راه‌کارهای استانداردسازی در ارزیابی محصولات رمزنگاری

پژوهشگاه توسعهٔ فناوری‌های پیشرفتهٔ
خواجه نصیرالدین طوسی

تالیف:

دکتر محمدعلی ارومیه‌چی‌ها

مهندس سیده نرگس موسوی

مهندس حامد یوسفی

ناشر:

مؤسسهٔ فرهنگی و هنری سخن‌پردازان خواجه نصیر

سال ۱۳۹۸

سرشناسه : ارومیه‌چی‌ها، محمدعلی، ۱۳۵۸-
عنوان و نام پدیدآور : راه‌کارهای استانداردسازی در ارزیابی محصولات رمزنگاری / تألیف محمّدعلی ارومیه‌چی‌ها ؛ سیده نرگس موسوی ، حامد یوسفی ؛ ویراستار محمّداسماعیل قاصدی ؛ [برای] پژوهشگاه توسعهٔ فناوری‌های پیشرفتهٔ خواجه نصیرالدین طوسی.
مشخصات نشر : تهران: مؤسسهٔ فرهنگی هنری سخن‌پردازان خواجه نصیر، ۱۳۹۷.
مشخصات ظاهری : ۲۳۸ص.
شابک : ۹۷۸-۶۰۰-۹۴۳۵۱-۸-۰
وضعیت فهرست نویسی : فیپا
موضوع : رمزگذاری داده‌ها
موضوع : Data encryption (Computer science)
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : Computer networks -- Security measures
شناسه افزوده : موسوی، سیده نرگس، ۱۳٦٤-
شناسه افزوده : یوسفی، حامد، ۱۳٦۷ -
شناسه افزوده : پژوهشگاه توسعهٔ فناوری‌های پیشرفتهٔ خواجه نصیرالدین طوسی.
رده بندی کنگره : ۹/QA۷٦ /ر۸الف ٤ ۷۹۳۱
رده بندی دیویی : ۸۲/۰۰۵
شماره کتابشناسی ملی :

انتشارات مؤسسهٔ فرهنگی هنری سخن‌پردازان خواجه‌نصیر

- **نام کتاب:** راه‌کارهای استانداردسازی در ارزیابی محصولات رمزنگاری
- **نویسندگان:** محمدعلی ارومیه‌چی‌ها، سیده نرگس موسوی و حامد یوسفی
- **ویراستار:** محمّداسماعیل قاصدی
- **صاحب امتیاز:** پژوهشگاه توسعهٔ فناوری‌های پیشرفتهٔ خواجه نصیرالدین طوسی
- **ناشر:** مؤسسهٔ فرهنگی و هنری سخن‌پردازان خواجه نصیر
- **چاپ و صحافی:** مؤسسهٔ فرهنگی و هنری سخن‌پردازان خواجه نصیر
- **نوبت چاپ:** چاپ نخست (۱۳۹۸)
- **شمارگان:** ۵۰ نسخه
- **قیمت:** ۳۰,۰۰۰ تومان
- **تلفن:** ۰۲۱-۲۲۸۸۰۰۸۱ ۰۲۱-۲۲۸۷۴۵۶۴ **همراه:** ۰۹۳۶-۲۳۳-۷۶۷۴
- **شابک:** ۹۷۸-۶۰۰-۹۴۳۵۱-۸-۰ ISBN: 978-600-94351-8 -0

فهرست مطالب

پیش‌گفتار مؤلّفان

بی‌تردید هر محصول در حوزه‌های فناوری اطلاعات ادعاهایی را، در مورد امنیت، ویژگی‌های عملکردی، و حتی مزیت‌های اقتصادی خود مطرح می‌سازد. برخی از این ادعاها، در بازار کسب و کار و برخی دیگر در آزمایشگاه‌های اعتبارسنجی در بوتهٔ آزمایش قرار می‌گیرند. برای نمونه، سازندهٔ محصول در رابطه با ویژگی‌هایی از قبیل کارکرد در فرکانس‌های مشخص، طول عمر بالا، استفاده از الگوریتم‌ها و پروتکل‌های خاص ظهارنامه‌ای را ارایه می‌کند که ارزیابی آنها توسط خریداران، بهره‌برداران و حتی رقبای تجاری امکان‌پذیر نیست؛ چون به‌طوراصولی یا دانش کافی برای ارزیابی آن محصول در اختیار آنها وجود ندارد و یا با فرض دانش کافی، جزئیات فنّی موردنیاز محصول تجاری نمی‌تواند در دسترس آنها قرار گیرد. بنابر ترتیب، ارزیابی محصول به مرجع شناخته شده و قابل اطمینانی به نام "آزمایشگاه ارزیابی" واگذار می‌شود. حوزهٔ این ادعاها نیز می‌تواند در طیف وسیعی از ارزیابی‌های کارکردی تا ارزیابی‌های امنیتی محصول گنجانده شود. بنابراین آزمایشگاه‌ها نیز به‌صورت تخصصی، ارزیابی یک یا چند ویژگی مشخص محصول را برعهده می‌گیرند. با درنظرگرفتن تخصص‌های مختلف، ارزیابی امنیتی یک محصول می‌تواند بخش مهمی از ارزیابی‌های آن محصول را در بر گیرد.

