مروری بر طرح‌واره ارزیابی ماژول‌های رمزنگاری CMVP

علیرضا جواهری[۱] و راضیه سالاری فرد[۲]

[۱] کارشناسی، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران
alireza.javaheri1376@gmail.com

[۲] استادیار، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران
r_salarifard@sbu.ac.ir

چکیده

یکی از نکات حائز اهمیت در علم اطلاعات، چگونگی رمزنگاری داده‌ها برای محافظت از دسترسی غیرمجاز یا دست‌کاری آن‌ها است. به این منظور ماژول‌هایی برای رمزنگاری طراحی می‌شوند تا فرآیندهای رمزنگاری را به‌درستی پیاده‌سازی کنند. حال چالشی که به‌وجود می‌آید محافظت از خود این ماژول‌ها است؛ بنابراین پس از طراحی یک ماژول نیاز به ارزیابی امنیت آن تحت یک طرح‌واره داریم تا اطمینان پیدا کنیم که الزامات امنیتی به‌خوبی فراهم شده‌اند. از مهم‌ترین طرحواره‌های ارزیابی می‌توان به CMVP اشاره کرد. این برنامه شامل استانداردهایی است که یکی از اساسی‌ترین آن‌ها استاندارد ISO/IEC 19790 است که در چهار سطح امنیتی و یازده حوزه الزامات تدوین شده است. هدف از این پژوهش، تشریح این سطوح و حوزه‌ها با تأکید بر حوزه الزامات امنیت فیزیکی و امنیت غیر تهاجمی است، زیرا که این دو حوزه از رایج‌ترین حوزه‌های حملات به ماژول رمزنگاری است. همچنین یکی از مهم‌ترین اصولی که در کشور توجه کمتری به آن شده است ارزیابی ماژول‌های رمزنگاری بومی است. ارزیابی این ماژول‌ها تحت استانداردهای جهانی و در آزمایشگاه‌های ارزیابی امنیتی کشور بسیار ضروری و موجب تقویت زیرساخت‌های امنیتی است.

واژگان کلیدی: ماژول رمزنگاری، امنیت فیزیکی، امنیت غیر تهاجمی، CMVP، ISO/IEC 19790، FIPS 140-3

۱ – مقدمه

در سامانه‌های کامپیوتری که وظیفه پشتیبانی از انتقال داده‌ها و اطلاعات را دارند، نیاز جدی به منظور به‌کارگیری از فرآیندهای رمزنگاری برای محافظت از داده‌ها در برابر افشا یا دستکاری غیرمجاز و احراز هویت کاربرانی که خواهان دسترسی به اطلاعات می‌باشند، ضروری است. امنیت و قابلیت اطمینان به چنین فرآیندهایی به‌طور مستقیم به ماژول‌های رمزنگاری که در آن پیاده‌سازی می‌شوند بستگی دارد. مهم‌ترین مرحله پس از طراحی و ساخت یک ماژول رمزنگاری، ارزیابی آن تحت یک طرحواره ارزیابی و دریافت گواهی از آزمایشگاه‌های مربوطه است. درجه امنیت کلی ماژول رمزنگاری باید به گونه‌ای انتخاب شود که سطح امنیتی آن متناسب با نیازهای امنیتی محلی که ماژول در آن استفاده می‌شود، باشد. الزامات امنیت اطلاعات برای کاربردهای مختلف متفاوت است. سازمان‌ها باید منابع اطلاعاتی خود را شناسایی کرده و حساسیت و تأثیر احتمالی خسارت را با اجرای کنترل‌های مناسب تعیین کنند. این کنترل‌ها شامل کنترل‌های فیزیکی و محیطی، کنترل دسترسی، توسعه نرم‌افزار، برنامه‌های پشتیبان و کنترل اطلاعات و داده‌ها می‌شود اما فقط محدود به این موارد نیست [۱،۲].

یکی از مهم‌ترین طرحواره‌های ارزیابی ماژول‌های رمزنگاری، CMVP[1] است. با توجه به شرایط تحریم کشور، امروزه در ایران، شرکت‌های بسیاری در حوزه طراحی و ساخت ماژول‌های رمزنگاری و آزمایشگاه‌هایی به‌منظور ارزیابی این ماژول‌ها فعالیت می‌کنند. یکی از اصلی ترین استانداردهای تعریف شده در CMVP، ISO/IEC-19790 است. این استاندارد، امنیت یک ماژول را در یازده حوزه الزامات و چهار سطح امنیتی بررسی می‌کند. بسیاری از آزمایشگاه‌ها و کشورها امروزه از این استاندارد بهره می‌گیرند که می‌توان به آزمایشگاه‌های تحت نظر NIST اشاره کرد [۲،۱۲].

۲ – سطوح امنیتی ماژول رمزنگاری

استاندارد بین‌المللی ISO/IEC-19790 دارای چهار سطح کیفی و رو به افزایش از الزامات امنیتی است تا طیف

[1] Cryptographic Module Validation Program

* نویسندهٔ عهده‌دار مکاتبات: راضیه سالاری فرد

گسترده‌ای از برنامه‌ها و محیط‌های بالقوه‌ای که نیازمند رمزنگاری هستند را پوشش دهد. راهکارهای استفاده شده برای رمزنگاری در چهار سطح امنیتی یکسان است. این الزامات امنیتی، محدوده‌های مربوط به طراحی و پیاده‌سازی یک ماژول رمزنگاری را پوشش می‌دهد که شامل مشخصات ماژول رمزنگاری، رابط‌های ماژول رمزنگاری، نقش‌ها، خدمات، احراز هویت، امنیت نرم‌افزار/ثابت‌افزار، محیط عملیاتی، امنیت فیزیکی، امنیت غیرتهاجمی، مدیریت پارامترهای حساس امنیتی، خودآزمایی، اطمینان از امنیت در چرخه حیات و کاهش احتمال سایر حملات است [۱،۸].

۲-۱- سطح امنیتی اول

این سطح ابتدایی‌ترین سطح امنیتی است و امنیت فیزیکی در این سطح بدون نیاز به سخت‌افزار خاص برقرار می‌شود.. این سطح مناسب برنامه‌های امنیتی است که در آن‌ها کنترل‌هایی مانند امنیت فیزیکی، امنیت شبکه و روندهای اجرایی که خارج از ماژول اما در همان محیطی که ماژول مستقر شده است مورد استفاده قرار می‌گیرند و به سازمان‌ها این امکان را می‌دهد که امنیت کلی را فراهم آورند [۱].

