

لایه هشتم، لایه امنیت

مؤلف

محمد حیدری تفرشی



فرازان‌دیش سبز

بهار ۱۳۸۶

سیرشناسه	حیدری تفرشی، محمد، ۱۳۶۰ -
عنوان و پدیدآور	لایه هشتم، لایه امنیت / مؤلف محمد حیدری تفرشی.
مشخصات نشر	تهران: فرازاندیش سبز، ۱۳۸۵.
مشخصات ظاهری	VI، ۲۱۶ ص.: مصوره، جدول، نمودار.
شابک	۳۵۰۰۰ ریال: 978-964-8034-48-6
وضعیت فهرست‌نویسی	فیا
موضوع	کامپیوترها -- ایمنی اطلاعات.
موضوع	شبکه‌های کامپیوتری -- اقدامات تأمینی.
رده‌بندی کلّی	ح ۹ / الف ۹ / ۹۶ QA
رده‌بندی دیوینی	۰۰۵/۸:
شماره کتابخانه ملی	۵۰۷۸۴-۵-۸۵م



لایه هشتم، لایه امنیت

مؤلف : محمد حیدری تفرشی
 ناشر : مؤسسه انتشارات فرازاندیش سبز
 چاپ : اول - بهار ۱۳۸۶
 تیراژ : ۱۰۰۰ جلد
 چاپ و صحافی : شرکت چاپ فرازاندیش سبز
 شابک : ۹۷۸-۹۶۴-۸۰۳۴-۴۸-۶

فرازاندیش سبز: ۱۰۰۴۳۱۶-۰۹۱۲ و ۶۶۹۶۹۵۰۵ فکس: ۶۶۴۶۰۸۳۲
 نشانی: خ انقلاب، خ دانشگاه، تقاطع لبافی‌نژاد، پلاک ۱۳۵، طبقه دوم، واحد ۴

قیمت: ۳۵۰۰ تومان
 قیمت DVD: ۱۵۰۰ تومان

فهرست مطالب

عنوان	صفحه
پیشگفتار مؤلف.....	الف
فصل اول - مقدمه ای بر امنیت اطلاعات.....	۱
فصل دوم - مقدمه ای بر رمزنگاری.....	۵۳
فصل سوم - تهدیدها و آسیب پذیربها.....	۸۳
فصل چهارم - ملاحظات امنیتی سیستم عامل.....	۱۲۱
فصل پنجم - امنیت در پایگاه داده.....	۱۳۷
فصل ششم - امنیت شبکه.....	۱۵۳
فصل هفتم - نقش مدلسازی و شبیه سازی در امنیت اطلاعات.....	۱۷۳

فهرست شکلها و جداول

شکل (۱-۱): خسارت مالی ناشی از انواع تهدیدهای امنیتی	۵
شکل (۱-۲): نمونه ای از یک Dongle بیسیم	۸
جدول (۱-۱): خلاصه ای از انواع سیستم های بیومتریک های معمول	۱۰
شکل (۱-۳): نمونه ای از یک سیستم بیومتریک امضاء	۱۳
شکل (۱-۴): مدلی برای مدیریت امنیت اطلاعات	۱۸
شکل (۱-۵): چرخه مدیریت ریسک	۲۴
شکل (۱-۶): سطوح مختلف RAID	۲۷
شکل (۱-۷): روند کاری ^۱ بازیابی منابع اطلاعاتی صدمه دیده ناشی از حوادث امنیتی	۳۳
شکل (۱-۸): وظایف تیم واکنش سریع	۳۵
شکل (۱-۹ الف): شاخصه های امنیت	۳۷
شکل (۱-۹ ب): شاخصه های قابل اعتماد بودن	۳۷
شکل (۱-۱۰): شاخصه های امنیت اطلاعات از دید رفتاری/حفاظتی	۳۸
شکل (۱-۱۱): شاخصه های رفتاری	۳۹
شکل (۱-۱۲): مدل سیستم پیشنهادی	۴۰
شکل (۱-۱۳): مراحل ایمن سازی بر اساس استاندارد BS7799:2002	۴۵
شکل (۱-۱۴): مراحل ایمن سازی بر اساس گزارش فنی ISO/IEC 13335	۴۶
شکل (۱-۱۵): میزان آسیب پذیری های گزارش شده	۴۸
شکل (۲-۱): روشهای رمزنگاری فیزیکی	۵۶
شکل (۲-۲): ماشین رونور	۵۸
شکل (۲-۳): مثالی از رمز تک حرفی	۶۱
شکل (۲-۴): نقشه فرودگاه که باید پنهان سازی شود	۶۴
شکل (۲-۵): فایل Gif، حامل نقشه فرودگاه (پس از پنهان سازی)	۶۴
شکل (۲-۶ الف و ب): پالت شکل (۲-۵) قبل / بعد از پنهان سازی نقشه فرودگاه	۶۴
شکل (۲-۷): فایل حامل نقشه فرودگاه در فرمت JPEG	۶۶
شکل (۲-۸): تصویر سیگنال صوتی حامل قبل / بعد از پنهان سازی نقشه فرودگاه	۶۷
شکل (۲-۹): یک فرایند درهم سازی ساده	۶۸
شکل (۲-۱۰): دو سناریو از رمزنگاری متقارن	۷۱
شکل (۲-۱۱): سیستم رمزنگاری کلید عمومی	۷۳
شکل (۲-۱۲): سناریویی برای RA و CA	۷۷

