

سرشناسه: هاسلر، وسنا
 Hassler, Vesna
 عنوان و نام پدیدآور: اصول امنیت برای تجارت الکترونیکی/ نویسنده وسنا هاسلر؛ ترجمه آرش حبیبی لشکری، یاشار علی مجدزاده،
 مجدتقی فرامرزی.
 مشخصات نشر: تهران : علوم ایران ، ۱۳۹۵ .
 مشخصات ظاهری : ۲۱۲ص.؛ مصور ، جدول ، نمودار .
 شابک : ۹۷۸-۹۶۴-۲۷۵۰۰۵۱-۱
 وضعیت فهرست نویسی: فیبا
 بادداشت: عنوان اصلی: Security fundamentals for e-commerce.
 موضوع: بازرگانی الکترونیکی -- تدابیر ایمنی
 موضوع: Electronic commerce -- Security measures
 موضوع: سامانه‌های ارتباطی باند پهن
 موضوع: Broadband communication systems
 شناسه افزوده: علی مجدزاده، یاشار، ۱۳۷۰ - مترجم
 شناسه افزوده: فرامرزی، محمدتقی، ۱۳۳۹ - مترجم
 شناسه افزوده: حبیبی لشکری، آرش، ۱۳۵۳ - مترجم
 رده بندی کنگره: ۱۳۹۵ ۶۱۷/۳۳/ HF۵۵۴۸
 رده بندی دیویی: ۶۸۵/۸۴
 شماره کتابشناسی ملی: ۲۴۲۳۲۳۸



انتشارات علوم ایران

انتشارات علوم ایران: تهران - تلفن ۰۹۱۲۵۳۶۷۶۲۱ و ۶۶۸۷۵۴۴۹

صندوق پستی: تهران ۳۵۳ - ۱۳۱۴۵

www.olomiran.net

نام کتاب: اصول امنیت برای تجارت الکترونیکی نویسنده: وسنا هاسلر
 ترجمه: دکتر آرش حبیبی لشکری - مهندس یاشار علی مجدزاده - مهندس محمدتقی فرامرزی
 ناشر: علوم ایران
 نوبت و سال چاپ: سوم - ۱۴۰۱
 تیراژ: ۵۰ نسخه
 انتشارات علوم ایران
 ۹۶۴ - ۹۷۸
 ۲۵۰ هزار تومان

مرکز پخش:

کتاب کوشا - میدان انقلاب، ابتدای کارگر جنوبی، کوچه رشتچی، پن بست یکم،

پلاک ۴ طبقه دوم واحد ۴ تلفن همراه: ۰۹۱۲۳۰۳۳۰۵۸

تلفن: ۶۶۹۴۱۱۶۷ و ۶۶۹۴۱۰۳۴ فکس: ۶۶۹۴۱۶۸۵

خرید آنلاین: ketabmail.com

هرگونه کپی برداری و یا تکثیر و یا انتشار و یا شبیه سازی 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

هر یک چندی یکی برآید که منم با نعمت و با سیم و زر آید که منم
چون کارک او نظام گیرد روزی ناگه اجل از کمین برآید که منم

انتشارات علوم ایران در تلاش است تا کُتبی 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

مدیر انتشارات علوم ایران

پیش‌گفتار

سخن مترجمین

امروزه اهمیت و جایگاه تجارت الکترونیکی و امنیت آن نه تنها برای متخصصین علوم رایانه و الکترونیکی بلکه برای عموم اقشار جامعه نیز پوشیده نیست. چراکه، بی شک در دنیای الکترونیکی امروز از یک سو تجارت الکترونیکی با سرعت زیاد به عضوی جدانشدنی در زندگی روزمره ما بدل گردیده و از طرف دیگر امنیت در دنیای الکترونیکی نیز مهم ترین و غیر قابل انکارترین چالش موجود به شمار می‌رود.

کتاب حاضر ترجمه ویرایش اول کتاب "اصول امنیت برای تجارت الکترونیکی" بقلم دکتر وسنا هسلر از دانشگاه وین اتریش به همراه کلیه منابع و مواخذ مورد استفاده در هر فصل می‌باشد.

