

راه کارهای استانداردسازی در ارزیابی محصولات رمزنگاری

پژوهشگاه توسعه فناوری های پیشرفته
خواجه نصیرالدین طوسی

تألیف:

دکتر محمدعلی ارومیه چی ها

مهندس سیده نرگس و موی

مهندس حامد یوسنی

ناشر:

مؤسسه فرهنگی و هنری سخن پردازان خواجه نصیر

سال ۱۳۹۸

سرشناسه	: ارومیه‌چی‌ها، محمدعلی، ۱۳۵۸-
عنوان و نام پدیدآور	: راه‌کارهای استانداردسازی در ارزیابی محصولات رمزنگاری / تألیف محمدعلی ارومیه‌چی‌ها ؛ سیده نورگس موسوی ، حامد یوسفی ؛ ویراستار محمداسماعیل قاصدی ؛ [برای] پژوهشگاه توسعه فناوری‌های پیشرفته خواجه نصیرالدین طوسی.
مشخصات نشر	: تهران: مؤسسه فرهنگی هنری سخن‌پردازان خواجه نصیر، ۱۳۹۷.
مشخصات ظاهری	: ۲۳۸ص.
شابک	: ۹۷۸-۶۰۰-۹۴۳۵۱-۸-۰
وضعیت فهرست نویسی	: فیبا
موضوع	: رمزگذاری داده‌ها
موضوع	: Data encryption (Computer science)
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: Computer networks -- Security measures
شناسه افزوده	: موسوی، سیده نورگس، ۱۳۶۴-
شناسه افزوده	: یوسفی، حامد، ۱۳۶۷ -
شناسه افزوده	: پژوهشگاه توسعه فناوری‌های پیشرفته خواجه نصیرالدین طوسی.
ردمک	: ۷۹۳۱ ۴/QA۷۶ / ۹۱الف
رده بندی دیویی	: ۸۲/۰۰۵
شماره کتابشناسی	:



انتشارات مؤسسه فرهنگی هنری سخن‌پردازان خواجه نصیر

- نام کتاب: راه‌کارهای استانداردسازی در ارزیابی محصولات رمزنگاری
- نویسندگان: محمدعلی ارومیه‌چی‌ها، سیده نورگس موسوی و حامد یوسفی
- ویراستار: محمداسماعیل قاصدی
- صاحب امتیاز: پژوهشگاه توسعه فناوری‌های پیشرفته خواجه نصیرالدین طوسی
- ناشر: مؤسسه فرهنگی و هنری سخن‌پردازان خواجه نصیر
- چاپ و صحافی: مؤسسه فرهنگی و هنری سخن‌پردازان خواجه نصیر
- نوبت چاپ: چاپ نخست (۱۳۹۸)
- شمارگان: ۵۰ نسخه
- قیمت: ۳۰,۰۰۰ تومان
- تلفن: ۰۲۱-۲۲۸۸۰۰۸۱ ۰۲۱-۲۲۸۷۴۵۶۴ همراه: ۰۲۳۳-۷۶۷۴-۰۹۳۶
- شابک: ۹۷۸-۶۰۰-۹۴۳۵۱-۸-۰ ISBN: 978-600-94351-8-0

کلیه حقوق، اعم از چاپ، تکثیر، نسخه‌برداری و اقتباس برای مؤسسه فرهنگی و هنری سخن‌پردازان خواجه نصیر محفوظ و تکثیر یا تولید مجدد آن به‌طور کلی یا جزئی، در هر قالبی (چاپ، فتوکپی، صدا، تصویر و فایل الکترونیک) تحت هر شرایطی، بدون اجازه کتبی ناشر ممنوع است.

نسخه الکترونیک این اثر با مراجعه به پایگاه اطلاع‌رسانی مؤسسه و دریافت اپلیکیشن کتاب‌خوان فیدیبو قابل دسترس است.

