

مہذب 

مرجع برای دروس

تألیف و تدوین:

دکتر ناصر مدیری

مهندس ناصر ولی



Mehregane Ghalam

سرشناسه: مدیری، ناصر
عنوان: مهندسی ارزیابی امنیت سیستم‌های کامپیوتری

تالیف و تدوین: ناصر مدیری، ناصر ولی

مشخصات فشرده: تهران، مهرگان قلم

مشخصات ظاهری: ۳۴۲ ص.، مقبوض

شابک: 978-600-6236-28-5

وضعیت فهرست‌نویسی: نه

یادداشت: واژه‌نامه

یادداشت: کتابخانه

موضوع: مهندسی امنیت - مهندسی نرم افزار - آزمون نرم افزار - مهندسی

شناسه افزوده: ناصر ولی

شناسه افزوده: مرجع برای درس‌های مهندسی امنیت و مهندسی نرم افزار و مباحث ویژه در نرم افزار

رده‌بندی کنگره: ۱۳۹۱ م ۲۹/۵۹/۵۱۰۵/۲۸۵۱

رده‌بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۲۹۱۱۹۴۱



انتشارات مهرگان قلم

www.mehreganeghalam.com

مهندسی ارزیابی امنیت سیستم‌های کامپیوتری

مؤلف: ناصر مدیری - ناصر ولی

ناشر: مهرگان قلم

نوبت چاپ اول: ۱۳۹۱

چاپ و صحافی: مهرنوین

تیراژ: ۵۰۰ نسخه

قیمت: ۱۴۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۲۸-۵

کلیه حقوق این اثر متعلق به انتشارات مهرگان قلم می‌باشد.

تهران، خیابان انقلاب، خیابان دانشگاه، بین خیابان روانمهر و خیابان وحید نظری، کوچه قدیری، پلاک ۲۲، واحد ۳

تلفن: ۶۶۹۵۸۵۵۸ - ۶۶۹۶۰۷۶۳

پیشگفتار

ن وَالْقَلَمِ وَمَا يَسْطُرُونَ

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 همچنان کودکانه‌ای را در وجود فعالان این حوزه پدیدار کرده است و تصور رقابت در مایه توانایی بشر در این ستیز طولانی و پایان ناپذیر انگیزه‌های کافی برای هر دو طرف دعوی (سوداگران امنیت و متخصصان امنیت) ایجاد کرده است.

رشد چشمگیر اخبار این تضادها و این مارا مبرهن است و مباحث مهندسی امنیت معنا نخواهد داشت مگر اینکه پاسخ سؤال‌هایی چون: حفظ امنیت چه سازه‌ای؟ 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 نفوذهای 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 سؤال 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 یافته 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 روشن‌تر 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 در این کتاب نوعا به هم مربوط خواهند بود و گاهی 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 علاقه‌مند 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 بالا رفتن درصد احتمال بازگشت سرمایه نیست و گاهی تلاش بیشتر برای امنیت یا ضمانت بیشتر فقط هزینه های تولید را افزایش می دهد! از سوری دیگر امروزه کاملاً محرز است که، پرداختن به مقوله های غیر کارکردی همچون امنیت در آغازین مراحل تولید منجر به کاهش هزینه ها و کنترل اصولی خسارات می شود و مهمتر اینکه در طول فاز نگه داری سیستم با وجود مستندات تهیه شده از الزامات امنیتی از همان مراحل اولیه، به راحتی می توان تدابیر انعطاف پذیری برای امنیت سیستم و محیط عملیاتی در قبال حملات و نقص ها و شکست های مختلف ایجاد کرد این ایده نکته بسیار مهمی را نشان می دهد 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 می شود و این امر ادغام و یکپارچگی مباحث مهندسی نرم افزار و مهندسی امنیت را نشان می دهد بعبارت دیگر سطح تضمین بالاتر به معنای پایبندی و رعایت موازین دقیق مهندسی نرم افزار است. با در نظر داشتن این مطالب، می توان کلیه مطالب این کتاب را بعنوان یک کتاب نشانه برای محققان، کارشناسان و مدیران در هر سه سطح تولید، ارزیابی و مصرف محصولات فن آوری اطلاعات دانست، به گونه ای که ایده های خلاقانه و جسورانه ارائه شده در این کتاب گره گشای دغدغه های 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 بومی سازی و بکارگیری مرحله سریعتر آن و اعتماد بیشتر به دانش مهندسان نرم افزار در این حوزه می باشد.

