دانشگاه علامه طباطبایی
دانشکده مدیریت و حسابداری

مطالعه تکنولوژی های مورد استفاده در کارت هوشمند

راهنمایی برای انتخاب بهترین تکنولوژی

نگارش ۰/۲

مرداد ۱۳۸۹

شناسنامه سند

نام سند	مطالعه تکنولوژی‌های مورد استفاده در کارت هوشمند
نگارش	۰/۲
تاریخ صدور	۱۳۸۹/۰۵/۱۵
نام فایل	Smart card-v.0.2
شرح سند	مستند حاضر، مطالعه و تحقیق پیرامون تکنولوژی‌های مورد استفاده در کارت‌های هوشمند و مباحث مرتبط با آن می‌باشد که به عنوان کار کلاسی در درس فناوری اطلاعات جناب دکتر حجاریان در دانشگاه علامه طباطبایی توسط اینجانب گردآوری شده است.
نویسنده/مترجم/گردآورنده	سمیه عابدیان- شماره دانشجویی ۸۸۱۲۴۱۷۱۲۰۵- مدیریت فناوری اطلاعات

فهرست مطالب

فهرست تصاویر و جداول

۱. هدف

هدف این سند بررسی کارت های هوشمند اعم از تاریخچه، انواع، اجزای سخت افزاری، سیستم های عامل، چرخه ی حیات، استانداردها، امنیت است. همچنین به مختصری از ملاحظات پدافند غیر عامل که باید در سیستم های کارت هوشمند مورد توجه قرار بگیرند پرداخته می شود.

۲. تاریخچه کارت هوشمند

بخشی از وقایعی که در سابقه تاریخی طراحی و پیاده‌سازی کارت هوشمند در جهان وجود دارد به صورت زیر است:

۱۹۷۰- دکتر کونیتاکا آریموری ژاپنی، مفهوم کارت هوشمند را برای اولین بار به طور انحصاری به ثبت رساند.

۱۹۷۴- رولاند مورنوی فرانسوی کارت IC را ثبت اختراع کرد. کارت IC بعدا به کارت هوشمند تغییر نام داد.

۱۹۷۷- سه شرکت تجاری Bull CP8، SGS Thomson و Schlumberger شروع به تولید کارت IC کردند.

۱۹۷۹- کمپانی موتورولا اولین تراشه ریزکنترلر ایمن را برای استفاده در سیستم بانکی فرانسه ساخت.

۱۹۸۲- آغاز آزمایش میدانی کارت تلفن عمومی در فرانسه

۱۹۸۴- آزمایش میدانی موفقیت آمیز کارت های خودپرداز در فرانسه

۱۹۸۶- تعداد ۱۴۰۰۰ کارت Bull CP8 بین مشتریان بانک های ویرجینیا و مریلند توزیع شد و ۵۰۰۰۰کارت کاسیو بین مشتریان بانک های Palm Beach و Mall توزیع شد.

۱۹۸۷- اولین پروژه ی گسترده ی کارت هوشمند توسط وزارت کشاورزی ایالات متحده پیاده سازی شد.

۱۹۹۲- اولین پروژه ی ملی کارت های پیش پرداخت، در دانمارک کلید خورد.

۱۹۹۳- اولین آزمایش میدانی کارت های چند کاربرده در رن فرانسه و فعال سازی کارت های Smart Bank Card

۱۹۹۴- Europay، MasterCard و Visa به طور مشترک استانداردی برای کارت های بانکی تدوین کردند. توزیع ۸۰میلیون کارت تراشه سریال در قالب کارت سلامت شهروندی آلمان

۱۹۹۶- تعداد مشترکین موبایل که از کارت هوشمند برای برقراری تماس استفاده می کردند، به بیش از ۳ میلیون رسید.

توزیع ۱.۵ میلیون کارت پیش پرداخت در المپیک آتلانتا. توسعه Java Card با پشتیبانی VISA و MultOS تحت حمایت MasterCard

۱۹۹۸- معرفی سیستم عامل کارت هوشمند مایکروسافت. توزیع ۵۰میلیون کارت هوشمند سلامت در فرانسه

۱۹۹۹- کمپانی GemPlus به رکورد بیش از ۵۰میلیون سیم کارت در سطح جهان دست یافت.

۲۰۰۰- عرضه ی کارت هوشمند غیرتماسی خودرو توسط AutoSmart. این کارت های علاوه بر نگهداری سابقه ی تعمیرات اتومبیل، کاربرد ضد سرقت نیز داشتند.

۲۰۰۲-عرضه ی کارت های JCB که در کنار ترمینال های Hypercom قابلیت های امنیتی بیشتری را در اختیار می گذاشتند.

۲۰۰۳- دستگیری یک محصل ۱۹ ساله که اطلاعات کارت هوشمند ماهواره ای را رمزگشایی و در اینترنت منتشر کرد. رواج گسترده ی کارت های هوشمند در هنگ کنگ

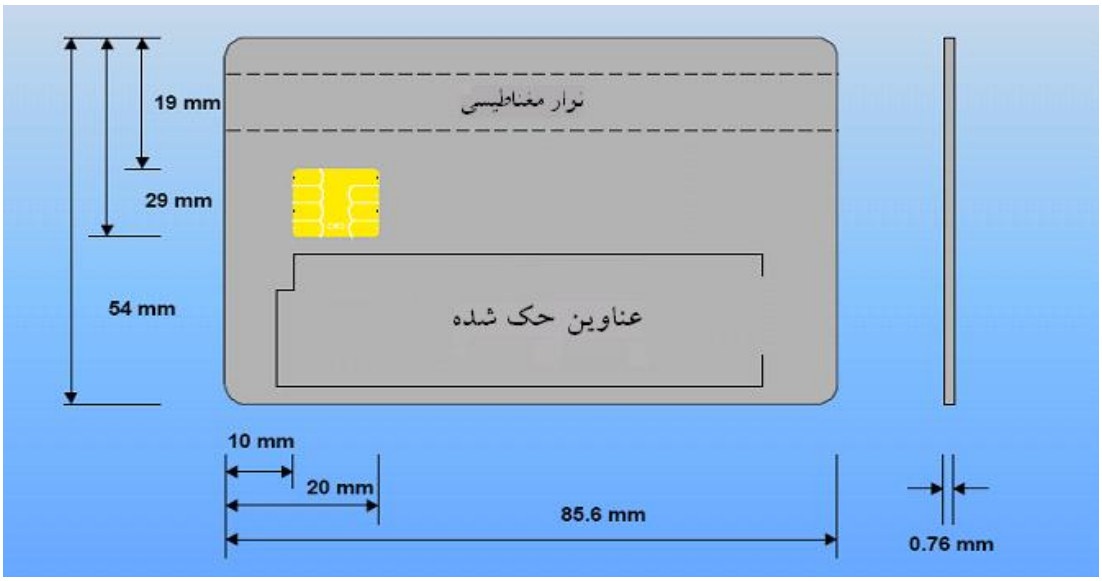
۲۰۰۶- توزیع کارت شناسایی هوشمند در وزارتخانه های دفاع و خارجه ایالات متحده

۲۰۰۷- تولید کارت هوشمند 64 کیلوبایتی که قادر است ۲۷ صفحه پرونده ی پزشکی را در خود نگه دارد.

۲۰۰۸- ادغام دو شرکت Gemplus و Axalto و تشکیل Gemalto که در حال حاضر از پیشگامان فناوری های کارت هوشمند است.

۳. مبانی کارت هوشمند

کارت هوشمند کارتی است پلاستیکی، در ابعاد یک کارت اعتباری، که دارای اجزایی برای انتقال، ذخیره سازی و پردازش داده است. به صورت دلخواه ممکن است، یک روی آن مجهز به نوار مغناطیسی[1] باشد و در روی دیگر آن نیز ممکن است کدی به صورت برجسته پرس[2] شده باشد. مشخصات فیزیکی کارت هوشمند در بخش ۱ استاندارد ISO 7816 تعریف شده است.(شکل ۱)



شکل ۱: تصویر مشخصات فیزیکی کارت هوشمند

[1] Magnetic Stripe

[2] Embossed

به طور معمول کارت هوشمند دارای اجزایی مثل باتری، صفحه نمایش یا صفحه کلید نیست، بلکه برای ارتباط با جهان خارج باید در نزدیکی یا درون یک کارت خوان که معمولا با یک کامپیوتر در ارتباط است، قرار بگیرد.