۲-۲- سطح امنیتی دوم

در این سطح علاوه‌بر الزامات مورد استفاده در سطح اول، الزامات شهود دستکاری[1] اضافه می‌شود که به معنی استفاده از پوششی است که آثار حمله روی آن به جا می‌ماند یا برچسبی به منظور پلمپ کردن ماژول که اگر خدشه‌ای به آن وارد شود قابل مشاهده باشد یا پوششی قابل برداشتن که دارای قفلی باشد تا برای حمله کننده به راحتی قابل باز کردن نباشد که مجبور به شکستن آن شود و در نتیجه آثار حمله قابل مشاهده بماند. این الزامات بر روی درب‌ها یا پوشش‌ها قرار دارد و احراز هویت مبتنی بر نقش[2]، حفاظت در برابر اجرای غیر مجاز، تغییر و خواندن نرم‌افزار رمزنگاری را شامل می‌شود [۱،۱۷].

۲-۳- سطح امنیتی سوم

این سطح به منظور کاهش دسترسی غیر مجاز به پارامترهای امنیتی حساس[3] استفاده می‌شود. راه‌کارهای امنیتی به کار گرفته شده در این سطح، به‌محض بازشدن پوشش‌ها یا درب‌های ماژول رمزنگاری، تمام پارامترهای امنیتی بحرانی[4] را صفر می‌کند. این سطح امنیتی شامل احراز هویت مبتنی بر هویت[5] است و از یک کانال معتبر[6] یا روش تقسیم ورود و خروج استفاده می‌کند. همچنین ماژول را در برابر به خطر افتادن امنیت به دلیل شرایط محیطی (مانند دما و ولتاژ) خارج از محدوده عملیاتی، محافظت می‌کند. در این سطح، چرخه حیات ماژول باید از ابتدای طراحی تا تولید و استفاده، دارای الزامات اضافه‌ای مانند مدیریت پیکربندی خودکار، آزمایشات سطح پایین و احراز هویت اپراتور با استفاده از اطلاعات هویتی ارائه شده توسط فروشنده باشد [۱،۲۰].

۲ – ۴ – سطح امنیتی چهارم

این سطح بالاترین سطح امنیتی تعریف شده در این استاندارد را شامل می‌شود که شامل تمام ویژگی‌های امنیتی مناسب برای سطوح پایین و همچنین ویژگی‌های توسعه یافته است. در این سطح سازوکارهای امنیت فیزیکی، یک پوشش محافظتی کامل را در اطراف ماژول رمزنگاری با هدف شناسایی و پاسخ به همه تلاش‌های غیرمجاز برای دسترسی فیزیکی تا هنگامی که SSP ها در ماژول هستند فراهم می کند. بنابراین، نفوذ به محفظه ماژول با احتمال بالایی قابل شناسایی است و باعث صفرسازی[7] سریع همه SSP های محافظت نشده می‌شود. به همین جهت ماژول‌های رمزنگاری سطح امنیتی چهارم برای کار در محیط‌هایی که از نظر فیزیکی حفاظت نشده‌اند، مناسب است.

این سطح به معرفی احراز هویت چندگانه[8] اپراتور می‌پردازد که باید شامل دو ویژگی از سه ویژگی زیر باشد [۱،۱۴].

- اطلاعاتی که کاربر می‌داند مانند رمز عبور مخفی
- چیزی که کاربر در اختیار دارد مانند توکن یا کلید فیزیکی
- یک ویژگی که مختص خود کاربر هست مانند اطلاعات بیومتریک

۳- الزامات امنیت

الزامات امنیتی که در استاندارد ISO/IEC-19790 برای طراحی و پیاده‌سازی یک ماژول رمزنگاری بیان شده است

[1] Temper-evidence
[2] Role-based authentication
[3] Sensitive Security Parameters (SSPs)
[4] Critical Security Parameters (CSPs)
[5] Identity-based authentication
[6] Trusted channel
[7] Zeroisation
[8] Multi-factor authentication

در این بخش مورد بررسی قرار می‌گیرند. ماژول رمزنگاری برای هر بخش نمره‌ای کسب و همچنین یک امتیاز کلی برای نشان‌دادن اینکه امنیت را در کدام سطح امنیتی برآورده می‌کند، دریافت می‌کند [۱۰،۱۱].

۳-۱- مشخصات ماژول رمزنگاری

یک ماژول رمزنگاری باید مجموعه‌ای از سخت‌افزار، نرم‌افزار، ثابت‌افزار یا ترکیبی از آن‌ها باشد که حداقل یک خدمت[1] رمزنگاری تعریف شده را در محدوده رمزنگاری مشخص شده برای ماژول، با استفاده از الگوریتم رمزنگاری شده، تابع امنیتی یا فرآیند تایید شده پیاده‌سازی کند. در هر چهار سطح امنیتی باید کلیه مشخصات ماژول، مرز رمزنگاری، توابع امنیتی تایید شده و حالت‌های عملیاتی عادی یا تنزل یافته مشخص باشد. مفهوم عملیات عادی اشاره به محلی که مجموعه الگوریتم‌ها، توابع امنیتی، خدمات یا فرآیندها در دسترس یا قابل تنظیم باشد، دارد. همچنین عملیات تنزل یافته برای زمانی طراحی می‌گردد که ماژول وارد حالت خطا شود. مرز رمزنگاری باید از یک محیط صریحا مشخص شده تشکیل شده باشد که مرز همه اجزای ماژول را تعیین می‌کند. الگوریتم‌ها، توابع امنیتی و فرآیندها باید به گونه‌ای اجرا شوند که عملکرد تایید شده ماژول را مختل نکرده یا به خطر نیندازند [۱].

۳-۲- رابط‌های ماژول رمزنگاری

یک ماژول باید کلیه جریان اطلاعات منطقی را فقط به نقاط دستیابی فیزیکی و رابط‌های منطقی که به عنوان ورودی و خروجی به مرز رمزنگاری ماژول مشخص می‌شود، محدود کند. انواع رابط‌های یک ماژول به رابط‌های سخت‌افزاری، نرم‌افزاری یا ترکیبی خلاصه می‌شود. یک ماژول باید دارای پنج رابط ورودی، خروجی، کنترل کننده ورودی، کنترل کننده خروجی و وضعیت خروجی باشد. همچنین در ماژول‌هایی که نرم‌افزاری نیستند، باید دارای رابط تغذیه نیز باشد که وظیفه تأمین برق الکتریکی ورودی به ماژول را دارد. در سطح امنیتی اول و دوم شامل رابط‌های اجباری و اختیاری، مشخصات همه رابط‌ها و مسیرهای ورود و خروج داده‌ها می‌شود و در سطح امنیتی سوم و چهارم شامل کانال ارتباطی مورد اعتماد است. یک کانال مورد اعتماد، پیوندی است که بین ماژول و فرستنده یا گیرنده برای ایجاد امنیت ایجاد شده است [۱].