فهرست مطالب

صفحه

عنوان

فصل ۱: رویکرد جهانی در استانداردسازی محصولات امنیتی

۳	۱-۱- مقدمه
۴	۱-۲- معرفی سازمان‌های استانداردسازی برخی کشورها
۴	۱-۲-۱- سازمان‌های استاندارد در آمریکای شمالی
۸	۱-۲-۲- سازمان‌های استانداردسازی در اروپا
۹	۱-۲-۳- سازمان استاندارد روسیه
۱۰	۱-۲-۴- سازمان‌های استاندارد در ژاپن
۱۰	۱-۳- معرفی سازمان‌های جهانی
۱۰	۱-۳-۱- سازمان جهانی IF
۱۱	۲-۳-۱- اتحادیه جهانی IEC
۱۱	۱-۳-۳- سازمان جهانی ISO
۱۵	۱-۴- جمع‌بندی

فصل ۲: استاندارد ISO 15408 معیارهای مشترک برای ارزیابی امنیت محصولات

فناوری اطلاعات

۱۹	۲-۱- مقدمه
۲۲	۲-۲- مفاهیم کلی و مدل عمومی استاندارد معیارهای مشترک (CC)
۲۲	۲-۲-۱- مقدمه و اهداف
۲۲	۲-۲-۲- تعریف مفاهیم اصلی
۲۴	۲-۲-۳- دید کلی از استاندارد
۲۸	۲-۲-۴- مدل عمومی
۳۶	۲-۲-۵- نتایج ارزیابی این استاندارد
۳۸	۲-۳- الزامات کارکردی امنیتی طبق استاندارد معیارهای مشترک
۳۸	۲-۳-۱- مقدمه
۳۸	۲-۳-۲- دسته‌های الزامات کارکردی امنیتی
۴۰	۲-۴- الزامات تضمین امنیت طبق استاندارد معیارهای مشترک
۴۰	۲-۴-۱- مقدمه
۴۰	۲-۴-۲- معرفی دسته‌های الزامات تضمین امنیت
۴۱	۲-۴-۳- دسته ارزیابی هدف امنیتی (ASE)

۴۸	۴-۲-۴-دسته مستندات راهنما (AGD)
۴۹	۴-۲-۴-۵-دسته توسعه (ADV)
۵۳	۴-۲-۴-۶-دسته چرخه حیات (ALC)
۵۶	۴-۲-۴-۷-دسته آزمون‌ها (ATE)
۵۹	۴-۲-۴-۸-دسته ارزیابی آسیب‌پذیری (AVA)
	فصل ۳: استاندارد ISO 19790، الزامات امنیتی ماژول‌های رمزنگاری
۶۳	۳-۱-مقدمه
۶۴	۳-۲-منظورهای استاندارد ISO 19790
۶۷	۳-۳-مشخصات ماژول رمزنگاری
۶۹	۳-۴-دگاه‌ها و واسط‌های ماژول رمزنگاری
۷۱	۳-۵-نشر، خدمات، احراز اصالت
۷۱	۳-۵-۱-نقش‌ها
۷۲	۳-۵-۲-خدمات
۷۴	۳-۵-۳-احراز اصالت
۷۶	۳-۶-مدل حالت محالود
۷۷	۳-۷-امنیت فیزیکی
۸۰	۳-۷-۱-الزامات عمومی امنیت فیزیکی
۸۲	۳-۷-۲-ماژول رمزنگاری تک‌تراشه‌ای
۸۳	۳-۷-۳-ماژول‌های رمزنگاری درج‌شده بر روی چیپ تراشه
۸۴	۳-۷-۴-ماژول‌های رمزنگاری چندتراشه‌ای به صورت خودکفا
۸۶	۳-۷-۵-آزمون/حفاظت در برابر نواقص محیطی
۸۷	۳-۸-محیط عملیاتی
۸۸	۳-۸-۱-الزامات محیط عملیاتی
۹۱	۳-۹-مدیریت کلید رمزنگاری
۹۲	۳-۹-۱-مولدهای عدد تصادفی (RNGs)
۹۲	۳-۹-۲-تولید کلید
۹۳	۳-۹-۳-استقرار کلید
۹۴	۳-۹-۴-وارد و خارج کردن کلید
۹۵	۳-۹-۵-ذخیره کلید
۹۵	۳-۹-۶-صفرسازی کلید
۹۶	۳-۱۰-تداخل الکترومغناطیسی/سازگاری الکترومغناطیسی