۳.۱. انواع کارت هوشمند

تقسیم بندی های گوناگونی برای کارت های هوشمند وجود دارد. بر اساس یک تقسیم بندی کارت های هوشمند به دو دسته ی کارت های حافظه[۳] و کارت های ریزپردازنده[۴] تقسیم می شوند. براساس واسط ارتباطی، کارت های هوشمند به کارت های تماسی[۵] کارت های غیر تماسی[۶] و کارت های هیبرید دسته بندی می شوند.

براساس تراشه

- **کارت حافظه**

نخستین کارت های هوشمند که در حد انبوه تولید شدند، کارت های حافظه بودند. کارت های حافظه در حقیقت هوشمند نیستند چرا که فاقد پردازنده هستند. آن ها به یک چیپ حافظه یا چیپی دارای حافظه، اما غیرقابل برنامه ریزی مجهزند و به طور معمول حافظه آن ها بین ۱ تا ۴ کیلوبایت است. عمده ترین کاربرد آن ها به عنوان کارت تلفن عمومی است. در موارد دیگری نیز که هزینه از قبل پرداخت می شود نیز کاربرد دارند.

از آن جایی که کارت های حافظه فاقد پردازنده برای پردازش داده هستند، مداری درون آن ها تعبیه می شود که عملیات پردازشی محدودی که از پیش تعریف شده اند را انجام می دهد. این مدار نمی تواند دوباره برنامه ریزی شود. بنابراین هنگامی که ارزش کارت مصرف شد، دیگر کاربردی ندارد.

براساس نیازمندی امنیتی داده های ذخیره شده، دسترسی به داده می تواند با استفاده از یک مدار امنیتی یا حافظه حفاظت شده، محدود شود. برای مثال در کارت های تلفن می توان با یک مدار مانع افزایش ارزش کارت شد. اما جعل کارت های حافظه به نسبت آسان است. البته می توان با استفاده از کد شناسایی PIN[۷] امنیت کارت را تا حدی بالا برد. عمده دلیل استفاده از این کارت ها ارزانی آن ها است چرا که از فناوری به نسبت ساده ای بهره می برند.

---

[3] Memory Card

[4] Microprocessor Card

[5] Contact Card

[6] Contactless Card

[7] Personal Identification Number

- **کارت ریزپردازنده**

کارت های ریزپردازنده، چنانکه از اسمشان بر می آید، حاوی یک پردازنده هستند. آن ها دارای قابلیت های زیادی در مقوله های امنیت و چند کارکردی بودن هستند. در کارت های ریزپردازنده، داده ها هیچ موقع به طور مستقیم در دسترسی برنامه های بیرونی قرار نمی گیرند، بلکه ریزپردازنده، براساس دستورالعمل های خارجی و تأمین برخی شرایط نظیر رمز عبور، داده ها را مدیریت می کند و در دسترس محیط خارج قرار می دهد. بعضی از مدل های جاری کارت های هوشمند قابلیت هایی درونی برای رمزنگاری نیز دارند. نقش این گونه کارت ها مخصوصا در کاربردهای امنیتی برجسته تر است.کارت های ریزپردازنده انعطاف بالایی دارند. می توان آن ها را برای برنامه ای خاص بهینه کرد یا حتی چند برنامه را در یک کارت مجتمع کرد. شاید تنها محدودیت آن ها، حافظه و توان محاسباتیشان باشد.

از عمده ترین کاربردهای این کارت ها می توان به کنترل دسترسی، کاربردهای بانکی و ارتباطات بی سیم راه دور که در آن ها امنیت اطلاعات و حریم خصوصی اهمیت بالایی دارد اشاره کرد.

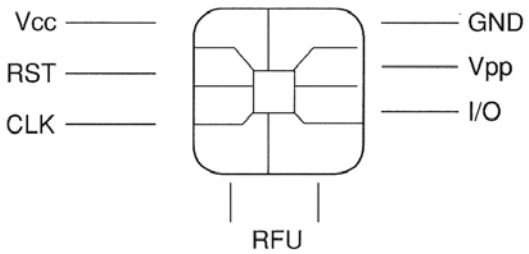
با تولید انبوه کارت های ریز پردازنده، قیمت آن ها به طور قابل ملاحظه ای کاهش یافته است. بسته به میزان حافظه و کارایی نرم افزاری که کارت به آن تجهیز شده است، قیمتی بین ۱ تا ۲۰ دلار دارند.

به طور معمول لفظ کارت هوشمند هم در مورد کارت های حافظه به کار می رود و هم در مورد کارت های ریزپردازنده. اما عده ای عقیده دارند که فقط کارت های ریزپردازنده، هوشمند هستند، چرا که آن ها از یک پردازنده استفاده می کنند. اما اصطلاح کارت چیپ یا کارت IC برای هر دو مورد به کار می روند.

بر اساس واسط

- **کارت تماسی**

کارت های تماسی برای عملکرد باید درون کارت خوان قرار بگیرند. ارتباط از طریق یک واسط تماسی سریال که دارای ۸ نقطه اتصال۸(شکل ۲) است، برقرار می شود. کارت خوان حسب شرایط می تواند کارت را قفل کند و محدودیت در حجم انتقال داده بین کارت و کارت خوان وجود ندارد.



[8] Contact Point

شکل ۲ : تصویر اتصالات کارت تماسی

از نکات منفی این کارت ها، این است که باید دقت شود کارت به درستی و در جهت صحیح درون کارت خوان قرار بگیرد. بنابراین در مواردی مانند قطار شهری و مترو، که زمان اهمیت دارد، کارت های تماسی مناسب نیستند. همچنین باید دقت شود که واسط ارتباطی کثیف نشود. البته واسط ارتباطی این کارت ها در اثر کثرت استفاده فرسوده می شود.

- **کارت غیرتماسی**

کارت های غیر تماسی برای عملکرد نیازی به قرار گرفتن درون کارت خوان ندارند. ارتباط با کارت از طریق آنتنی صورت می گیرد که درون کارت تعبیه شده است. توان لازم برای عملکرد کارت معمولا توسط همین آنتن جذب می شود. ارتباط کارت و کارت خوان با استفاده از امواج الکترومغناطیسی انجام می شود. کارت های غیرتماسی مشکلات کارت های تماسی را ندارند، اما این کارت ها هم نکات منفی مخصوص به خود را دارند. مثلا باید کارت در نزدیکی کارت خوان قرار بگیرد تا ارتباط صورت پذیرد. از آنجایی که کارت مدت کوتاهی در کنار کارت خوان قرار می گیرد حجم انتقال داده محدود است. ممکن است ارتباطی صورت بگیرد یا داده های ارسالی رهگیری شوند بدون این که استفاده کننده ی کارت متوجه شود. به علاوه کارت های غیر تماسی معمولا گرانتر از کارت های تماسی هستند.

۳.۲. کارت هیبرید

کارت هایی که از واسط های گوناگونی برای ارتباط با جهان خارج بهره می برند. مثلا هم دارای واسط تماسی و هم واسط غیر تماسی هستند. آن ها ممکن است به نوار مغناطیسی و کد برجسته تجهیز شوند.

٤. سخت افزار کارت هوشمند

کارت های هوشمند (ریزپردازنده) دارای واحد های پردازش مرکزی، چند نوع حافظه و در نوع تماسی دارای چند نقطه اتصال در سطح پلاستیکی کارت هستند. ممکن است کمک پردازنده ای نیز برای عملیات ریاضی درون کارت تعبیه شده باشد.

