طراحی و پیاده سازی مینیمم سیستم سخت افزاری امنیتی ضد مداخله

نفیسه محمدی شکیبا[۱]، محمد علی دوستاری[۲] و شیما حسن زاده[۳]

چکیده

در دنیای دیجیتال حفاظت از اطلاعات امری مهم و ضروری می باشد. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات می باشد. رمزنگاری اطلاعات، روشی مناسب به منظور حفاظت از اطلاعات حساس است و از آنجایی که تنها افرادی که دارای کلید مناسب رمزگشائی می باشند، قادر به استفاده از این اطلاعات محافظت شده می باشند کلیدهای رمزنگاری دارای اهمیتی بالاتر از خود اطلاعات است از این رو سیستم های سخت افزار امن، محافظی گرانقدر برای کلیدها به شمار می آیند. در این مقاله به معرفی سیستم پیاده سازی شده- توسط نویسندگان- پرداخته می شود.

کلمات کلیدی

ماژول سخت افزاری امنیتی[۴]، امنیت کلیدهای رمزنگاری، تشخیص مداخله[۵]، استاندارد امنیتی FIPS

---

[۱] کارشناس ارشد فناوری اطلاعات، دانشگاه شاهد
آدرس پست الکترونیکی: shakiba@shahed.ac.ir
[۲] دکترا، دانشگاه شاهد
آدرس پست الکترونیکی: doostari@shahed.ac.ir
[۳] کارشناسی، دانشگاه شاهد
آدرس پست الکترونیکی: shima.hassanzadeh@yahoo.com
[۴] HSM(Hardware Security Module)
[۵] Tamper Detection

۱. مقدمه

در عصر اطلاعات با توجه به نیاز به انتقال اطلاعات که بعضا این اطلاعات جنبه ی خصوصی و محرمانه نیز دارند، ایمن سازی اطلاعات از نقطه نظر کاربران رایانه ای، دولت ها و مخصوصا سازمانهای نظامی دارای اهمیت فوق العاده ای می باشد؛ از این رو رمزنگاری اطلاعات تبدیل به روشی دفاعی برای حفظ حریم اطلاعات کاربران گشته است. در این خصوص با توجه به اهمیت کلیدهای رمزنگاری، ابزاری برای حفاظت از آن ها ضروری به نظر رسیده و همین امر سبب ایجاد سیستمی سخت افزاری برای حفاظت از اطلاعات حساس از قبیل کلیدهای رمزنگاری شده است.

سیستم های رمزنگاری امن، اغلب با دو هدف عمده ی تسریع در عملیات رمزنگاری و حفاظت از داده های حساس ایجاد شده اند. برای تضمین موفقیت این سیستمها در حفاظت از اطلاعات، بایستی خدماتی هم چون تشخیص حملات و واکنش مناسب و سریع به این سیستم ها افزوده گردد. این سیستم ها از لحاظ خدماتی که ارائه می دهند و درجه ی ایمن سازی اطلاعات، با یکدیگر متفاوت اند. از این رو موسسه ی NIST سندی را به عنوان استاندارد منتشر کرده است که سیستم ها ی مختلف را با معیارهایی چندگانه سنجیده و مدارک و سطوح امنیتی را به آنها اعطا می نماید.