۷۸	شکل (۲-۱۳): نمونه ای از گواهی X.509
۷۹	شکل (۲-۱۴): مدل سلسله مراتبی
۸۰	شکل (۲-۱۵): مدل پل
۸۰	شکل (۲-۱۶): مدل مشبک
۸۷	شکل (۳-۱): نمونه ای از یک CVE
۸۹	شکل (۳-۲): طبقه بندی کدهای مخرب
۹۳	شکل (۳-۳): بمب منطقی
۹۶	جدول (۳-۱): ویروسهای بیولوژیکی / ویروسهای کامپیوتری
۹۷	شکل (۳-۴): آناتومی ویروس
۹۸	شکل (۳-۵): طبقه بندی ویروسها
۹۹	شکل (۳-۶): مکانیزم ویروس فایلهای اجرایی
۱۰۳	شکل (۳-۷): کرم SQL Sapphire Slammer
۱۰۴	شکل (۳-۸): آناتومی کرمها
۱۰۵	شکل (۳-۹): پیغام کرم بلستر
۱۱۵	شکل (۳-۱۰): دست دادن سه طرفه TCP
۱۱۶	شکل (۳-۱۱): حمله اختلال در سرویس دهنی به روش گسیل بیتل آسی SYN ها
۱۱۹	شکل (۳-۱۲): معماری حمله DDOS
۱۲۷	شکل (۴-۱): روابط حفاظتی بین سگمنت ها
۱۲۹	شکل (۴-۲): ماتریس دسترسی
۱۳۰	شکل (۴-۴): فهرست های قابلیت
۱۳۲	شکل (۴-۵): کارکردهای سیستم عامل در مد هسته
۱۳۴	شکل (۶-۴): تقابض امنیتی سیستم عامل
۱۶۰	شکل (۶-۱): معماری IPsec
۱۶۱	شکل (۶-۲): حالت انتقال / حالت تونل
۱۶۴	جدول (۶-۱): مقایسه ای میان حالت انتقال و حالت تونل
۱۶۵	شکل (۶-۳): اجزاء هدر احراز هویت
۱۶۶	شکل (۶-۴): داده احراز هویت شده
۱۶۸	شکل (۶-۵): اجزاء بدنه امنیتی محفظه بندی شده (ESP)
۱۶۹	شکل (۶-۶): روش محاسبه (ESP)
۱۷۶	شکل (۷-۱): طبقه بندی مدل ها
۱۷۸	شکل (۷-۲): سه گونه نمایش متفاوت از یک مدل
۱۸۱	شکل (۷-۳): اجزاء HLA
۱۹۱	شکل (۷-۴): حمله DDOS - مدل سازی و شبیه سازی با OPNET
۱۹۲	شکل (۷-۵): نتایج شبیه سازی