مزیت عمده این کتاب نسبت به سایر کتب مشابه این است که در این کتاب نویسنده در پنج بخش به بررسی کامل و جامع امنیت در تجارت الکترونیکی پرداخته است. در بخش اول موضوع امنیت اطلاعات با تمرکز بر سرویس‌ها و مکانیزم‌های امنیتی مرتبط و همچنین مدیریت کلیدها و گواهی‌نامه‌ها مورد بررسی قرار می‌گیرد. سپس در بخش دوم امنیت تجارت الکترونیکی با بررسی امنیت تراکنش‌ها، پول و چک الکترونیکی مورد تحلیل قرار گرفته و یک چارچوب استاندارد امنیتی برای پرداخت‌های الکترونیکی معرفی می‌گردد. بخش سوم کتاب با تکیه بر مفاهیم امنیت شبکه برپایه لایه‌های دسترسی شبکه، انتقال، اینترنت و کاربردی به بررسی پروتکل‌ها و حملات مرتبط از دیدگاه تجارت الکترونیکی در این لایه‌ها خواهد پرداخت. بخش چهارم کتاب موارد مرتبط با امنیت وب را با تکیه بر امنیت سرویس‌دهندگان و سرویس‌گیرندگان وب بررسی نموده و بخش پایانی کتاب با هدف معرفی مفاهیم نوین امنیتی سعی نموده تا امنیت تجارت برپایه عامل‌های موبایل و کارت‌های هوشمند را مورد کندوکاو قرار دهد.

در هر فصل برای درک بهتر و عمیقتر مفاهیم کتاب و سایر مطالب مشابه در زمینه امنیت تجارت الکترونیکی به زبان انگلیسی بخشی باعنوان کلمات کلیدی و اختصارها در نظر گرفته شده و همچنین منابع مختلف جهت مطالعه و درک بهتر مفاهیم و مطالب مرتبط با هر فصل نیز گردآوری 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، درخواست ما از خوانندگان عزیز به ویژه همکاران، اساتید محترم و دانشجویان گرامی اینست که نظرات و پیشنهادهای 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 سپاس

فروردین ۱۳۹۶

درباره مولفین

وسنا هسلر، لیسانس و فوق لیسانس خود را در رشته مهندسی الکترونیکی از دانشگاه زاگرب، کرواسی در سال‌های 1988 و 1991 گرفت. از 1989 تا 1992 به عنوان دستیار تحقیقاتی در دپارتمان ارتباطات راه دور در دانشکده مهندسی الکترونیکی و کامپیوتر دانشگاه زاگرب کار کرد. از 1992 تا 1996 دستیار تحقیقاتی در موسسه ارتباطات و پردازش اطلاعات کاربردی در دانشگاه فن‌آوری گراس کشور اتریش بود، همان دانشگاهی که دکترای خود را نیز در رشته مهندسی کامپیوتر و ارتباطات در دسامبر 1995 از آنجا گرفت. از ژوئن 1996 او عضو گروه سیستم‌های توزیع شده دانشگاه فنی وین اتریش است.

علايق تحقیقاتی فعلی دکتر هسلر شامل امنیت شبکه، زیرشاخه سرویس‌ها و سیستم‌های پرداخت الکترونیکی می‌باشد. وی همچنین شبکه و امنیت تجارت الکترونیکی نیز تدریس می‌کند. از 1996 تا 2000 او دو پروژه تحقیق و توسعه را مدیریت کرده است (استدلال معماری برای سیستم‌های توکار یا ARES بعنوان چهارمین پروژه چارچوب کاری اروپایی #20477# و پروژه انطباق سیاست‌های امنیتی تقویت شده میان عامل‌ها یا SPARTA، چهارمین پروژه چارچوب کاری اروپایی #12637#). از سال 1989 وی چندین مقاله در زمینه سیستم‌های کنترل ارتباطات راه دور، رمزنگاری، امنیت شبکه، سیستم‌های پرداخت، و کارت‌های هوشمند در کنفرانس‌ها و ژورنال‌های بین‌المللی منتشر نموده است. دکتر هسلر همچنین بعنوان مشاور در یک پروژه زیرساخت کلیدعمومی در بانک ملی اتریش و راهبر بانک‌های تجاری اتریش نیز فعالیت داشته است (A-trust).

پدريکا مور، ویرایشگر فنی این کتاب، یک مشاور زبان با 20 سال تجربه در آموزش زبان انگلیسی برای افراد غیربومی است. او فارغ التحصیل دانشگاه ویرجینیا (آلمان) بوده و کار ترجمه و ویرایش انتشارات تجاری، تحقیق‌ها و مقالات دانشگاهی و فیلم نامه‌ها را انجام می‌دهد. مشتریان وی شامل شرکت‌ها، موسسات تحقیقاتی، دانشگاهی، هنرمندان و متخصصین می‌باشند. ایشان زمان‌های کاری خود را بین وین و یک تاستان در جنوب انگلستان تقسیم می‌کند.