[1] Service

۳-۳- نقش، خدمت‌ها و احراز هویت

یک ماژول باید از نقش‌های مجاز برای اپراتورها و خدمت‌های مربوطه در هر نقش پشتیبانی کند. ماژول باید حداقل از نقش افسر[2] رمزنگاری پشتیبانی کند که وظیفه مقداردهی اولیه رمزنگاری، توابع مدیریتی و خدمت عمومی امنیت را دارد [۱].

خدمت به کلیه خدمات، عملیات یا توابعی که می‌تواند توسط یک ماژول انجام شود، گفته می‌شود. قابلیت بای‌پس[3] یکی از توانایی‌های خدمت است که می‌تواند عملکرد یا فرآیند رمزنگاری را به‌طور جزئی یا کامل دور بزند [۱].

برای احراز هویت، اپراتوری که به ماژول دسترسی دارد با تایید اینکه اپراتور مجاز به پذیرش نقش درخواستی و انجام خدمات در آن نقش است، دسترسی‌های لازم را از ماژول می‌گیرد. ممکن است فرآیندهایی برای احراز هویت مورد نیاز باشد که به‌عنوان مثال می‌توان به احراز هویت مبتنی بر نقش و احراز هویت مبتنی بر شناسایی اشاره کرد [۱،۶].

در سطح امنیتی اول تفکیک منطقی نقش‌ها و خدمات بصورت اختیاری است. در سطح امنیتی دوم احراز هویت مبتنی بر نقش یا شناسایی صورت می‌گیرد. در سطح امنیتی سوم احراز هویت مبتنی بر شناسایی صورت می‌گیرد. در سطح امنیتی چهارم احراز هویت چندگانه صورت می‌گیرد [۱،۶].

۳-۴- امنیت نرم‌افزار، ثابت‌افزار

ماژول رمزنگاری به عنوان یک ماژول سخت‌افزاری، نرم‌افزاری، ثابت‌افزاری یا ترکیبی تعریف می‌شود.

به منظور بررسی یکپارچگی کد نرم‌افزار/ثابت‌افزار، در سطح امنیتی اول از کد تشخیص خطا[4] استفاده می‌شود. در سطح امنیتی دوم از امضای دیجیتال مورد تأیید استاندارد[5] یا احراز هویت پیام کلید شده مبتنی بر کد[6] برای بررسی یکپارچگی استفاده می‌شود. در سطح امنیتی سوم و چهارم تایید آزمون یکپارچگی مبتنی بر امضای دیجیتال صورت می‌گیرد [۱].

[2] Officer role
[3] Bypass
[4] Error Detection Code (EDC)
[5] Approved digital signature
[6] Keyed message authentication code- based

۳-۵- محیط عملیاتی

محیط عملیاتی یک ماژول به مدیریت نرم‌افزار، ثابت‌افزار یا سخت‌افزار مورد نیاز برای کارکرد ماژول اشاره دارد. محیط عملیاتی یک نرم‌افزار، ثابت‌افزار یا ماژول ترکیبی، حداقل شامل اجزای ماژول، بستر محاسباتی و ثابت‌افزاری است که اجازه اجرای نرم‌افزار یا ثابت‌افزار در بستر کامپیوتر را کنترل می‌کند. یک ماژول سخت‌افزاری ممکن است دارای یک محیط عملیاتی در داخل ماژول رمزنگاری باشد که متشکل از یک ثابت‌افزار است تا امکان اجرای نرم‌افزار داخلی یا ثابت‌افزار را فراهم کند [۱].

به طور کلی سه محیط عملیاتی خاص داریم:

- محیط عملیاتی غیر قابل تغییر که به گونه‌ای طراحی و پیکربندی می‌شود که از اصلاح توسط اپراتور یا فرآیند جلوگیری کند.
- محیط عملیاتی محدود که به گونه‌ای طراحی و پیکربندی می‌شود که امکان تغییر کنترل شده توسط اپراتور یا فرآیند را فراهم می‌کند.
- محیط عملیاتی قابل اصلاح که قابلیت پیکربندی مجدد مانند افزودن، حذف، ایجاد یا قابلیت‌های عمومی ثابت‌افزار را دارا باشد.

در سطح امنیتی اول غیر قابل اصلاح، محدود یا قابل اصلاح است. همچنین کنترل SSP ها در این سطح انجام می‌گیرد. در سطح امنیتی دوم قابل اصلاح است. در سطح امنیتی سوم و چهارم نیاز به الزامات اضافه‌ای نیست.

۳-۶- امنیت فیزیکی

در این بخش به امنیت سخت‌افزار ماژول رمزنگاری اشاره شده است. حفاظت فیزیکی از ماژول رمزنگاری به سه تجسم کلی فیزیکی تقسیم می‌شود که عبارتند از ماژول‌های تک تراشه‌ای[1]، چند تراشه‌ای نهفته[2] و چند تراشه‌ای مستقل[3] [۱۹].

امنیت فیزیکی الزاماتی به صورت کلی دارد که همه تجسم‌ها باید آن را رعایت کنند و همچنین هر تجسم الزاماتی مختص به خود دارد که در هر سطح امنیتی تبیین شده است. دو مورد از مهم‌ترین الزامات فیزیکی مورد استفاده در سطوح امنیتی، حفاظت از خرابی محیط و آزمایش خرابی محیط است. این موضوع به تفصیل در بخش چهارم آورده شده است.

[1] Single-chip
[2] Multiple-chip embedded
[3] Multiple-chip standalone

۳-۷- امنیت غیر تهاجمی[4]

مجموعه حملاتی که سعی بر به دست آوردن پارمترهای بحرانی ماژول دارد حملات غیر تهاجمی نامیده می‌شود. این حملات بدون هیچ‌گونه آسیب فیزیکی به ماژول رمزنگاری، اطلاعات مورد نیاز خود را از ماژول استخراج می‌کند. ضمیمه F این استاندارد به بررسی راهکارهای مورد استفاده در مقابل این حملات اختصاص یافته است. این موضوع به تفصیل در بخش پنجم آورده شده است [۹].

۳-۸- مدیریت پارامترهای امنیتی حساس

پارامترهای امنیتی حساس از پارامترهای امنیتی حیاتی و پارامترهای امنیتی عمومی[5] تشکیل شده‌اند. الزامات امنیتی برای مدیریت SSP ها شامل کل چرخه عمر SSP استفاده شده توسط ماژول است. مدیریت SSP شامل مولدهای بیت تصادفی[6]، تولید SSP، استقرار SSP، ورودی/خروجی SSP، ذخیره سازی SSP و صفرسازی SSP محافظت نشده است. در سطح امنیتی اول و دوم امکان وارد کردن دستی SSP هایی که وارد یا خارج می‌شوند به‌صورت متن رمز نشده وجود دارد. در سطح امنیتی سوم الزام به امکان وارد کردن دستی SSP هایی که وارد یا خارج می‌شوند، به‌صورت رمزگذاری شده، از طریق یک کانال مورد اعتماد است و همچنین CSP هایی که کلید مخفی رمزنگاری متن رمز نشده هستند باید با استفاده از روش‌های تقسیم دانش[7] با استفاده از یک کانال امن به ماژول وارد یا از آن خارج شوند. در سطح امنیتی چهارم باید از چند فاکتور مجزا برای احراز هویت مبتنی بر شناسایی به منظور ورود و خروج هر قسمت کلید اصلی استفاده شود [۱].