پیشگفتار

امنیت در عصری که مهمترین کالای تبدل‌پذیر آن اطلاعات است مفوله‌ای در خور توجه و بازنگری است. نه می‌توان آن را پدیده‌ای تشریفاتی و زاید پنداشت چنان‌که در نظر اکثر تصمیم‌سازان و مجریان سامان‌انگاشته‌اند و نه می‌توان تحصیل آن را دور از دسترس دید چنان‌که جسد و جبهه‌هایی می‌شود تا در باورمان بگنجانیم: کشوری که میزبانی اطلاعاتش در دست دیگری است و خرد و کلان سخت‌فزاری و نرم‌افزاری اش از آن سری مرزها می‌آید، چه کارش به امنیت! که:

تو کز معامله جز باد دستگیرت نیست حدیث باد فروشان چه می‌کنی باور

باری هر دوی این آفات بر انگاره‌مان سایه افکنده است. هتروگونه آنکه در این میان، گروه‌سومی سخن از طراحی امن‌ترین سیستم عامل را بر زبان می‌رانند. (لینوکس شریف) بی‌آنکه بیچاره خلق را متقاعد سازند که حجت بالغه‌شان بر این مدعا چیست.

انگیزه نگارش چنین کتابی دغدغه‌ای بود که طی این سالیان نگارنده با خود داشت و آن وجود مداخل و منابعی (به زبان فارسی) است که در گزینش آنها برای آراستن به زیور طبع و در شیوه ترجمه‌شان کمترین ملاحظات علمی و آکادمیک در نظر گرفته نشده است؛ که این نه سزای اهل علم و دانش پژوهان است. از اینروست که در طول نگارش این کتاب سعی بر آن بود تا از میان موضوعات مطروحه در مفوله امنیت اطلاعات، مباحث به گونه‌ای گلچین شوند که دارای یک روند منطقی و علمی باشد. از سویی دیگر نیک می‌دانید که دانش‌آموختگان کامپیوتر در مقطع کارشناسی به پاس ژرف‌اندیشی و آینده‌نگری الوالایب و تصمیم‌سازان این دیار، حتی کلمه‌ای در باره این واجب (امنیت اطلاعات) در طول دوران تحصیل فرا نمی‌گیرند، شاید به همین دلیل فصول این کتاب بگونه‌ای تدوین شد تا با سرفصلهای درسی دوره‌های کارشناسی همگون باشد، و شاید اگر چنین وسواسی نبود این کتاب باید فربه‌تر می‌نمود.

در دوران نگارش این کتاب، نگارنده مکرراً در ترجمه واژگان تخصصی و آوردن واژگان معادل یا مواعی مواجه بوده است. شاید دلیل چنین نقصانی این باشد که اساتید فن، پای خویش را در بحر ترجمه متون تخصصی، تر نمی‌کنند و از همین حیث فخر می‌فروشند که جستار نانوشت‌شان عاری از هر سهو و خطایی است!

این حقیر از سال ۲۰۰۳ میلادی مبادرت به نوشتن مقالاتی^۱ در حیطه امنیت اطلاعات نمودم. این مقالات در برخی از مراجع و مداخل امنیتی نامدار بر روی وب منتشر گردید^۲ و روزانه مورد بازدید هزاران نفر

از سراسر جهان قرار گرفت. این امر موجب شد تا این مقالات (مروری / پژوهشی) در معرض نقد علمی بازدید شوندگان قرار گیرد. شاید از دیگر دلایل پیدایش این کتاب، وجود چنین مقالاتی است.

با توجه به ملاحظات فوق کتابی که پیش روی شماست مشتمل بر هفت فصل است. در فصل اول به رسم معهود، به بیان معانی واژگان و مفاهیم کلیدی عرصه امنیت اطلاعات پرداخته‌ام. در این فصل امنیت فیزیکی و ملاحظات آن مورد توجه قرار گرفته است. استفاده از سیستم‌های بیومتریک بعنوان یک مکانیزم امنیتی کارا در تامین امنیت فیزیکی بررسی شده است. ارائه یک مدل ابتکاری برای مدیریت امنیت اطلاعات و بررسی اجزای آن از دیگر موضوعات تشکیل دهنده این فصل است. از دیگر مطالب این فصل بررسی چارچوب جدیدی برای امنیت اطلاعات است. در این چارچوب شاخصه "قابل اعتماد بودن" به مفهوم امنیت اضافه شده است. در انتهای این فصل چشم انداز آینده امنیت اطلاعات از دو دیدگاه "تحلیل اطلاعات آماری" و "ریسک گرا" مورد بررسی قرار گرفته است.

