
آشنایی با

مبانی امنیت شبکه (امنیت اطلاعات)

تألیف:

مهندس رمضان عباس نژاد و رزی

مهندس آتنا فرحی



فن آوری نوین

سرشناسه
عنوان و نام پدیدآور : آشنایی با مبانی امنیت شبکه (امنیت اطلاعات) / تألیف رمضان
عباس نژادورزی، آتنا فرجی
مشخصات نشر : بابل: فن آوری نوین، ۱۳۸۹
مشخصات ظاهری : ۱۹۲ ص. مصور، جدول.
شابک : ۶۰۰۰۰ ریال: ۹۷۸۶۰۰۹۱۴۱۳۸۸
وضعیت فهرست نویسی : فیا
پاداشت : کتابنامه
موضوع : شبکه های کامپیوتری -- اقدامات تأمینی
موضوع : کامپیوترها -- ایمنی اطلاعات
شناسه افزوده : فرجی، آتنا، ۱۳۶۱-
رده بندی کنگره : TK۵۱۰۵/۵۹/ع۲۱۵ ۱۳۸۹
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۲۱۸۴۶۶۸

www.fanavarinovin.net

تلفن: ۰۱۱۱-۲۲۵۶۶۸۷

بابل، کدپستی ۴۷۱۹۷-۷۳۴۴۸



فن آوری نوین

آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)

تألیف: مهندس رمضان عباس نژادورزی - مهندس آتنا فرجی

نوبت چاپ: چاپ اول

سال چاپ: زمستان ۱۳۸۹

شمارگان: ۱۰۰۰ جلد

قیمت: ۶۰۰۰ تومان

نام چاپخانه و صحافی: فرنگاررنگ

شابک: ۹۷۸ - ۶۰۰ - ۹۱۴۱۳ - ۸ - ۸

نشانی ناشر: بابل، چهارراه نواب، کاظم بیگی، جنب حسینیه منصور کاظم بیگی، طبقه همکف

طراح جلد: کانون آگهی و تبلیغات آبان (احمد فرجی)

تهران، خ اردیبهشت، پش وحید نظری، پلاک ۱۴۲ تلفکس: ۶۶۴۰۰۱۴۴-۶۶۴۰۰۲۲۰

فهرست مطالب

فصل اول: مقدمه‌ای بر امنیت

- ۱-۱. اهمیت امنیت اطلاعات ۹
- ۱-۲. مقایسه امنیت اطلاعات در گذشته و حال ۱۲
- ۱-۳. مهاجمان و انگیزه‌ها ۱۲
- ۱-۴. مفاهیم اولیه امنیت اطلاعات ۱۳
- ۱-۵. حمله ۱۴
- ۱-۵-۱. حمله غیر فعال ۱۴
- ۱-۵-۲. حملات فعال ۱۶
- ۱-۶. سرویس امنیتی ۱۸
- ۱-۶-۱. سرویس‌های امنیتی X.800 ۱۸
- ۱-۶-۲. مکانیزم‌های امنیتی ۲۰
- ۱-۷. یک مدل امنیت شبکه ۲۱
- ۲-۱. مدل رمزگذاری متقارن ۲۳
- ۲-۲. رمز نویسی ۲۵
- ۲-۳. رمز شکنی خطی ۲۶
- ۲-۳-۱. رمز شکنی خطی ۲۶
- ۲-۳-۲. حمله جستجوی جامع ۲۷
- ۲-۴. روش‌های کلاسیک رمزگذاری متقارن ۲۹
- ۲-۴-۱. روش‌های جانشینی ۲۹
- ۲-۴-۲. روش‌های انتقال ۳۷

فصل دوم: رمزگذاری‌های کلاسیک

- ۳-۱. الگوریتم رمزگذاری فستل ۴۷
- ۳-۲. الگوریتم رمزگذاری استاندارد (DES) ۴۸
- ۳-۲-۱. رمزگذاری DES ۴۹
- ۳-۲-۲. جایگشت اولیه ۵۰
- ۳-۲-۳. جزئیات یک مرحله از DES ۵۱
- ۳-۲-۴. رمز گشایی DES ۵۴
- ۳-۲-۵. خاصیت بهمنی DES ۵۴
- ۳-۲-۶. امنیت DES ۵۴
- ۳-۲-۷. رمز شکنی DES ۵۵
- ۳-۵. رمز AES ۵۶
- ۳-۶. الگوریتم RC4 ۵۸
- ۳-۷. الگوریتم RC5 ۵۹
- ۳-۸. الگوریتم رمزگذاری نامتقارن (کلید عمومی) ۶۰
- ۳-۸-۱. انواع حملات به سیستم‌های رمز نامتقارن ۶۱
- ۳-۹. الگوریتم RSA ۶۱
- ۳-۹-۱. تولید کلید در الگوریتم RSA ۶۲
- ۳-۹-۲. محاسبه از الگوریتم RSA ۶۲
- ۳-۹-۳. نکاتی در رابطه با تولید کلید ۶۲

