

۱۲۵۵۴۶۵

۶۵۵۱۰



بررسی امنیت در شبکه و نرم افزار

(تهدیدات و استانداردها)

تدوین و گردآوری:

دکتر فضل الله ادیب نیا

مهندس مهیلا دادفر نیا

سرشناسه	: ادیب‌نیا، فضل‌الله، ۱۳۴۱ -
عنوان و نام پدیدآور	: بررسی امنیت در شبکه و نرم‌افزار (تهدیدات و استانداردها)
مشخصات نشر	: یزد: دانشگاه یزد، ۱۳۹۴.
مشخصات ظاهری	: ۲۰۰ص.: مصور، جدول، نمودار
شابک	: 978-600-6309-61-3
وضعیت فهرست‌نویسی	: فبیای مختصر
یادداشت	: فهرست‌نویسی کامل این اثر در نشانی: http://opac.nliai.ir قابل دسترسی است
یادداشت	: واژه نامه .
شناسه افزوده	: دادفر، مهیلا، ۱۳۶۱-
شناسه افزوده	: دانشگاه یزد
شماره کتابشناسی ملی	: ۲۸۶۴
کد پیگیری	: ۳: ۳۳۷

مرکز انتشارات دانشگاه یزد

یزد، صفائییه، بلوار دانشگاه، صندوق پستی ۷۴۱-۸۹۱۹۵ تلفن: ۹-۳۸۲۱۱۶۷۰-۰۳۵

دورنگار ۸۲۰۰۱۰۶-۰۳۵۱

عنوان کتاب: بررسی امنیت در شبکه و نرم‌افزار (تهدیدات و استانداردها)
تدوین و گردآوری: دکتر فضل‌الله ادیب‌نیا، مهندس مهیلا دادفر
ناشر: انتشارات دانشگاه یزد

لیتوگرافی، چاپ و صحافی: یزد- انتشارات شاهنده

نوبت چاپ: اول

سال چاپ: ۱۳۹۴

شمارگان: ۱۰۰۰ نسخه

قیمت پشت جلد: ۱۲۰،۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۳۰۹-۶۱-۳

مرکز پخش: موسسه کتابیران

تهران، میدان انقلاب، کارگر شمالی، خیابان نصرت، خیابان دکتر قریب، نرسیده به فرصت، پلاک ۷.

تلفن: ۱۵-۶۶۵۶۶۵۱۰-۰۲۱

فهرست

۱.....پیش گفتار

۳.....مقدمه

فصل اول

۹.....مبانی امنیت

۱۰.....۱-۱ مقدمه

۱۱.....۲-۱ اصول امنیت اطلاعات

۱۵.....۳-۱ امنیت ارتباطات

۱۷.....۴-۱ رمز نگاری

۱۸.....۴-۱-۱ سیستم‌های رمز نگاری

۱۸.....الف) رمز نگاری متقارن

۱۹.....ب) رمز نگاری نامتقارن

۲۰.....ج) درهم‌سازی

۲۱.....د) شور سازی

۲۲.....۴-۱-۲ برخی از روش‌های شکستن رمز

۲۲.....الف) جدول رنگین کمان

۲۳	 (ب) حمله فرهنگ لغات
۲۵	 (ج) حمله جستجوی فراگیر
۲۵	 ۵-۱ استانداردهای برنامه نویسی امن
۲۶	 ۱-۵-۱- CWE استاندارد
۲۷	 ۱-۵-۲- CERT استاندارد
۳۰	 ۱-۵-۳- OWASP استاندارد
۳۱	 ۱-۶-۱ مدل سازی تهدید
۳۱	 الف) رویکردهای چرخه حیات
۳۲	 ب) رویکرد نرم افزار
۳۲	 ج) رویکرد دارایی
۳۲	 ۱-۶-۱ سیر تکاملی مدل سازی تهدید
۳۳	 ۱-۶-۲ مراحل تولید مدل تهدید
۳۳	 مرحله اول : تجزیه نرم افزار
۳۸	 مرحله دوم : شناسایی و رتبه بندی تهدیدات
۴۱	 مرحله سوم : تعیین اقدامات متقابل و کاهش اثرات تهدیدات
۴۲	 ۱-۶-۳ استراتژی کاهش تاثیرات تهدید
۴۳	 خلاصه مطالب فصل
۴۵	 پرسش