۹۶	۱۱-۳- خودآزمون‌ها
۹۷	۱-۱۱-۳- آزمون‌های حین روشن‌شدن
۹۸	۲-۱۱-۳- آزمون‌های شرطی
۱۰۰	۱۲-۳- ضمانت طراحی
۱۰۱	۱-۱۲-۳- مدیریت پیکربندی
۱۰۱	۲-۱۲-۳- تحویل و اجرا
۱۰۱	۳-۱۲-۳- توسعه
۱۰۳	۴-۱۲-۳- مستندات راهنما
۱۰۴	۱۳-۳- کاهش دیگر حملات
۱۰۶	۱۴-۳- ارزیابی ماژول‌های رمزنگاری
۱۰۶	۱-۱۴-۳- معرفی برنامه ارزیابی CMVP
۱۰۷	۲-۱۴-۳- فرایند اعتباربخشی آزمایشگاه
۱۰۸	۳-۱۴-۳- روال ارزیابی مطابق با CMVP
	فصل ۴: استاندارد ISO 17825، روش‌های آزمون برای ارزیابی ماژول رمزنگاری در برابر حملات غیرمخرب
۱۱۳	۱-۴- مقدمه
۱۱۴	۲-۴- روش‌های حمله غیرتهاجمی
۱۱۸	۳-۴- توابع امنیتی مرتبط
۱۲۰	۴-۴- روش‌های آزمون حمله غیرتهاجمی
۱۲۰	۱-۴-۴- مقدمه
۱۲۱	۲-۴-۴- راهبرد آزمون
۱۲۲	۳-۴-۴- رویه کاری تحلیل کانال جانبی
۱۲۹	۵-۴- تحلیل کانال جانبی سامانه‌های رمز کلید متقارن
۱۲۹	۱-۵-۴- مقدمه
۱۲۹	۲-۵-۴- حملات زمانی
۱۳۰	۳-۵-۴- SPA/SEMA
۱۳۱	۴-۵-۴- DPA/DEMA
۱۳۸	۶-۴- تحلیل‌های کانال جانبی پیشرفته روی رمزنگاری نامتقارن
۱۳۸	۱-۶-۴- مقدمه
۱۳۸	۲-۶-۴- تفصیل چهارچوب آزمون مقاومت در برابر کانال جانبی
۱۴۰	۳-۶-۴- حملات زمانی

۱۴۲	SPA/SEMA-۴-۶-۴
۱۴۴	DPA/DEMA-۴-۶-۵
۱۵۰	۴-۷- معیارهای موفقیت یا شکست آزمون کاهش اثرات حمله غیرتهاجمی
۱۵۰	۴-۷-۱- مقدمه
۱۵۰	۴-۷-۲- سطح امنیتی سه
۱۵۲	۴-۷-۳- سطح امنیتی چهار
	فصل ۵: استاندارد ISO 30104، معرفی حملات و الزامات امنیت فیزیکی
۱۵۷	۵-۱- مقدمه
۱۵۸	۵-۲- امنیت فیزیکی
۱۶۰	۵-۳- سازوکارهای تهاجمی امنیت فیزیکی
۱۶۰	۵-۳-۱- گواه دست‌کاری
۱۶۱	۵-۳-۲- مقاوم در برابر دست‌کاری
۱۶۱	۵-۳-۳- نسخه دست‌کاری
۱۶۲	۵-۳-۴- گواه دست‌کاری
۱۶۲	۵-۳-۵- ملاحظات دیگر امنیت فیزیکی
۱۶۳	۵-۴- حملات تهاجمی امنیت فیزیکی دفاع در مقابل آنها
۱۶۴	۵-۴-۱- سازوکارهای حمله
۱۷۰	۵-۴-۲- سازوکارهای دفاع در برابر
۱۸۵	۵-۵- سازوکارهای غیرمخرب امنیت فیزیکی
۱۸۵	۵-۵-۱- سامانه‌های ترکیبی و لایه‌لایه
۱۸۵	۵-۶- حملات غیرمخرب امنیت فیزیکی و مقاوم‌سازی‌ها
۱۸۵	۵-۶-۱- حملات
۱۸۸	۵-۶-۲- مقاوم‌سازی‌ها
۱۸۸	۵-۷- مفهوم محدوده عملیاتی
۱۸۹	۵-۸- ملاحظات توسعه، تحویل و عملکرد
۱۸۹	۵-۸-۱- معرفی
۱۹۰	۵-۸-۲- توسعه
۱۹۱	۵-۸-۳- تحویل
۱۹۳	۵-۸-۴- عملکرد
۱۹۳	۵-۹- ارزیابی و آزمون امنیت فیزیکی
۱۹۵	پیوست‌ها

