



اصول امنیت برای تجارت الکترونیکی

نویسنده: وسنا هسار

ترجمه:

دکتر آرش حبیبی لشکری

(عضو هیئت علمی دانشگاه آزاد اسلامی)

مهندس یاشار علی محمدزاده

مهندس محمدتقی فرامرزی

سرشناسه: هاسلر، وسنا
Hassler, Vesna
عنوان و نام پدیدآور: اصول امنیت برای تجارت الکترونیکی/ نویسنده وسنا هاسلر؛ ترجمه آرش حبیبی لشکری، یاشار علی مجزاده، محمدتقی فرامرزی.
مشخصات نشر: تهران : علوم ایران ، ۱۳۹۶.
مشخصات ظاهری : ۲۲۸ص.؛ صور، جدول ، نمودار .
شابک : ۹۷۸-۹۶۴-۲۷۵۰-۴۴۰۳
وضعیت فهرست نویسی: فیا
بازداشت: عنوان اصلی: Security fundamentals for e-commerce.
موضوع: با: گانی الکترونیکی -- تدابیر امنیتی
موضوع: Electronic commerce -- Security measures
موضوع: مانه‌های ارتباطی باند پهن
موضوع: Broadband communication systems
شناسه اول: شناسه اول: حسیبی لشکری، آرش، ۱۳۵۳ - مترجم
شناسه دوم: شناسه دوم: علی مجزاده، یاشار، ۱۳۷۰ - مترجم
شناسه افزودنی: شناسه افزودنی: فرامرزی، محمدتقی، ۱۳۳۰ - مترجم
رده بندی کنگره: ۳۹۶.۰۱۷/۶۱۷.۰۴۸/HF0048
رده بندی دیویی: ۶۸۵
شماره کتابشناسی: ۳۸۲۹۵



انتشارات علوم ایران

www.olomiran.net

انتشارات علوم ایران: تهران - تلفن ۰۹۱۲۵۳۶۷۱۱ و ۶۶۸۷۵۴۴۹

سندوق پستی: تهران ۳۵۳ - ۱۳۱۴۵

نام کتاب: اصول امنیت برای تجارت الکترونیکی	نویسنده: وسنا هاسلر
ترجمه: دکتر آرش حبیبی لشکری - مهندس یاشار علی مجزاده - مهندس محمدتقی فرامرزی	
ناشر: علوم ایران	
نوبت و سال چاپ: دوم - ۱۳۹۸	شابک: ۹۷۸ - ۹۶۴ - ۲۷۵۰ - ۴۴۰۳
تیراژ: ۱۰۰ نسخه	قیمت: ۴۷۰۰ تومان

مرکز پخش:

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

یکم، پلاک ۴ طبقه دوم واحد ۴ تلفن همراه: ۰۹۱۲۳۰۳۳۰۵۸

تلفن: ۶۶۹۴۱۱۶۷ و ۶۶۹۴۱۰۳۴ فکس: ۶۶۹۴۱۶۱۵

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 ممتثلان 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

حره بدانی که نخورده است ترا

انتشارات علوم ایران در تلاش است تا کمی از دست خوانندگان برساند که توسط آنها حداقل گوشه‌ای از نیازهای علمی کشور برآورده شود. لذا از اساتید و مدرسین، اعضاء هیئت علمی دانشگاه‌ها و دانشجویان در مقاطع و رشته‌های مختلف تحصیلی و تمامی افرادی که می‌خواهند کتابی را ترجمه 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

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. رمزها، یکپارچگی داده / ۲۶

۱.۲. توان هش رمزنگاری شده / ۲۶

۱.۲. تد احراز هویت پیام / ۲۸

۲.۲. مکانیزم‌های رمزنگاری / ۲۹

۱.۲.۲. مکانیزم‌های هاش / ۲۹

۲.۲.۲. مکانیزم‌های کد عملی / ۳۶

۳.۲. مکانیزم‌های امضاء / ۳۶

۱.۳.۲. امضاء دیجیتال DSA / ۴۵

۲.۳.۲. الگوریتم امضاء دیجیتال / ۴۵

۳.۳.۲. قیاس منحنی بیضوی DSA / ۴۷

۴.۳.۲. مدیریت کلید عمومی / 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. کوئیلو و کوئیز کوآتر / 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 کلید عمومی / ۵۵