فصل دوم

۴۷	 ریسک های معمول در سازمان ها
۴۸	 ۲-۱ مقدمه
۵۰	 ۲-۲ جدی ترین ریسک های سازمانی

۵۰	۲-۱-تزریق
۵۱	الف) بررسی وجود آسیب پذیری تزریق
۵۲	ب) شیوه جلوگیری از آسیب پذیری تزریق
۵۴	ج) مثال از سناریوی حمله
۵۷	۲-۲-دسترسی غیرمجاز و مدیریت جلسه
۵۸	الف) بررسی وجود آسیب پذیری دسترسی غیرمجاز و مدیریت جلسه
۶۱	ب) شیوه جلوگیری از دسترسی غیرمجاز و مدیریت جلسه
۶۲	ج) مثال از سناریوی حمله
۶۳	۲-۳-حمله XSS
۶۶	الف) بررسی وجود آسیب پذیری XSS
۶۷	ب) شیوه جلوگیری از حمله XSS
۷۰	ج) مثال از سناریوی حمله
۷۱	۲-۴-ارجاع مستقیم شی نامن
۷۱	الف) بررسی وجود آسیب پذیری ارجاع مستقیم شی نامن
۷۲	ب) شیوه جلوگیری از ارجاع های مستقیم شی نامن
۷۴	ج) مثال از سناریوی حمله
۷۴	۲-۵-پیکربندی نادرست امنیتی
۷۵	الف) بررسی وجود آسیب پذیری پیکربندی نادرست امنیتی
۷۷	ب) شیوه جلوگیری از خطای پیکربندی نادرست امنیتی
۷۷	ج) مثال از سناریوی حمله
۷۹	۲-۶-افشای داده های حساس
۷۹	الف) بررسی وجود آسیب پذیری افشای داده های حساس
۸۰	ب) شیوه جلوگیری از افشای داده های حساس

- ۸۱..... (ج) مثال از سناریوی حمله
- ۸۴..... ۷-۲-۲- کنترل سطح دسترسی
- ۸۴..... (الف) بررسی وجود آسیب پذیری کنترل سطح دسترسی توابع
- ۸۵..... (ب) شیوه جلوگیری از کنترل سطح دسترسی توابع
- ۸۶..... (ج) مثال از سناریوی حمله
- ۸۸..... ۸-۲-۲- جعل درخواست بین سایتی (CSRF)
- ۸۸..... (الف) بررسی وجود آسیب پذیری جعل درخواست بین سایتی
- ۸۹..... (ب) شیوه جلوگیری از جعل درخواست بین سایتی
- ۹۱..... (ج) مثال از سناریوی حمله
- ۹۳..... ۹-۲-۲- استفاده از امنی با آسیب پذیری های شناخته شده
- ۹۳..... (الف) بررسی وجود آسیب پذیری استفاده از اجزاء آسیب پذیر
- ۹۴..... (ب) شیوه جلوگیری از آسیب پذیری استفاده از اجزاء آسیب پذیر
- ۹۶..... (ج) مثال از سناریوی حمله
- ۹۷..... ۱۰-۲-۲- تغییر مسیر دهی های (FCID و REDIRECT) غیر معتبر
- ۹۸..... (الف) بررسی وجود آسیب پذیری تغییر مسیر دهی
- ۹۹..... (ب) شیوه جلوگیری از تغییر مسیر دهی
- ۱۰۰..... (ج) مثال از سناریوی حمله
- ۱۰۲..... ۳-۲-۲- آسیب پذیری های دیگر
- ۱۰۲..... ۱-۳-۲- سرریز بافر
- ۱۰۵..... ۲-۳-۲- فرمت رشته
- ۱۰۶..... ۳-۳-۲- کلیک دزدی
- ۱۰۶..... ۴-۳-۲- حمله ممانعت از خدمات (DOS)
- ۱۰۷..... ۵-۳-۲- نشت اطلاعات و مدیریت نادرست خطا
- ۱۰۸..... ۶-۳-۲- ثبت ناکافی وقایع

۱۰۸	۷-۳-۲ اجرای فایبل مخرب
۱۰۸	۸-۳-۲ انتساب زیاد
۱۰۹	۴-۲ امنیت در برنامه‌های وب
۱۱۱	خلاصه مطالب فصل
۱۱۱	پرسش