۲. تعریف ماژول سخت افزاری امن

یک ماژول سخت افزاری امن یک دستگاه امنیتی مبتنی بر سخت افزار می باشد که کلیدهای رمزنگاری را تولید، ذخیره و نگهداری می نماید. این ماژول که گاهی ماژول امنیتی میزبان[۱] هم نامیده می شود، یک جزء امنیتی فیزیکی در حوزه ی فن آوری اطلاعات می باشد که پردازش های رمزنگاری امن را برای محدوده ی عظیمی از برنامه های کاربردی که توسط سیستم بانکداری و موسسات مالی، دولتی، تبادلات بورس، نظامی ودیگر صنایع استفاده می شود، انجام می دهد. یک پردازنده ی امن در واقع یک محیط محاسباتی همه منظوره است که در مقابل حملات فیزیکی و منطقی مقاومت می نماید. ماژول های سخت افزاری امنیتی می تواند در اشکال و قالب های متفاوتی مانند کارت های هوشمند، کارت های PCI برای اتصال به رایانه های شخصی، نشانه های قابل اتصال[۲] و جعبه های Rack Mount که در قالب کانال هایی مانند TCP/IP، گذرگاه سریال جهانی[۳] و پورت سریال[۴] ارتباط برقرار می کنند، عرضه شوند. اما صرفنظر از شکل، همگی دو هدف اصلی تسریع عملیات رمزنگاری و نگهداری کلیدها بصورت امن را دنبال می کنند [1] - [5].

در حوزه ی امنیت اطلاعات، بعضی اوقات از ماژول های نرم افزاری برای نگهداری داده های حساس و انجام عملیات بحرانی استفاده می شود. این ماژول ها در رتبه بندی استاندارد های امنیتی مانند FIPS، سطوح پایین تری را به خود اختصاص می دهند؛ حال آنکه اکثر مدلهای تجاری ماژول های سخت افزاری امن، دارای مدرک سطح سوم بوده و اگر خصوصیت ضد مداخله هم بدانها افزوده شود، سطح چهارم استاندارد FIPS را هم می توانند دریافت کنند. مهمترین مزیت یک ماژول سخت افزاری امن در مقایسه با نمونه های نرم افزاری مشابه، محیط امنتر آن می باشد. چراکه یک ماژول سخت افزاری امن قادر است کلیدهای رمزنگاری را درداخل خودش تولید و ذخیره نماید؛ بدون آنکه نیاز به ارسال، دریافت و یا خروج آنها داشته باشد. یک ماژول سخت افزاری امناز ورود غیر مجاز افراد، از طریق احراز هویت دو فاکتوری جلوگیری می کند و مجهز به یک محیط فیزیکی امن و ضد مداخله با حداکثر مقاومت در برابر مداخله و حداقل دسترسی با دنیای خارج می باشد.

بنابراین دلایل، یک ماژول سخت افزاری استاندارد شده در مقایسه با ماژول های نرم افزاری استاندارد شده ی مشابه، سطح امنیتی به مراتب بالاتری را دریافت می نماید[6,7] .

به طور کلی هر ماژول سخت افزاری امن شامل اجزای زیر می باشد:

- یک پردازنده ی مرکزی: برای کنترل و هماهنگ کردن عملیات خاص منظوره ی درون کارت (پاسخ به در خواستهای دریافتی از میزبان)
- موتورهای رمزنگاری: برای انجام عملیات رمزنگاری DES، AES، RSA، Hash و چهار عمل اصلی امضا[۵]، تشخیص[۶]، رمزنگاری[۷]، رمزگشایی[۸].
- تولید کننده ی اعداد تصادفی: برای تولید کاملا امن کلیدهای رمزنگاری و یا متغیرهای تصادفی و مهرهای زمانی که در پروتکل های امنیتی متعددی استفاده می شوند.
- مدار تشخیص و پاسخ به مداخله[۹].
- واسط ارتباطی: برای ارتباط میان کارت و برنامه ی کاربردی برای رد و بدل کردن پیام های ثبت وقایع[۱۰].
- حافظه ی امن مجهز به باتری پشتیبان[۱۱]: برای نگهداری کلیدهای رمزنگاری و داده های حساس درون سازمانی.

۳. استانداردها و معیارها ی سنجش یک واحد رمزنگاری

برای ایجاد تفاهم و اطمینان متقابل میان تولید کننده و مصرف کننده ی یک واحد رمزنگاری، استانداردهایی مشخص شده اند که از میان آنها FIPS140-2 را می توان نام برد[8-10]. این استاندارد معیاری برای تعیین میزان امنیت و درجه ی اطمینان یک محصول رمزنگاری می باشد و شامل چهار سطح امنیتی است که بدین ترتیب محصولات نرم افزاری صرف، سطح ۱ و محصولات سخت افزاری تا سطح چهارم را می توانند کسب کنند.