۳-۹- خودآزمایی

خودآزمایی‌های پیش عملیاتی[8] و مشروط[9] ماژول این اطمینان را به اپراتور می‌دهد که خطایی وارد نشده است که مانع عملکرد صحیح ماژول شود. در همه سطوح امنیتی باید قبل از بهره برداری ماژول، یکپارچگی نرم افزار/ ثابت‌افزار، بای پس و تست عملکردهای حیاتی مورد آزمایش قرار گیرند [۱].

[4] Non-Invasive Security
[5] Public Security Parameters (PSP)
[6] Random Bit Generators (RBGs)
[7] Split knowledge
[8] Pre-operational
[9] Conditional

۱۰-۳- چرخه اطمینان حیات

چرخه اطمینان حیات به استفاده از بهترین روش‌ها توسط فروشنده ماژول رمزنگاری در طول طراحی، توسعه، بهره برداری و پایان عمر ماژول گفته می‌شود [۱].

این چرخه شامل موارد زیر است:

- مدیریت سامانه پیکربندی ماژول رمزنگاری، اجزا، مستندات آن و مدیریت پیکربندی اتوماتیک
- طراحی ماژول رمزنگاری با استفاده از یک ماشین حالت متناهی[1] برای آزمودن تمام خدمت‌های امنیتی مرتبط
- فرآیند توسعه‌ی متناسب با سیاست‌های امنیتی و مشخصات عملکرد ماژول
- آزمایش ماژول توسط فروشنده به منظور مشخص کردن آزمایش عملکردی و سطح پایین ماژول
- روش‌های تحویل و بهره برداری ماژول برای توزیع، نصب ایمن، راه اندازی اولیه و احراز هویت اپراتور مجاز
- روش های پایان حیات ماژول برای سالم سازی و تخریب ایمن
- راهنمای کاربر مدیر و غیر مدیر

۱۱-۳- کاهش حملات دیگر

حساسیت ماژول رمزنگاری در برابر حملاتی که در جای دیگری در استاندارد بین المللی ISO/IEC 19790 تعریف نشده است، به نوع ماژول، پیاده سازی و محیط بستگی دارد. چنین حملاتی ممکن است مورد توجه ویژه ماژول‌های رمزنگاری که در محیط‌های خصمانه اجرا می‌شوند، باشد. این حملات معمولاً به تجزیه و تحلیل اطلاعات به دست آمده از منابعی که از نظر فیزیکی خارج از ماژول هستند، متکی است. در همه موارد، این گونه حملات سعی در تعیین دانش در مورد CSPها در ماژول رمزنگاری دارند. در سطح امنیتی اول و دوم و سوم، باید مشخصات کاهش حملاتی که در حال حاضر هیچ مورد آزمایشی برای آنها در دسترس نیست مورد بررسی قرار گیرد. در سطح امنیتی چهارم، باید مشخصات کاهش حملات با الزامات قابل آزمایش بررسی گردد [۱].

۴- امنیت فیزیکی

امنیت فیزیکی اقدامات امنیتی را توصیف می‌کند که برای جلوگیری از دسترسی غیرمجاز به ماژول رمزنگاری صورت می‌گیرد.

[1] Finite-state machine (FSM)

۱-۴- تجسم‌های امنیت فیزیکی

یک ماژول رمزنگاری باید از فرآیندهای امنیت فیزیکی [۱۳] در هنگام نصب استفاده کند تا دسترسی فیزیکی غیرمجاز به محتویات ماژول را محدود و از استفاده غیرمجاز یا اصلاح ماژول جلوگیری کند. کلیه سخت‌افزارها، نرم‌افزارها، ثابت‌افزارها، اجزای داده و SSP ها در مرز رمزنگاری محافظت می‌شوند. اگر ماژول رمزنگاری به طور کامل در نرم‌افزار به گونه‌ای پیاده‌سازی شود که امنیت فیزیکی صرفاً از طریق پلتفرم پردازشی تأمین شود، نیازمند رعایت بند امنیت فیزیکی این استاندارد بین المللی نیست. الزامات این بند در مورد ماژول‌های سخت‌افزار، ثابت‌افزار و اجزای ثابت‌افزار ماژول‌های ترکیبی قابل اجرا خواهد بود. الزامات امنیتی فیزیکی برای سه تجسم فیزیکی تعریف شده از یک ماژول رمزنگاری مشخص شده است:

- ماژول‌های رمزنگاری تک تراشه‌ای تجسم‌های فیزیکی هستند که در آن‌ها از یک مدار مجتمع مجزا به عنوان یک دستگاه مستقل استفاده می‌شود یا ممکن است در یک محفظه یا محصولی جاسازی شده باشد که هیچ محافظت فیزیکی نداشته باشد. نمونه‌هایی از ماژول‌های رمزنگاری تک تراشه‌ای شامل تراشه‌های تک IC[2] یا تراشه کارت‌های هوشمند است.
- ماژول‌های رمزنگاری نهفته چند تراشه‌ای تجسم‌های فیزیکی هستند که در آن‌ها دو یا چند تراشه IC به هم پیوسته‌اند و در یک محفظه یا محصولی جاسازی شده‌اند که ممکن است از نظر فیزیکی محافظت نشود. نمونه‌هایی از ماژول‌های رمزنگاری نهفته با تراشه‌های متعدد شامل آداپتورها و بردهای ارتقاء[3] است.
- ماژول‌های رمزنگاری مستقل چند تراشه‌ای تجسم‌های فیزیکی هستند که در آن‌ها دو اتصال بهم پیوسته است و کل محفظه از نظر فیزیکی محافظت می‌شود. از نمونه‌های آن شامل رمزگذاری مسیریاب‌ها[4] و توکن‌های USB است.

بسته به فرآیندهای امنیت فیزیکی یک ماژول رمزنگاری، تلاش غیر مجاز برای دستیابی، استفاده یا تغییر فیزیکی با احتمال بالا شناسایی می‌شود. همچنین هر تلاشی جهت حمله با به جا گذاشتن علائمی قابل مشاهده است و در طی یک تلاش دسترسی، اقدامات فوری مناسب

[2] Integrated Circuit
[3] Expansion boards
[4] Encrypting routers

توسط ماژول رمزنگاری برای محافظت از CSP ها انجام می‌شود.