فصل دوم

۱۱۳	استاندارد بررسی امنیتی نرم‌افزار
۱۱۴	۱-۳ مقدمه
۱۱۴	۲-۳ رویکرد
۱۱۶	۱-۲-۳ سطح صفر: مقدماتی
۱۱۶	۲-۲-۳ سطح ۱: معمولی
۱۱۷	۳-۲-۳ سطح ۲: استاندارد
۱۱۸	۴-۲-۳ سطح ۳: پیشرفته
۱۱۹	۳-۳ جزئیات بررسی نیازمندی‌ها
۱۲۰	۱-۳-۳ - نیازمندی‌های بررسی احراز هویت (V2)
۱۲۲	۲-۳-۳ - نیازمندی‌های بررسی مدیریت جلسه (V3)
۱۲۵	۳-۳-۳ - نیازمندی‌های بررسی کنترل دسترسی (V4)
۱۲۶	۴-۳-۳ - نیازمندی‌های مدیریت ورودی مخرب (V5)
۱۲۹	۵-۳-۳ - نیازمندی‌های بررسی رمزنگاری (V7)
۱۳۱	۶-۳-۳ - نیازمندی‌های بررسی ثبت و مدیریت خطا (V8)
۱۳۳	۷-۳-۳ - نیازمندی‌های بررسی حفاظت داده‌ها (V9)

۱۳۴	۳-۳-۸- نیازمندی‌های بررسی امنیت ارتباطات (V10)
۱۳۵	۳-۳-۹- نیازمندی‌های بررسی امنیت HTTP (V11)
۱۳۶	۳-۳-۱۰- نیازمندی‌های بررسی کنترل‌های مخرب (V13)
۱۳۸	۳-۳-۱۱- نیازمندی‌های بررسی منطق تجاری (V15)
۱۴۰	۳-۳-۱۲- نیازمندی‌های بررسی منابع و فایل‌ها (V16)
۱۴۱	۳-۳-۱۳- نیازمندی‌های بررسی سیار (V17)
۱۴۳	۳-۳-۱۴- راه‌ها برای برنامه‌نویسان
۱۴۳	۳-۴-۱- بررسی کد
۱۴۸	۳-۴-۲- آزمون
۱۵۰	خلاصه مطالب فصل
۱۵۱	پیش
	پیوست ۱
۱۵۳	گروه واکنش اضطراری رایانه
	پیوست ۲
۱۷۲	مثال از مدل‌سازی تهدید
۱۸۲	واژه نامه
۱۸۸	منابع

پیش گفتار

باتوجه به توسعه روزافزون سیستم‌ها و دنیای فناوری اطلاعات، فراهم آوردن امنیت در سامانه‌ها از جایگاه ویژه‌ای برخوردار می‌باشد؛ زیرا همراه با پیشرفت علم و حرفه‌ای‌تر شدن برنامه‌ها، هکرها نیز پیشرفت فوق‌العاده‌ای کرده‌اند و روزانه خبرهای زیادی درباره نفوذ بیگانگان و هکرها در سیستم‌ها شنیده می‌شود. بنابراین آشنایی با امنیت و نحوه برقراری آن و همچنین مقابله با خطرات احتمالی جهت بقای سازمان‌ها ضروری می‌باشد. به همین دلیل در این کتاب سعی شده است، در باره امنیت در سازمان‌ها نوشته شود.

با توجه به اینکه موضوع امنیت در کشورمان در طی "پانزده سال اخیر مطرح و حساس گردیده است و کتاب‌های فارسی کمی درباره امنیت سایبری وجود دارد. تلاش نویسندگان بر این بوده که این کتاب به روزترین مطالب را در ارتباط با استاندارد به‌روز دنیا به زبان ساده بیان کند و مطالب آن به نحوی انتخاب شده که جهت پژوهش و برنامه‌نویسان ساده‌فهم مفید بوده و سوالات کارکنان را نیز پاسخ دهد؛ مخصوصاً که نویسندگان کتاب، سابقه اجرایی در سازمان‌ها را دارند. علاوه بر این، نیاز آموزشی دانشجویان را در درس‌های امنیتی مقطع کارشناسی و کارشناسی ارشد پاسخ دهد. همچنین جهت درک بهتر مفاهیم خواننده کتاب، در قسمت‌هایی که جنبه عمومی بیشتری دارد، مثال‌ها و توضیحات بیشتری به متون ترجمه شده اضافه نمودیم.