فهرست مطالب

پیشگفتار / ۱۵

بخش اول: امنیت اطلاعات

فصل اول: مقدمه‌ی بر امنیت / ۲۰

۱.۱ تهدیدهای امنیتی / ۲۰

۲.۱ مدیریت ریسک / ۲۰

۳.۱ سرویس‌های امنیتی / ۲۱

۴.۱ مکانیزم‌های امنیتی / ۲۲

۵.۱ منابع پیشنهادی / ۲۴

فصل دوم: مکانیزم‌های امنیتی / ۲۶

۱.۲ مکانیزم‌های یکپارچگی داده / ۲۶

۱.۱.۲ توابع هش رمزنگاری شده / ۲۶

۲.۱.۲ کد احراز هویت پیام / ۲۸

۲.۲ مکانیزم‌های رمزنگاری / ۲۹

۱.۲.۲ مکانیزم‌های متقارن / ۲۹

۲.۲.۲ مکانیزم‌های کلیدعمومی / ۳۶

۳.۲ مکانیزم‌های امضاء دیجیتال / ۴۴

۱.۳.۲ امضاء دیجیتال RSA / ۴۵

۲.۳.۲ الگوریتم امضاء دیجیتال / ۴۵

۳.۳.۲ قیاس منحنی بیضوی DSA / ۴۷

۴.۳.۲ مدیریت کلیدعمومی / ۴۷

۴.۲ مکانیزم‌های کنترل دسترسی / ۴۸

۱.۴.۲ کنترل دسترسی مبتنی بر هویت / ۴۸

۲.۴.۲ کنترل دسترسی مبتنی بر قانون / ۴۸

۵.۲ مکانیزم‌های تبادل احراز هویت / ۴۹

۱.۵.۲ پروتکل دانش صفر / ۴۹

۲.۵.۲ کوئیز کواتر / ۵۰

۶.۲ مکانیزم‌های لایه‌گذاری ترافیک / ۵۱

۷.۲ تازگی پیام / ۵۱

۸.۲ اعداد تصادفی / ۵۱

۹.۲ منابع پیشنهادی / ۵۲

فصل سوم: مدیریت کلید و گواهی‌نامه‌ها / ۵۴

۱.۳ پروتکل‌های تبادل کلید / ۵۴

۱.۱.۳ دیفی-هلمن / ۵۴

۲.۱.۳ قیاس منحنی بیضوی دیفی-هلمن / ۵۵

۲.۳ زیرساخت کلیدعمومی / ۵۵

۱.۲.۳ فرمت گواهی X.509 / ۵۶

۲.۲.۳ زیرساخت کلیدعمومی اینترنتی / ۶۰

۳.۳ روش‌های کدگذاری / ۶۱

۴.۳ منابع پیشنهادی / ۶۲

بخش دوم: امنیت پرداخت الکترونیکی

فصل چهارم: سیستم‌های پرداخت الکترونیکی / ۶۶

۱.۴ تجارت الکترونیکی / ۶۶

۲.۴ سیستم‌های پرداخت الکترونیکی / ۶۷

۱.۲.۴ آنالیز در برابر آفلاین / ۶۷

۲.۲.۴ بدهکاری در برابر اعتبار / ۶۸

۳.۲.۴ خرد در برابر کلان / ۶۸

۴.۲.۴ ابزارهای پرداخت / ۶۹

۵.۲.۴ کیف پول الکترونیکی / ۷۲

۶.۲.۴ کارت‌های هوشمند / ۷۲

۳.۴ امنیت پرداخت الکترونیکی / ۷۳

۴.۴ منابع پیشنهادی / ۷۵

فصل پنجم: سرویس‌های امنیتی پرداخت / ۷۶

۱.۵ سرویس‌های امنیتی پرداخت / ۷۶

۱.۱.۵ امنیت تراکنش پرداخت / ۷۷

۲.۱.۵ امنیت پول الکترونیکی / ۷۹

۳.۱.۵ امنیت چک الکترونیکی / ۷۹

۲.۵ دسترس‌پذیری و قابلیت اطمینان / ۷۹

۳.۵ منابع پیشنهادی / ۸۰

فصل ششم: امنیت تراکنش پرداخت / ۸۲

۱.۶ گمنامی کاربر و عدم ردیابی مکانی / ۸۲

۱.۱.۶ زنجیره ترکیب‌ها / ۸۲

۲.۶ گمنامی پرداخت‌کننده / ۸۴

۱.۲.۶ نام‌های مستعار / ۸۴

۳.۶ عدم قابلیت ردیابی تراکنش‌های پرداخت / ۸۶