فهرست عناوین

۲۰	۱. امنیت فن آوری
۲۰	۱.۱. خلاصه فصل
۲۰	۱.۲. مقدمه
۲۱	۱.۳. معرفی مؤسسه پونمن
۲۱	۱.۳.۱. هزینه‌های ناشی از سرقت اطلاعات
۲۲	۱.۳.۲. توزیع هزینه‌های تخلقات رایانه‌ای بر اساس اندازه سازمان
۲۲	۱.۳.۳. تحلیل‌های هزینه بر اساس تعداد پست سازمانی
۲۳	۱.۳.۴. متوسط زمان بازیابی سرویس‌ها
۲۴	۱.۴. مفاهیم پایه
۲۴	۱.۴.۱. ریسک
۲۵	۱.۴.۲. سرمایه‌ها
۲۶	۱.۴.۳. تهدیدها
۲۶	۱.۴.۴. آسیب‌پذیری‌ها
۲۷	۱.۴.۴.۱. انواع آسیب‌پذیری
۲۷	۱.۴.۴.۲. اهمیت آسیب‌پذیری‌ها
۲۹	۱.۴.۴.۳. علت آسیب‌پذیری‌ها
۲۹	۱.۴.۴.۴. منابع نا امنی یا آسیب‌پذیری‌ها
۳۰	۱.۴.۵. رابطه بین تهدیدها، کاستی‌ها و ریسک
۳۰	۱.۵. الزامات اساسی چارچوب مدیریت ریسک نرم افزار
۳۱	۱.۵.۱. درک حوزه تجارت و کسب و کار
۳۲	۱.۵.۲. تشخیص ریسکهای تکنیکی و تجاری
۳۳	۱.۵.۳. تحلیل و اولویت‌بندی ریسک‌ها و تولید مجموعه‌های مرتب
۳۳	۱.۵.۴. تعریف استراتژی تسهیل ریسک
۳۴	۱.۵.۵. انجام فعالیت‌های تأییدی و بازایی
۳۴	۱.۶. متدهای ارزیابی ریسک
۳۵	۱.۷. تشخیص ریسک
۳۵	۱.۷.۱. گام‌های تشخیص ریسک
۳۶	۱.۷.۲. برخی تکنیک تشخیص ریسک
۳۷	۱.۸. تحلیل ریسک
۳۷	۱.۸.۱. اثرات تجارت و کسب و کار



