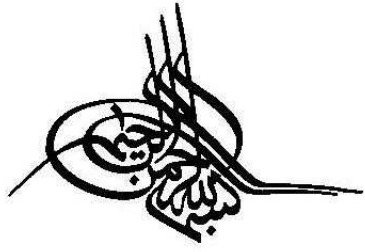

اصول امنیت
برای تجارت الکترونیکی

نویسنده: وسنا هسا

ترجمه:
دکتر آرش حبیبی لشکری
(عضو هیئت علمی دانشگاه آزاد اسلامی)
مهندس یاشار علی‌محمدزاده
مهندس محمدتقی فرامرزی

سرشناسه: هاسلر، وسنا
Hassler, Vesna
عنوان و نام پدیدآور: اصول امنیت برای تجارت الکترونیکی/ نویسنده وسنا هاسلر؛ترجمه آرش حبیبی‌لشکری،یاشار علی‌مجدزاده، مجدتقی فرامرزی.
مشخصات نشر: تهران : علوم ایران ، ۱۳۹۶.
مشخصات ظاهری : ۲۲۸ص.: مصور ،جدول ، نمودار .
شابک : ۹۷۸-۹۶٤-۲۷۵۰-٤٤-۳
وضعیت فهرست نویسی:فیپا
یادداشت: 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: حبیبی‌لشکری، آرش، ۱۳۵۳ -، مترجم
شناسه افزوده: علی‌مجدزاده، یاشار، ۱۳۷۰ -، مترجم
شناسه افزوده: فرامرزی، محمدتقی، ۱۳۴۰ -، مترجم
رده بندی کنگره: ۱۳۹۶ الف۱۷/HF۵۵٤۸
رده بندی دیویی: ٦۸۵٤
شماره کتابشناسی ملی: ۴۸۲۹۰۶

انتشارات علوم ایران

انتشارات علوم ایران: تهران، خیابان ... تلفن ۰۹۱۲۵۳۶۷۰۱ و ٦٦۸۷۵٤٤۹

صندوق پستی: تهران ۳۵۳ -- ۱۳۱٤۵

www.olomiran.net

نام کتاب: اصول امنیت برای تجارت الکترونیکی	**نویسنده:** وسنا هسلر
ترجمه: دکتر آرش حبیبی لشکری - مهندس یاشار علی مجدزاده - مهندس محمدتقی فرامرزی	
ناشر: علوم ایران	
نوبت و سال چاپ: دوم -- ۱۳۹۸	**شابک:** ۳ - ٤٤ - ۲۷۵۰ - ۹٦٤ - ۹۷۸
تیراژ: ۱۰۰ نسخه	**قیمت:** ٤۷۰۰ تومان

مرکز پخش:

کتاب کوشا -- میدان انقلاب، ابتدای کارگر جنوبی، کوچه رشتچی، بن بست یکم، پلاک ٤ طبقه دوم واحد ٤ تلفن همراه: ۰۹۱۲۳۰۳۳۰۵۸

تلفن: ٦٦۹٤۱۱٦۷ و ٦٦۹٤۱۰۳٤ فکس: ٦٦۹۲۱٦۸۵

سخن ناشر

بر چرخ فلک هیچ کسی چیر نشد — وز خوردن آدمی زمین سیر نشد

خرم بدانی که نخورده‌ست ترا — تعجیل مکن هم بخورد دیر نشد

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، 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 پستی۳۵۳ - ۱۳۱۴۵ پیشنهادات خود را ارسال نمایید. آدرس سایت انتشارات علوم ایران www.olomiran.net می‌باشد.

با تشکر

مدیر انتشارات علوم ایران

فهرست مطالب

پیشگفتار

درطول سال‌های پیش از کمتر مقاله‌ای منتشر شده است که مملو از عباراتی از قبیل "تجارت الکترونیک"، "اینترنت"، "وب" یا "امنیت" نبوده باشد. تجارت الکترونیکی 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 گسترده جهانی (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. به 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 دراین کتاب پوشش داده شده است

تجارت الکترونیکی می‌تواند بین شرکت‌ها و مشتریان (شرکت-به-مشتری)، مابین شرکت‌ها (شرکت-به-شرکت) یا بین مشتریان/شرکت‌ها و مدیریت عمومی (دولت) انجام شود. یک تراکنش معمول تجارت الکترونیکی در بردارنده اطلاعات در مورد کالاها و سرویس‌ها، پیشنهادها، سفارش‌ها، تحویل، و پرداخت می‌باشد. بدیهی است که این پردازش‌ها در شبکه‌های نامطمئن رخ می‌دهند که دارای مشکلات امنیتی بسیاری از قبیل عدم تایید شناسایی شرکت‌کنندگان، 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 مفاهیم اصلی این حوزه می‌باشند (پرداخت الکترونیکی). هدف این کتاب ایجاد یک دید عمیق از تمامی مسائل امنیتی پایه و راه‌حل‌های 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 خطرآفرین 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 گواهی‌نامه 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 متاسفانه 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 براین 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 شرکت سومی که مورد اعتماد دو طرف باشد، تحت ارزیابی و تایید قرار گیرد. در نهایت، امنیت حوزه‌ایست که با توجه به افزایش مداوم توان عملیاتی و توسعه مهارت‌های 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. کنفرانس‌ها و کارگاه‌های متعدد 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 کتابی بود که تمام موضوعات مرتبط این حوزه را پوشش داده باشد و نویسنده بتواند آن را به دانشجویان خود پیشنهاد نماید. این کتاب حاصل هشت سال تجربه تدریس نویسنده در زمینه برنامه‌نویسی 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 جزییات بحث نمی‌کند ولی منابع بسیاری در مورد آنها ارائه می‌دهد. در صورت نیاز برای شما آدرس‌های وبسایت‌های مرتبط هم فراهم شده است ولی متاسفانه نمی‌توان تضمین نمود که هنوز هم وقتی شما در حال خواندن این کتاب هستید، این صفحات وب دردسترس 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 قراردادند، تشکر می‌نماید که نام برخی از آنها در اینجا ذکر می‌شود. تشکر ویژه از Rolf Oppiłger 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 توام با مهربانی‌هایشان. تشکر ویژه از پروفسورMehdi Jazayeri رئیس دپارتمان و همکار نویسنده، 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. نهایتا تشکر ویژه از همسرم Hannes 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. پیشاپیش از بازخوردهایی که برای من ارسال می‌نمایید، نیز تشکر می‌کنم.