۱.۳.۶ استفاده از جمع هش تصادفی در IKB / ۸۶

۲.۳.۶ استفاده از جمع هش تصادفی در SET / ۸۶

۴.۶ محرمانگی داده‌های تراکنش پرداخت / ۸۷

۱.۴.۶ تابع شبه تصادفی / ۸۷

۲.۴.۶ امضای دوگانه / ۸۸

۵.۶ عدم انکار پیام‌های تراکنش پرداخت / ۹۰

۱.۵.۶ امضای دیجیتال / ۹۰

۶.۶ تازگی پیام‌های تراکنش پرداخت / ۹۲

۹۶ / شماره‌های یکبار مصرف و برچسب‌های زمان

۷۶ منابع پیشنهادی / ۹۴

فصل هفتم: امنیت پول دیجیتالی / ۹۶

۱.۷ عدم قابلیت ردیابی تراکنش پرداخت / ۹۶

۱.۱.۷ امضای کور یا ناخوانا / ۹۶

۲.۱.۷ سکه‌های مبادله / ۹۷

۲.۷ حفاظت در برابر خرج کردن مجدد / ۹۷

۱.۲.۷ گمنامی شرطی توسط بریدن - و - انتخاب کردن / ۹۸

۲.۲.۷ امضای کور / ۹۸

۳.۲.۷ مبادله سکه‌ها / ۹۸

۴.۲.۷ نگهبان / ۹۹

۱.۴.۲.۷ امضای نگهبان / ۹۹

۲.۴.۲.۷ امضای صادرکننده / ۱۰۱

۳.۷ حفاظت در برابر جعل سکه / ۱۰۲

۱.۳.۷ سکه‌هایی با هزینه تولید بالا / ۱۰۳

۴.۷ حفاظت در برابر دزدی سکه‌ها / ۱۰۳

۱.۴.۷ سکه‌های سفارشی شده / ۱۰۳

۱.۱.۴.۷ سکه‌های مختص - مشتری و همچنان گمنام / ۱۰۴

۲.۱.۴.۷ سکه‌های مختص - مشتری / ۱۰۵

۳.۱.۴.۷ سکه‌های مختص - مشتری و مختص - تاجر / ۱۰۶

۵.۷ منابع پیشنهادی / ۱۰۷

فصل هشتم: امنیت چک الکترونیکی / ۱۱۰

۱.۸ انتقال مجوز پرداخت / ۱۱۰

۱.۱.۸ پروکسی‌ها / ۱۱۰

۱.۱.۱.۸ کرپروس / ۱۱۱

۲.۱.۱.۸ پروکسی محدود شده / ۱۱۲

۳.۱.۱.۸ پروکسی آبخاری / ۱۱۲

۲.۸ منابع پیشنهادی / ۱۱۳

فصل نهم: یک چارچوب پرداخت الکترونیکی / ۱۱۴

۱.۹ پروتکل تجارت باز اینترنتی / ۱۱۴

۲.۹ مسائل امنیتی / ۱۱۵

۳.۹ یک مثال با امضاها دیجیتالی / ۱۱۶

۴.۹ منابع پیشنهادی / ۱۱۹

بخش سوم: امنیت ارتباط

فصل دهم: شبکه ارتباط / ۱۲۴

۱.۱۰ مقدمه / ۱۲۴

- ۱.۰ ۲.۰ مدل مرجع OSI / ۱۲۴
- ۱.۰ ۳.۰ مدل اینترنت / ۱۲۶
- ۱.۰ ۴.۰ تکنولوژی‌های شبکه / ۱۲۸
- ۱.۰ ۵.۰ امنیت در لایه‌های مختلف / ۱۳۰
- ۱.۰ ۵.۱ ضوابط انتخاب پروتکل / ۱۳۲
- ۱.۰ ۶.۰ برنامه‌های مخرب / ۱۳۳
- ۱.۰ ۶.۱ کرم اینترنت / ۱۳۳
- ۱.۰ ۶.۲ محتوای ماکرو و قابل اجرا / ۱۳۴
- ۱.۰ ۷.۰ مشکلات امنیتی ارتباطی / ۱۳۵
- ۱.۰ ۷.۱ تهدیدهای امنیتی / ۱۳۵
- ۱.۰ ۷.۲ گفتگوهای امنیتی / ۱۳۷
- ۱.۰ ۷.۳ پروتکل‌های پشتیبانی TCP/IP / ۱۳۸
- ۱.۰ ۷.۴ آسیب‌پذیری‌ها و نقص‌ها / ۱۳۸
- ۱.۰ ۸.۰ دیوار آتش / ۱۴۰
- ۱.۰ ۹.۰ شبکه خصوصی مجازی (VPN) / ۱۴۱
- ۱.۰ ۱۰.۰ منابع پیشنهادی / ۱۴۳