امنیت سامانه‌های اطلاعاتی و ارتباطی یکی از بزرگترین چالش‌های حوزهٔ فناوری اطلاعات در سراسر دنیا محسوب می‌شود. نهادهای حکومتی، صنعت و بخش خصوصی برای امن‌سازی داده‌های مورد استفاده در تجارت الکترونیک، زیرساخت‌های حیاتی و دیگر حوزه‌های کاربردی، از رمزنگاری استفاده می‌کنند. جهت امن‌سازی هر محصول امنیتی در دنیای فناوری اطلاعات، یک ماژول رمزنگاری مشخص با ویژگی‌های مرتبط با آن محصول طراحی و تأمین می‌شود.

ماژول رمزنگاری تمامی فعالیت‌های مربوط به الگوریتم‌ها و پروتکل‌های رمزنگاری از قبیل تولید کلید، تبادل کلید، ذخیره‌سازی کلید و داده‌های حساس، تولید اعداد تصادفی موردنیاز، رمزنگاری و رمزگشایی پیام، احراز اصالت پیام، احراز اصالت کاربر، تعیین یک‌پارچگی پیام و غیره را انجام می‌دهد. این ماژول ممکن است به‌صورت سخت‌افزاری[1]، ثابت‌افزاری[2] و نرم‌افزاری[3] پیاده‌سازی شود و در سامانه امنیتی مورد بهره‌برداری قرار گیرد. از آنجا که هستهٔ 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 درجهت افزایش اطمینان از امنیت محصول قلمداد می‌شود.

سؤال قابل طرح این است که چه رویکرد و چارچوبی برای ارزیابی یک ماژول رمزنگاری استفاده گردد. آیا هر 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 هر آزمایشگاه ارزیابی مستقل نباید متفاوت باشد، استفاده از چارچوبی استاندارد به‌عنوان یک راهکار مؤثر مورد توجه قرار می‌گیرد.

مجموعهٔ پیش رو، به‌صورت تخصصی به راه‌کارهای استانداردِ ارزیابیِ امنیتیِ 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. به‌لحاظ تخصص‌های شغلی، طراحان 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 تلفن همراه، صنایع نفت و گاز، تولید و انتقال نیرو نیز می‌توانند از جنبه‌های استانداردسازی و توجه به استانداردهای بین‌المللی این کتاب بهره ببرند. همچنین برای بخش‌های حاکمیتی نیز در راستای تدوین مقررات و نظارت بر پیاده‌سازی استانداردهای امنیتی، این اثر قابل استفاده است.

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

---

[1] Hardware
[2] Firmware
[3] Software

بین‌المللی (ISO[1]) 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[2]) نیز از آن یاد می‌شود، به‌عنوان چارچوب کلی جهت ارزیابی امنیت محصولات حوزهٔ 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، علاوه‌براین استاندارد، از دسته‌ای از استانداردهای مرتبط دیگر نیز کمک گرفته می‌شود. به‌طورخاص، 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 و دقت متون استاندارد، بخش‌های اصلی آنها را بدون دخل و تصرف به فارسی برگردان کرده و این کار 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 حوزهٔ امنیت باشد و مورد توجه و استفاده متخصّصان قرار گیرد. با ارائهٔ پیشنهادها و انتقادات، ما را در هرچه بهترکردن این اثر و پیمودن این مسیر یاری فرمایید.

نویسندگان این مجموعه

تابستان ۱۳۹۱

---

[1] International Standards Organization

[2] Common Criteria