۱.۲.۳ فرمت گواهی X.509 / ۵۶

۲.۲.۳ زیرساخت کلید عمومی اینترنتی / ۶۰

۳.۳ روش های کدگذاری / ۶۱

۴.۳ منابع پیشنهادی / ۶۲

بخش دوم: امنیت پرداخت الکترونیکی

فصل چهارم: سیستم های پرداخت الکترونیکی / ۶۶

۱.۴ تجارت الکترونیکی / ۶۶

۲.۴ سیستم های پرداخت الکترونیکی / ۶۷

۱.۲.۴ آنلاین در برابر آفلاین / ۶۷

۲.۲.۴ بدهکاری در برابر اعتبار / ۶۸

۳.۲.۴ خرید در برابر کلان / ۶۸

۲.۱ ابزارهای پرداخت / ۶۹

۵.۲.۱ کیف پول الکترونیکی / ۷۲

۶.۲.۴ کارت های اعتباری / ۷۳

۳.۴ امنیت پرداخت الکترونیکی / ۷۳

۴.۴ منابع پیشنهادی / ۷۵

فصل پنجم: سرویس های سیستم پرداخت / ۷۶

۱.۵ سرویس های امنیتی پرداخت / ۷۶

۱.۱ امنیت تراکنش پرداخت / ۷۶

۲.۱ امنیت پول الکترونیکی / ۷۹

۳.۱ امنیت چک الکترونیکی / ۷۹

۲.۵ دسترس پذیری 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 زنجیره ترکیب ها / ۸۲

۲.۶ گمنامی پرداخت کننده / ۸۴

۱.۲ نام های مستعار / ۸۴

۳.۶ عدم قابلیت ردیابی تراکنش های پرداخت / ۸۶

۱.۳ استفاده از جمع هش تصادفی در IKB / ۸۶

۲.۳ استفاده از جمع هش تصادفی در SET / ۸۶

۴.۶ محرمانگی داده های تراکنش پرداخت / ۸۷

۱.۴ تابع شبه تصادفی / ۸۷

۲.۴ امضای دوگانه / ۸۸

۵.۶ عدم انکار پیام های تراکنش پرداخت / ۹۰

۱.۵ امضای دیجیتال / ۹۰

۶.۶ تازگی پیام های تراکنش پرداخت / ۹۲

۶. شماره‌های یکبار مصرف و برچسب‌های زمان / ۹۲

۶. 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 بریلن - و - انتخاب کردن / ۹۸

۲.۲.۷. امضای کور / ۹۸

۳.۲.۷. مبادله سکه‌ها / ۹۸

۴.۲.۷. نگهداری / ۹۹

۱.۲.۷. امضای نگهداری / ۹۹

۲.۱.۷. امضای صادرکننده / ۱۰۱

۳.۷. حفاظت در برابر جعل سکه / ۱۰۲

۱.۳.۷. سکه‌های با هزینه تولید بالا / ۱۰۳

۴.۷. حفاظت در برابر ردی سکه‌ها / ۱۰۳

۱.۴.۷. سکه‌های دیجیتال شده / ۱۰۳

۱.۱.۴.۷. سکه‌های معتمد مشترک و همچنین 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. کربروس / ۱۱۱

۲.۱.۱.۸. پروکسی محدود شده / ۱۱۲

۳.۱.۱.۸. پروکسی آشنایی / 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 امضاهای دیجیتالی / ۱۱۶