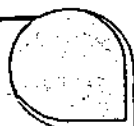
۳۷	۱.۸.۱.۱ مدل DREAD
۳۸	۱.۸.۲ احتمال
۳۹	۱.۸.۳ ارزشیابی ریسک
۳۹	۱.۹ طبقه‌بندی و اولویت‌بندی
۴۰	۱.۱۰ متریک‌های امنیتی
۴۳	۱.۱۰.۱ تهیه متریک‌هایی مناسب امنیت سیستم‌های کامپیوتری
۴۵	۱.۱۰.۲ چالش‌های پیش روی پیشرفت تهیه متریک‌های امنیت فناوری اطلاعات
۴۶	۱.۱۱ برگشت سرمایه در امنیت فن آوری
۴۶	۱.۱۱.۱ برگشت سرمایه و تحلیل ریسک
۴۹	۱.۱۱.۲ مدل‌های برگشت سرمایه
۴۹	۱.۱۱.۲.۱ مدل Pay Back
۵۰	۱.۱۱.۲.۲ مدل NVP
۵۱	۱.۱۲ نتیجه‌گیری
۵۲	۱.۱۳ سئوالات آخر فصل
۵۲	۱.۱۴ منابعی برای مطالعات بیشتر
۵۴	۲. استانداردهای امنیت فن آوری
۵۴	۲.۱ خلاصه فصل
۵۴	۲.۲ مقدمه
۵۵	۲.۳ استاندارد چیست
۵۶	۲.۴ روند تهیه استانداردهای جهانی
۵۷	۲.۴.۱ زیر گروه امنیت سازمان ITU
۵۷	۲.۴.۲ زیر کمیته تخصصی JTC
۵۸	۲.۴.۳ مروری بر چگونگی ساختار JTC
۵۹	۲.۵ معرفی استانداردها
۵۹	۲.۵.۱ ISO/IEC 24765: 2010 لغت نامه مهندسی نرم افزار
۵۹	۲.۵.۲ ISO /IEC 2382-8 : 1998 لغت نامه امنیت فناوری اطلاعات
۶۰	۲.۵.۳ استانداردهای اولیه مدیریت امنیت
۶۱	۲.۵.۳.۱ BS7799 اولین استاندارد مدیریت امنیت اطلاعات
۶۳	۲.۵.۳.۲ استاندارد ISO/IEC 17799 موسسه بین‌المللی استاندارد
۶۴	۲.۵.۳.۳ راهنمای فنی ISO/IEC TR13335
۶۶	۲.۵.۴ خانواده استانداردهای ISO/IEC 27000
۶۶	۲.۵.۴.۱ ISO/IEC 27000

۶۷	ISO/IEC 27001 ۲۵.۴.۲
۷۰	ISO/IEC 27002 ۲۵.۴.۳
۷۹	ISO/IEC 27003 ۲۵.۴.۴
۸۰	ISO/IEC 27004 ۲۵.۴.۵
۸۰	ISO/IEC 27005 ۲۵.۴.۶
۸۳	استاندارد ISO/IEC 15443 ۲۵.۵
۸۶	۱۵۵.۱ فرایند ارزیابی
۸۹	۱۵۵.۳ مراحل ارزیابی
۹۰	۲۶ نتیجه گیری
۹۰	۲۷ سئوالات آخر فصل
۹۱	۲۸ منابعی برای مطالعات بیشتر
۹۴	۳ مهندسی امنیت
۹۴	۳.۱ خلاصه فصل
۹۴	۳.۲ مقدمه
۹۷	۳.۳.۱ دلایل نبود سیستم نظام یافته و زیر بنایی امنیت
۹۷	۳.۴ امنیت اطلاعات چیست؟
۹۸	۳.۴.۱ امنیت در قبال ایمنی
۹۸	۳.۴.۲ برخی اهداف مهندسی امنیت
۹۹	۳.۴.۳ انواع سازمانهای مهندسی امنیت
۱۰۰	۳.۵ ضمانت نرم افزار
۱۰۰	۳.۵.۱ تعریف ضمانت
۱۰۱	۳.۵.۱.۱ سیستم نرم افزاری و خدمات
۱۰۱	۳.۵.۱.۲ میرا بودن از آسیب‌پذیری‌های داخلی و تصادفی
۱۰۲	۳.۵.۱.۳ توانایی امنیتی مناسب برای مقابله با تهدیدهای محیطی
۱۰۲	۳.۵.۱.۴ توان تحمل خرابی و بازیابی از خسارت
۱۰۲	۳.۵.۱.۵ ایده‌ها و اهداف ضمانت نرم افزار
۱۰۳	۳.۶ مهندسی امنیت
۱۰۴	۳.۷ پیچیدگی تعاریف و لغات حوزه امنیت
۱۰۵	۳.۷.۱ سیستم
۱۰۵	۳.۷.۲ موضوع، شخص، مشارکت
۱۰۶	۳.۷.۳ اعتماد و قابلیت اعتماد
۱۰۶	۳.۷.۴ محرمانگی، حریم خصوصی و مخفی‌سازی و حفاظت از اطلاعات