در امنیت سطح ۱ تنها نیازهای امنیتی پایه برای یک ماژول رمزنکاری در نظر گرفته شده است و نیازمندی های امنیتی فیزیکی برای دستگاه ها در نظر گرفته نشده است. در این رابطه، یک برد رمزشده کامپیوتر شخصی نمونه ای از یک ماژول رمزنگاری امنیتی سطح ۱ می باشد.

در سطح امنیتی ۲، امنیت در سطح را ۱ با اضافه کردن تجهیزاتی –هم چون پوشش برای آشکار کردن مداخله یا مهر وموم و پلمپ یا قفل های مقاوم در برابر سرقت[۱۲] روی پوشش یا درهای برداشتنی ماژول - برای آشکار نمودن مداخله افزایش داده است.

در سطح ۳ علاوه بر مکانیزمهای سطح ۲، تجهیزاتی نیز برای جلوگیری از مداخله حمله کننده برای ماژول در نظر گرفته شده است. مکانیزم امنیت فیزیکی در این سطح به گونه ای است که نفوذ را تشخیص داده و مانع از افشاء، سوء استفاده و یا تغییر داده های مهم و حساس شود.

در آخرین سطح امنیتی که سطح ۴ می باشد بالاترین سطح امنیتی تعریف شده در این استاندارد را در بر می گیرد. در این سطح باید ماژول در برابر تمامی حملات مقاوم و ضد مداخله باشد. ماژول رمزنگاری سطح ۴ امنیتی عمدتا برای عمل در محیط هایی که از لحاظ فیزیکی حفاظت نشده اند، مفید اند.

این استاندارد، ۱۱ حیطه از نیازمندی های امنیتی را برای این ۴ سطح تعریف می کند تا طیف وسیعی از اطلاعات حساس و محیط های کاربردی متنوع را پوشش دهد.

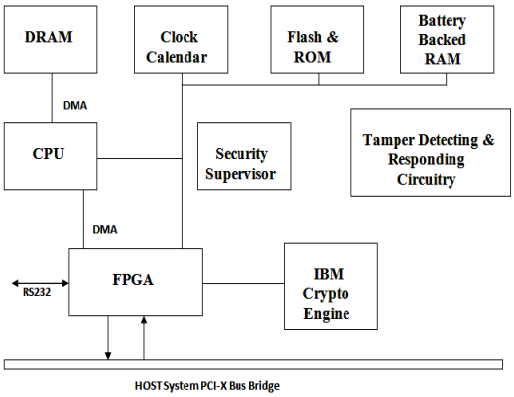
۴. بررسی IBM PCIXCC و مینیم سیستم پیاده سازی شده

واحدهای امنیتی از لحاظ ظاهر، ساختار، اجزای سازنده، شیوه ی طراحی و قابلیت ها با یکدیگر تفاوت های عمده ای دارند. در این بخش به معرفی یک محصول از شرکت IBM پرداخته می شود[11,12]. سپس قابلیت های مینیم سیستم پیاده سازی شده بیان شده و در نهایت مقایسه ای میان آن ها انجام می گیرد.

۴-۱. IBM PCIXCC

این ماژول یکی از جدیدترین ماژول های رمزنگاری IBM است که به طور کلی شامل اجزای زیر می باشد:

- تولید کننده اعداد تصلدفی بصورت کاملا[۱۳] سخت افزاری
- میکروپروسسور IBM PowerPC*405GPr
- 64M حافظه ی RAM پویا
- 16M حافظه فلش
- 128K حافظه امن مجهز به باتری پشتیبان
- پردازنده رمزنگاری Otello
- میکرو کنترلر AVR



تصویر ۱: نمایی از IBM PCIXCC

از آنجایی که سیستم ضد مداخله از اهمیت بالایی برخوردار است تنها به توضیح این بخش از سیستم در این مقاله می پردازیم(سایر بخش ها بطور کامل در [11]توضیح داده شده است).