۴.۹. منابع پیشنهادی / ۱۱۹

بخش سوم: امنیت ارتباط

فصل دهم: شبکه ارتباط / ۱۲۴

۱.۱۰. مقدمه / ۱۲۴

- ۱.۰.۲ مدل مرجع OSI / ۱۲۴
- ۱.۰.۳ مدل اینترنت / ۱۲۶
- ۱.۰.۴ تکنولوژی‌های شبکه / ۱۲۸
- ۱.۰.۵ امنیت در لایه‌های مختلف / ۱۳۰
- ۱.۰.۵.۱ ضوابط انتخاب پروتکل / ۱۳۲
- ۱.۰.۶ برنامه‌های مخرب / ۱۳۳
- ۱.۰.۶.۱ کرم اینترنت / ۱۳۳
- ۱.۰.۶.۲ محتوای ماکرو و قابل اجرا / ۱۳۴
- ۱.۰.۷ مشکلات امنیتی ارتباطی / ۱۳۵
- ۱.۰.۷.۱ تهدیدهای امنیتی / ۱۳۵
- ۱.۰.۷.۲ گز-گوه‌های امنیتی / ۱۳۷
- ۱.۰.۷.۳ پروتکل‌های پشتیبانی TCP/IP / ۱۳۸
- ۱.۰.۷.۴ آسیب‌پذیری‌ها و نقص‌ها / ۱۳۸
- ۱.۰.۸ دیوال‌ش / ۴
- ۱.۰.۹ شبکه خصوصی مجازی (VPN) / ۱۴۱
- ۱.۰.۱۰ منابع پیشنهادی / ۴۳
- فصل یازدهم: امنیت لایه ترانسپورت / ۱۴۴**
 - ۱.۱۱ مقدمه / ۱۴۴
 - ۲.۱۱ حالت انتقال غیرهمزمان (ATM) / ۴۵
 - ۱.۲.۱۱ سرویس‌های امنیتی ATM / ۴۵
 - ۲.۲.۱۱ امنیت چندبخشی / ۱۵۰
 - ۳.۲.۱۱ تبادل پیام امنیتی ATM / ۱۵۱
 - ۴.۲.۱۱ شبکه خصوصی مجازی ATM / ۱۵۱
 - ۳.۱۱ پروتکل نقطه - به - نقطه (PPP) / ۱۵۱
 - ۱.۳.۱۱ پروتکل احراز هویت رمز عبور / ۱۵۴
 - ۲.۳.۱۱ پروتکل CHAP / ۱۵۵
 - ۳.۳.۱۱ پروتکل احراز هویت توسعه‌پذیر (EAP) / ۱۵۶
 - ۴.۳.۱۱ پروتکل کنترل رمزنگاری / ۱۵۹
 - ۴.۱۱ پروتکل ایجاد تونل در لایه دوم (L2TP) / ۱۵۹
 - ۵.۱۱ منابع پیشنهادی / ۱۶۱
- فصل دوازدهم: امنیت لایه اینترنت / ۱۶۴**
 - ۱.۱۲ مقدمه / ۱۶۴
 - ۲.۱۲ فیلتر کردن بسته / ۱۶۴
 - ۱.۲.۱۲ فیلتر کردن بر اساس آدرس‌های شبکه / ۱۶۴
 - ۲.۲.۱۲ فیلتر کردن برپایه آدرس‌های شبکه و شماره‌های پورت / ۱۶۶
 - ۳.۲.۱۲ مشکلات TCP / ۱۶۹
 - ۴.۲.۱۲ 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
- ۱۲.۵ تشخیص نفوذ برپایه - شبکه / ۱۸۴
- ۱۲.۵.۱ مدل تشخیص نفوذ شبکه / ۱۸۵
- ۱۲.۵.۲ روش‌های تشخیص نفوذ / ۱۸۶
- ۱۲.۵.۳ امضاهای حمله / ۱۸۷
- ۱۲.۶ منابع پیشنهادی / ۱۸۹

فصل سیزدهم: امنیت لایه انتقال / ۱۹۲

- ۱۳.۱ مقدمه / ۱۹۲
- ۱۳.۲ برار TCP Wrapper / ۱۹۳
- ۱۳.۳ رازهای مداری / ۱۹۳
- ۱۳.۳.۱ رایش حجم SOCKS / ۱۹۴
- ۱۳.۴ امنیت / ۱۹۵
- ۱۳.۴.۱ پروتکل ثبت S / ۱۹۶
- ۱۳.۴.۲ پروتکل دست‌در / ۱۹۷
- ۱۳.۵ احراز هویت ساده و لایه ثبت (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
- ۱۳.۷ 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