به طور کلی، سطح امنیتی اول، مجموعه‌ای اساسی از نیازها را فراهم می‌کند. سطح امنیتی دوم نیازمند اضافه کردن فرآیندهای شهود دستکاری است و توانایی جمع آوری اطلاعات در مورد عملیات داخلی مناطق حیاتی ماژول را ندارد. سطح امنیتی سوم الزاماتی را برای استفاده از محفظه‌های قوی یا سخت‌همسان[1] یا ناهمسان[2] با امکان تشخیص و پاسخ به دستکاری برای پوشش‌ها و درب‌های قابل جابجایی، فراهم می‌کند. همچنین این سطح باید الزاماتی را برای مقاومت در برابر کاوش مستقیم از طریق درزها و شکاف‌ها فراهم آورد. حفاظت از خرابی محیط[3] یا آزمایش خرابی محیط[4] در سطح امنیتی سوم مورد نیاز قرار می‌گیرد. سطح امنیتی چهارم الزامات استفاده از محفظه‌های قوی یا سخت‌همسان یا ناهمسان را با فرآیندهای تشخیص و پاسخ دستکاری برای کل محفظه یا آسیب قابل توجه، اضافه می‌کند. EFP و محافظت در برابر حملات ناشی از خطا در سطح امنیتی چهارم لازم است [۱].

۴-۲- الزامات کلی امنیت فیزیکی

الزاماتی که باید برای همه تجسم‌های فیزیکی اعمال شود شامل موارد زیر است:

- اسناد باید تجسم فیزیکی و سطح امنیتی که فرآیندهای امنیتی فیزیکی ماژول رمزنگاری برای آن اجرا می‌شود را مشخص کند.
- در هر زمان که عملیات صفرسازی برای اهداف امنیتی فیزیکی مورد نیاز است، این عملیات باید در یک دوره زمانی کاملاً کوتاه اتفاق بیفتد تا از بازیابی داده‌های حساس بین زمان تشخیص و صفرسازی واقعی جلوگیری شود.
- در صورتی که ماژول شامل نقش تعمیر و نگهداری است به طوری که نیاز به دسترسی فیزیکی به محتوای ماژول دارد، نیازمند تعریف یک رابط دسترسی تعمیر و نگهداری است. همچنین اگر ماژول برای اجازه دسترسی فیزیکی طراحی شده باشد نیز تعریف این رابط ضروری است.
- رابط دسترسی تعمیر و نگهداری باید شامل تمام مسیرهای دسترسی فیزیکی به محتویات ماژول رمزنگاری، از جمله درب‌ها یا پوشش‌های قابل جابجایی باشد.
- هرگونه پوشش یا درب قابل جابجایی که در رابط دسترسی تعمیر و نگهداری موجود است باید با استفاده از فرآیندهای امنیتی فیزیکی مناسب محافظت شود.

در سطح امنیتی اول الزامات زیر برای ماژول اعمال می‌شود:

ماژول رمزنگاری باید از اجزای protection grade که شامل راه‌کارهای استاندارد انفعال است، تشکیل شده باشد (به‌عنوان مثال یک پوشش همسان[5] یا یک پوشش آب‌بندی[6] که از مدارهای ماژول در مقابل محیط زیست یا سایر آسیب‌های فیزیکی محافظت می‌کند). هنگام انجام تعمیر و نگهداری فیزیکی، صفرسازی باید توسط اپراتور یا به‌صورت خودکار توسط ماژول رمزنگاری انجام شود [۱].

در سطح امنیتی دوم علاوه بر الزامات عمومی برای سطح امنیتی اول، الزامات زیر برای کلیه ماژول‌های رمزنگاری اعمال می‌شود:

هنگامی که دسترسی فیزیکی به ماژول ایجاد می‌شود، ماژول رمزنگاری باید شواهدی از دستکاری (به عنوان مثال روی جلد، محفظه و مهر و موم) بر جای بگذارد. مواد، پوشش یا محفظه قابل دستکاری باید مات یا نیمه شفاف (در نور با طول موج ۴۰۰ نانومتر تا ۷۵۰ نانومتر) باشد تا از جمع آوری اطلاعات در مورد عملیات داخلی مناطق بحرانی ماژول جلوگیری کند. اگر ماژول رمزنگاری دارای سوراخ یا شکاف‌های تهویه هوا است، ماژول باید به گونه‌ای ساخته شود که با مشاهده مستقیم دیداری با استفاده از منابع نور مصنوعی در طیف دیداری ماژول، از جمع آوری اطلاعات مربوط به ساختار داخلی یا اجزای آن جلوگیری کند [۱،۱۷].

در سطح امنیتی سوم علاوه بر الزامات عمومی برای سطوح امنیتی اول و دوم، باید الزامات زیر برای ماژول‌های رمزنگاری اجرا گردد:

اگر ماژول رمزنگاری شامل درب یا پوشش قابل جابجایی است یا اگر یک رابط دسترسی تعمیر و نگهداری برای ماژول تعریف شده است، باید بتواند به دستکاری پاسخ دهد و قابلیت صفرسازی داشته باشد. در این سطح ماژول موظف است با باز شدن درب، برداشته شدن درپوش یا دسترسی به رابط دسترسی تعمیر و نگهداری، بلافاصله به دستکاری پاسخ دهد و تمام SSP های محافظت نشده را

[1] Hard conformal
[2] Non-conformal
[3] Environmental Failure Protection (EFP)
[4] Environmental Failure Testing (EFT)
[5] Conformal
[6] Sealing

صفر کند. اگر ماژول رمزنگاری دارای سوراخ‌های تهویه یا شکاف است، ماژول باید به گونه ای ساخته شود که از کاوش فیزیکی در داخل محفظه آن جلوگیری کند. محفظه‌ها، پوشش‌ها یا مواد تشکیل‌دهنده آن‌ها باید ویژگی‌های مقاومت و سختی را در محدوده دمای محیط نگهداری، توزیع و عملیاتی شدن ماژول حفظ کند. در صورت استفاده از مهر و موم‌های شهود دستکاری، آن‌ها باید دارای شماره منحصر به فرد یا به طور مستقل قابل شناسایی باشد (به‌عنوان مثال دارای نواری که دارای شماره یا مهر و موم هولوگرافی قابل شناسایی منحصر به فرد). همچنین ماژول باید شامل ویژگی‌های محافظت از خرابی محیط باشد یا تحت آزمایش خرابی محیط قرار گیرد [۱،۱۸].