فصل یازدهم: امنیت لایه دسترسی شبکه / ۱۴۴

- ۱.۱۱ ۱.۱۴۴ مقدمه / ۱۴۴
- ۱.۱۱ ۲.۱۱ حالت انتقال غیرهمزمان (ATM) / ۱۴۵
- ۱.۱۱ ۱.۲.۱۱ سرویس‌های امنیتی ATM / ۱۴۷
- ۱.۱۱ ۲.۲.۱۱ امنیت چندبخشی / ۱۵۰
- ۱.۱۱ ۳.۲.۱۱ تبادل پیام امنیتی ATM / ۱۵۱
- ۱.۱۱ ۴.۲.۱۱ شبکه خصوصی مجازی ATM / ۱۵۱
- ۱.۱۱ ۳.۱۱ پروتکل نقطه - به - نقطه (PPP) / ۱۵۱
- ۱.۱۱ ۱.۳.۱۱ پروتکل احراز هویت رمز عبور / ۱۵۴
- ۱.۱۱ ۲.۳.۱۱ پروتکل CHAP / ۱۵۵
- ۱.۱۱ ۳.۳.۱۱ پروتکل احراز هویت توسعه‌پذیر (EAP) / ۱۵۶
- ۱.۱۱ ۴.۳.۱۱ پروتکل کنترل رمزنگاری / ۱۵۹
- ۱.۱۱ ۴.۱۱ پروتکل ایجاد تونل در لایه دوم (L2TP) / ۱۵۹
- ۱.۱۱ ۵.۱۱ منابع پیشنهادی / ۱۶۱

فصل دوازدهم: امنیت لایه اینترنت / ۱۶۴

- ۱.۱۲ ۱.۱۶۴ مقدمه / ۱۶۴
- ۱.۱۲ ۲.۱۶۴ فیلتر کردن بسته / ۱۶۴
- ۱.۱۲ ۱.۲.۱۶۴ فیلتر کردن بر اساس آدرس‌های شبکه / ۱۶۴
- ۱.۱۲ ۲.۲.۱۶۴ فیلتر کردن بر پایه آدرس‌های شبکه و شماره‌های پورت / ۱۶۶
- ۱.۱۲ ۳.۲.۱۶۴ مشکلات TCP / ۱۶۹
- ۱.۱۲ ۴.۲.۱۶۴ برگردان آدرس شبکه (NAT) / ۱۷۱