پیش گفتار مؤلفان

بی تردید هر محصول در دنیای فناوری اطلاعات ادعاهایی را، در مورد امنیت، ویژگی های عملکردی، و حتی مزیت های اقتصادی خود مطرح می سازد. برخی از این ادعاها، در بازار کسب و کار و برخی دیگر در آزمایشگاه ها، اعتبارسنجی در بوته آزمایش قرار می گیرند. برای نمونه، سازنده محصول در رابطه با ویژگی های از قبیل کارکرد در فرکانس های مشخص، طول عمر بالا، استفاده از الگوریتم ها و پروتکل های خاص، اظهار می کند که ارزیابی آنها توسط خریداران، بهره برداران و حتی رقبای تجاری امکان پذیر نیست؛ چون به طور اصولی یا دانش کافی برای ارزیابی آن محصول در اختیار آنها وجود ندارد و یا با فرض دانش کافی، جزئیات فنی مورد نیاز محصول تجاری نمی تواند در دسترس آنها قرار گیرد. با این ترتیب، ارزیابی محصول به مرجع شناخته شده و قابل اطمینانی به نام "آزمایشگاه ارزیابی" سپرده می شود. حوزه این ادعاها نیز می تواند در طیف وسیعی از ارزیابی های کارکردی تا ارزیابی های امنیتی محصول گنجانده شود. بنابراین آزمایشگاه ها نیز به صورت تخصصی، ارزیابی یک یا چند ویژگی مشخص محصول را برعهده می گیرند. با در نظر گرفتن تخصص های مختلف، ارزیابی امنیتی یک محصول می تواند بخش مهمی از ارزیابی های آن محصول را در بر گیرد.

امنیت سامانه های اطلاعاتی و ارتباطی یکی از بزرگترین چالش های حوزه فناوری اطلاعات در سراسر دنیا محسوب می شود. نهادهای حکومتی، صنعت و بخش خصوصی برای امن سازی داده های مورد استفاده در تجارت الکترونیک، زیرساخت های حیاتی و دیگر حوزه های کاربردی، از رمزنگاری استفاده می کنند. جهت امن سازی هر محصول امنیتی در دنیای فناوری اطلاعات، یک ماژول رمزنگاری مشخص با ویژگی های مرتبط با آن محصول طراحی و تأمین می شود.

ماژول رمزنگاری تمامی فعالیت‌های مربوط به الگوریتم‌ها و پروتکل‌های رمزنگاری از قبیل تولید کلید، تبادل کلید، ذخیره‌سازی کلید و داده‌های حساس، تولید اعداد تصادفی مورد نیاز، رمزنگاری و رمزگشایی پیام، احراز اصالت پیام، احراز اصالت کاربر، تعیین یک پارچگی پیام و غیره را انجام می‌دهد. این ماژول ممکن است به صورت سخت‌افزاری^۱، ثابت‌افزاری^۲ و نرم‌افزاری^۳ پیاده‌سازی شود و در سامانه امنیتی مورد بهره‌برداری قرار گیرد. از آنجا که هسته اصلی امنیت هر محصول در ماژول رمزنگاری آن شکل می‌گیرد، تهدید امنیتی علیه این بخش، می‌تواند منجر به شکست امنیت محصول شود. با وجود استفاده از رمزنگاری، نقص‌ها و ضعف‌های طراحی و پیاده‌سازی این ماژول نیز باعث ناامنی محصول می‌شوند و داده‌های حساس را در معرض خطر قرار می‌دهند. بنابراین کشف این نقاط ضعف در مرحله طراحی، پیاده‌سازی و به‌کارگیری ماژول‌های رمزنگاری گام مؤثری در جهت افزایش اطمینان از امنیت محصول قلمداد می‌شود.

سوال قابل طرح این است که چه رویکرد و چارچوبی برای ارزیابی یک ماژول رمزنگاری استفاده گردد. آیا به آزمایشگاه می‌تواند روال و فرآیند ارزیابی خود را بر مبنای دانش تخصصی و احصای نیازهای امنیتی یک ماژول رمزنگاری به‌کار گیرد. از آنجا که نتیجه ارزیابی امنیتی یک ماژول رمزنگاری در آزمایشگاه ارزیابی مستقل نباید متفاوت باشد، استفاده از چارچوبی استاندارد به عنوان یک رویکرد مورد توجه قرار می‌گیرد.