فصل چهارم: امنیت شبکه و محیط کاری

- ۴-۱. دسترسی افراد غیر مجاز در شبکه ۶۳
- ۴-۱-۱. اتصالات فیزیکی شبکه ۶۳
- ۴-۱-۲. سرور و زیر ساخت مرکزی و اصلی ۶۵
- ۴-۱-۳. کامپیوترهای رومیزی ۶۶
- ۴-۲. تخریب داده‌ها در شبکه ۶۷
- ۴-۳. برقراری امنیت محیط کاری ۶۷
- ۴-۳-۱. لیست کنترل امنیتی برای سازمان‌ها ۶۷
- ۴-۳-۲. چک لیست امنیت شخصی ۶۸

فصل سوم: رمزگذاری‌های پیشرفته

مقارن و نامتقارن

- ۳-۱. رمزگذاری‌های پیشرفته ۴۳
- ۳-۲. رمزگذاری بلوکی ۴۳
- ۳-۲-۱. اصول رمزهای بلوکی ۴۳
- ۳-۲-۲. رمزکننده دنباله‌ای و بلوکی ۴۳
- ۳-۲-۳. هدف ساختار رمزکننده فستل ۴۴
- ۳-۳. رمز فستل ۴۶
- ۳-۳-۱. ساختار رمز فستل ۴۶