فصل پانزدهم: پروتکل انتقال ابرمتن / ۲۲۰

۱.۱۵ مقدمه / ۲۲۰

۲.۱۵ پروتکل انتقال ابرمتن (HTTP) / ۲۲۱

۱.۲ پیام‌های HTTP / ۲۲۲

۲.۲ سرپارها اطلاعات حساس را افشا می‌کنند / ۲۲۴

۳.۲ مشکلات امنیتی حافظه کش پروتکل HTTP / ۲۲۴

۴.۲ احراز هویت سرویس گیرنده پروتکل HTTP / ۲۲۵

۵.۲ ایجاد تونل SSL / ۲۲۸

۳.۱۵ امنیت تراکنش وب / ۲۲۹

۱.۳ S-HTTP / ۲۳۰

۱.۱۵ منابع پیشنهادی / ۲۳۱

فصل شانزدهم: امنیت سرویس دهنده وب / ۲۳۲

۱.۱۶ واسطه دهنده عمومی (CGI) / ۲۳۲

۲.۱۶ سرورها یا Services / ۲۳۴

۳.۱۶ انتشار گمنام در وب / Rewebber / ۲۳۴

۴.۱۶ امنیت پایگاه داده / ۲۳۷

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 فرستندگان مجدد گمنام / ۲۴۳

۲.۳ مسیر یابی گمنام: مسیر یابی پیازی / ۲۴۴

۳.۳ مسیر یابی گمنام: Crowds / ۲۴۵

۴.۳ گمنام کننده در وب / ۲۴۷

۵.۳ 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 پلاگین‌ها / ۲۵۲

۳.۱۸ جاوا / ۲۵۲

۱.۳ ایمنی جاوا / ۲۵۳

۲.۳ ایمنی نوع جاوا / ۲۵۵

۳.۳ تهدیدهای جاوا و حمله‌های زمان بندی / ۲۵۶

۴.۳ اپلت‌های جاوا / ۲۵۷

۵.۳ اپلت‌های دشمن و مخرب / ۲۵۸

۱۸. ۳. ۶ بازرسی پشته / ۲۵۹

۱۸. ۳. ۷ دامنه‌های حفاظتی در JDK 1.2.X / ۲۶۰

۱۸. ۳. ۸ نوشتن برنامه‌های کاربردی امن در جاوا / ۲۶۲

۱۸. ۴ کنترل‌های ActiveX و Authenticode / ۲۶۲

۱۸. ۵ جاوا اسکریپت / ۲۶۳

۱۸. ۶ منابع پیشنهادی / ۲۶۵

فصل نوزدهم: مفاهیم تجارت الکترونیکی برپایه-وب / ۲۶۸

۱۹. ۱ مقدمه / ۲۶۸

۱۹. ۲ مفاهیم مبتنی بر-XML / ۲۶۸

۱۹. ۳ کارگروه Markup Micropayment / ۲۷۰

۱۹. ۴ کارگروه JEPI / ۲۷۰

۱۹. ۵ تجارت جاوا / ۲۷۱

۱۹. ۶ منابع پیشنهادی / ۲۷۳

بخش پنجم: امنیت سیار

فصل بیستم: امنیت عامل سیار / ۲۷۶

۲۰. ۱ مقدمه / ۲۷۶

۲۰. ۲ عامل‌های سیار / ۲۷۶

۲۰. ۳ تصورات امنیتی / ۲۷۸

۲۰. ۴ حفاظت پلتفرم‌ها در برابر عامل‌های دشمن / ۲۷۹

۲۰. ۵ حفاظت از پلتفرم‌ها در برابر عامل‌های دوستی / ۲۷۹

۲۰. ۵. ۱ تاریخچه مسیر / ۲۸۰

۲۰. ۵. ۲ ارزیابی وضعیت / ۲۸۱

۲۰. ۵. ۳ امضای اطلاعات عامل تغییر پذیر / ۲۸۱

۲۰. ۶ حفاظت عامل‌ها از پلتفرم‌های دشمن / ۲۸۱

۲۰. ۶. ۱ ردیابی رمزنگارانه / ۲۸۲

۲۰. ۶. ۲ زنجیره نتایج جزئی / ۲۸۳

۲۰. ۶. ۳ تولید کلید محیطی / ۲۸۵

۲۰. ۶. ۴ محاسبه با توابع رمزگشایی شده / ۲۸۵

۲۰. ۶. ۵ مبهم‌سازی کد / ۲۸۶

۲۰. ۶. ۶ سخت افزار ضد دستکاری / ۲۸۶

۲۰. ۶. ۷ عامل‌های همکار / ۲۸۶

۲۰. ۶. ۸ عامل‌های تکرار شده / ۲۸۷

۲۰. ۷ تلاش‌های استاندارد سازی / ۲۸۸

۲۰. ۸ منابع پیشنهادی / ۲۸۹

فصل بیست و یکم: امنیت تجارت سیار / ۲۹۲

۲۱. ۱ مقدمه / ۲۹۲

۲۱. ۲ مروری بر تکنولوژی / ۲۹۳

۲۹۴ / امنیت GSM / ۳.۲۱

۲۹۶ / ۱.۳.۲۱ محرمانگی شناسه مشترک /