مجموعه پیش رو، به صورت تخصصی به راه‌کارهای استاندارد ارزیابی امنیتی محصولاتی که در آنها از ماژول‌های رمزنگاری استفاده شده است می‌پردازد و دانش موجود در آن به ارزیاب در بررسی امنیت ماژول‌های رمزنگاری کمک می‌کند. طیف وسیعی از مخاطبان می‌توانند از این اثر بهره‌مند شوند. به لحاظ تخصص‌های شلی، طراحی و تحلیل‌گران سامانه‌های امنیتی، توسعه‌دهندگان و برنامه‌نویسان و همچنین آزمایشگاه‌های تخصصی ارزیابی امنیت می‌توانند از موضوعات مطرح‌شده در این کتاب استفاده کنند. تولیدکنندگان و بهره‌برداران در عرصه‌های کاری، نظیر صنایع الکترونیک، رایانه، مخابرات، اپراتورهای تانک، صنایع نفت و گاز، تولید و انتقال نیرو نیز می‌توانند از جنبه‌های استانداردسازی و توجه به استانداردهای بین‌المللی این کتاب بهره‌برند. همچنین برای بخش‌های حاکمیتی نیز در راستای تدبیر مقررات و نظارت بر پیاده‌سازی استانداردهای امنیتی، این اثر قابل استفاده است.

مؤلفان این مجموعه ضمن بررسی راه‌کارهای مختلف و مطالعه تطبیقی آنها، به انتخاب برخی استانداردهای مؤثر جهت ارزیابی امنیتی ماژول‌های رمزنگاری خواهند پرداخت. توجه عمده نگارندگان کتاب معطوف به استانداردهای پیشنهادشده توسط سازمان استانداردهای

^۱ Hardware

^۲ Firmware

^۳ Software

بین‌المللی (ISO^۱) بوده که چه در سطح بین‌الملل و چه در سطح ملی مورد استفاده و ارجاع علمی و فنی قرار گرفته است. در فصل نخست، رویکردهای استانداردسازی ارزیابی امنیتی محصولات رمزنگاری در کشورهای مختلف و سازمان‌های بین‌المللی فعال به‌اجمال بررسی می‌شوند. فصل دوم کتاب، استاندارد ISO 15408 را، که با عنوان استاندارد معیارهای مشترک (CC^۲) نیز از آن یاد می‌شود، به‌عنوان چارچوب کلی جهت ارزیابی امنیت محصولات حوزه فناوری اطلاعات، در سه بخش مجزا معرفی می‌کند. برای ارزیابی امنیتی آن دسته از محصولات فناوری اطلاعات که از ماژول رمزنگاری استفاده می‌کنند، استاندارد ISO 19790 پیشنهاد شده است. فصل سوم بر مبنای این استاندارد به بیان الزامات ارزیابی امنیتی یک ماژول رمزنگاری از یازده منظر مختلف می‌پردازد. در ارزیابی ماژول‌های رمزنگاری، علاوه‌بر این استاندارد، از دسته‌ای از استانداردهای مرتبط دیگر نیز کمک گرفته می‌شود. به‌طور خاص، استاندارد ISO 17825 معیارهای ارزیابی تعیین میزان مقاومت محصول در برابر حملات کانال جانبی و استاندارد ISO 30104 روش‌های تأمین و ارزیابی امنیت فیزیکی محصولات را بیان می‌کنند. در فصل‌های چهارم و پنجم، به‌ترتیب این دو استاندارد توصیف و تشریح شده‌اند. لازم به ذکر است، این مجموعه با توجه به حساسیت دقت متون استاندارد، بخش‌های اصلی آنها را بدون دخل و تصرف به فارسی برگردان کردیم. این م. طبق واژگان مصوب انجمن رمز ایران و فرهنگستان زبان و ادب فارسی صورت گرفته است.

امید است این مجموعه گام مثبتی در راستای اعتلای کشور در حوزه امنیت باشد و مورد توجه و استفاده متخصصان قرار گیرد. با ارائه پیشنهادها و انتقادات، ما را در هرچه بهترکردن این اثر و پیمودن این مسیر یاری فرمایید.

نویسندگان این مجموعه

خرداد ۱۳۹۱

^۱ International Standards Organization

^۲ Common Criteria