در خاتمه با سپاس از عنایت الهی در تهیه این کتاب، از حمایت و پشتیبانی ستاد توسعه فناوری اطلاعات، ارتباطات و میکروالکترونیک معاونت علمی و فناوری ریاست جمهوری و مرکز آپای دانشگاه یزد، دکتر کیارش میزانیان جهت بازنگری کتاب، دکتر عبدالمجید انصاری مدیر امور پژوهشی دانشگاه یزد و سایر مسئولین دانشگاه که در چاپ این کتاب همکاری داشته‌اند، تشکر و قدردانی می‌گردد. لازم به یاد آوری است که این کتاب را تعدادی از اساتید صاحب نام در حوزه دانشگاه بازیینی و داوری نموده‌اند و نقطه نظرات آنان در اصلاح، تغییر و تکمیل مندرجات آن لحاظ شده است. با این وصف، اگر همچنان اشتباهی در آن مشاهده شود، به طور قطع به عهده نویسندگان می‌باشد و پیشاپیش تمام کاستی‌های این کتاب را پذیرفته و از هر پیشنهاد یا انتقادی به منظور بهتر شدن کتاب استقبال می‌شود و خواهشمند است نویسندگان را با اشاراتی به آدرس na@ices.yazd.ac.ir ، m-dadfarnia@stu.yazd.ac.ir مستحضر فرمایید تا اصلاحات انجام و تکمیل گردد. امید است این خدمت ناچیز مورد قبول خداوند متعال قرار گرفته و قابل استفاده برای شما عزیزان باشد.

مقدمه

در دنیای سایبری امروز، افزایش تعداد برنامه‌های تحت وب و پیچیدگی تهاجم روی شبکه‌های کامپیوتری باعث شده است که مسئله محافظت و مراقبت یکی از مسائل کلیدی در بحث امنیت کامپیوتر شود و جرایم رایانه‌ای به یکی از مباحث جدی و مهم تبدیل گردد. از آنجا که یک سازمان از صدها فرد تشکیل شده که خود یک شبکه بزرگ‌تری را تشکیل می‌دهند و از طریق رایانه با دیگر تعامل دارند، ارتباط اجتماعی در کنار تکنیک‌های فنی باعث چالش‌هایی در زمینه امنیت شده است. به همین منظور، شناسایی حملات ممکن در این ارتباطات اجتماعی به منظور یافتن تکنیک‌های قابل استفاده توسط هکر¹ و همچنین جهت مقابله توسط مدیر سیستم ضروری می‌باشد.

در دنیای کامپیوتر، در یک تعریف ساده می‌توان هکر را فردی نامید که در یک سیستم نفوذ می‌کند و آن سیستم را مجبور به کار می‌کند که می‌خواهد را انجام دهد؛ حتی اگر سیستم نخواهد. اما تعریف دقیق‌تر، هکر را برنامه‌نویس حرفه‌ای و هوشمندی معرفی می‌کند که با استفاده از تخصص و تسلط خود بر حیطه‌های مختلف دنیای کامپیوتر و وب، قادر است در لایه‌های پیچیده‌تر سیستم‌ها نفوذ کرده و موانع آن را برطرف کند و از آن به هر نحو بهره‌برداری و سوء استفاده نماید² یا بر آن اساس سیستمی نو خلق کند. از مشخصه‌های یک هکر می‌توان این موارد را عنوان کرد:

- کسی که از یادگیری جزئیات یک زبان برنامه‌نویسی یا سیستم‌ها لذت می‌برد.
- کسی که از انجام دادن یک برنامه لذت می‌برد.
- کسی که ارزش هک دیگران را درک کرده و به آن احترام می‌گذارد.

¹ Hackers

² Exploit

- کسی که در عمق یک سیستم فرو می‌رود تا حداکثر توانایی‌های آن را درک و از آن استفاده کند.
- کسی که معمولاً به همان میزان که در یاد گرفتن شوق دارد، یاد دادن را هم دوست دارد.

در واقع، اولین کسانی که هکر نامیده شدند، افرادی بودند که در موسسه فناوری ماساچوست به هر کاری به جز درس خواندن می‌پرداختند. واژه هکر از سال ۱۹۸۶ بین دانشجویان این موسسه شکل گرفت و به کسانی که همواره در پشت بام و محل‌های غیرمجاز بودند، گفته می‌شد. هکرها، امنیت را می‌توان به چهار مجموعه زیر تقسیم نمود [۸]:

هکر کلاه سفید یا **هکرها خوب**: هکری که از دانش خود برای محافظت و ارتقای سطح امنیتی یک سیستم و شبکه، بهره‌مند استفاده می‌کند و از طرف شرکت‌های زیادی با حقوق بسیار بالا به کار گرفته می‌شود.