۲۹۶ / ۲.۳.۲۱ احراز هویت مشترک /

۲۹۷ / ۳.۳.۲۱ محرمانگی داده و اتصال /

۲۹۸ / ۴.۲۱ پروتکل برنامه بی سیم /

۲۹۹ / ۱.۴.۲۱ امنیت لایه انتقال بی سیم (WTLS) /

۳۰۰ / ۲.۴.۲۱ مازول شناسه WAP /

۳۰۰ / ۳.۴.۲۱ مسائل امنیتی WML /

۳۰۱ / ۵.۲۱ کیت ابزار برنامه کاربردی سیم کارت /

۳۰۱ / ۶.۲۱ محیط اجرای برنامه کاربردی ایستگاه سیار (MEXE) /

۳۰۲ / ۲۰۲ چشر انداز /

۳۰۳ / ۸.۱ منابع پیشنهادی /

فصل بیست و دوم: امنیت کارت‌های هوشمند / ۳۰۴

۳۰۴ / ۱.۲۲ مقد /

۳۰۵ / ۲.۲۲ امنیت /

۳۰۷ / ۳.۲۲ امنیت سیستم عامل کارت /

۳۰۸ / ۴.۲۲ امنیت برنامه کاربردی کارت /

۳۰۹ / ۵.۲۲ کارت Java /

۳۱۰ / ۶.۲۲ سیم کارت /

۳۱۰ / ۷.۲۲ بیومتریک /

۳۱۲ / ۱.۷.۲۲ مشخصات فیزیولوژیکی /

۳۱۳ / ۲.۷.۲۲ مشخصات رفتاری /

۳۱۳ / ۸.۲۲ منابع پیشنهادی /

نتیجه‌گیری / ۳۱۶

ضمائم / ۳۱۸

پیشگفتار

در طول سال‌های پیش، دهمتر مقاله‌ای منتشر شده است که مملو از عباراتی از قبیل "تجارت الکترونیک"، "اینترنت"، "وب" یا "امنیت" نبوده باشد. تجارت الکترونیک، نتیجه انتقال تجارت به رسانه‌های جدیدی است، که شبکه‌های کامپیوتری یکی از آنهاست. شبکه‌های به هم پیوسته، سراسر جهان اقلب از پروتکل‌های یکسانی استفاده می‌کنند (TCP/IP) که موجب ایجاد اینترنت شده است. شبکه مسترد چهار (WWW) که به عنوان یک برنامه سرویس‌گیرنده - سرویس‌دهنده شروع به کار نموده بود، حال به پلتفرم جدیدی تبدیل شده که مراکز اطلاعاتی مجازی، فروشگاه‌ها، مراکز تجاری، بازارهای سهام و موارد مشابه بسیاری را تحت پوشش قرار می‌دهد. تازگی اینترنت شروع به انتشار در هوا، یا ترکیب شبکه‌های ارتباطی سیار نیز نموده است، که چشم‌اندازهای جدیدی برای یک "اقتصاد-الکترونیکی" همه‌گیر بوجود آورده است.

مواردی که در این کتاب پوشش داده شده است

تجارت الکترونیکی می‌تواند بین شرکت‌ها و مشتریان (شرکت-به-شرکت)، مابین شرکت‌ها (شرکت-به-شرکت) یا بین مشتریان/شرکت‌ها و مدیریت عمومی (دولت) انجام شود. یک تراکنش در حوال تجارت الکترونیکی در بردارنده اطلاعات در مورد کالاها و سرویس‌ها، پیشنهادها، سفارش‌ها، تحویل، و پرداخت می‌باشد. به نظر می‌رسد که این پردازش‌ها در شبکه‌های نامطمئن رخ می‌دهند که دارای مشکلات امنیتی بسیاری از قبیل عدم تایید شناسه شرکت کنندگان، یا عدم حفاظت کافی از انتقال داده می‌باشند. مسائل امنیتی در برنامه‌های تجارت الکترونیکی در بسیاری از شبکه‌های دیگر نیز یافت می‌شوند. با وجود این برخی نیازمندی‌های امنیتی تنها مختص تجارت‌های الکترونیکی و وابسته به مقایسه‌ای این حوزه می‌باشند (پرداخت الکترونیکی). هدف این کتاب ایجاد یک دید عمیق از تمامی مسائل امنیتی پایه و راه‌های مرتبطی است که می‌توانند به نوعی با برنامه‌های تجارت الکترونیکی ارتباط داشته باشند.

