی) به آدرس www.pearsonhighered.com/stallings یا با کلیک‌کردن بر روی لینک "Pearson Resources for Instructors" در وب‌سایت کتاب با آدرس WilliamStallings.com/NetworkSecurity قابل دسترسی است. برای دسترسی به IRC از طریق سایت زیر:

pearsonhighered.com/educator/replocator/requestSalesRep.page

یا تماس با بخش سرویس با تلفن 1-800-526-0485 اقدام کنید.

وب‌سایت کتاب با آدرس WilliamStallings.com/NetworkSecurity حاوی موارد ذیل است:

- لینک‌هایی به وب‌سایت‌های دروس دیگری که با استفاده از این کتاب تدریس می‌شوند.
- اطلاعات ثبت‌نام برای لیست پستی اینترنتی برای اساتیدی که از این کتاب استفاده می‌کنند (برای مبادله‌ی اطلاعات، پیشنهادات، و سوال از یکدیگر و سوال از مولف).

پروژه‌ها و سایر تمرین‌های دانشجو

برای بسیاری از اساتید، یک بخش مهم از درس امنیت شبکه، پروژه یا مجموعه‌ای از پروژه‌ها است که دانشجویان از طریق آن تجربه کسب می‌کنند یا مفاهیم درسی را یاد می‌گیرند. این کتاب از پروژه‌ها نیز استفاده می‌کند. IRC حاوی مجموعه‌ای از پروژه‌ها و رهنمودهایی درباره‌ی آن‌ها است که موضوعات وسیعی از کتاب را دربرمی‌گیرد:

- **پروژه‌ی هک‌کردن:** این تمرین طراحی شد تا مسائل مهم در تشخیص و پیشگیری از نفوذ را روشن سازد.
- **تمرین‌های آزمایشگاهی:** مجموعه‌ای از پروژه‌ها که شامل برنامه‌سازی و کسب تجربه با مفاهیم کتاب است.
- **پروژه‌های تحقیقاتی:** مجموعه‌ای از تکالیف تحقیقاتی که دانشجو را وادار می‌کند موضوع خاصی را در اینترنت تحقیق کند و گزارش بنویسد.
- **پروژه‌های برنامه‌سازی:** مجموعه‌ای از پروژه‌های برنامه‌سازی که بازه‌ی وسیعی از موضوعات را دربرمی‌گیرد که می‌تواند در هر زبان مناسبی در هر پلتفرم پیاده‌سازی شود.
- **ارزیابی‌های امنیت عملی:** مجموعه‌ای از تمرین‌ها برای بررسی اعمال و زیرساخت فعلی سازمان موجود است.

- **پروژه‌های فایروال:** یک شبیه‌ساز مجازی‌سازی فایروال شبکه‌ی قابل حمل، همراه با تمرین‌هایی برای تدریس مفاهیم اساسی فایروال‌ها است.
- **مطالعات موردی:** مجموعه‌ای از مطالعات موردی دنیای واقعی، شامل اهداف یادگیری، توصیف مورد، و مجموعه‌ای از پرسش‌های مباحثه‌ای است.
- **تکالیف نوشتاری:** مجموعه‌ای از تکالیف نوشتاری پیشنهادی که بر اساس فصل‌ها سازمان‌دهی شده‌اند.
- **تکالیف خواندنی/گزارش‌نویسی:** لیستی از مقالات در متون (برای هر فصل یک مقاله) که دانشجو باید آن‌ها را بخواند و تحلیل کند و گزارش کوتاهی ارائه دهد.

این مجموعه‌ی متنوع از پروژه‌ها و سایر تمرین‌های دانشجویی، استاد را قادر می‌سازد از این کتاب به عنوان یک منبع غنی استفاده نماید و برنامه‌ی درسی را تنظیم کند. جزییات این پروژه‌ها در پیوست (ب) آمده است.

اسناد آنلاین برای دانشجویان

برای این ویراست جدید، منابع و اسناد متعددی به صورت آنلاین برای دانشجویان در وب‌سایت ارائه می‌شود. وب‌سایت با آدرس WilliamStallings.com/NetworkSecurity (و کلیک‌کردن بر روی لینک **Student Resources Link**)، حاوی لیستی از لینک‌های مرتبط است که بر اساس فصل سازمان‌دهی شد و لیست خطاهای کتاب نیز در آن آمده است.

دانشجویان با خرید این کتاب شش ماه می‌توانند به وب‌سایت **"Premium Content"** دسترسی داشته باشند که حاوی مطالب زیر است:

- **فصل‌های آنلاین:** برای صرفه‌جویی در حجم و هزینه‌ی کتاب، سه فصل از کتاب با فرمت PDF ارائه شده است. این فصل‌ها شامل فصل درباره‌ی SHA-3، فصلی درباره‌ی امنیت SNMP و فصلی درباره‌ی موضوعات قانونی و اخلاقی است.
- **پیوست‌های آنلاین:** موضوعات جالبی وجود دارد که از مطالب کتاب پشتیبانی می‌کند ولی در نسخه‌ی چاپی نیامده است. تعدادی از پیوست‌های آنلاین این موضوعات را برای دانشجویان علاقمند، ارائه می‌کند.
- **جواب‌های مسأله‌های تکلیف:** برای کمک به دانشجو در درک مطالب، مسأله‌های جداگانه‌ای همراه با حل آن‌ها ارائه شد، که به دانشجویان کمک می‌کند تا مطالب کتاب را بیاموزند.
- **مقالات کلیدی:** تعدادی از مقالات از متون حرفه‌ای، که یافتن آن‌ها دشوار است، برای خواندنی‌های بیشتر ارائه شده است.
- **اسناد پشتیبان:** اسناد متنوع دیگری که در کتاب به آن‌ها مراجعه شد، به صورت آنلاین وجود دارد.

برای دسترسی به سایت **"Premium Content"**، لینک **"Premium Content"** را در وب‌سایت کتاب یا در pearsonhighered.com/Stallings کلیک کنید و کد دسترسی دانشجو را در کارتی که در جلوی کتاب است وارد کنید.