در سطح امنیتی چهارم علاوه بر الزامات کلی برای سطوح امنیتی اول و دوم و سوم، الزامات زیر برای کلیه ماژول‌های رمزنگاری اعمال می‌شود:

ماژول رمزنگاری باید توسط یک پوشش مات غیرقابل جابه‌جایی و یا یک پوشش با امکان تشخیص و پاسخ به دستکاری (قابلیت صفرسازی) محافظت شود. همچنین باید شامل ویژگی‌های EFP باشد و از القای خطا[1] محافظت کند [۱،۱۸].

۳-۴- الزامات امنیت فیزیکی برای هر تجسم فیزیکی

هر کدام از سه تجسم فیزیکی علاوه بر الزامات کلی امنیت، دارای الزامات منحصر به فردی برای خود هستند که رعایت آن‌ها برای فراهم آوردن امنیت مورد توجه است.

۱-۳-۴- ماژول‌های رمزنگاری تک‌تراشه‌ای

علاوه بر الزامات کلی امنیت فیزیکی، برای سطح امنیتی دوم باید توجه داشت که ماژول رمزنگاری با روشی برای شهود دستکاری مثل پوشاندن آن در محفظه‌ای برای جلوگیری از مشاهده مستقیم، کاوش یا دستکاری محافظت شود. برای سطح امنیتی سوم ماژول باید با یک پوشش سخت مات پوشانده شود. در سطح امنیتی چهارم ماژول باید با پوشش سخت مات غیرقابل جابه‌جایی به همراه ویژگی‌های سختی و چسبندگی پوشانده شود به گونه‌ای که تلاش برای کندن، لایه‌برداری یا سوراخ‌کردن پوشش با احتمال زیاد منجر به آسیب جدی به ماژول شود. پوشش غیرقابل جابه‌جایی باید دارای ویژگی‌های حل شوندگی باشد به طوری که محلول در پوشش احتمال حل کردن ماژول یا آسیب جدی به آن را داشته باشد. در سطح امنیتی اول نیاز به الزامات اضافه‌ای برای ماژول‌های رمزنگاری تک‌تراشه‌ای نیست [۱،۲۱].

۲-۳-۴- ماژول‌های رمزنگاری چندتراشه‌ای نهفته

علاوه بر الزامات کلی امنیت فیزیکی، برای سطح امنیتی اول، ماژول باید درون یک پوشش قابل جابجایی باشد یا از محفظه protection grade استفاده کند. برای سطح امنیتی دوم، اجزای ماژول برای جلوگیری از مشاهده مستقیم و ارائه شواهد دستکاری، باید با یک پوشش قابل رویت پوشانده شود یا باید به طور کامل در محفظه‌ای از درجه تولید فلز یا پلاستیک سخت که ممکن است شامل درب‌ها یا پوشش‌های قابل جابجایی باشد، قرار بگیرد. در صورتی که محفظه شامل هرگونه درب یا پوشش قابل جابجایی است، درب‌ها یا روکش‌ها باید با قفل‌های مکانیکی مقاوم در برابر استفاده از کلیدهای فیزیکی یا منطقی قفل شوند یا با مهر و موم‌هایی که دستکاری را تشخیص می‌دهد، محافظت شود. برای سطح امنیتی سوم، تراشه‌های چندگانه مدار ماژول رمزنگاری باید با پوشش سخت مثل یک ماده اپوکسی[2] سخت پوشانده شود یا ماژول باید در یک محفظه محکم باشد، به طوری که تلاش برای برداشتن یا نفوذ به محفظه آن با احتمال زیاد باعث آسیب جدی به ماژول شود. در سطح امنیتی چهارم، اجزای ماژول باید در یک محفظه قوی یا سخت‌همسان یا ناهمسان قرار گیرد. محفظه باید توسط یک پوشش مشخص کننده دستکاری محصور شود که دستکاری را از طریق برش، حفاری، فرز، آسیاب، سوزاندن، ذوب شدن، یا حل کردن محفظه تا حدی که برای دسترسی به SSPها کافی است، تشخیص دهد. همچنین ماژول باید شامل مدار تطبیق پاسخ و صفرسازی باشد که بر روی پوشش تشخیص دستکاری نظارت کند و با تشخیص دستکاری، بلافاصله تمام SSP های محافظت نشده را صفر کند. همچنین مدار پاسخ دستکاری باید هنگامی که SSP های محافظت نشده در ماژول رمزنگاری وجود دارد، عملیاتی باقی بماند [۱].

۳-۳-۴- ماژول‌های رمزنگاری چندتراشه‌ای مستقل

علاوه بر الزامات کلی امنیت فیزیکی، در سطح امنیتی اول، ماژول رمزنگاری باید در محفظه‌ای با protection grade

[1] Fault induction

[2] Epoxy

فلز یا پلاستیک سخت قرار گیرد که ممکن است شامل درب‌ها یا پوشش‌های قابل جابجایی باشد. در سطح امنیتی دوم، اگر محفظه ماژول رمزنگاری شامل هرگونه درب یا پوشش قابل جابجایی است، درب‌ها یا روکش‌ها با قفل‌های مکانیکی مقاوم در برابر استفاده از کلیدهای فیزیکی یا منطقی قفل شود یا با مهر و موم‌های شواهد دستکاری محافظت شود (به عنوان مثال نوار یا مهر و موم هولوگرافی). در سطح امنیتی سوم ماژول باید در یک محفظه محکم قرار گیرد، به طوری که تلاش برای حذف یا نفوذ به محفظه با احتمال زیاد باعث آسیب جدی به ماژول می‌شود. در سطح امنیتی چهارم، محفظه ماژول رمزنگاری باید شامل یک پوشش تشخیص دستکاری باشد که از فرآیندهای تشخیص دستکاری مانند سوئیچ‌های پوششی (به‌عنوان مثال میکرو سوئیچ‌ها، سوئیچ‌های اثر مغناطیسی هال، محرک‌های مغناطیسی دائمی و غیره)، آشکارسازهای حرکت (به‌عنوان مثال فراصوت، مادون قرمز) یا سایر فرآیندهای تشخیص دستکاری در مقابل حملات مانند برش، حفاری، فرز، آسیاب، سوزاندن، ذوب شدن یا حل شدن تا حدی که برای دسترسی به SSP کافی است، استفاده کند. همچنین ماژول رمزنگاری باید شامل پاسخ دستکاری و قابلیت صفرسازی باشد که بطور مداوم پوشش تشخیص دستکاری را کنترل می‌کند و با تشخیص دستکاری، بلافاصله تمام SSP های محافظت نشده را صفر می‌کند. قابلیت پاسخ‌دهی و صفرسازی باید هنگامی که SSP های محافظت نشده در ماژول رمزنگاری وجود دارد، همچنان عملیاتی باقی بماند [۱].