٤.١. نقاط اتصال کارت هوشمند

همانطور که ذکر شد کارت هوشمند تماسی دارای ۸ نقطه تماس است. ابعاد و مکان های نقاط اتصال در بخش دوم استاندارد ISO 7816 آمده است.[2]

٤.٢. واحد پردازش مرکزی

واحد پردازش مرکزی کارت های جاری معمولا ۸بیتی است و از مجموعه دستورالعمل های Intel 8051 یا Motorola 6805 پشتیبانی می کند. پالس ساعت آن ها معمولا تا ۵ مگاهرتز است و انواع دارای فناوریهای پیشرفته آن ها به تقویت کننده هایی مجهزند که اجازه می دهند پالس ساعت به ۴۰ مگاهرتز نیز برسد. کارت های نسل جدید از پردازنده های ۳۲ بیتی بهره می برند و معماری RISC را پشتیبانی می کنند.[2]

٤.٣. کمک پردازنده

کارت های هوشمندی که برای کاربردهای امنیتی طراحی شده اند، معمولا به کمک پردازنده نیز مجهزند. کمک پردازنده ی رمزنگاری، مدار مجتمعی است که محاسبات را تسریع می کند. به عنوان مثال محاسبات اعداد بزرگ که که در الگوریتم های رمزنگاری مانند RSA به کار می روند.[2]

٤.٤. سیستم حافظه

کارت های هوشمند معمولا سه نوع حافظه دارند: حافظه غیر قابل تغییر مانا، حافظه قابل تغییر مانا، حافظه فرار قابل تغییر. معمولا ROM، EEPROM و RAM به ترتیب برای این نوع حافظه ها به کار می روند.

:ROM

برای ذخیره برنامه های ثابت در کارت به کار می رود و برای حفظ اطلاعات نیاز به انرژی ندارد. وقتی کارت ساخته شد دیگر نمی توان بر روی آن نوشت. معمولا سیستم عامل و داده ها و برنامه های ثابت کاربر در آن قرار می گیرد.

:EEPROM

معادل دیسک سخت یک کامپیوتر است. برای حفظ داده نیازی به انرژی ندارد، اما برخلاف ROM در هنگام استفاده محتویاتش قابل تغییر است. بنابراین حتی پس از ساخت کارت می توان برنامه روی آن قرار داد. در کارت های رایج می توان تا ۱۰۰۰۰۰ دفعه روی آن نوشت و تا ۱۰ سال داده ها را نگهداری کرد. خواندن از آن با همان سرعت بالای RAM صورت می گیرد، اما نوشتن آن ۱۰۰۰ بار کندتر از RAM است. داده هایی نظیر PIN، شماره سریال کارت و داده های برنامه های کاربردی معمولا در ROM قرار می گیرند.

:RAM

به عنوان محیط کاری برای ذخیره و تغییر داده ها به کار می رود. فرار است و با قطع توان، محتویاتش از بین می رود. این حافظه هیچ کدام از محدودیت های EEPROM را ندارد.

اخیرا انواع دیگری از حافظه نظیر حافظه فلش نیز در کارت های هوشمند با اقبال روبرو شده است. حافظه فلش هم از لحاظ فضا و هم از لحاظ توان از EEPROM بهینه تر است. انتقال داده ها در آن به صورت بلوکی انجام می شود و برای انتقال داده های بزرگ مفیدتر است.[2]

۵. اجزای سیستم کارت هوشمند

پیکربندی یک سیستم کارت هوشمند براساس رویکرد مدیریت کارت، رویه شخصی سازی و صدور کارت، قابلیت ها و کاربردهای کارت، و نیز محیط فنی پروژه، دارای تنوع گوناگونی است. اما در این جا مواردی که عموما در میان همه ی پیکربندی ها رایج است را بررسی می کنیم.

۵.۱ کارت

کارت های هوشمند همانطور که گفته شد، دارای یک تراشه هستند که قابلیت هایی مشابه یک PC را فراهم می آورد. آن ها قابلیت را هایی برای پیاده سازی انواع فناوری های تصدیق هویت و بیومتریک دارند. علاوه بر این مقدار مشخصی حافظه دارند و در انواع مختلفی نظیر تماسی و غیرتماسی موجودند.[2]

۵.۲ سیستم مدیریت مرکزی کارت

هسته ی سیستم کارت هوشمند است و دارای واسط هایی برای ارتباط با تمامی اجزای سیستم است. این بخش پایگاه داده مرکزی صاحبان کارت را در خود جای می دهد که مسئول دریافت، ذخیره سازی، بازیابی، نگهداری، یکپارچگی و مدیریت داده های مورد نیاز در مدیریت چرخه حیات کارت هوشمند است. مدیریت چرخه حیات نیز شامل مراحلی همچون پیش از صدور، صدور، وضعیت، جایگزینی، تجدید و پس از صدور است.[2]

۵.۳ نرم افزارها و تجهیزات کارت

مجموعه ی کامپیوترها، دستگاه های جانبی و نرم افزارهای مورد احتیاج جهت دریافت اطلاعات برای نام نویسی صاحب کارت، شخصی سازی کارت ، بارگذاری اسناد تشخیص هویت در کارت، صدور کارت و موارد پس از صدور، نظیر بازنشانی PIN و به روز رسانی اسناد کارت است. تجهیزات صدور کارت نیز عبارتند از:

- **ایستگاه کاری نام نویسی:** برای ضبط اطلاعات نام نویسی به کار می رود و این اطلاعات را در اختیار سیستم مرکزی مدیریت کارت و سیستم شخصی سازی قرار می دهد. افزونه های این ایستگاه کاری شامل یک دوربین دیجیتال برای گرفتن عکس صاحب کارت، یک دستگاه برای گرفتن امضای شخص، یک دستگاه برای گرفتن اطلاعات بیومتریک و یک صفحه کلید برای گرفتن PIN است. براساس رویه گرفتن اطلاعات دموگرافیک، ممکن است دستگاهی برای جمع آوری اطلاعات دموگرافیک نیز موجود باشد.

- **ایستگاه کاری تولید کلید:** یکی از مکانیسم های امنیتی که در کارت هوشمند به کار می رود، روش کلید عمومی/ خصوصی است. معمولا خود کارت این کلید ها را تولید می کند. اما ممکن است، ایستگاهی کاری برای تولید کلید در نظر گرفته شود. این کلید ها نهایتا از طریق یک بستر مطمئن به کارت منتقل می شوند.
- سیستم شخصی سازی: این سیستم، کارت را با عکس و اطلاعات صاحب کارت و مواردی دیگر همچون امضای دیجیتال شخصی می کند. معمولا دو افزونه با سیستم شخصی سازی در ارتباط هستند. یک کارت خوان که اطلاعات خام کارت را در اختیار سیستم قرار می دهد و یک چاپگر که اطلاعات و عکس را روی کارت چاپ می کند.
- **سیستم اعتبار ثبت نام:** سیستمی است که کلید عمومی کارت را می خواند، صحت اطلاعات بیومتریک را بررسی می کند، اطلاعات شناسایی را مستند می کند و یک امضای دیجیتال تحویل می دهد.
- کارت خوان: همانطور که قبلا گفته شد واسط میان کارت و سیستم میزبان است. توان و پالس ساعت کارت را تامین می کند و واسط های تماسی و غیر تماسی دارد. [2]

۵.۴. برنامه های کاربردی

بنا به کاربردی که از کارت هوشمند انتظار داریم، برنامه های کاربردی مورد نظر تهیه و درون کارت و سایر اجزا تعبیه می شوند. براساس کاربرد این برنامه ها دارای واسط هایی برای ارتباط با سایر اجزا، مثلا بانک های اطلاعاتی هستند.[2]

۵.۵. واسط های پایگاه داده

ممکن است اطلاعات شخصی سازی کارت از طریق پایگاه داده ای که از قبل وجود دارد، تأمین شود. بنابراین برخورداری از یک واسط ایمن با پایگاه داده، از اجزای مهم معماری سیستم کارت هوشمند محسوب می شود.[2]

۶. معماری مدیریت چرخه حیات کارت

۶.۱. خرید

کارتی که خریداری می شود باید با کاربرد و امنیتی که از آن انتظار داریم، سازگار باشد. مثلا اگر قرار است در سیستم حمل و نقلی، نظیر مترو استفاده شود، نباید از کارت های تماسی استفاده کنیم. شرکت های زیادی در زمینه تولید کارت فعالیت می کنند، بنابراین مناسبتر است که سیستم به گونه ای طراحی شود که به تولید کننده خاصی وابسته نباشد و بتوان کارت ها را در یک فضای رقابتی آزاد تهیه کرد. با توجه به رشد استانداردها، این امر امکان پذیرتر شده است. [2]

۶.۲. قالب بندی

قالب بندی کارت، فرایند برنامه ریزی کارت ها با داده هایی یکسان است(مثلا یک ساختار فایل). قالب بندی شامل مواردی همچون چاپ لوگو روی دسته کارت ها نیز می شود. معمولا این اعمال توسط سازنده کارت، قبل از عرضه انجام می شود، اما ممکن است قالب

بندی به فرایند شخصی سازی کارت موکول شده باشد. اعمال عمده ای که سازنده ممکن است در قالب بندی کارت انجام می دهد عبارتند از:[2]

- بارگذاری سیستم عامل در ROM
- تخصیص نواحی کارت برای عکس، امضا و...
- بارگذاری سریال منحصر به فرد در ROM
- تولید کلیدهای امنیتی

بنا به درخواست خریدار ممکن است کارهای دیگری نیز توسط سازنده ی کارت انجام شود.

