بسم الله الرحمن الرحیم

مهندسی

ارزیابی امنیت سیستم‌های کامپیوتری

مرجعی برای دروس

مهندسی نرم افزار و مهندسی امنیت و مباحث ویژه در نرم افزار

تألیف و تدوین:

دکتر ناصر مدیری

مهندس ناصر ولی

Publication Mehregane Ghalam

سرشناسه: مدیری،ناصر
عنوان: مهندسی ارزیابی امنیت سیستم‌های کامپیوتری
تالیف وتدوین: ناصر مدیری، ناصر ولی
مشخصات نشر: تهران، مهرگان قلم
مشخصات ظاهری: ۳۲۲ ص.: مصور
شابک: 978-600-6236-28-5
وضعیت فهرست‌نویسی: فیپا
یادداشت: واژه‌نامه
یادداشت: کتابنامه
موضوع: مهندسی امنیت — مهندسی نرم افزار — آزمون نرم افزار - مهندسی
شناسه افزوده: ناصر ولی
شناسه افزوده: مرجعی برای درس‌های مهندسی امنیت و مهندسی نرم افزار و مباحث ویژه در نرم افزار
رده‌بندی کنگره: ۱۳۹۱ ۹م۴م/۱۱۸۵۱۰۵/۵۹
رده‌بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۲۹۱۱۹۴۱

انتشارات مهرگان قلم
www.mehreganeghalam.com

مهندسی ارزیابی امنیت سیستم‌های کامپیوتری

مولف:.....ناصر مدیری — ناصر ولی
ناشر:.....مهرگان قلم
نوبت چاپ اول:.....۱۳۹۱
چاپ و صحافی:.....سپهرنوین
تیراژ:.....۵۰۰ نسخه
قیمت:.....۱۴۰۰۰۰ریال
شابک:.....۹۷۸-۶۰۰-۶۲۳۶-۲۸-۵

تهران، خیابان انقلاب، خیابان دانشگاه ، بین خیابان روانمهرو خیابان وحید نظری، کوچه قدیری، پلاک ۲۲، واحد ۳
تلفن: ۶۶۹۵۸۵۵۸ — ۶۶۹۶۰۷۶۳

پیشگفتار

ن و القَلَمِ وَ ما یَسطُرُونَ

پروردگار دانای حکیم را سپاس که با الطاف بیکران خود این توفیق را بر ما ارزانی داشت تا کتابی را در جهت یکی از اساسی‌ترین مباحث مهندسی کامپیوتر و در راه ارتقای دانش و فرهنگ این مرز و بوم به تألیف برسانیم.

در حقیقت هر ایده امنیت غیر قابل نفوذ، شاید از مسیری که از نظر طراحان آن حتی کوچکترین احتمال هم نمی‌رود، روزی نفوذ پذیر شود. این مسئله هیجان کودکانه‌ای را در وجود فعالان این حوزه پدیدار کرده است و تصور رقابت در ماوراء توانایی بشر در این ستیز طولانی و پایان ناپذیر انگیزه های کافی برای هر دو طرف دعوی (سوداگران امنیت و متخصصان امنیت) ایجاد کرده است.

رشد چشمگیر اخبار این تضادها و این مبارزه مبرهن است و مباحث مهندسی امنیت معنا نخواهد داشت مگر اینکه پاسخ سئوال هایی چون: حفظ امنیت چه سازمانی؟ چه سرمایه‌ای؟ در مقابل چه کسانی؟ در مقابل چه گستره‌ای از حملات یا تهدیدات؟ سیستمهای ما چقدر امن هستند؟ واقعا چند درصد از تجهیزات ما در قبال این نفوذها مقاوم هستند؟ چقدر مقاومت دارند؟ چقدر هزینه برای تعیین میزان امنیت سیستم‌های کامپیوتری سازمان باید پرداخت؟ چه میزان از امنیت مورد نیاز ما است؟ و صدها سئوال مشابه که هر کدام زمینه‌های تحقیقی بسیاری را فراهم آورده است را بدانیم. در این میان نیاز به یک مدل و اسلوب اساسی برای مدل‌سازی تهدیدات، ارائه فرایندهای بهبود یابنده برای تولید محصولات فن آوری، ارائه روشهای سودمند و مقرون به صرفه در ارزیابی امنیت سیستم‌ها و مسائلی از این دست به شدت احساس می‌شود.