EFT/EFP -۴-۴

دستگاه‌ها و مدارهای الکترونیکی برای کار در محدوده خاصی از شرایط محیطی طراحی شده اند. نوسان عمدی یا تصادفی خارج از محدوده‌های عادی عملکرد ولتاژ و دما می تواند باعث عملکرد نامناسب یا خرابی دستگاه‌های الکترونیکی یا مدار شود که می‌تواند امنیت ماژول رمزنگاری را به خطر بیندازد. با استفاده از ویژگی‌های محافظت از خرابی محیط یا انجام آزمایش خرابی محیط، می‌توان اطمینان منطقی مبنی بر اینکه امنیت یک ماژول رمزنگاری توسط شرایط شدید محیطی به خطر نیفتد، پیدا کرد. برای سطح امنیتی اول و دوم، الزامی برای استفاده از ویژگی‌های EFP یا انجام EFT برای ماژول نیست. اما در سطح امنیتی سوم، ماژول باید از ویژگی‌های EFP استفاده کند یا EFT را انجام دهد. همچنین در سطح امنیتی چهارم، باید از ویژگی‌های EFP استفاده کند [۱،۱۸].

۴-۴-۱- ویژگی‌های EFP

ویژگی‌های حفاظت از خرابی محیط باید از ماژول رمزنگاری در برابر شرایط غیرعادی محیطی که می تواند امنیت آن را در خارج از محدوده عملکرد عادی به خطر بیندازد، محافظت کند. ماژول رمزنگاری باید بتواند هنگامی که دما و ولتاژ، عملکردی خارج از محدوده طبیعی مشخص شده دارند، عملکرد و پاسخ صحیحی داشته باشد. اگر دما یا ولتاژ خارج از محدوده عملکرد عادی ماژول رمزنگاری باشد، حفاظت باید آن را برای جلوگیری از عملکرد بیشتر خاموش کند یا بلافاصله تمام SSP های محافظت نشده را صفر کند [۱].

۴-۴-۲- فرآیند EFT

آزمایش خرابی محیط شامل ترکیبی از تجزیه و تحلیل، شبیه‌سازی و آزمایش یک ماژول رمزنگاری است تا اطمینان پیدا کند که شرایط محیطی در خارج از محدوده عملکرد طبیعی برای دما و ولتاژ، امنیت ماژول را به خطر نمی‌اندازد. EFT نشان می‌دهد که اگر دمای کار یا ولتاژ، خارج از محدوده عملکرد عادی ماژول باشد که منجر به خرابی شود، امنیت ماژول رمزنگاری همواره تضمین می‌شود [۱،۱۸].

دامنه دمایی که باید آزمایش شود باید از دمایی در محدوده دمای کاری عادی تا کمترین (یعنی سردترین) دما باشد که یا ماژول را خاموش کند تا از کار بیشتر جلوگیری کند یا بلافاصله همه SSPهای محافظت نشده را صفر کند و از یک درجه حرارت در محدوده دمای عملکرد طبیعی تا بالاترین (یعنی داغ‌ترین) دمایی که یا خاموش شود یا به حالت خطا برود یا تمام SSP های محافظت نشده را صفر کند.

دامنه دما برای آزمایش باید از ۱۰۰ درجه تا ۲۰۰ درجه سانتی‌گراد باشد. اما به محض خاموش شدن ماژول، آزمون قطع می‌شود تا از کارکرد بیشتر جلوگیری شود و بلافاصله همه SSP های محافظت نشده صفر می‌شود یا ماژول به حالت خرابی وارد می‌شود. دما باید علاوه بر مرزهای فیزیکی، در اجزای حساس و دستگاه‌های حیاتی نیز کنترل شود.

دامنه ولتاژ آزمایش شده باید به تدریج از یک ولتاژ در محدوده ولتاژ عملکرد طبیعی به یک ولتاژ پایین‌تر کاهش یابد که یا ماژول را خاموش می‌کند تا از کار بیشتر

جلوگیری کند یا بلافاصله تمام SSPهای محافظت نشده را صفر می‌کند و به تدریج از ولتاژ در محدوده ولتاژ عملیاتی عادی به یک ولتاژ بالاتر تبدیل می‌شود که یا ماژول را خاموش می‌کند تا از کار بیشتر جلوگیری کند یا بلافاصله تمام SSPهای محافظت نشده را صفر می‌کند [۱].

۵- امنیت غیرتهاجمی

حملات غیر تهاجمی با به دست آوردن دانش CSP های ماژول بدون تغییر فیزیکی یا تهاجم به ماژول، سعی در به خطر انداختن یک ماژول رمزنگاری می‌کند. ماژول‌ها ممکن است راهکارهای مختلفی را برای کاهش این نوع حملات استفاده کنند. معیارهای آزمون برای کاهش حمله غیر تهاجمی برای هر یک از عملکردهای امنیتی مرتبط با این استاندارد بین‌المللی در ضمیمه F ذکر شده است. اگر ماژول رمزنگاری برای محافظت از SSP های محافظت نشده ماژول از حملات غیر تهاجمی که در این ضمیمه ذکر شده است، از راه‌کارهای کاهش حمله غیر تهاجمی استفاده نکند، این زیر بند قابل اجرا نیست [۱،۳].

در سطح امنیتی اول و دوم، اسناد و مدارک باید تمام روش‌های کاهشی را برای محافظت از CSP های ماژول در برابر حملات غیر تهاجمی مشخص کند. در سطح امنیتی سوم، ماژول رمزنگاری باید آزمایش شود تا معیارهای تایید شده برای کاهش سطح حملات غیر تهاجمی را تأیید کند. در سطح امنیتی چهارم، رمزنگاری برای پاسخگویی به معیارهای تأیید شده برای کاهش سطح حملات غیر تهاجمی آزمایش می‌شود [۱].

۵-۱- حملات غیر تهاجمی

انواع حملات غیر تهاجمی به حملات کانال جانبی، تجزیه و تحلیل توان، تجزیه و تحلیل الکترومغناطیسی و زمان بندی خلاصه می‌شود. مهم‌ترین حمله غیر تهاجمی، حملات کانال جانبی است که بر اساس اطلاعات به دست آمده از پیاده‌سازی یک سامانه تا ضعف‌های الگوریتم‌های پیاده‌سازی آن را شامل می‌شود [۴،۹].

انواع کلی حملات کانال جانبی به حمله به حافظه پنهان، حمله زمانی، حمله تحلیل توان، حملات الکترومغناطیسی، حمله راه اندازی سرد[1]، حملات خطای مبتنی بر نرم‌افزار و نوری خلاصه می‌شود، که در همه آنها اصل اساسی این است که اثرات فیزیکی ناشی از عملکرد ماژول رمزنگاری مورد بررسی قرار گیرد و اطلاعات پنهان استخراج شود. اطلاعات پنهان ممکن است بصورت پدیده‌های فیزیکی شامل: مصرف برق، انتشار الکترومغناطیسی، انتشار فوتون یا زمان اجرا نشت کند [۵].