۶.۳. شخصی سازی

بعد از ساخت کارت انجام می شود و فرایندی است شامل چاپ اطلاعات روی کارت، رمزنگاری نوارمغناطیسی(در صورت وجود) و برنامه ریزی کارت به نحوی که صاحب کارت را به صورت منحصر به فرد مشخص کند. روش‌های های متفاوتی برای جمع آوری اطلاعات مورد نیاز در شخصی سازی وجود دارد. ممکن است از اطلاعات پایگاه داده فعلی در صورت وجود استفاده شود، اطلاعات از طریق وب جمع آوری شود، یا با افراد مصاحبه شود. بعد از جمع آوری اطلاعات باید از واسط مناسبی که کارا و ایمن باشد و وقوع خطا را به حداقل برساند، برای انتقال اطلاعات استفاده کرد. بنا به کاربرد کارت فرایند شخصی سازی می تواند شامل موارد زیر باشد:[2]

- رمزنگاری نوار مغناطیسی
- رمزنگاری بارکد
- بارگذاری برنامه های کاربردی، اطلاعات دموگرافیک پایه ای و یا کلیدها روی تراشه
- چاپ عکس، اطلاعات شخصی و اطلاعات شرکت روی کارت.

۶.۴. صدور

صدور کارت در حقیقت همان فرایند توزیع کارت میان افراد استفاده کننده است. براساس کاربرد و ساختار سازمانی، ممکن است چاپ و شخصی سازی کارت در یک مرکز انجام شود و توزیع از یک نقطه مرکزی صورت گیرد. یا ممکن است به خاطر گستردگی جغرافیایی، شخصی سازی به صورت غیرمتمرکز صورت گیرد و به تبع آن توزیع نیز غیرمتمرکز باشد. در این تصمیم گیری یکی از مهمترین فاکتورها بحث امنیت سیستم است. در هنگام تحویل کارت، مشخصات کارت با اطلاعات هویتی شخص تطبیق داده می شود و پس از آن کارت به شخص داده می شود.[2]

۶.۵. تعویض

فرایندی است که در آن کارت المثنی برای فردی که کارت خود را گم کرده است، یا کارت او سرقت یا معیوب شده است صادر می گردد. دفتر صدور وظیفه دارد اسناد کارت را باطل کند و کارت را در لیست کارت های نامعتبر قراردهد. کارت المثنی باید همان داده ها، مزایا و دسترسی های کارت اولیه را داشته باشد و واژه ی "المثنی" روی آن قید شده باشد.[2]

۶.۶. مسدود کردن

وقتی که کارتی گم یا دزدی می شود، باید غیرفعال شود تا از سوء استفاده جلوگیری شود. بنابراین سیستم باید به لیستی مجهز باشد که اطلاعات کارت های غیرفعال در آن نگهداری شود. حوزه های دیگری نیز که کارت در آن ها کاربرد دارد، باید بلافاصله در جریان قراربگیرند.

ممکن است کارت در اثر اشتباه وارد کردن PIN مسدود شود. سیستم باید این قابلیت را داشته باشد که کارت را از حالت مسدود خارج کند. در همین راستا هنگام پیکربندی اولیه کارت، کدی به این منظور تولید و رمزنگاری می شود و در سیستم نگهداری می شود.[2]

۶.۷. بازنشانی PIN

دارنده ی کارت باید این امکان را داشته باشد که بدون مراجعه به دفاتر صدور کارت، PIN کارت خود را عوض کند. به این منظور مکانیسم های متفاوتی می تواند در اختیار دارندگان کارت قرار بگیرد. مثلا یک واسط گرافیکی تعبیه شده در یک ترمینال، که رمز قبلی کاربر را بگیرد و رمز جدید او را ثبت کند. یا یک پرتال مبتنی بر وب که کاربر مشخصات خود و رمز قبلی خود را در آن وارد کند و رمز جدید خود را ثبت کند.[2]

۷. ارتباطات کارت هوشمند

۷.۱. کارت خوان و برنامه های میزبان

کارت خوان

از طریق درگاه سریال، موازی یا USB به کامپیوتر وصل می شود و واسطی میان کارت و کامپیوتر می شود. کارت خوان اسلاتی دارد که کارت در آن قرار می گیرد یا ارتباط از طریق میدان الکترومغناطیسی با کارت برقرار می شود. کارت خوان مسئول تأمین توان کارت و تولید پالس ساعت جهت عملکرد آن است. معمولا تکنیک هایی جهت تشخیص و تصحیح خطا نیز در کارت خوان تعبیه می شود.

ترمینال

ترمینال ها به نوعی کامپیوترهایی هستند که اجزای مختلفی از جمله کارت خوان، به صورت مجتمع در آن ها تعبیه می شود. خودپردازها، دستگاه های POS و نازل های بنزین، نمونه هایی رایج از ترمینال محسوب می شوند. ترمینال ها اجزایی درون خود دارند که پردازش داده های انتقالی میان کارت و کارت خوان را برعهده می گیرند.

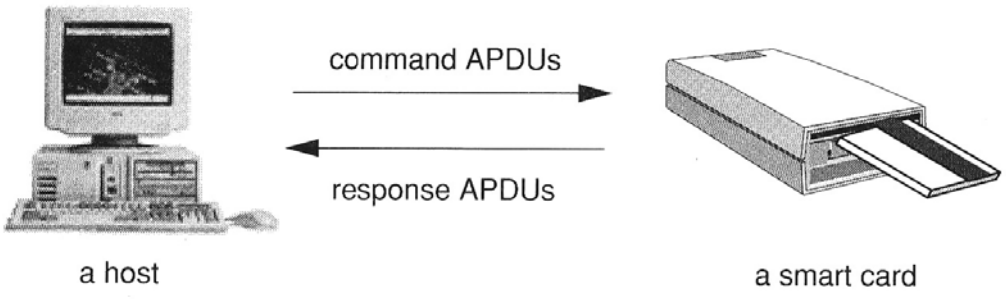
برنامه های میزبان

برنامه هایی که در ترمینال یا کامپیوتر مقیم هستند و با کارت ها در ارتباط هستند، برنامه های میزبان نامیده می شوند. طبعا یکی از وظایف آن ها مدیریت ارتباطات با کارت است که در ادامه تشریح می شود.[2]

۷.۲. مدل ارتباطی کارت هوشمند

ارتباط میان کارت و کارت خوان نیمه دوطرفه است. به این معنا که یا کارت به کارت خوان داده ارسال می کند، یا کارت خوان به کارت داده ارسال می کند و هر دو همزمان امکان پذیر نیست.

وقتی دو کامپیوتر با هم ارتباط برقرار می کنند، بسته هایی به یکدیگر ارسال می کنند که براساس پروتکلی مانند TCP/IP ساخته می شوند. به طور مشابه وقتی ارتباطی میان کارت و کامپیوتر صورت می گیرد، بسته هایی به نام APDU[۹] میان آن ها تبادل می شود. هر APDU حاوی یک فرمان یا یک پاسخ است.



شکل ۳: تصویر ارتباط کارت و کارت خوان

در ارتباطات کارت هوشمند مدل ارباب – برده[۱۰] به کار گرفته می شود.(شکل ۳) کارت همیشه نقش برده را بازی می کند و منتظر APDU از طرف میزبان می ماند. آنگاه دستورالعمل ارسالی را اجرا می کند و یک APDU حاوی پاسخ به میزبان ارسال می کند. به همین ترتیب APDU فرمان و پاسخ به طور متناوب بین کارت و میزبان تبادل می شوند.