۱۲.۳ امنیت IP (IPSec) / ۱۷۲

۱۲.۳.۱ انجمن امنیتی / ۱۷۳

۱۲.۳.۲ تبادل کلید اینترنتی (IKE) / ۱۷۵

۱۲.۳.۳ مکانیزم‌های امنیتی / ۱۷۸

۱۲.۴ امنیت سرویس نام دامنه (DNS) / ۱۸۳

۱۲.۴.۱ تشخیص نفوذ برپایه - شبکه / ۱۸۴

۱۲.۴.۵ مدل تشخیص نفوذ شبکه / ۱۸۵

۱۲.۴.۵.۲ روش‌های تشخیص نفوذ / ۱۸۶

۱۲.۴.۵.۳ امضاهای حمله / ۱۸۷

۱۲.۴.۶ منابع پیشنهادی / ۱۸۹

فصل سیزدهم: امنیت لایه انتقال / ۱۹۲

۱۳.۱ مقدمه / ۱۹۲

۱۳.۲ ابزار TCP Wrapper / ۱۹۳

۱۳.۳ دروازه‌های مداری / ۱۹۳

۱۳.۳.۱ ویرایش پنجم SOCKS / ۱۹۴

۱۳.۴ امنیت لایه انتقال (TLS) / ۱۹۵

۱۳.۴.۱ پروتکل ثبت TLS / ۱۹۶

۱۳.۴.۲ پروتکل دست‌دهی TLS / ۱۹۷

۱۳.۵ احراز هویت ساده و لایه امنیتی (SASL) / ۲۰۱

۱۳.۵.۱ یک مثال LDAPv3 با SASL / ۲۰۲

۱۳.۶ پروتکل مدیریت کلید و انجمن امنیتی اینترنت (ISAKMP) / ۲۰۳

۱۳.۶.۱ دامنه تفسیر (DOI) / ۲۰۴

۱۳.۶.۲ گفتگوها ISAKMP / ۲۰۴

۱۳.۶.۷ منابع پیشنهادی / ۲۰۸

فصل چهاردهم: امنیت لایه کاربردی / ۲۱۰

۱۴.۱ مقدمه / ۲۱۰

۱۴.۲ دروازه‌های برنامه کاربردی و فیلترهای محتوا / ۲۱۰

۱۴.۳ کنترل دسترسی و صدور مجوز / ۲۱۱

۱۴.۴ امنیت سیستم عامل / ۲۱۲

۱۴.۵ تشخیص نفوذ برپایه - میزبان / ۲۱۴

۱۴.۵.۱ رکوردهای ممیزی / ۲۱۴

۱۴.۵.۲ انواع نفوذگرها / ۲۱۴

۱۴.۵.۳ تشخیص نفوذ آماری / ۲۱۵

۱۴.۶ برنامه‌های اینترنتی بهبود یافته - امنیتی / ۲۱۶

۱۴.۷ ارزیابی امنیتی / ۲۱۶

۱۴.۸ منابع پیشنهادی / ۲۱۶

بخش چهارم: امنیت وب

- ۱.۰ ۲.۰ مدل مرجع OSI / ۱۲۴
- ۱.۰ ۳.۰ مدل اینترنت / ۱۲۶
- ۱.۰ ۴.۰ تکنولوژی‌های شبکه / ۱۲۸
- ۱.۰ ۵.۰ امنیت در لایه‌های مختلف / ۱۳۰
- ۱.۰ ۵.۱ ضوابط انتخاب پروتکل / ۱۳۲
- ۱.۰ ۶.۰ برنامه‌های مخرب / ۱۳۳
- ۱.۰ ۶.۱ کرم اینترنت / ۱۳۳
- ۱.۰ ۶.۲ محتوای ماکرو و قابل اجرا / ۱۳۴
- ۱.۰ ۷.۰ مشکلات امنیتی ارتباطی / ۱۳۵
- ۱.۰ ۷.۱ تهدیدهای امنیتی / ۱۳۵
- ۱.۰ ۷.۲ گفتگوهای امنیتی / ۱۳۷
- ۱.۰ ۷.۳ پروتکل‌های پشتیبانی TCP/IP / ۱۳۸
- ۱.۰ ۷.۴ آسیب‌پذیری‌ها و نقص‌ها / ۱۳۸
- ۱.۰ ۸.۰ دیوار آتش / ۱۴۰
- ۱.۰ ۹.۰ شبکه خصوصی مجازی (VPN) / ۱۴۱
- ۱.۰ ۱۰.۰ منابع پیشنهادی / ۱۴۳

فصل یازدهم: امنیت لایه دسترسی شبکه / ۱۴۴

- ۱.۱۱ ۱.۱۴۴ مقدمه / ۱۴۴
- ۱.۱۱ ۲.۱۱ حالت انتقال غیرهمزمان (ATM) / ۱۴۵
- ۱.۱۱ ۲.۱۱ ۱.۲ سرویس‌های امنیتی ATM / ۱۴۷
- ۱.۱۱ ۲.۲.۱ امنیت چندبخشی / ۱۵۰
- ۱.۱۱ ۲.۲.۱ ۳.۲ تبادل پیام امنیتی ATM / ۱۵۱
- ۱.۱۱ ۲.۲.۱ ۴.۲ شبکه خصوصی مجازی ATM / ۱۵۱
- ۱.۱۱ ۳.۱۱ پروتکل نقطه - به - نقطه (PPP) / ۱۵۱
- ۱.۱۱ ۳.۱۱ ۱.۳ پروتکل احراز هویت رمز عبور / ۱۵۴
- ۱.۱۱ ۳.۱۱ ۲.۳ پروتکل CHAP / ۱۵۵
- ۱.۱۱ ۳.۳.۱ پروتکل احراز هویت توسعه‌پذیر (EAP) / ۱۵۶
- ۱.۱۱ ۳.۳.۱ ۴.۳ پروتکل کنترل رمزنگاری / ۱۵۹
- ۱.۱۱ ۴.۱۱ پروتکل ایجاد تونل در لایه دوم (L2TP) / ۱۵۹
- ۱.۱۱ ۵.۱۱ منابع پیشنهادی / ۱۶۱