آیا امنیت مانعی برای توسعه تجارت الکترونیکی می‌باشد؟

در اصل امنیت فن‌آوری اطلاعات مانع اصلی برای استفاده گسترده تجارت الکترونیکی نیست. البته افراد زیادی بر این عقیده نیستند، اما در اصل گزارشات متعددی در مورد حملات امنیتی و حملات محرومیت - از - خدمات باعث این امر شده است. یک نتیجه مثبت از این حملات این است که برخی دولت‌ها به اهمیت زیرساخت امنیت شبکه پی‌برده‌اند، چرا که آسیب پذیری‌ها در یک نقطه از شبکه می‌تواند برای همگان خطر آفرین باشد. در بیشتر مواقع تکنولوژی‌های امنیتی برای تجارت الکترونیکی باید کاملترین باشند. تا حدی هم باید استاندارد سازی شده باشند تا حداقل قابلیت همکاری در آنها تضمین شود.

(مانند قالب گواهی نامه X.509)، با این وجود کار بیشتر باید روی پروفایل سازی انجام شود تا از قابلیت همکاری اطمینان حاصل شود. تکنولوژی‌های پایه‌ای امنیتی هنوز توسط قوانین بین‌المللی مناسبی پشتیبانی نشده‌اند، برای مثال هنوز چارچوب کاری بین‌المللی قانونی برای پذیرش امضاهای دیجیتال وجود ندارد، که البته این عدم وجود قوانین مناسب متأسفانه تنها به حوزه امنیت محدود نمی‌شود. زیرا جنبه‌های دیگر تراکنش‌های تجارت الکترونیکی نیز از قبیل مالیات، بدهکاری و مالکیت هنوز در بیشتر کشورها قانونمند نشده‌اند. مشکل دیگر این است که برخی کشورها استفاده از تکنیک‌های رمزنگاری را محدود و یا کنترل می‌کنند و بیشتر دولت‌ها بر این باورند که این امر مانعی برای توسعه اقتصادی است. برای نمونه دولت ایالات متحده در ژانویه 2000 قوانین صادرات را به طرز قابل توجهی آزاد کرد (Netscape 4.7 می‌تواند با کلیدهای رمزنگاری 128-بیتی صادر شود). بعلاوه محصولات فن‌آوری اطلاعات با کارکرد امنیتی حساس باید همانند محصولات مرتبط با آسانسورها و قطارها و سایر سیستم‌های عمومی که وابستگی زیادی با ایمنی دارند، به دقت توسط شرکت‌های سوم مورد اعتماد دولت بازرسی و تحت ارزیابی و تایید قرار گیرد. در نهایت، امنیت حوزه‌ایست که با توجه به افزایش ملوم توان عملیاتی و رسمه‌های مهاجمین نیازمند نظارت و به روزرسانی متوالی است.

دلیل نوشتن این کتاب

انگیزه اصلی نوشتن این کتاب پشتیبانی از کنفرانس نویسنده کتاب در حوزه امنیت شبکه و تجارت الکترونیکی در دانشگاه فنی وین کشور اتریش بود. کتاب‌ها و کارهای مفید زیادی در زمینه امنیت تجارت الکترونیکی از قبیل رمزنگاری، امنیت وب و شبکه، و سیستم‌های پرداخت آنلاین تاکنون تهیه و به چاپ رسیده است، با این حال نویسنده در جستجوی کتبی بود که تمام موضوعات مرتبط این حوزه را پوشش داد. نباشد. نویسنده بتواند آن را به دانشجویان خود پیشنهاد نماید این کتاب حاصل هشت سال تجربه تدریس نویسنده در زمینه سامپیر و امنیت شبکه می‌باشد. این کتاب همچنین برای متخصصین فن‌آوری اطلاعاتی که دارای پیش زمینه اندکی در امنیت تجارت الکترونیکی می‌باشند، نیز پیشنهاد می‌شود.