در تجزیه و تحلیل توان، داده‌های مصرف توان بی‌درنگ، ممکن است حاوی اطلاعات مربوط به عملیات رمزنگاری در حال انجام باشد. این حمله به دو صورت تجزیه و تحلیل توان ساده[2] (SPA) و تجزیه و تحلیل توان تفاضلی[3] (DPA) صورت می‌گیرد. در SPA با مشاهده شکل موج اندازه‌گیری شده مصرف توان جاری و در DPA با پردازش آماری آن کلید مخفی استخراج می‌شود [۳،۴].

از آنجا که حملات کانال جانبی به رابطه اطلاعات فاش شده از طریق یک کانال جانبی و داده‌های مخفی متکی است، اقدامات متقابل به دو دسته عمده تقسیم می‌شود، اولی حذف یا کاهش انتشار این دست اطلاعات و دومی حذف ارتباط بین اطلاعات فاش شده و داده‌های مخفی، که برای آن باید اطلاعات درز شده، غیر مرتبط با داده‌های مخفی قرار گیرد. برای دسته اول استفاده از نمایشگرهایی با محافظ مخصوص به منظور کاهش تشعشعات الکترومغناطیسی گزینه مناسبی است. همچنین گمراه سازی کانال انتشار اطلاعات با نویز از دیگر اقدامات متقابل است [۵].

۵-۲- ضمیمه F

معیارهای آزمون کاهش حمله غیر تهاجمی تایید شده در این ضمیمه آورده می‌شود. این ضمیمه لیستی از معیارهای آزمون کاهش حملات غیر تهاجمی مورد تایید ISO/IEC را که در این استاندارد بین المللی اعمال می‌شود، ارائه می‌دهد. این لیست کامل نیست اما این مانع استفاده از معیارهای آزمون کاهش حملات غیر تهاجمی تأیید شده توسط مرجع تأیید نیست. یک مرجع تصویب کننده می تواند این پیوست را به طور کامل با لیست خود با معیارهای آزمون کاهش حملات غیر تهاجمی تایید کند. در حال حاضر معیارهای آزمون کاهش حملات غیر تهاجمی تایید شده‌ای در این استاندارد وجود ندارد [۱].

۶- جمع‌بندی و پیشنهادها

با توجه به بررسی استاندارد ISO/IEC 19790 و سطوح مختلف امنیتی و الزامات آن، توصیه می‌شود که تولید

[1] Cold boot

[2] Simple Power Analysis
[3] Differential Power Analysis

کنندگان ادوات رمزنگاری از این استاندارد برای ساخت و ارزیابی ماژول‌های رمزنگاری خود بهره گیرند. اما باید توجه داشت که این استاندارد در سطوح امنیتی سوم و چهارم نیازمند بازنگری و ارائه پروتکل‌های دقیق‌تری است. همچنین در قسمت امنیت غیر تهاجمی پیشنهاد می‌شود که روش‌های آزمون و معیارهای آزمون برای آن تعیین شود زیرا که ضمیمه F استاندارد بصورت تکمیل نشده و ناقص است.

۷- مراجع

[1] Information technology, Security techniques, Security requirements for cryptographic module, ISO/IEC 19790, 2020

[2] Federal information processing standards publication, FIPS PUB 140-3, 2019

[3] Hirofumi Sakane, Caroline Scace (2010), FIPS 140-3 Non-Invasive Attack Testing, https://csrc.nist.gov/presentations/2010/fips-140-3-non-invasive-attack-testing-presentatio

[4] Jan Blonk, TNO ITSEF(2005), Introduction to side channel attacks and non-invasive attacks, https://people.eecs.berkeley.edu/~culler/AIIT/papers/security/physecpaper02.pdf

[5] https://en.wikipedia.org/wiki/Side-channel_attack

[6] Kim B. Schaffer, CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24759:2017

[7] Michael J. Cooper, Kim B. Schaffer, Security Requirements for Cryptographic Modules, 2019

[8] Apostol T. Vassilev, Larry Feldman, Gregory A. Witte, Cryptographic Module Validation Program (CMVP), 2014

[9] Kim B. Schaffer, CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759:2017, 2020

[10] Information technology, Security techniques, Test requirements for cryptographic modules, ISO/IEC 24759:2017, https://www.iso.org/standard/72515.html

[11] Rebecca M. Blank, Acting Secretary, Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, CMVP program staff, 2011

[12] https://en.wikipedia.org/wiki/FIPS_140-3

[13] Randall J. Easter, Ken Lu, FIPS 140-3 Section 5 – Physical Security, 2005

[14] Kim B. Schaffer, CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B, 2020

[15] Beverly Trapnell, Carolyn French, Cryptographic Module Validation Program, module validation lists, 2013

[16] Johnston, Tamper-Indicating Seals: Practices, Problems, and Standards, World Customs Organization Security, Brussels, 2019

[17] Defeating Existing Tamper-Indicating Seals, Argonne National Laboratory, Archived from the original, 2008

[18] Travis Spann, Fault Induction and Environmental Failure Testing, NIST CMVP Physical Security Conference, 2005

[19] Ken Lasoski and Scott Ehrlich, FIPS 140-2 and FIPS 140-3: What's the Diff? – Part 3: Let's Get Physical, 2019

[20] Ryan Thomas and Raghu Vamshi Vadlakunta, FIPS 140-2 and FIPS 140-3: What's the Diff – Part 4: You down with S.S.P?, 2019

[21] Travis span and the aegisolve team, FIPS 140-2 single-chip level 3 physical security, 2018

علیرضا جواهری در سال ۱۴۰۰ از مقطع کارشناسی، رشته مهندسی کامپیوتر، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی فارغالتحصیل شده است. در حاضر دانشجوی رشته فناوری اطلاعات گرایش سیستم‌های چندرسانه‌ای، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی است. موضوعات پژوهشی مورد علاقه ایشان رمزنگاری، گرافیک کامپیوتری و هوش مصنوعی است.

راضیه سالاری فرد به‌ترتیب در سال‌های ۹۱، ۹۳ و ۹۷ از مقاطع کارشناسی، کارشناسی ارشد و دکتری، رشته معماری کامپیوتر، دانشکده کامپیوتر، دانشگاه صنعتی شریف فارغالتحصیل شده است. حدود ۴ سال سابقه کاری در حوزه طراحی و امنیت سخت افزار دارد و در حال حاضر استادیار دانشکده مهندسی و علوم کامپیوتر دانشگاه شهید بهشتی است. حوزه پژوهشی وی طراحی و پیاده‌سازی کارا و امن الگوریتم‌های رمزنگاری است.