هدف این کتاب توانا‌سازی و ارائه درک روشن تر و بهتر از میزان امنیت و صحت کارکرد سیستم‌ها است. برای دست یافتن به این مهم مهندسان می‌بایست سیستم‌های کنونی، چگونگی کارکرد این سیستم‌ها و مهمتر از همه نقص‌های پیش آمده احتمالی و چگونگی رفع آن و خسارات احتمالی در صورت وقوع را بشناسند.

به دلیل در هم تنیده بودن کلیه مباحث و تجهیزات فن آوری اطلاعات، کاملا مشخص است که همه مباحث ارائه شده دراین کتاب نوعا به هم مربوط خواهند بود و گاها تکرار مطالب الزامی به نظر می‌رسد. آخرین نکته بارز در طول مطالعه این کتاب این است که سنجش امنیت و ارائه یک معیار کمی و قابل

اندازه‌گیری به شرطی میسر است که همه مفاهیم و همه جنبه‌های مختلف این علم مورد بررسی قرار گیرد و مدیران پروژه و سازمانها اهمیت اعتماد به استانداردها و دانش متخصصان جوان را درک کنند.

بدین منظور این کتاب در ۸ فصل کلی طراحی شده است:

- فصل اول به بیان مشکلات و دلایل مطالعه کتاب، اصول، قواعد، اصطلاحات رایج حوزه امنیت فن آوری و ارتباط این مفاهیم و چگونگی استفاده از این کلمات در جایگاه خود بحث می‌کند. هدف اصلی این فصل توانمندسازی فعالان حوزه فن آوری در بیان مسائل خود به صورت استاندارد با بیانی روشن و واضح است.
- فصل دوم به بیان استانداردهای مختلف ارائه شده در سالهای اخیر توسط سازمان ایزو پرداخته، و مهمترین استانداردهای مدیریت امنیت، پیاده‌سازی امنیت و همچنین ارزیابی امنیت با شرح کامل و چگونگی استفاده آن بیان شده است.
- فصل سوم به بیان تعاریف کاملی از مهندسی امنیت، شاخه‌ها و زمینه‌های تحقیقی آن پرداخته، پس از بیان چالشها و مسائل مربوطه در هر بخش به معرفی سیستم‌های چند جانبه و چند لایه امنیت می‌پردازد.
- فصل چهارم به بیان تعاریف اساسی ارزیابی امنیت سیستم‌های کامپیوتری، مستندات ضروری، شیوه‌های ارزیابی و آزمایشگاه‌های ارزیابی امنیت و سطوح ضمانت امنیت پرداخته و برخی مدلهای مهم معرفی می‌شود.
- فصل پنجم به طور کامل اختصاص به بخش دوم استاندارد ISO/EIC 15408، دارد به گونه‌ای که کلیه مولفه‌های عملکردی امنیت بیان شده در این بخش با تفصیل و توضیح کامل بیان شده است.
- فصل ششم به طور کامل اختصاص به بخش سوم استاندارد ISO/EIC 15408، دارد به گونه‌ای که کلیه کلاس‌های تضمین امنیت و عناصر تضمین شده در این بخش با تفصیل و توضیح کامل بیان شده است.
- فصل هفتم به معرفی چرخه حیات استاندارد مهندسی سیستم تحت استاندارد ISO/EIC 12207 پرداخته و چرخه حیات مهندسی امنیت و ملاحظات امنیت در چرخه حیات تحت مستند NIST به طور کامل بیان شده است.