پروتکل APDU

این پروتکل چنانکه در بخش چهارم استاندارد APDU تشریح شده است، یک پروتکل سطح برنامه است. بسته های APDU دو ساختار دارند: یک ساختار که به برنامه میزبان مربوط می شود و ساختار بسته حاوی فرمان را مشخص می کند و ساختار دیگر که به

[۹] Application Protocol Data Unit

[10] Master Slave

کارت مربوط می شود و ساختار بسته حاوی پاسخ را تعیین می کند. بدیهی است که هر APDU فرمان، یک APDU پاسخ به دنبال دارد.

ساختار APDU فرمان از دو قسمت سرآیند و بدنه تشکیل می شود. سرآیند آن از چهار قسمت یک بایتی تشکیل می شود:

CLA: کلاس دستورالعمل را مشخص می کند.

INS: حاوی کد دستورالعمل است.

P1 و P2: حاوی پارامترهای اضافی دستورالعمل هستند.

Command APDU structure

Mandatory header				**Optional body**		
CLA	INS	P1	P2	Lc	Data field	Le

بعد از سرآیند، بدنه ی اختیاری APDU قراردارد که طول آن متغیر است. فیلد Lc طول بدنه را مشخص می کند. فیلد داده حاوی داده های ارسالی به کارت جهت اجرای دستورالعملی است که در سرآیند آمده است. فیلد Le نیز تعداد بایت های مورد انتظار در پاسخ را تعیین می کند.

ساختار پاسخ APDU نیز متشکل از دو قسمت بدنه ی اختیاری و دنباله ی اجباری است. بدنه، شامل فیلد داده است که طول آن در فیلد Le فرمان متناظر مشخص شده است. دنباله، از دو فیلد تشکیل شده است که با هم کلمه ی وضعیت نامیده می شوند. کلمه وضعیت، حالت پردازشی کارت پس از اجرای دستورالعمل را مشخص می کند. برای مثال کلمه وضعیت 0x9000 به معنای اجرای موفقیت آمیز و درست فرمان است.

Response APDU structure

Optional body	**Mandatory Trailer**	
Data field	SW1	SW2

پروتکل[۱۱] TPDU

بسته های APDU با پروتکل سطح بعد که پروتکل انتقال است، ارسال و دریافت می شوند. این پروتکل در بخش سوم ISO 7816 تشریح شده است. ساختار داده هایی که با این پروتکل ارسال می شوند، TPDU نامیده می شوند. دو پروتکل که به طور عمده در سیستم های کارت هوشمند به کار می‌روند، پروتکل های T=0 و T=1 هستند. پروتکل T=0 بایت گراست به این معنا که کوچکترین واحد انتقال و پردازش بایت است. پروتکل T=1 بلوک گراست. بلوک که یک توالی از بایت هاست کوچکترین واحدی است که در این پروتکل بین کارت و میزبان انتقال می یابد.

ATR[۱۲]

به محض اینکه کارت شروع به کار می کند، یک پیام به میزبان ارسال می کند. این پیام ATR نامیده می شود. این پیام حاوی پارامترهایی است که برای برقراری ارتباط میان کارت و میزبان ضروری است. حجم آن تا ۳۳ بایت است و حاوی پارامترهای ارسال پیام، نظیر پروتکل انتقالی که کارت پشتیبانی می کند (T=0 یا T=1)، نرخ انتقال داده، پارامترهای سخت افزاری کارت مثل سریال چیپ، و اطلاعات دیگری است که میزبان احتیاج دارد.[2]

۸. سیستم عامل کارت هوشمند

در حال حاضر کارت‌های هوشمند تقریباً یک کامپیوتر کامل بدون نمایشگر و صفحه کلید هستند. هسته مرکزی کارت هوشمند، یک ریزپردازنده است که قادر است سلسله دستوراتی را که به آن داده می‌شود اجرا نماید. این سلسله دستورات کارآیی کارت را مشخص می‌کنند. جهت مدیریت و اجرای این دستورات، مجموعه‌ای از توابع سطح بالا درون حافظه کارت ریخته می‌شوند. مجموعه این توابع که به صورت دائمی درون حافظه کارت نوشته می‌شوند را سیستم‌عامل کارت گویند. بنابراین سیستم‌عامل کارت هوشمند[۱۳](COS رشته‌ای از دستورالعمل‌هاست که به طور ثابت در ROM کارت هوشمند قرار داده می‌شود. سیستم‌عامل، ریزپردازنده را قادر می‌سازد تا حافظه‌ی برنامه کاربردي را مطابق با فرامیني که توسط کاربر و از بیرون به کارت ارسال مي‌شود، مدیریت و کنترل نماید. همچنین سیستم‌عامل تامین امنیت داده‌هاي روي کارت نیز به عهده دارد؛ به عنوان مثال تبادل امن داده‌ها بین کارت و سیستم میزبان و کنترل دسترسي به حافظه از این قرار هستند.

دستورات COS مثل خانواده سیستم‌عامل DOS یا ویندوز، به برنامه کاربردی خاصی وابسته نیست ولی به دفعات توسط اغلب برنامه‌های کاربردی استفاده می‌شود. سیستم‌عامل در کارت‌های هوشمند، می‌تواند از جنبه‌های مختلف مورد تقسیم‌بندی قرار گیرد. مثلاً در یک نگاه می‌توان سیستم‌عامل‌های تراشه را به دو دسته تقسیم نمود:

---

[11] Transmission Protocol Data Unit

[۱۲] Answer To Reset

[۱۳] COS: Chip Operating System

۱) COS همه‌منظوره، در واقع مجموعه فرمان‌های عمومی هستند که اکثر برنامه‌های کاربردی را پوشش می‌دهند.
۲) COS اختصاصی، شامل فرمان‌هایی است که برای برنامه‌های کاربردی خاص طراحی می‌شود و حتی خودش نیز می‌تواند شامل برنامه‌های کاربردی باشد. یک مثال برای COS اختصاصی، می‌تواند کارتی باشد که برای پشتیبانی از کاربرد کیف پول الکترونیک طراحی شده است.

یک تقسیم‌بندی کلی دیگر می‌تواند از نظر سازگاری سیستم‌عامل با استانداردهای جهانی موجود، باشد. در این تقسیم‌بندی سیستم‌عامل کارت یکی از دو شکل زیر است:

- کارت‌های Open-OS،
- کارت‌های Native (کارت‌های با OS خاص).

کارت‌های Open-OS دارای سیستم‌عامل‌هایی هستند که در سراسر جهان به عنوان استاندارد شناخته شده است. این کارت‌ها به Open Smart Card نیز معروف هستند. استانداردهایی برای کارت‌هایی که از این نوع سیستم‌عامل استفاده می‌کنند، وجود دارد که برخی از آنها عبارتند از:

- کارت‌های جاوا[۱۴]،
- کارت‌های MULTOS [۱۵]،
- کارت‌های هوشمند ویندوز[۱۶]،

کارت‌های Native سیستم‌عامل مشخص و استانداردی ندارند. سیستم‌عامل در این کارت‌ها فقط شبیه OS بوده و توسط شرکت‌های مختلف با زبان‌های مختلف برنامه‌نویسی و یا با اسکریپت‌های خاص آن شرکت پیاده‌سازی می‌گردد. به همین دلیل امنیت نسبتاً خوبی را ارایه می‌دهد. با توجه به خصوصی بودن سیستم‌عامل، توسعه نرم‌افزار، و برنامه کاربردی برای این دسته از کارت‌ها بسیار مشکل است.

توابع پایه COS که معمولاً در تمام محصولات کارت هوشمند مشترک است، شامل:

۱) مدیریت مبادلات بین کارت و دنیای خارج که اصولا پروتکل مبادلات[۱۷] نامیده می‌شوند.
۲) مدیریت فایل‌ها و داده‌های نگهداری شده در حافظه،
۳) کنترل دسترسی به اطلاعات و توابع (به‌عنوان مثال، انتخاب فایل، خواندن، نوشتن، و به‌روز رسانی داده)،

[14] Java Card

[15] Multi Application Operating System (MULTOS)

[16] Microsoft Windows for Smart Cards

[17] Interchange Protocol

۴) مدیریت امنیت کارت، الگوریتم‌های رمز، ضوابط جامعیت داده،
۵) حفظ و بقای قابلیت اطمینان[۱۸]، به خصوص بر حسب سازگاری داده، وقفه‌های متوالی، و بازیابی یک خطا
۶) مدیریت فازهای مختلف چرخه زندگی کارت (شامل ساخت ریزتراشه، سفارشی‌کردن محصول، عمر فعال، و پایان عمر)

به طور کلی صادر کننده یک کارت باید برای هر سرویس یک توسعه دهنده برنامه کاربردی خاص، سیستم‌عامل، و تراشه فراهم نماید. به همین برای تغییر هر یک از مولفه‌ها می‌بایست بر روی پیاده‌سازی یک نرم‌افزار یا سخت‌افزار جدید سرمایه‌گذاری نمود. کارت‌های هوشمند اولیه بسیار پرهزینه و غیرمنعطف بودند.