هکر کلاه سیاه^۱ یا **هکرها مخرب**: این نوع هکر، نقطه مقابل کلاه سفید می‌باشد؛ تنها به فکر نفوذ است و زیاد به قانون اهمیت نمی‌دهد. معمولاً مهارت بالایی دارد. از نفوذ^۲ جهت آسیب رساندن به شبکه‌ها و سرورها استفاده می‌کند و به این وسیله کسب درآمد می‌کند.

هکر کلاه خاکستری^۳ یا **هکرها میانه‌رو**: هکری که به سبب گاهی با امن‌سازی و گاهی با نفوذ، هر جا که پول باشد همانجا است. این فرد خیلی خاص به یک طرف ندارد و بسته به موقعیت، گاهی اعمال خرابکارانه و گاهی هم اعمال مفید انجام می‌دهد.

^۱ Whitehat

^۲ Blackhat

^۳ Hack

^۴ Grayhat

هکر کلاه صورتی^۱ یا هکرهای خوشحال : هکر کلمه مناسبی برای این گروه نیست، فردی که با استفاده از انواع ابزار و آسیب‌پذیری عمومی با تخریب نرم‌افزارها و سایت‌ها خود را هکر جلوه می‌دهد و سعی بر کسب شهرت دارد.

در رابطه با امنیت اصطلاحات مختلفی مانند تهدید، آسیب‌پذیری و ریسک مطرح می‌شود که در ادامه تعریف آن آمده است:

تهدید : تهدید، خطری است که با استفاده از آسیب‌پذیری، در امنیت شکاف ایجاد می‌نماید و سبب آسیب و زیان می‌گردد. یک منبع (فیزیکی یا منطقی) می‌تواند یک یا چند آسیب‌پذیری داشته باشد که توسط یک عامل تهدید به کار گرفته شده است. مثلاً خرابی فنی سخت‌افزار (مثل خرابی تجهیزات) و خرابی نرم‌افزار (باگ‌ها، مشکلات کد و حفره‌های ناشناخته) و همچنین وقایع طبیعی همچون آسیب به مرکز داده برای وقوع زلزله از انواع تهدید می‌باشند.

آسیب‌پذیری (کاستی)^۲ : آسیب‌پذیری یک ضعف در دارایی است که می‌تواند توسط یک یا چند تهدید مورد بهره‌برداری قرار گیرد. به عنوان مثال یک مهاجم می‌تواند از آسیب‌پذیری سرریز برای نصب بدافزار و در نتیجه آسیب رساندن به سیستم در بحث امنیت کامپیوتر، آسیب‌پذیری ضعیفی است که به مهاجم اجازه کاهش تضمین اطلاعات سیستم را می‌دهد، بنابراین برطرف کردن این نوع ضعف‌ها اهمیت زیادی دارد. سه عنصر مستعد بودن و وجود نقص در سیستم، دسترسی مهاجم به نقص و توانایی مهاجم جهت نفوذ از طریق نقص در آسیب‌پذیری نقش دارند.

ریسک : ریسک یا مخاطره احتمال رخ دادن اتفاق ناگواری است که سبب زیان می‌شود. برای وجود ریسک باید هم آسیب‌پذیری و هم تهدید از این آسیب‌پذیری وجود داشته باشد. در صورت

^۱ Pink

^۲ Threat

^۳ Vulnerability

عدم وجود آن دو، ریسک ایجاد نمی‌گردد. یک هکر (تهدید) می‌تواند از یک آسیب‌پذیری سوء استفاده نماید و این دو در مجموع یک ریسک را تشکیل می‌دهند[۹].

حمله سایبری^۱ نیز هر گونه آسیب‌پذیری تفسیر می‌شود که از حالت بالقوه به بالفعل تبدیل شود. چنانچه حمله صفر روزه^۲ یا حمله روز-صفر باشد، یعنی یک آسیب‌پذیری در یک نرم‌افزار کاربردی به تا بیش از آن ناشناخته بوده است، بهره‌برداری می‌کند و توسعه‌دهندگان برای رفع آسیب‌پذیری صفر روز فرصت داشته‌اند. اما چنانچه بهره‌کشی از آسیب‌پذیری قبل از افشا شدن آسیب‌پذیری باشد حمله روز منفی و چنانچه بعد از آن باشد، حمله روز مثبت نامیده می‌شود.