- فصل هشتم به بررسی انواع چارچوب‌های مهندسی امنیت امروزی پرداخته، مشکلات و مزایای این مدل‌ها جمع‌بندی شده، و در نهایت سعی بر ارائه مجموعه‌ای از مشخصه‌ها که لازمه چارچوب‌های امروزی باشد، شده است. این فصل با بیان چند مدل ترکیبی و مشکلات آن خاتمه یافته است.

سرفصل‌های این کتاب بگونه‌ای است که بتوان مطالب مربوط به مفاهیم پایه‌ای مهندسی امنیت و اهمیت ارزیابی و چگونگی انجام آن فرا گرفته شود. این اثر می‌تواند مستند علمی بسیار مهمی در کسب ایده و انتخاب زمینه‌های مختلف مهندسی امنیت فن آوری اطلاعات و ارتباطات باشد بهمین دلیل و با توجه به گستردگی مباحث، در پایان هر فصل منابعی جهت مطالعه‌ی بیشتر برای محققان و پژوهشگران علاقه مند آورده شده است. خصوصیت بارز دیگر این کتاب، سادگی بیان به همراه استفاده از شکل‌ها و جداول و طرح سوالاتی برای سنجش میزان یادگیری خود در جهت درک بهتر مفاهیم در هر مبحث است.

در خاتمه بر خود لازم می‌دانیم از تمامی عزیزانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را بعمل آوریم.

بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم.

پست الکترونیکی انعکاس نظرات:

info@27000.ir
www.27000.ir
ناصر مدیری – ناصر ولی

جایگاه کتاب:

همانطور که می دانیم ضمانت امنیت بیشتر به معنای بالارفتن درصد احتمال بازگشت سرمایه نیست و گاها تلاش بیشتر برای امنیت یا ضمانت بیشتر فقط هزینه‌های تولید را افزایش می‌دهد! از سوی دیگر امروزه کاملا محرز است که، پرداختن به مقوله‌های غیر کارکردی همچون امنیت در آغازین مراحل تولید منجر به کاهش هزینه‌ها و کنترل اصولی خسارات می‌شود و مهمتر اینکه در طول فاز نگه داری سیستم با وجود مستندات تهیه شده از الزامات امنیتی از همان مراحل اولیه، به راحتی می‌توان تدابیر انعطاف‌پذیری برای امنیت سیستم و محیط عملیاتی در قبال حملات و نقص‌ها و شکست‌های مختلف ایجاد کرد

این ایده نکته بسیار مهمی را نشان می‌دهد و آن این که تا زمانی که خود محصول تولید نشده و به محیط عملیاتی نرسیده است، ارزیابی امنیت از روی مستندات در فرایند تولید محصول انجام می‌شود و این امر ادغام و یکپارچگی مباحث مهندسی نرم افزار و مهندسی امنیت را نشان می‌دهد بعبارت دیگر سطح تضمین بالاتر به معنای پایبندی و رعایت مرازین دقیق مهندسی نرم افزار است. با در نظر داشتن این مطالب، می‌توان کلیه مطالب این کتاب را بعنوان یکان نشانه برای محققان، کارشناسان و مدیران در هر سه سطح تولید، ارزیابی و مصرف محصولات فن آوری اطلاعات دانست، به گونه‌ای که ایده‌های خلاقانه و جسورانه ارائه شده در این کتاب گره گشای دغدغه‌های اصلی خوانندگان عزیز باشد، و در حقیقت نخستین گامها و ملزومات اساسی حرکت به سمت فن آوری برتر ارائه شده است. همه این مسائل مزیدی به تغییر نگرش سازمانها به استانداردها و بومی‌سازی و بکارگیری هرچه سریعتر آن و اعتماد بیشتر به دانش مهندسان نرم افزار در این حوزه می‌باشد.

فهرست عناوین