استاندارد CEN726 و ISO7816، علاوه بر تعیین خصوصیات و مشخصات فیزیکی کارت‌های هوشمند، محدوده‌ی گسترده‌ای از فرمان هایی را که کارت‌های هوشمند می‌توانند اجرا کنند، مشخص می‌کند. بیشتر تولیدکنندگان کارت‌های هوشمند، پیشنهاد تولید انواع کارت با سیستم‌عامل‌هایی می‌دهند که همه یا بعضی از این استانداردها را با الحاقات و اضافات خاص تولید کننده، اجرا کند. امروزه می توان به وضوح، توسعه سیستم‌عامل‌های باز را که از اجرای چندین برنامه کاربردی در یک کارت هوشمند حمایت می‌کنند، مشاهده نمود. برای توسعه برنامه‌های کاربردی موجود بر روی کارت که در داخل محیط امن تراشه کارت هوشمند اجرا می‌شوند، سیستم‌عامل هایی مانند سیستم‌عامل کارت جاوا، MULTOS، و ویندوز وجود دارند که برای توسعه برنامه‌های کاربردی که در داخل محیط امن تراشه کارت هوشمند اجرا می‌شوند، سیستم‌عامل‌های MULTOS و جاوا پیشنهاد می‌شوند.

بیشتر سیستم‌عامل‌های کارت هوشمند از فایل سیستم مبتنی بر استاندارد ISO7816 پشتیبانی می‌کنند. سیستم‌عامل‌های کارت هوشمند از انجام عملیات معمول بر روی فایل‌ها مانند تولید، حذف، خواندن و نوشتن، و بروزرسانی فایل‌ها بر روی تمام فایل‌ها حمایت می‌کنند. به‌علاوه این عملیات روی انواع خاصی از فایل‌ها نیز پشتیبانی می‌شوند. هر فایل یک کارت هوشمند یک لیست کنترل دسترسی دارد. در این لیست مشخص می‌شود که چه موجودیتی اجازه اجرای چه عملیاتی را بر روی فایل دارد. مثلاً موجودیت A ممکن است قادر باشد که یک فایل ویژه را بخواند اما نتواند آن را بروزرسانی کند، در حالی که موجودیت B ممکن است قادر باشد که فایل را بخواند، در آن بنویسد، و حتی لیست کنترل دسترسی موجود بر روی فایل را تغییر دهد.[3]

۸.۱. سیستم عامل جاوا

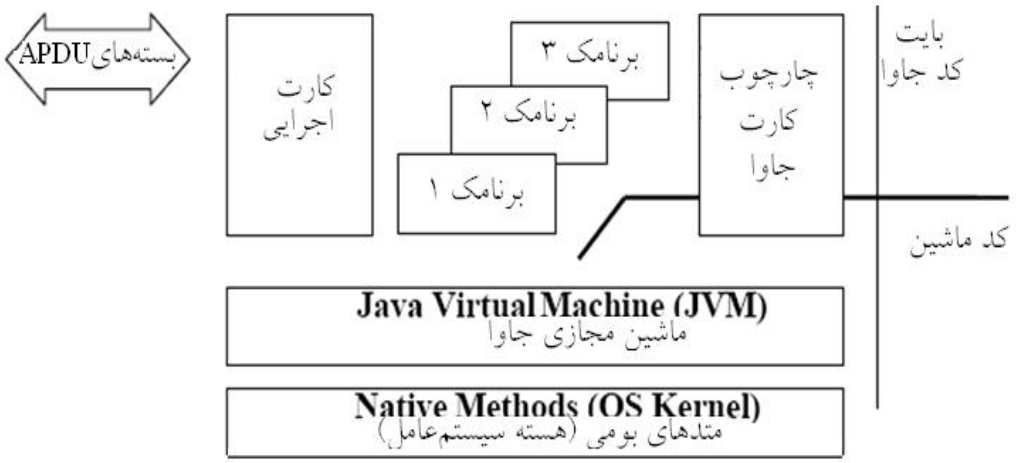
کارت جاوا توسط Schlumberger معرفی و سپس توسط JavaSoft به عنوان یک استاندارد ارایه شد. این کارت‌ها اجازه می‌دهند برنامک‌های[۱۹] جاوا مستقیما بر روی کارت‌های سازگار با استاندارد ISO7816 اجرا شوند. کارت‌های جاوا می‌توانند برنامه‌های کاربردی مختلف را به صورت امن و مستقل از تراشه، اجرا نمایند. مدیر امنیت این کارت‌ها اجازه‌ی اجرا شدن برنامک را روی کارت تصویب می کند. معماری سیستم‌عامل کارت جاوا در شکل ۴ آمده است. سیستم‌عامل کارت جاوا اجازه می‌دهد که برنامه‌های کاربردی (برنامک‌ها) روی کارت به زبان جاوا نوشته شوند. این مساله بستری[۲۰] مستقل از جاوا به منظور توسعه نرم‌افزار موجود بر روی کارت فراهم می‌کند

[18] Maintaining Reliability

[19] Applets

[20] Platform

که این بستر برای هر تولیدکننده‌ی سیستم‌عامل کارت به صورت بسیار اختصاصی استفاده می‌شود. همچنین مبنای مناسبی برای کارت‌های چند کاربردی که در یک زمان، چندین برنامه کاربردی را پشتیبانی می‌کنند، فراهم می‌کند. برنامه‌های قابل اجرا بر روی کارت، همان برنامک‌های کارت است که شامل بایت کد مخصوص کارت جاوا است و به وسیله محیط زمان اجرای کارت جاوا[۲۱] تفسیر و ترجمه می‌شود. این محیط، اجرای برنامه را کنترل کرده و اطمینان می‌دهد که برنامک‌های مختلف تداخل ایجاد نمی‌کند.



شکل ۴ : تصویر معماری سیستم عامل جاوا

فرآیند برنامه‌ریزی و توسعه یک برنامک کارت در شکل ۵ آمده است. فایل‌های منبع[۲۲] توسط یک کامپایلر استاندارد جاوا، به بایت کد جاوا کامپایل می‌شوند. فایل‌های "class" می‌توانند در محیط شبیه‌سازی کارت جاوا بررسی شوند. تبدیل‌کننده بایت کد[۲۳]، فایل class را بازبینی کرده و آن را برای منابع محدود کارت هوشمند، بهینه می‌کند. در نهایت این فایل‌ها به صورت ایستا به هم متصل شده و به فایل‌های "cap" تبدیل می‌شوند. فایل‌های cap می‌توانند در محیط نمونه‌ساز کارت جاوا[۲۴] بررسی شوند. کارت‌های جاوا به واسطه انعطافی که دارند، کار با آنها برای کاربران و همچنین توسعه برنامه‌های کاربردی آنها برای برنامه‌نویسان راحت‌تر است.[3]