۳.۷.۵	صحت و درستی	۱۰۷
۳.۷.۶	وضوح	۱۰۷
۳.۸	پروتکل	۱۰۸
۳.۹	گذرواژه	۱۰۹
۳.۹.۱	انواع روشهای استقرار گذرواژه	۱۱۰
۳.۹.۲	کاربرد مسائل روانشناختی	۱۱۰
۳.۱۰	مهندسی اجتماعی	۱۱۱
۳.۱۱	کنترل دسترسی	۱۱۲
۳.۱۱.۱	کنترل دسترسی سیستم عامل	۱۱۳
۳.۱۱.۲	گروه یا وظیفه	۱۱۵
۳.۱۱.۳	لیست کنترل دسترسی	۱۱۵
۳.۱۲	سیستمهای امنیت چند سطحی	۱۱۷
۳.۱۲.۱	نمونههای سیستمهای امنیت چند لایه	۱۲۰
۳.۱۲.۲	سیستمهای امنیت چند لایه آینده	۱۲۱
۳.۱۲.۳	مشکلات سیستمهای امنیت چند سطحی	۱۲۲
۳.۱۲.۴	قابلیت ترکیب	۱۲۲
۳.۱۲.۵	مشکل آشناری	۱۲۳
۳.۱۲.۶	کانالهای مخفی	۱۲۳
۳.۱۲.۷	تهدیدات ناشی از ویروس	۱۲۴
۳.۱۲.۸	چند نمونهسازی	۱۲۴
۳.۱۳	امنیت چند جانبه	۱۲۵
۳.۱۴	درخت حملات	۱۲۷
۳.۱۴.۱	ملاحظاتی و ویژگیهای درخت حملات	۱۲۸
۳.۱۵	نتیجه گیری	۱۳۰
۳.۱۶	سئوالات آخر فصل	۱۳۱
۳.۱۷	منابعی برای مطالعات بیشتر	۱۳۱
۴	مهندسی ارزیابی امنیت	۱۳۴
۴.۱	خلاصه فصل	۱۳۴
۴.۲	مقدمه	۱۳۴
۴.۳	تعریف استاندارد ISO/IEC 15408	۱۳۵
۴.۴	حایکاه CC	۱۳۶
۴.۴.۱	دیدگاه مشتریان در مورد CC	۱۳۸

۱۳۸	۴.۵. مستندات مهم
۱۳۸	۴.۵.۱. هدف مورد ارزیابی
۱۳۹	۴.۵.۲. الزامات امنیتی
۱۴۰	۴.۵.۳. ارتباط بین SFRها و اهداف امنیتی
۱۴۰	۴.۵.۴. الزامات ضمانت امنیت
۱۴۱	۴.۵.۵. هدف امنیتی
۱۴۲	۴.۵.۶. بسته‌ها
۱۴۲	۴.۵.۷. پروفایل محافظتی
۱۴۲	۴.۵.۷.۱. نویسندگان پروفایل محافظتی
۱۴۳	۴.۵.۸. مستندات دیگر
۱۴۳	۴.۵.۸.۱. تعریف مشکل امنیتی
۱۴۳	۴.۵.۸.۲. خط مشی‌ها، الزامات امنیتی و خط مشی‌های ابلاغی کشوری
۱۴۴	۴.۶. مخاطبان استاندارد CC
۱۴۴	۴.۷. ارزیابی در CC
۱۴۵	۴.۷.۱. انواع ارزیابی
۱۴۶	۴.۸. تضمین ISO/IEC 15408
۱۴۶	۴.۹. معرفی کلاسهای تضمین CC
۱۴۶	۴.۹.۱. کلاس APE
۱۴۶	۴.۹.۲. کلاس ASE
۱۴۷	۴.۹.۳. کلاس ADV
۱۴۷	۴.۹.۴. کلاس AGD
۱۴۷	۴.۹.۵. کلاس ALC
۱۴۷	۴.۹.۶. کلاس ATE
۱۴۸	۴.۹.۷. کلاس AVA
۱۴۸	۴.۹.۸. کلاس ACO
۱۴۸	۴.۱۰. سطوح تضمین ارزیابی
۱۴۸	۴.۱۰.۱. سطح اول - آزمون کارکرد
۱۴۹	۴.۱۰.۲. سطح دوم - آزمون ساختاری
۱۵۰	۴.۱۰.۳. سطح سوم - بررسی و آزمون متدولوژیک
۱۵۱	۴.۱۰.۴. سطح چهارم - مرور، آزمون و طراحی به لحاظ متدولوژیک
۱۵۱	۴.۱۰.۵. سطح پنجم - طراحی و آزمون نیمه رسمی
۱۵۲	۴.۱۰.۶. سطح ششم - آزمون و طراحی تحقیق شده ی نیمه رسمی