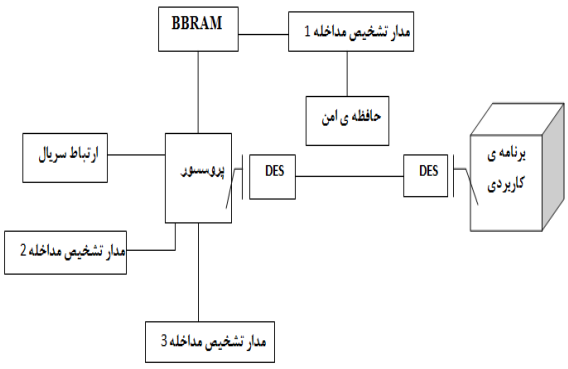
۴-۱-۱. سیستم ضد مداخله ی IBM PCIXCC

- تکنولوژی بسته بندی امن این ماژول، تمام حملات فیزیکی که احتمال دارد توسط مداخله گران برای استخراج کردن اطلاعات محرمانه و یا مداخله در اجرای عملیات های بحرانی درون کارت، انجام شود را تشخیص داده و جلوگیری می کند.
- ماژول امن روی کارت PCIXCC با ویژگی تشخیص مداخله طراحی شده است. تمام اجزای امنیتی، داخل یک مش منعطف که شامل خطوط رسانای نازک، تعبیه شده است جای گرفته اند که حملاتی هم چون دریل کردن، سایش شیمیایی را تشخیص می دهند.
- مدار داخلی نیز برای تشخیص مداخله داخل مرزهای رمزنگاری تعبیه شده است که در صورت آسیب دیدن خطوط رسانا، مدار داخل ماژول مداخله را تشخیص داده و داده های حساس به سرعت پاک می شوند. این کار توسط صفر کردن حافظه امن صورت می پذیرد. بنابراین تمام داده های موجود در حافظه امن و همچنین فلش - داده ها ی فلش توسط کلید TDESرمز شده و این کلید در حافظه امن ذخیره است- پاک می شود.
- مدار ویژه ی دیگری Imprinting در RAM را تشخیص می دهد. در طول کار RAM داده های متفاوتی در آن ریخته می شود ولی بار بعدی که تراشه تغذیه شود باز همان داده ی Imprinting را نشان می دهد. Imprinting از طریق قراردادن تراشه در دمای کم یا اشعه ی X بوجود می آید.

مدار تشخیص مداخله، این مداخله ها را تشخیص و RAM را پیش از Imprinting صفر می کند.

۴-۲. مینیمم سیستم پیاده سازی شده

پس از مطالعه استانداردهای امنیتی که ماژول های امن را معتبر می نمایند و هم چنین بررسی مدلهای تجاری از ماژول های سخت افزاری امنیتی که توسط شرکت های امنیتی قدر متندی هم چون IBM، Banksys و SafeNet در بازار های جهانی عرضه می شوند، بر آن شدیم تا مدلی را طراحی نماییم که نیازمندی های امنیت تئوری را را برآورده نماید و در عین حال کم هزینه تر و ساده تر پیاده سازی شود. از این رو ماژول سخت افزاری امنی طبق شکل ۲ طراحی گردید.



تصویر ۲: سیستم پیاده سازی شده

در این سیستم پیاده سازی شده از سه مدار متفاوت برای تشخیص و پاسخ به مداخله استفاده شده است که این سه مدار، قادرند تا تمام حملات فیزیکی وارد شده به ماژول را تشخیص و پاسخ دهند. در این ماژول سخت افزاری امن، برای نگهداری داده های حساس[۱۴] از یک حافظه امن خارجی متصل به مدار پاسخ و تشخیص مداخله استفاده شده است.