۴-۴. ایجاد محرمانگی با استفاده از

رمزگذاری ۷۷

۴-۴-۱. روش‌های رمزگذاری به منظور

جلوگیری از حملات ۷۸

فصل پنجم: بد افزار

۵-۱. ویروس ۸۰

۵-۲. کرم ۸۱

۵-۳. تروجان ۸۱

۵-۴. نرم افزار Bonus ۸۱

۵-۵. انواع عملیات نرم‌افزار مخرب

(بد افزار) ۸۲

۵-۶. محیط‌های هدف بد افزارها ۸۴

۵-۷. مکانیزم‌های انتشار بد افزارها ۸۵

۵-۸. روت‌کیت ۸۶

۵-۹. بات نت ۸۷

۵-۱۰. زامبی ۸۷

۵-۱۱. ماکرو ویروس‌ها ۸۷

۵-۱۲. ویروس‌های پست الکترونیکی ۸۸

۵-۱۳. روش‌های پیشگیری از ویروس ۸۹

۵-۱۳-۱. آنتی ویروس ۸۹

۵-۱۳-۲. تکنیک‌های پیشرفته آنتی

ویروس ۹۱

فصل ششم: فایروال

۶-۱. فایروال‌ها چگونه کار می‌کنند؟ ۹۶

۶-۲. اصول طراحی فایروال ۹۶

۶-۳. ویژگی‌های فایروال ۹۷

۶-۴. محدودیت‌های فایروال ۹۹

۶-۵. مشخصات فایروال قوی ۹۹

۶-۶. موفقیت‌یابی برای فایروال ۱۰۰

۶-۷. انواع فایروال ۱۰۱

۶-۷-۱. مسیریاب فیلتر بسته ۱۰۱

۶-۷-۲. دروازه سطح کاربرد ۱۰۳

۳-۷-۶. دروازه سطح مدار ۱۰۳

۸-۶. فایروال‌های شخصی ۱۰۴

۹-۶. امکانات فایروال برای مدیران شبکه ۱۰۴

۱۰-۶. نصب نرم‌افزار فایروال Plus در

ویندوز ۷ ۱۰۴

۱۱-۶. راهنمای استفاده از نرم‌افزار ۱۰۷

فصل هفتم: امنیت در تجارت الکترونیک

۱-۷. لایه سوکت امن (SSL) ۱۱۴

۲-۷. تراکنش الکترونیکی امن ۱۱۵

۳-۷. امنیت لایه انتقال (TLS) ۱۱۶

۴-۷. امضای دیجیتال ۱۱۷

۱-۴-۷. انواع امضای دیجیتال ۱۱۸

۵-۷. ایمن سازی شبکه‌های تجارت

الکترونیک ۱۲۲

۶-۷. امنیت کارت‌های اعتباری ۱۲۲

۷-۷. امنیت کارت‌های اعتباری مجازی ۱۲۳

۸-۷. امنیت کارت هوشمند ۱۲۳

۹-۷. نکات امنیتی در هنگام استفاده از

کارت‌های هوشمند ۱۲۴

۱۰-۷. سرویس‌های امنیت پرداخت ۱۲۴

۱-۱۰-۷. سرویس‌های امنیت تراکنش

پرداخت ۱۲۵

۲-۱۰-۷. سرویس‌های امنیت پول دیجیتال ۱۲۶

۳-۸-۷. سرویس‌های پرداخت چک

الکترونیک ۱۲۷

فصل هشتم: سرویس‌ها و برنامه‌های کاربردی امنیت اطلاعات

۱-۸. سرویس‌های امنیت پست الکترونیک ۱۲۸

۱-۱-۸. سرویس PGP ۱۲۸

۲-۱-۸. سرویس توسعه پست

الکترونیک چند منظوره (S/MIME) ۱۳۲

۱۱-۸ پروتکل مدیریت شبکه آسان	۲-۸ امنیت معماری IP..... ۱۳۵
(SNMP)..... ۱۶۱	۳-۸ کنترل دسترسی داده..... ۱۳۶
۱-۱۱-۸ فرامین پایه در SNMP..... ۱۶۱	۴-۸ سیستم زیست سنجی..... ۱۳۸
۲-۱۱-۸ پایگاه اطلاعات مدیریتی در	۱-۴-۸ خصوصیات رفتاری..... ۱۳۹
(MIB) SNMP..... ۱۶۲	۲-۴-۸ خصوصیات فیزیکی..... ۱۴۰
فصل نهم: هرزتماس و هرزنامه	۵-۸ احراز هویت..... ۱۴۱
۱-۹. مقایسه هرزتماس و هرزنامه..... ۱۶۴	۱-۵-۸ ملزومات احراز هویت..... ۱۴۱
۲-۹. علل گسترش هرزتماس..... ۱۶۵	۲-۵-۸ توابع احراز هویت..... ۱۴۲
۳-۹. انواع هرزتماس..... ۱۶۷	۳-۵-۸ رمزگذاری پیام..... ۱۴۲
۴-۹. هزینه‌های هرزتماس..... ۱۶۸	۶-۸. کد احراز هویت پیام (MAC)..... ۱۴۷
۵-۹. تبعات هرزتماس..... ۱۶۸	۷-۸ تابع درهم‌ساز..... ۱۴۹
۶-۹. معیارهای تشخیص هرزتماس..... ۱۶۹	۱-۷-۸ توابع درهم‌ساز..... ۱۵۰
۷-۹. مکانیزم‌های مقابله با هرزتماس‌ها..... ۱۷۰	۲-۷-۸. نیازمندی‌های تابع درهم‌ساز..... ۱۵۰
پیوست: پرسش‌های چهارگزینه‌ای ۱۷۳	۳-۷-۸ توابع درهم‌ساز ساده..... ۱۵۲
پاسخ تست: ۱۸۵	۴-۷-۸ الگوریتم درهم‌ساز امن..... ۱۵۳
واژه نامه: ۱۸۶	۸-۸ حمله روز تولد..... ۱۵۴
منابع: ۱۹۲	۹-۸ برنامه‌های کاربردی امنیت شبکه..... ۱۵۵
	۱-۹-۸ کربروس..... ۱۵۵
	۱۰-۸ امنیت IP..... ۱۵۸
	۱-۱۰-۸ کاربردهای امنیت IP (IPSec)..... ۱۵۹