فصل دوازدهم: امنیت لایه اینترنت / ۱۶۴

- ۱.۱۲ ۱.۱۶۴ مقدمه / ۱۶۴
- ۱.۱۲ ۲.۱۶۴ فیلتر کردن بسته / ۱۶۴
- ۱.۱۲ ۲.۱۶۴ فیلتر کردن بر اساس آدرس‌های شبکه / ۱۶۴
- ۱.۱۲ ۲.۲.۱۶۴ فیلتر کردن بر پایه آدرس‌های شبکه و شماره‌های پورت / ۱۶۶
- ۱.۱۲ ۳.۲.۱۶۴ مشکلات TCP / ۱۶۹
- ۱.۱۲ ۴.۲.۱۶۴ برگردان آدرس شبکه (NAT) / ۱۷۱

فصل پانزدهم: پروتکل انتقال ابرمتن / ۲۲۰+

۱.۱۵ مقدمه / ۲۲۰

۲.۱۵ پروتکل انتقال ابرمتن (HTTP) / ۲۲۱

۱.۲.۱۵ پیام‌های HTTP / ۲۲۲

۲.۲.۱۵ سربارها اطلاعات حساس را افشا می‌کنند / ۲۲۴

۳.۲.۱۵ مشکلات امنیتی حافظه کش پروتکل HTTP / ۲۲۴

۴.۲.۱۵ احراز هویت سرویس گیرنده پروتکل HTTP / ۲۲۵

۵.۲.۱۵ ایجاد تونل SSL / ۲۲۸

۳.۱۵ امنیت تراکنش وب / ۲۲۹

۱.۳.۱۵ S-HTTP / ۲۳۰

۴.۱۵ منابع پیشنهادی / ۲۳۱

فصل شانزدهم: امنیت سرویس دهنده وب / ۲۳۲

۱.۱۶ واسطه دروازه عمومی (CGI) / ۲۳۲

۲.۱۶ سرولت‌ها یا Servlet ها / ۲۳۴

۳.۱۶ انتشار گمنام در وب یا Rewebber / ۲۳۴

۴.۱۶ امنیت پایگاه داده / ۲۳۵

۵.۱۶ حفاظت از حق نشر / ۲۳۷

۶.۱۶ منابع پیشنهادی / ۲۳۸

فصل هفدهم: امنیت سرویس گیرنده وب / ۲۴۰+

۱.۱۷ اسپوفینگ وب / ۲۴۰

۲.۱۷ تجاوز به حریم خصوصی / ۲۴۱

۳.۱۷ تکنیک‌های گمنام‌سازی / ۲۴۲

۱.۳.۱۷ فرستندگان مجدد گمنام / ۲۴۳

۲.۳.۱۷ مسیریابی گمنام: مسیریابی پیازی / ۲۴۴

۳.۳.۱۷ مسیریابی گمنام: Crowds / ۲۴۵

۴.۳.۱۷ گمنام کننده در وب / ۲۴۷

۵.۳.۱۷ دستیار وب LPWA / ۲۴۸

۴.۱۷ منابع پیشنهادی / ۲۴۹

فصل هجدهم: امنیت کدهای موبایل / ۲۵۰+

۱.۱۸ مقدمه / ۲۵۰

۲.۱۸ برنامه‌های یاری دهنده و بلاگین‌ها / ۲۵۲

۳.۱۸ جاوا / ۲۵۲

۱.۳.۱۸ ایمنی جاوا / ۲۵۳

۲.۳.۱۸ ایمنی نوع جاوا / ۲۵۵

۳.۳.۱۸ تهدیدهای جاوا و حمله‌های زمان بندی / ۲۵۶

۴.۳.۱۸ اپلت‌های جاوا / ۲۵۷

۵.۳.۱۸ اپلت‌های دشمن و مخرب / ۲۵۸

- ۶.۳.۱۸ بازرسی پشته / ۲۵۹
- ۷.۳.۱۸ دامنه‌های حفاظتی در JDK 1.2.x / ۲۶۰
- ۸.۳.۱۸ نوشتن برنامه‌های کاربردی امن در جاوا / ۲۶۲
- ۴.۱۸ کنترل‌های ActiveX و Authenticode / ۲۶۲
- ۵.۱۸ جاوا اسکریپت / ۲۶۳
- ۶.۱۸ منابع پیشنهادی / ۲۶۵