رفع مسئولیت

این کتاب تمام جنبه‌های تجارت الکترونیکی و همچنین مدل‌های تجارت الکترونیکی و نیازمندی‌های خاص امنیتی آنها را مورد بحث قرار نمی‌دهد. همانطور که از نام آن پیداست، این کتاب با مسائل امنیتی پایه سروکار دارد که باید در توسعه برنامه‌های تجارت الکترونیکی در نظر گرفته شوند. این کتاب در مورد تمام موضوعات مطرح شده با جزئیات بحث نمی‌کند ولی منابع بسیاری در مورد آنها ارائه می‌دهد. در صورت نیاز برای شما آدرس‌های وبسایت‌های مرتبط هم فراهم شده است ولی متأسفانه نمی‌توان تضمین نمود که هنوز هم وقتی شما در حال خواندن این کتاب هستید، این صفحات وب در دسترس باشند. بعلاوه اسناد پیش‌نویس که پیشرفت کار را نشان می‌دهند (IETF, W3C و سایر بدنه‌های استانداردسازی) می‌توانند منقضی شده یا در دسترس نباشند. در این کتاب اسامی شرکت‌ها یا محصولات خاصی را نویسنده ذکر کرده است که در تمامی موارد هدف اصلی ارائه یک نمونه کاربردی بوده و ترجیح یا برتری از دیدگاه نویسنده بین شرکت یا محصول خاصی با شرکت یا محصول دیگری وجود نداشته است.

نحوه خواندن این کتاب

این کتاب پنج بخش دارد هر بخش می‌تواند جداگانه خوانده شود اما هر کدام بر اساس بخش قبل طراحی شده‌اند. برای نمونه مکانیزم‌های امنیتی پایه‌ای شرح داده شده در بخش اول وقتی در جاهای دیگر آورده شده‌اند دیگر توضیح داده نشدند. نیازی به مطالعه ریاضیات بخش اول برای فهم دیگر بخش‌ها نمی‌باشد. برای مثال کافی است ابتدای هر بخش که یک مکانیزم امنیتی خاص توضیح داده می‌شود را بخوانید تا ایده کلی آن مکانیزم را دریابید. بخش دوم روی نیازمندی‌های

امنیتی خاص سیستم‌های پرداخت الکترونیکی تمرکز دارد. بخش سوم به امنیت ارتباطات، مسائل امنیتی در انتقال داده روی شبکه‌های ناامن می‌پردازد و بخش چهارم مروری دارد بر مسائل و راه‌حل‌های امنیتی مربوط به وب. در نهایت بخش ۵ با جنبه‌های سیار بودن کد و مشتری از نقطه نظر امنیت (دستگاه‌های سیار و کارت‌های هوشمند) سروکار خواهد داشت.

سپاسگزاری

نویسنده از تمام اشخاصی که مستقیم و غیرمستقیم در نوشتن این کتاب وی را مورد حمایت قرار دادند، تشکر می‌نماید که نام برخی از آنها در اینجا ذکر می‌شود. تشکر ویژه از Rolf Oppilger برای معرفی نویسنده به Artech House و تشویق وی برای نوشتن این کتاب و حمایت از طرح پیشنهادی یا پروپوزال وی تا مورد قبول واقع شود. ایشان با ارائه نکات تخصصی و کارشناسی و همچنین در اختیار گذاشتن منابع مهم برای بهبود کیفیت محتوی این کتاب بسیار موثر بودند. تشکر ویژه از Peddie Moore برای دوستی و کمک‌های روحی از ابتدا تا انتهای این پروژه. او نه تنها به بهتر شدن زبان و قالب متن کمک کرد بلکه بسیاری از توضیحات مبهم و نامناسب را نیز تصحیح نمود. تشکر ویژه از Matthew Quirk برای حمایت از Peddie و بازنگری کل کار. سپاس فراوان از Viki Wiliam، Susanna Tagarth، و Ruth Young برای پشتیبانی بسیار تخصصی و توأم با مهربانی‌هایشان. تشکر ویژه از پروفیسور Mehdi Jazayeri رئیس دپارتمان و همکار نه‌منده، گروه سیستم‌های توزیعی برای همکاری و حمایت‌های بی‌دریغ ایشان. تشکر از دانشجویانی که در کنفرانس امنیت تجارت الکترونیکی حضور یافتند و بحث‌های کلاسی جالبی را رقم زدند. نهایتاً تشکر ویژه از همسر Hanne برای حمایت، عشق، درک و کتاب‌های فنی بسیاری که برای کتابخانه منزل خریداری کرد و بخصوص آشپزی عالی که در زمان تعطیلاتی که من مشغول کار در تعطیلات آخر هفته بودم، انجام می‌داد. امیدوارم که از خواندن این کتاب لذت ببرید و مطالبی از آن یاد بگیرید. شاید پیش از بازخوردهایی که برای من ارسال می‌نمایید، نیز تشکر می‌کنم.