دیگر آثار مولف

نام کتاب	انتشارات	نام کتاب	انتشارات
حل مسائل C (مرجع کامل)	فن آوری نوین	آموزش گام به گام Crystal Report	علوم رایانه
حل مسائل C++ (مرجع کامل)	فن آوری نوین	آشنایی با شبکه GSM	علوم رایانه
آموزش گام به گام برنامه نویسی بانک اطلاعات با C# (مرجع کامل)	فن آوری نوین	آموزش گام به گام سیستم عامل لینوکس	علوم رایانه
حل مسائل C# (مرجع کامل)	فن آوری نوین	خود آموز اکسس	علوم رایانه
حل مسائل پایسکال (مرجع کامل)	فن آوری نوین	آموزش گام به گام Word	علوم رایانه
آموزش گام به گام برنامه نویسی بانک اطلاعات با ویژوال بیسیکنت (مرجع کامل)	فن آوری نوین	آموزش گام به گام اکسل	علوم رایانه
آموزش گام به گام برنامه نویسی LING با C# (مرجع کامل)	فن آوری نوین	ICDL مهارت ۱: مفاهیم پایه اطلاعات	علوم رایانه
تجارت الکترونیکی	فن آوری نوین	ICDL مهارت ۲: به کارگیری کامپیوتر و مدیریت	علوم رایانه
آموزش گام به گام برنامه ویژوال بیسیک	علوم رایانه	ICDL مهارت ۳: واژه پردازی به کمک کامپیوتر	علوم رایانه
آموزش گام به گام برنامه ویژوال بیسیکنت	علوم رایانه	ICDL مهارت ۴: صفحات گسترده	علوم رایانه
برنامه نویسی به زبان اسمبلی	علوم رایانه	ICDL مهارت ۵: پایگاه داده	علوم رایانه
برنامه نویسی با دلفی	علوم رایانه	ICDL مهارت ۶: ارائه مطلب	علوم رایانه
آموزش گام به گام دلفی نت	علوم رایانه	ICDL مهارت ۷: اطلاعات و ارتباطات	علوم رایانه
آموزش گام به گام C#.NET	علوم رایانه	آموزش گام به گام FLASH MX	علوم رایانه
آموزش گام به گام VisualC++ .NET	علوم رایانه	درس و کنکور برنامه نویسی به زبان C	علوم رایانه
آموزش گام به گام برنامه نویسی با ویژوال C++	علوم رایانه	برنامه سازی سیستم	علوم رایانه
آموزش گام به گام J#.NET	علوم رایانه	پرسش های چهار گزینه ای پاسکال	علوم رایانه
آموزش گام به گام SQL Server	علوم رایانه	آموزش گام به گام VC++	علوم رایانه
آموزش گام به گام SQL	علوم رایانه	کارور رایانه ۱	علوم رایانه
رهیافت و پرسش های چهار گزینه ای C	علوم رایانه	کارور رایانه ۲	علوم رایانه
رهیافت و پرسش های چهار گزینه ای C++	علوم رایانه	مبانی فناوری اطلاعات	علوم رایانه
نست و پرسش های چهار گزینه ای C	علوم رایانه		

مقدمه

امروزه اینترنت و یکی از مهم‌ترین مدل‌های ارتباطی در آن، یعنی شبکه جهانی وب (World Wide Web)، تغییرات اساسی در زندگی و روابط بین انسان‌ها ایجاد کرده است. به طوری که در عصر اطلاعات، فعالیت‌هایی از قبیل اطلاع رسانی، کسب و کار و تجارت، مدیریت و غیره به صورت مجازی انجام می‌شوند. فضای مجازی، در معرض چالش‌ها، آسیب‌ها و تهدیدهای مختلفی از قبیل تخریب اطلاعات، جاسوسی، خراب‌کاری، نقض حریم خصوصی، حملات انکار سرویس و دسترسی غیرمجاز می‌باشد. از طرف دیگر، کلیه کاربردهای فناوری اطلاعات مانند دولت الکترونیک، کسب‌وکار الکترونیک، تجارت الکترونیک، بانکداری الکترونیک، سلامت الکترونیک و دیگر کاربردها نیاز به زیرساخت اینترنت و شبکه‌های کامپیوتری دارند.

بی‌شک هیچ یک از این کاربردها بدون وجود امنیت نمی‌توانند مورد استفاده قرار گیرند. ایجاد امنیت در شبکه‌های کامپیوتری و اینترنت به امر خطیری تبدیل شده است، به طوری که در رشته‌های فناوری اطلاعات (IT) و فناوری اطلاعات و ارتباطات (ICT) درسی به نام آشنایی با مبانی امنیت شبکه تدوین شده است.

کتاب حاضر براساس سال‌ها تجربه در زمینه تألیف کتب دانشگاهی و تدریس طراحی گردید. این کتاب براساس سر فصل جدید وزارت علوم، تحقیقات و فناوری اطلاعات برای درس‌های آشنایی با مبانی امنیت شبکه، امنیت اطلاعات و امنیت شبکه در رشته‌های IT و ICT تدوین شده است.

در پایان امیدواریم این اثر نیز مورد توجه اساتید و دانشجویان عزیز قرار گیرد.

از تمامی عزیزانی که در جمع‌آوری این اثر ما را یاری نمودند، صمیمانه تشکر می‌کنیم.

بابل، زمستان ۱۳۸۹

مؤلفین

www.Fanavarienovin.net