مینیم سیستم امن مذکور، در قالب یک کارت PCI می باشد که از طریق گذرگاه ارتباطی سریال با رایانه و برنامه کاربردی مرتبط می شود. پروتکل ارتباطی -که زبان استاندارد ارتباطی میان کارت و میزبان می باشد - با استفاده از زبان برنامه نویسی C# طراحی و پیاده سازی گردید. این محیط گرافیکی ارتباطی، امکانات متعددی را در اختیار کاربران قرار می دهد. تمامی این توابع روی میکروی ATMEGA32 و توسط برنامه ی codevision پیاده سازی و نوشته گردید. همچنین با توجه به نیازمندی های بررسی شده در استاندارد PKCS#11، در زمینه ی نقش ها و تصدیق کاربران، برای مینیمم سیستم پیاده سازی شده، کاربرانی با حقوق دسترسی متفاوت تعریف شد و برای تصدیق اینها، از تصدیق نقش محور استفاده شد.

یکی از ایده های بکار گرفته شده در این سیستم این است که تمام اجزا را داخل یک جعبه قرار داده و تنها یک واسط ارتباطی با دنیای بیرون دارد و این جعبه همان طور که گفته شد از طریق سه نوع مدار محافظت می شود و تنها در صورتی نفوذ به داخل سیستم سبب پاک شدن حافظه ی امن نمی شود که نقشی با هویت متصدی تعمیر و نگهداری از طریق برنامه ی کاربردی اطلاعاتش تصدیق شود- با وارد کردن نام کاربر و رمز یا به طور امن تر می توان از اسکنر برای تایید اثر انگشت استفاده کرد- در این شرایط به پروسسور مرکزی اطلاع داده می شود تا سیستم امنیتی را از کار بیاندازد تا متصدی قادر به تعویض باتری پشتیبان حافظه ی امن یا در صورت لزوم قطعات دیگر سیستم باشد.

۴-۳. مقایسه و نتایج ارزیابی

در این قسمت مقایسه ای میان اجزای سیستم IBM PCIXCC و مینیمم سیستم پیاده سازی شده صورت گرفته است که در جدول ۱ نشان داده شده است.

جدول ۱ مقایسه میان IBM PCIXCC و مینیم سیستم

اجزا	IBM PCIXCC	مینیم سیستم
سیستم امنیتی	حسگرهای تشخیص مداخله	مجهز به سه حسگرهای مختلف برای تشخیص، پاسخگویی و مقاومت در برابر مداخله
واحد پردازنده مرکزی	ریز پردازنده PowerPC*405GPr متعلق به شرکت IBM	میکرو کنترلر AVR به عنوان پرو سسور نظارتی و اجرایی
سیستم رمزنگاری	پردازنده رمزنگاریOtello	موتور رمزنگاری نرم افزاری DES
مولد اعداد تصادفی	سیستم تولید اعداد تصادفی مجزا	استفاده از سیستم تولید اعداد تصادفی AVR
کنترلر وضعیت	میکرو کنترلر AVR	میکرو کنترلر AVR
RAM	64M حافظه ی RAM پویا SDRAM	حافظه ی داخلی میکرو
FLASH	16M حافظه فلش	حافظه ی داخلی میکرو
حافظه امن مجهز به باتری پشتیبان	128K حافظه RAM	تراشه ی DS2016 مجهز به باتری پشتیبان و سیستم پاسخ به مداخله
واسط ارتباطی	RS-232(مجزای از PCI)	اتصال سریال
نشان دادن وضعیت ماژول	موردی ذکر نشده است	استفاده از I/O میکرو و اتصال LCD

با توجه به مقایسه های انجام شده مشاهده می شود که در طراحی مینیمم سیستم پیاده سازی شده، سعی گردیده است تا تمامی نیازمندی ها پوشش داده شوند و از حداقل امکاناتی که در ماژول وجود دارد حداکثر استفاده شود. این مدل هم چنین با مدل طرح شده در [14] برابری نموده و حتی برخی از ایرادات مدل مذکور هم چون فقدان یک حافظه امن خارجی و متصل به باتری پشتیبان برای نگهداری کلید های رمزنگاری و مجهز نبودن به بیش از یک مدار تشخیص و پاسخ به مداخله در شرایط بحرانی، را برطرف نموده است.