۱۵۳	۴.۱۰.۷. سطح هفتم - آزمون و طراحی تحقیق شده ی رسمی
۱۵۴	۴.۱۱. مهندسی ضمانت نرم افزار
۱۵۴	۴.۱۱.۱. اساسی ترین موضوعات در ضمانت نرم افزار
۱۵۶	۴.۱۱.۲. ارزیابی ضمانت
۱۵۷	۴.۱۲. طراحی مدل های تجاری ارزیابی ضمانت نرم افزار
۱۵۷	۴.۱۲.۱. اهمیت و ضرورت طراحی مدل های ارزیابی تجاری به صرفه
۱۵۸	۴.۱۲.۲. طراحی مدل های تجاری ارزیابی به صرفه
۱۶۰	۴.۱۲.۳. روند ساخت یک مدل ارزیابی تجاری امنیت
۱۶۲	۴.۱۳. مرور مدل های COST/BENEFIT
۱۶۳	۴.۱۴. نتیجه گیری
۱۶۴	۴.۱۵. سوالات آخر فصل
۱۶۴	۴.۱۶. منابعی برای مطالعات بیشتر
۱۶۸	۵. مولفه های عملکردی امنیت
۱۶۸	۵.۱. خلاصه فصل
۱۶۸	۵.۲. مقدمه
۱۶۹	۵.۳. کلیات و ساختار بخش دوم استاندارد CC
۱۷۲	۵.۴. کلاس ممیزی امنیت FAU
۱۷۴	۵.۴.۱. FAU_SAR. بازبینی ممیزی: قابلیت خواندن اطلاعات را از مستندات ممیزی ایجاد می نماید.
۱۷۵	۵.۵. کلاس ارتباطات: FC
۱۷۶	۵.۶. کلاس پشتیبانی رمزنگاری: FCS
۱۷۷	۵.۷. کلاس محافظت از داده های کاربری: FDP
۱۸۵	۵.۸. کلاس تشخیص و احراز هویت: FIA
۱۸۷	۵.۹. کلاس مدیریت امنیت: FMT
۱۹۰	۵.۱۰. کلاس حریم خصوصی: FPR
۱۹۲	۵.۱۱. کلاس محافظت از TSF: FPT
۱۹۸	۵.۱۲. کلاس استفاده از منابع: FRU
۱۹۹	۵.۱۳. کلاس دسترسی به TOE: FTA
۲۰۱	۵.۱۴. کلاس کانال ها/ مسیر مطمئن: FTP
۲۰۲	۵.۱۵. نتیجه گیری
۲۰۲	۵.۱۶. سوالات آخر فصل
۲۰۳	۵.۱۷. منابعی برای مطالعات بیشتر