[21] Java Card Runtime Environment

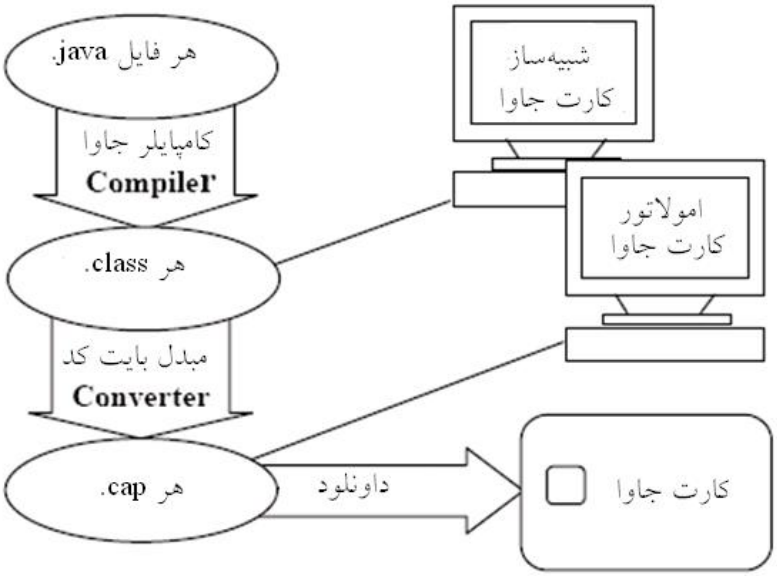
[22] Source Files

[23] Byte Code Converter

[24] Java Card Emulator

۸.۲. سیستم‌عامل MULTOS

سیستم‌عاملMULTOS، که در اصل توسط Mondex International ایجاد شد، یک سیستم‌عامل باز چند کاربردی است که امنیت بالایی را برای کارت‌های هوشمند فراهم می‌کند. این سیستم‌عامل امکان نگهداری همزمان چندین برنامه کاربردی مختلف را با امنیت بالا بر روی کارت فراهم می‌کند. کمپانیMondex International برای توسعه برنامه‌های کاربردی، یک زبان بهنیه به نام MEL[۲۵] را همراه با مشخصات MULTOS API بر روی کارت هوشمند ایجاد نموده است. مهمترین خصوصیت MULTOS عدم وابستگی آن به زبان است. به همین دلیل



شکل ۵ : تصویر فرایند برنامه ریزی و توسعه برنامک کارت

برنامه‌نویس می‌تواند به انتخاب خود از هر یک از زبان‌های برنامه‌نویسی که در ادامه معرفی خواهند شد، به عنوان بستر مناسب استفاده نماید، چرا که زبان انتخاب شده به زبان MEL ترجمه خواهد شد.

- زبان برنامه‌نویسی اسمبلی،
  MULTOS تنها بستری است که دارای یک زبان اسمبلر است که کارکردن با آن آسان است.
- زبان برنامه‌نویسی C،

[25] MULTOS Enabling Language

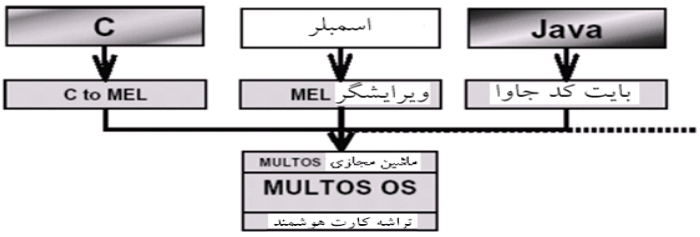
در حال حاضر، MULTOS تنها بستری است که یک کامپایلر C دارد و تا این زمان، این زبان رایج‌ترین زبان تعبیه شده[۲۶] است. ابزار توسعه SwiftC (مربوط به کارت SwiftCard) یک کامپایلر منطبق با ANSI است که به کاربر اجازه می‌دهد خیلی سریع هر برنامه کاربردی را به سیستم‌عامل MULTOS منتقل کند.

- زبان برنامه‌نویسی جاوا،

کارت‌های جاوا و MULTOS هر دو می‌توانند جاوا را پشتیبانی کنند. در هر دو مورد یک کامپایلر جاوا کد منبع[۲۷] را به کلاس جاوا ترجمه می‌کند. برای کارت جاوا، کلاس‌ها به بایت کد کارت جاوا تبدیل می‌شوند. برای MULTOS، کامپایلر SwiftJ(مربوط به کارت SwiftCard) کلاس‌های جاوا (یا بیسیک یا Modula2) را به کد MELترجمه می‌کند.

- زبان برنامه‌نویسی ویژوال بیسیک،

در کارت‌های ویندوز (کارت هوشمند با سیستم‌عامل ویندوز) از این زبان به‌عنوان زبان توسعه برنامه کاربردی استفاده می‌شود. برای اینکه MULTOS برای انجمن ویژوال بیسیک قابل قبول واقع شود، تکنولوژی SwiftCard در حال حاضر بر روی ویژوال بیسیک به عنوان یک مترجم MEL کار می‌کند.



شکل ۶ : تصویر زبان های برنامه ریزی و سیستم عامل Multos

MULTOS با توجه به ماهیتی که دارد خیلی فراتر از یک سیستم‌عامل است. MULTOS در واقع یک طرح کامل برای مدیریت برنامه‌های کاربردی کارت هوشمند است که این طرح فرآیندی ایمن، قابل اطمینان، و مقرون‌به‌صرفه برای مدیریت برنامه‌های کاربردی در دنیای جدید تعریف می‌کند. این در حالی است که یک کارت، ممکن است برنامه‌های کاربردی فراوانی از منابع مختلف در خود جای داده باشد. در شکل ۶ مراحل اجرای چندین برنامه کاربردی بر روی کارت نشان داده شده است، این زبان‌ها می‌بایست توسط MULTOS پشتیبانی شوند.

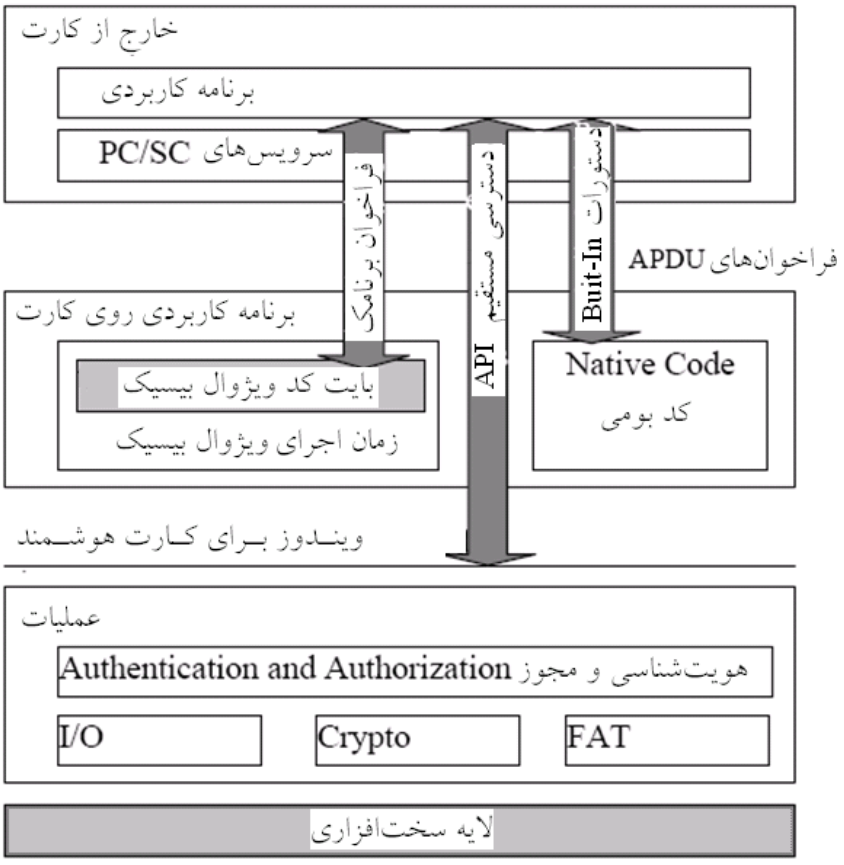
[26] Embedded Language

[27] Source

MULTOS پس از طراحی، به طور مستقل با سطح بالایی از امنیت سنجیده می‌شود تا اطمینان حاصل شود که منتشرکنندگان یا توسعه‌دهندگان برنامه کاربردی و دیگر تولیدکنندگان خدمات MULTOS می‌توانند طرح‌های تجاری‌شان را بدون اینکه مجبور به تقبل هزینه بالا و ارزیابی طولانی تکنولوژی باشند، تولید کنند.[3]

۸.۳. کارت های ویندوز

در ۱۹۹۹، مایکروسافت تجارت کارت هوشمند را آغاز کرد و ویندوز را به عنوان سیستم‌عامل کارت‌های هوشمند ارایه کرد. ویندوز کارت‌های هوشمند به عنوان جدیدترین عضو خانواده ویندوز، مزایای محیط ویندوز را بر روی کارت‌های هوشمند توسعه داده است. این سیستم‌عامل هشت بیتی و چند کاربردی، به هشت کیلو بایت ROM نیاز دارد. این سیستم‌عامل به گونه‌ای طراحی شده است که بستری با قیمت پایین و آسان برای برنامه‌ریزی باشد و بتواند برنامه‌های کاربردی ویژوال بیسیک را اجرا کند. معماری ویندوز برای کارت هوشمند در شکل ۷ آمده است.