فصل دوم این کتاب به مقوله رمزنگاری پرداخته است. در این فصل با ارائه یک دسته بندی ابتکاری کلیه روشهای رمزنگاری به سه دسته رمزنگاری فیزیکی، رمزنگاری ریاضی و رمزنگاری کوآنتوم طبقه بندی شده است. بررسی روشهای نوین پنهان نویسی پیام در قالب فایل های گرافیکی و صوتی از نکات برجسته این فصل است. در انتهای این فصل زیرساخت کلید عمومی و ملاحظات آن مورد توجه قرار گرفته است.

فصل سوم به تهدیدها و آسیب پذیریهایی مبتلاء به در حیطه امنیت اطلاعات اشاره دارد. در این فصل به دو گروه عمده از این تهدیدها و آسیب پذیریا (کدهای مخرب و حملات اختلال در سرویس های) اشاره شده است.

در فصل چهارم به ملاحظات امنیتی یکی از زیرساخت‌های نرم افزاری (سیستم عامل) پرداخته شده است. در این فصل مکانیزم‌های امنیتی سیستم عامل که میان سیستم عامل‌های متن باز و غیر آن مشترک است، مورد بررسی قرار گرفته است.

در فصل پنجم با توجه به کار ارزشمندی که از جناب آقای دکتر برائتی وجود داشت به بررسی مکاتیرم‌های امنیتی در پایگاه داده بعنوان یکی از حیاتی‌ترین سیستم‌های نرم‌افزاری در دنیای تجارت الکترونیک امروزی پرداخته شده است.

فصل ششم، ملاحظات امنیتی نسخه ششم اینترنت را به بحث نهشته است. پروتکل‌های ارتباطی به طور عام و پروتکل TCP/IP به طور خاص نقش بسزایی در پیاده سازی شبکه‌های ارتباطی و اطلاعاتی دارد از این رو برقراری امنیت در این شبکه‌ها مستلزم وجود پروتکل‌های امن ارتباطی است.

فصل هفتم این رساله که بحق وامدار اشارات و انشانات استاد فرزانه جناب آقای دکتر قاسم آقایی است به موضوع نقش و جایگاه مدلسازی و شبیه سازی در حیطه امنیت اطلاعات می پردازد. در این فصل ضمن تبیین جایگاه مدلسازی و شبیه سازی در امنیت اطلاعات به بررسی وضع موجود آن در حیطه امنیت اطلاعات پرداخته شده است و چالشهای فرا روی آن مورد تحلیل قرار گرفته است.

به همراه این کتاب یک لوح DVD عرضه شده است. در این DVD رکوردهای اطلاعاتی مربوط به وب سایت Astalavista عرضه شده است که در جای خود می تواند مورد رجوع و استفاده علاقه مندان قرار گیرد. همچنین پیاده سازی دو الگوریتم رمزنگاری DES و RSA به همراه اسلایدهای تدوین شده از روی متن کتاب از دیگر مطالب تشکیل دهنده این لوح می باشد.

از افاضل زمان، چنان که رسم است، نخواستم که دیباچه و مقدمه ای بر کتاب من بنویسد و عیبها و ضعفهای آن را با برگ انجیری از تقریظ و تمجید بیوشانند. این دفتر حاصل بالاترین تلاش و برترین تکاپوی پژوهشی من است. اگر حق مطلب ادا نشده است کاستی ها را بحساب ضعف بیان و بنان من بگذارید که خدا هیچکس را جز به اندازه توانش مکلف نمی کند. امید که صاحب نظران فهیم و فرزانه با ذهن نقاد و ضیع وقاد خویش این وجیزه را با دیده ملاطفت و اغماض بشگرند و کاستی هایم را کریمانه بنگارند. نقدهای سازنده و رهنمودهای ارزنده شما را چشم در راهم.

مهندس محمد حیدری تفرشی

STh.Layer@gmail.Com