۲۰۶	۶. مولفه‌های تضمین امنیت
۲۰۶	۶.۱ خلاصه فصل
۲۰۶	۶.۲ مقدمه
۲۰۷	۶.۳ کلیات
۲۰۷	۶.۳.۱ مولفه‌های تضمین امنیت
۲۰۷	۶.۳.۲ خانواده‌های تضمین
۲۰۸	۶.۳.۳ سطوح تضمین ارزیابی و ساختار آن
۲۰۹	۶.۳.۴ ساختار CAP
۲۰۹	۶.۳.۵ ارتباط بین تضمین‌ها و سطوح تضمین
۲۱۰	۶.۴ کلاس‌های تضمین
۲۱۰	۶.۴.۱ کلاس ارزیابی هدف امنیتی ASE
۲۱۱	ادعاهای انطباق ASE_CCL
۲۱۲	تعریف مساله امنیت ASE_SPD
۲۱۵	۶.۴.۲ کلاس APE ارزیابی پروتکل محافظت
۲۱۶	۶.۴.۳ کلاس ADV توسعه
۲۲۴	۶.۴.۴ کلاس AGD اسناد راهنما
۲۲۷	۶.۴.۵ کلاس ALC پشتیبانی چرخه حیات
۲۲۸	۶.۴.۵.۱ قابلیت‌های ALC_CMC, CM
۲۳۱	۶.۴.۵.۲ هدف ALC_CMS, CM
۲۳۴	۶.۴.۵.۳ تحویل ALC_DEL
۲۳۵	۶.۴.۵.۴ امنیت توسعه ALC_DVS
۲۳۶	۶.۴.۵.۵ تصحیح نقص ALC_FLR
۲۳۸	۶.۴.۵.۶ تعریف چرخه حیات
۲۴۰	۶.۴.۵.۷ ابزار و فنون
۲۴۱	۶.۴.۶ کلاس آزمون‌ها: ATE
۲۴۲	۶.۴.۶.۱ پوشش ATE_COV
۲۴۴	۶.۴.۶.۲ عمق ATE_DPT
۲۴۵	۶.۴.۶.۳ آزمون‌های کارکردی ATE_FUN
۲۴۶	۶.۴.۶.۴ آزمون مستقل ATE_IND
۲۴۹	۶.۴.۷ گروه ارزیابی آسیب‌پذیری: AVA
۲۵۰	۶.۴.۸ گروه ترکیب: ACO
۲۵۰	۶.۴.۸.۱ مولفه‌های کلاس ترکیب



۶۵	نتیجه گیری	۲۵۱
۶۶	سئوالات آخر فصل	۲۵۱
۶۷	منابعی برای مطالعات بیشتر	۲۵۲
۷	مهندسی امنیت چرخه حیات توسعه	۲۵۴
۷.۱	خلاصه فصل	۲۵۴
۷.۲	مقدمه	۲۵۴
۷.۳	استاندارد ISO/IEC 12207	۲۵۵
۷.۳.۱	معرفی	۲۵۵
۷.۳.۱.۱	اهداف اصلی آخرین نسخه از ISO/IEC 12207	۲۵۶
۷.۳.۱.۲	چگونگی استفاده	۲۵۶
۷.۳.۱.۳	ضوابط فرایندها	۲۵۷
۷.۳.۲	فرایندهای توافق (اکتساب)	۲۵۸
۷.۳.۲.۱	اکتساب مقدماتی	۲۵۸
۷.۳.۲.۲	فرایندهای تامین	۲۶۰
۷.۳.۳	فرایندهای توانمندسازی سازمانی در پروژه	۲۶۲
۷.۳.۴	فرایندهای پروژه	۲۶۲
۷.۳.۵	فرایندهای فنی و تکنیکال	۲۶۳
۷.۳.۶	فرایندهای اختصاصی نرم افزار	۲۶۵
۷.۳.۶.۱	پیاده سازی نرم افزار	۲۶۵
۷.۳.۶.۲	فرایند تحلیل نیازمندی های نرم افزار	۲۶۶
۷.۳.۶.۳	فرایند طراحی معماری نرم افزار	۲۶۶
۷.۳.۶.۴	فرایندهای طراحی تفصیلی نرم افزار	۲۶۷
۷.۳.۶.۵	فرایند ساخت نرم افزار	۲۶۷
۷.۳.۶.۶	فرایند جامعیت نرم افزار	۲۶۸
۷.۳.۶.۷	فرایند تست کیفیت نرم افزار	۲۶۸
۷.۳.۷	فرایندهای پشتیبانی	۲۶۹
۷.۳.۸	فرایندهای قابلیت استفاده مجدد نرم افزار	۲۶۹
۷.۴	ملاحظات امنیتی در چرخه حیات توسعه سیستم	۲۷۰
۷.۴.۱	مزایای ادغام امنیت در SDLC	۲۷۰
۷.۴.۲	مخاطبان این روش	۲۷۱
۷.۴.۳	دروازه ها و نقاط کنترلی	۲۷۲
۷.۴.۴	فعالیت های مشترک در همه فازهای چرخه حیات	۲۷۲