۵. نتیجه گیری

ماژول سخت افزاری امنی که در این پژوهش طراحی و پیاده سازی شد، از دیدگاه استاندارد امنیتی FIPS قادر به کسب اعتباراتی می باشد: در حوزه ی نقشها در استاندارد FIPS، این سیستم از مدل نقش محور برای تصدیق هویت کاربران استفاده نموده است؛ به این مفهوم که چند کاربر با نام کاربری و رمز عبور کاملا مجزا از یکدیگر تعریف شده است و در هنگام ورود به سیستم تنها نقش کاربران مورد بررسی و تصدیق قرار می گیرد. بنابر مفاد استاندارد FIPS، در حوزه نقشها سیستم پیاده سازی شده، قادر به کسب سطح ۲ استاندارد می باشد. هم چنین در حوزه امنیت فیزیکی، به دلیل مجهز بودن ماژول به چندین محرکه تشخیص مداخله و همچنین مدار پاسخگو به مداخله- که قادر بودند سخت افزاری و نرم افزاری تریگر شوند- این ماژول در حوزه ی امنیت فیزیکی قادر به کسب سطح ۳ استاندارد می باشد.

منابع و مراجع

[1] Jansen, J., "*An introduction to the use of HSM* ", NLnet Labs document 2008-draft, May 13, 2008.

زیر نویسها

---

۱ Host Security Module
۲ USB Token
۳ USB
۴ RS232
۵ Sign
۶ Verify
۷ Encrypt
۸ Decrypt
۹ Tamper Response
۱۰ Log Messages
۱۱ BBRAM(Battery Backed RAM)
۱۲ Pick-resistant
۱۳ Random Number Generator(RNG)
۱۴ CSP (Critical Security Parameter)

[2] Kömmerling, O., Kuhn, MG., "Design *Principles for Tamper-Resistant Smartcard Processors*", Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard 99), Chicago, Illinois, USA, May 10-11, 1999.

[3] Kuhn, M. , "*Hardware security – Part 1: Smartcards and other tamper-resistant modules*", Computer Laboratory, University of CAMBRIDGE, 2007

[4] MOTOROLA, "*FIPS 140-2 Level 2 Security Policy for MOTOROLA RFS7000 RF Switch*", Document version 0.4, 2007.

[5] NIST, "*FIPS PUB 140-2:FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*", Supersedes FIPS PUB 140-1, Information Technology Laboratory National Institute of Standards and Technology, 1994 January 11.

[6] NIST, "*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*" ,Communications Security Establishment, National Institute of Standards and Technology, April 13, 2010

[7] Weingart, S., Engineer, S., "*The IBM 4758 Cryptographic Coprocessor Hardware Architecture & Physical Security*", Secure Systems and Smart Cards, IBM T.J. Watson Research Center Hawthorne, NY, 2008.

[8] IBM, "*IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessor*", in G221-9091-04, vol. 2006, May 2004.

[9] Arnold, T.W, Van Dorn, L.P., "*The IBM PCIXCC:A new cryptographic cooperocessor for the IBM server*", IBM, VOL. 48, NO. 3/4 MAY/JULY 2004.

[10] IBM, "*IBM 4764 Model 001 PCI-X Cryptographic Coprocessor*", in G221-9091-05, October 2005.

[11] IBM, "*IBM PCI Cryptographic Coprocessor General Information Manual*" ,vol. 2006, Sixth Edition, May 2002.

[12] Lavancier, José, "BULL *TrustWay PCI cryptographic card Security Target*", Version 3.2, October, 2004.

[13] RSA Laboratories,"*PKCS#11 V2. 20: CRYPTOGRAFIC TOKEN INTERFACE STANDARD*", 16 April 2009.

[۱۴] مهجوری، علی.، حبیبی، هاشم.، شیرازی، حسین.، **طراحی و ساخت واحد رمزنگاری سخت افزاری سطح ۳،**