فصل نوزدهم: مفاهیم تجارت الکترونیکی بر پایه وب - ۲۶۸

- ۱.۱۹ مقدمه / ۲۶۸
- ۲.۱۹ مفاهیم مبتنی بر XML / ۲۶۸
- ۳.۱۹ کارگروه Micropayment Markup / ۲۷۰
- ۴.۱۹ کارگروه JEPI / ۲۷۰
- ۵.۱۹ تجارت جاوا / ۲۷۱
- ۶.۱۹ منابع پیشنهادی / ۲۷۳

بخش پنجم: امنیت سیار

فصل بیستم: امنیت عامل سیار / ۲۷۶

- ۱.۲۰ مقدمه / ۲۷۶
- ۲.۲۰ عامل‌های سیار / ۲۷۷
- ۳.۲۰ تصورات امنیتی / ۲۷۸
- ۴.۲۰ حفاظت پلتفرم‌ها در برابر عامل‌های دشمن / ۲۷۹
- ۵.۲۰ حفاظت از پلتفرم‌ها در برابر عامل‌های دستکاری شده / ۲۷۹
- ۱.۵.۲۰ تاریخچه مسیر / ۲۸۰
- ۲.۵.۲۰ ارزیابی وضعیت / ۲۸۱
- ۳.۵.۲۰ امضای اطلاعات عامل تغییر پذیر / ۲۸۱
- ۴.۲۰ حفاظت عامل‌ها از پلتفرم‌های دشمن / ۲۸۱
- ۱.۶.۲۰ ردیابی رمزنگارانه / ۲۸۲
- ۲.۶.۲۰ زنجیره نتایج جزئی / ۲۸۳
- ۳.۶.۲۰ تولید کلید محیطی / ۲۸۵
- ۴.۶.۲۰ محاسبه با توابع رمزگشایی شده / ۲۸۵
- ۵.۶.۲۰ مبهم‌سازی کد / ۲۸۶
- ۶.۶.۲۰ سخت افزار ضد دستکاری / ۲۸۶
- ۷.۶.۲۰ عامل‌های همکار / ۲۸۶
- ۸.۶.۲۰ عامل‌های تکرار شده / ۲۸۷
- ۷.۲۰ تلاش‌های استاندارد سازی / ۲۸۸
- ۸.۲۰ منابع پیشنهادی / ۲۸۹

فصل بیست و یکم: امنیت تجارت سیار / ۲۹۲

- ۱.۲۱ مقدمه / ۲۹۲
- ۲.۲۱ مروری بر تکنولوژی / ۲۹۳

- ۳.۲۱ امنیت GSM / ۲۹۴
- ۱.۳.۲۱ محرمانگی شناسه مشترک / ۲۹۶
- ۲.۳.۲۱ احراز هویت مشترک / ۲۹۶
- ۳.۳.۲۱ محرمانگی داده و اتصال / ۲۹۷
- ۴.۲۱ پروتکل برنامه بی سیم / ۲۹۸
- ۱.۴.۲۱ امنیت لایه انتقال بی سیم (WTLS) / ۲۹۹
- ۲.۴.۲۱ مازول شناسه WAP / ۳۰۰
- ۳.۴.۲۱ مسائل امنیتی WML / ۳۰۰
- ۵.۲۱ کیت ابزار برنامه کاربردی سیم کارت / ۳۰۱
- ۶.۲۱ محیط اجرای برنامه کاربردی ایستگاه سیار (MExE) / ۳۰۱
- ۷.۲۱ چشم انداز / ۳۰۲
- ۸.۲۱ منابع پیشنهادی / ۳۰۳

فصل بیست و دوم: امنیت کارت‌های هوشمند / ۳۰۴

- ۱.۲۲ مقدمه / ۳۰۴
- ۲.۲۲ امنیت سخت‌افزار / ۳۰۵
- ۳.۲۲ امنیت سیستم عامل کارت / ۳۰۷
- ۴.۲۲ امنیت برنامه کاربردی کارت / ۳۰۸
- ۵.۲۲ کارت Java / ۳۰۹
- ۶.۲۲ سیم کارت / ۳۱۰
- ۷.۲۲ بیومتریک / ۳۱۰
- ۱.۷.۲۲ مشخصات فیزیولوژیکی / ۳۱۲
- ۲.۷.۲۲ مشخصات رفتاری / ۳۱۳
- ۸.۲۲ منابع پیشنهادی / ۳۱۳

نتیجه‌گیری / ۳۱۶

ضمائم / ۳۱۸