۲۷۳	۷.۴.۵. پست‌های کلیدی و مسئولیت‌های اصلی در SDLC
۲۷۵	۷.۴.۶. فاز آغازین از چرخه حیات
۲۷۵	۷.۴.۶.۱. مهمترین فعالیت‌های فاز آغازین
۲۷۶	۷.۴.۶.۲. دروازه‌های کنترلی مورد ممیزی در انتهای فاز
۲۷۶	۷.۴.۶.۳. دسته‌بندی مهمترین بخشهای فاز آغازین
۲۷۹	۷.۴.۷. فاز اکتساب/توسعه
۲۷۹	۷.۴.۷.۱. مهمترین فعالیت‌های فاز اکتساب/توسعه
۲۸۰	۷.۴.۷.۲. دروازه‌های کنترلی مورد ممیزی در انتهای این مرحله
۲۸۱	۷.۴.۷.۳. دسته‌بندی مهمترین فعالیت‌های فاز اکتساب/توسعه
۲۸۵	۷.۴.۸. فاز پیاده‌سازی و ارزیابی
۲۸۵	۷.۴.۸.۱. مهمترین فعالیت‌های فاز پیاده‌سازی و ارزیابی
۲۸۶	۷.۴.۸.۳. دسته‌بندی فعالیت‌های این فاز
۲۸۷	۷.۴.۹. عملیاتی کردن و نگه‌داری سیستم
۲۸۷	۷.۴.۹.۱. فعالیت‌های مهم فاز عملیاتی و نگه‌داری کردن سیستم
۲۸۸	۷.۴.۹.۲. دروازه‌های کنترلی مورد ممیزی و بازرسی در این فاز
۲۸۸	۷.۴.۹.۳. دسته‌بندی فعالیت‌های این فصل
۲۹۰	۷.۴.۱۰. منسوخ شدن
۲۹۰	۷.۴.۱۰.۱. مهمترین فعالیت‌های این فاز
۲۹۱	۷.۴.۱۰.۲. دروازه‌های کنترلی مورد ممیزی و بازرسی در این فاز
۲۹۲	۷.۴.۱۰.۳. دسته‌بندی فعالیت‌های این فاز
۲۹۳	۷.۵. نتیجه‌گیری
۲۹۴	۷.۶. سئوالات آخر فصل
۲۹۴	۷.۷. منابعی برای مطالعات بیشتر
۲۹۶	۸. مهندسی امنیت چرخه حیات نرم افزار
۲۹۶	۸.۱. خلاصه فصل
۲۹۶	۸.۲. مقدمه
۲۹۷	۸.۳. الزامات اساسی مهندسی امنیت
۲۹۸	۸.۴. معرفی SSE-CMM
۲۹۹	۸.۴.۱. انواع دسته‌بندی‌های و پیاده‌سازی‌های مختلف
۲۹۹	۸.۴.۲. معماری SSE-CMM
۳۰۱	۸.۴.۲.۱. خصوصیات فعالیت‌های پایه
۳۰۱	۸.۴.۲.۲. خصوصیات حوزه‌های فرایندی