برای نشان دادن شدت آسیب‌پذیری‌های امنیتی در بسیاری از پژوهش‌ها، از معیار CVSS استفاده می‌شود که یک استاندارد صنعت و سازمان‌ها می‌باشد. بانک اطلاعاتی آسیب‌پذیری ملی (NVD^۳) نیز شامل اطلاعات آسیب‌پذیری‌ها با بردار اندازه CVSS می‌باشد. در واقع چنانچه مقدار CVSS برای یک آسیب‌پذیری از محدوده [۷.۰ و ۱۰.۰] باشد، از نظر شدت خطرناک بودن آسیب‌پذیری، خطر جدی محسوب می‌شود و در بانک اطلاعاتی NVD در محدوده [۳.۹ و ۱۰.۰] باشد، از نظر شدت خطرناک بودن آسیب‌پذیری، خطر کم محسوب می‌شود.

کلید این مجموعه در بانک اطلاعاتی، CVE ID می‌باشد. عناصر دیگر در CVSS، محدوده حمله آسیب‌پذیری (اعم از سرویس از راه دور یا مشتری محلی) از راه دور، نتایج (در دسترس‌پذیری، یکپارچگی، محرمانیت) و غیره می‌باشد. این معیارها، اطلاعات پایه‌ای و مهم را برای تحلیل امنیتی خودکار ایجاد می‌نمایند و تلاش می‌کنند تا معیاری را ایجاد نمایند تا نشان دهد که چقدر آسیب‌پذیری در مقایسه با سایر آسیب‌پذیری‌ها مهم می‌باشد و CVSS نه تنها یک معیار عددی می‌باشد، بلکه یک معیار اندازه‌گیری در توصیف جنبه‌های مختلف آسیب‌پذیری می‌باشد و از سه گروه اصلی تشکیل شده است:

¹ Attack

² Zero-day attack

³ Nvd.nist.gov

(۱) معیارهای ذاتی و اصلی یک آسیب‌پذیری که مستقل از زمان و محیط بوده و زیر مجموعه آن، بردار دسترسی، پیچیدگی دسترسی، تصدیق هویت، تاثیر محرمانگی، تاثیر یکپارچگی و تاثیر در دسترس پذیری می‌باشد.

(۲) معیارهای زمانی که خصوصیات آسیب‌پذیری را نشان می‌دهد و در طول زمان تغییر می‌یابند (نه محیط کاربر) و شامل قابلیت سوء استفاده، سطح بازسازی و اطمینان گزارشی می‌باشد.

(۳) معیار محیطی خصوصیات آسیب‌پذیری مرتبط با محیط کاربر در گروه معیار محیطی ذخیره می‌شود که شامل برابر، موازی، توزیع هدف، نیازمندی امنیتی می‌باشد. این معیارها در [۲] برای اولویت‌بندی در راهبرد ریسک استفاده شده‌اند. با این وجود، معیارها به خودی خود می‌توانند بدون در نظر گرفتن تهدیدات امنیتی در یک محیط سرمایه گذاری فقط اطلاعات محدودی را در اختیار قرار دهند.

این کتاب شامل ۳ فصل می‌باشد که برای ترجمه اصلاحات متن کتاب، از ترجمه انجمن رمز استفاده شده است و بخش عمده آن بر اساس استانداردهای OWASP تهیه شده و برای درک بهتر مفاهیم مرتبط با آن، بیشتر از مثال‌ها و توضیحات استفاده شده است. OWASP سازمانی بین‌المللی می‌باشد که در راستای ایمن‌سازی طراحی، پیاده‌سازی، توسعه و تست پروژه‌های نرم‌افزاری فعالیت می‌کند و استانداردهای مختلفی انتشار داده است. در این کتاب در فصل اول، به مقدمات و مفاهیم امنیتی، در فصل دوم به مطرح‌ترین ریسک‌های سازنده‌ها و چگونگی پیشگیری از این خطرات در سال‌های اخیر پرداخته می‌شود و در نهایت، فصل سوم به استاندارد مطرح بررسی امنیت نرم‌افزار می‌پردازد.