۳۰۲	۸.۴.۲.۳ فعالیتهای عمومی
۳۰۳	۸.۴.۳ سطوح بلوغ
۳۰۴	۸.۴.۳.۱ بررسی تفصیلی سطوح بلوغ قابلیت
۳۰۵	۸.۴.۳.۲ فرآیندهای موجود در هر سطح بلوغ
۳۰۶	۸.۴.۴ شفافیت فرآیندها از دید مدیریت در سطوح مختلف بلوغ
۳۰۷	۸.۵ مدل‌های تریبلی مهندسی امنیت
۳۰۷	۸.۵.۱.۱ مدل‌های CC به درون SSE-CMM
۳۰۸	۸.۵.۱.۲ تغییر SSE-CMM
۳۰۹	۸.۵.۱.۳ تشریح مدل CC-SSE-CMM
۳۰۹	۸.۵.۱.۴ نکات BPها و GPها با توجه به سطوح CC
۳۰۹	۸.۵.۱.۵ فرایند ارزیابی محصول و CC-SSE-CMM به ازای هر سطح
۳۱۰	۸.۵.۲ معرفی مدل CC-SSE-CMM-CS
۳۱۰	۸.۵.۲.۱ تشریح مدل CC-SSE-CMM-CS
۳۱۳	۸.۶ بررسی مدل‌های مهندسی امنیت موجود
۳۱۳	۸.۶.۱ انواع چارچوب‌های پیاده‌سازی مهندسی امنیت
۳۱۴	۸.۶.۲ ISO/IEC 2700x و ISO/IEC 17799
۳۱۵	۸.۶.۳ Assurance Frameworks و CISSP و تکنیک‌های ممیزی و بازرسی
۳۱۵	۸.۶.۴ ISO 9001
۳۱۵	۸.۶.۵ خانواده CMMi
۳۱۶	۸.۶.۶ SSE-CMM
۳۱۶	۸.۶.۷ CC-SSE-CMM
۳۱۷	۸.۶.۸ CC-SSE-CMM-CS
۳۱۷	۸.۶.۹ ISO/IEC 12207
۳۱۷	۸.۶.۱۰ Common Criteria
۳۱۸	۸.۶.۱۲ جمع‌بندی از بررسی ویژگی‌های در مدل‌های موجود
۳۱۹	۸.۷ مدل‌های احتمالی آینده
۳۱۹	۸.۷.۱ مزایای ISO/IEC 12207 برای ادغام CC
۳۲۱	۸.۷.۲ پیشنهاد یک چارچوب
۳۲۲	۸.۷.۳ قواعد و الزامات چارچوب پیشنهادی
۳۲۲	۸.۷.۴ پیش نیازهای ضروری برای شرح چارچوب
۳۲۳	۸.۷.۵ گروه‌بندی فازهای تولید نرم افزار
۳۲۴	۸.۷.۶ شرح چارچوب

۳۲۵	۸.۷.۶.۱ اصطلاحات به کار رفته در لایه‌های سوم
۳۲۵	۸.۷.۶.۲ چگونگی ممیزی و تعیین استقرار کلاسهای تضمین CC در لایه سوم
۳۲۶	۸.۷.۶.۳ محتویات مستند وضعیت امنیت یا SSD
۳۲۶	۸.۷.۶.۴ جداول پیشنهادی خانواده‌ها و عناصر کلاسهای تضمین
۳۲۶	۸.۷.۶.۵ ارائه پست‌های کلیدی امنیت و ممیزی استقرار کلاسهای تضمین CC
۳۲۷	۸.۸ نتیجه‌گیری
۳۲۷	۸.۹ سؤالات آخر فصل
۳۲۸	۸.۱۰ منابع برای مطالعات بیشتر
۳۴۱	جدول کلمات اختصاری