شکل ۷ : تصویر معماری ویندوز برای کارت هوشمند

مانند کارت جاوا، توسعه برنامه‌های کاربردی در حال اجرا بر روی یک کارت هوشمند با فراهم کردن یک زبان برنامه‌نویسی سطح بالا در تعادل است. مایکروسافت به جای جاوا از بایت کد تولید شده از ویژوال بیسیک استفاده می‌کند که در یک محیط زمان اجرا بر روی

کارت اجرا می‌شود. برنامک روی کارت با استفاده ازAPDU های عمومی با یک برنامه کاربردی متناظر که خارج از کارت وجود دارد، ارتباط برقرار می‌کند. سیستم‌عامل یک API را برای کار با محتویات کارت هوشمند، عرضه می‌کند. این API به‌صورت مستقل از زبان طراحی شده و می‌تواند توسط ویژوال بیسیک و برنامک‌های اصلی، در دسترس قرار گیرد. فایل سیستم کارت‌های ویندوزFAT است که از لیست‌های کنترل دسترسی برای جلوگیری از دسترسی بدون اجازه به برنامه‌های کاربردی و فایل‌های داده، استفاده می‌کند.[3]

۹. امنیت کارت هوشمند

مراحل چرخه عمر یک کارت هوشمند را با در نظر گرفتن زمان‌بندی حمله‌های ممکن (طبق استاندارد ISO 10202-1) و طول عمر یک کارت هوشمند می‌توان در سه فاصله زمانی تقسیم‌بندی نمود.

۱) زمان طراحی و توسعه،
۲) زمان تولید،
زمان استفاده از کارت.

از آنجایی که اکثر حملات شناخته شده در زمان استفاده از کارت انجام می‌شود، انواع این حملات مبتنی بر استاندارد ISO 13491-1 در سه دسته زیر قابل اجرا هستند.

- حمله در سطح اجتماع،
- حمله در سطح فیزیکی،
- حمله در سطح منطقی.

در عمل ممکن است انواع ترکیبی حمله‌ها نیز اتفاق بیافتد. به عنوان مثال یک حمله در سطح فیزیکی می‌تواند راهی برای اجرای حمله‌ای در سطح منطقی ایجاد نماید. مثال آن یک حمله از طریق تحلیل نقص تفاضلی است.

حمله‌های در سطح اجتماع حملاتی هستند که علیه افرادی که با کارت هوشمند کار می‌کنند هدایت می‌شود. این افراد طراحان تراشه که برای کارخانه‌های نیمه‌هادی کار می‌کنند یا طراحان نرم‌افزار و یا دارندگان کارت هستند. این حملات توسط روش‌های سازماندهی شده قابل پیشگیری هستند. به طور مثال قرار دادن صفحاتی برای جلوگیری از خوانده شدن عدد PIN در طرفین صفحه کلید یک روش عمومی است.

از آنجایی که برای اجرای حملات روی کارت‌های هوشمند در سطح فیزیکی، لزوما نیاز به دسترسی فیزیکی به سخت‌افزار میکروکنترلر کارت هوشمند است، معمولاً نیاز به تجهیزات فنی خاص دارند. چنین حمله‌هایی می‌توانند ایستا و یا پویا باشند. ایستا به آن معنی است که هیچ توانی به میکروکنترلر اعمال نمی‌شود و پویا بر روی میکروکنترلرِ در حال عملکرد، اجرا می‌شود. در حمله‌های ایستای فیزیکی هیچگونه محدودیت زمانی به حمله کننده‌ای که عمل خود را در مکانش اجرا می‌کند، اعمال نمی‌شود؛ اما در حمله پویا تحلیل‌گر می‌بایست به تجهیزات موثر برای اکتساب و ارزیابی داده‌ها دسترسی داشته باشد.

تاکنون اکثر حمله‌های موفق شناخته شده روی کارت‌های هوشمند در سطح منطقی بوده‌اند. این حمله‌ها غالبا از ایده‌های ناب و خلاق یا محاسبات محض به‌دست می‌آیند. این دسته شامل تحلیل‌های کلاسیک می‌شوند؛ مانند حمله‌هایی که از نقص‌های شناخته شده‌ی سیستم‌عامل‌های کارت هوشمند بهره می‌گیرند و یا برنامه‌های اسب‌های تروا که در کدهای اجرایی برنامه‌های کاربردی کارت‌های هوشمند وجود دارند.

حمله‌های فیزیکی (سخت‌افزاری) که در انواع فعال و غیرفعال انجام می‌شوند، شامل انواع تحلیل‌های کانال جانبی[۲۸]، روش‌های مهاجم[۲۹] ، روش‌های نیمه مهاجم[۳۰] و روش‌های غیرمهاجم[۳۱] است که معمولاً بر روی سخت‌افزار کارت هوشمند اعمال می‌گردند و هر تکنیک آن در دو حالت ایستا و پویا قابل اجرا است. حمله‌های منطقی نیز معمولاً بر روی الگوریتم‌ها و پروتکل‌های بکار رفته اعمال شده و نرم‌افزار و سیستم‌عامل کارت را مورد تهدید قرار می‌دهند. در ادامه هر یک از این حملات توصیف شده و راه‌های مقابله با آنها ارائه خواهد شد.[2]

۹.۱. حملات در هنگام توسعه کارت و معیارهای دفاعی

امنیت فاکتوری است که از ابتدای توسعه می‌بایست در محصول در نظر گرفته شده باشد. در هنگام توسعه می‌بایست امنیت دو عامل ریزتراشه و سیستم‌عامل که نقش مهمی در امنیت کارت هوشمند دارند، در نظر گرفته شود. طیف وسیعی از معیارهای دفاعی با آغاز توسعه سخت‌افزار و نرم‌افزار ریزتراشه، برای سیستم‌عامل کارت هوشمند بکار گرفته می‌شوند.

ملاحظات امنیتی ریزتراشه کارت هوشمند

ملاحظات امنیتی مورد نیاز در هنگام طراحی ریزتراشه به شرح ذیل است.

- معیارهای طراحی

حسگرها و سایر المان‌های حفاظتی ممکن است در شرایط خاص عمل نکنند و یا بسادگی از کار بیافتند. برای این منظور تعدادی از اصول طراحی پایه وجود دارند که به تعاریف توابع ریزتراشه یک کارت هوشمند اعمال می‌شوند تا از کارت در برابر حمله‌های ایستا و پویا محافظت نمایند. این اصول باید در کنار المان‌های حفاظتی به کار گرفته شوند تا تضمینی برای ایجاد مقاومت کارت در برابر حملات باشند.

یک اصل طراحی که با سایر اصول استاندارد متفاوت است آن است که حداقل یک مکانیزم منتشر نشده در تراشه وجود داشته باشد.

- شماره منحصر به‌فرد تراشه

[28] Side Channel Attack

[29] Invasive Attack

[30] Semi Invasive Attack

[31] Non Invasive Attack

زمانی که سخت‌افزار نیمه‌هادی توسعه می‌یابد، تمامی مولفه‌های امنیت سخت‌افزار می‌بایست در ابتدا تعریف شده و به صورت سخت‌افزار در میکروکنترلر نهایی قرار گیرد. چنین بخشی یک حافظه WORM یا یکبار نوشتنی و چند بار خواندنی است که می‌تواند به صورت یک حافظه OTP است که تنها قابلیت یک‌بار برنامه‌ریزی را داراست. زمانی که تراشه‌های نیمه‌هادی ساخته می‌شوند، یک شماره تراشه یکتا در این حافظه نوشته می‌شود و این به معنی آن است که هر تراشه متفاوت از سایرین است و کارت هوشمند به طور واضحی قابل شناسایی است. از این شماره می‌توان برای سایر مکانیزم‌های امنیتی به عنوان کلید استفاده نمود؛ به عنوان مثال می‌توان از آن به عنوان کلید اصلی در رمزنگاری استفاده نمود.

ملاحظات امنیتی سیستم‌عامل کارت هوشمند

جهت توسعه سیستم‌عامل کارت هوشمند، بایستی موارد زیر مد نظر قرار گیرند.

- **قواعد توسعه،**

سیستم توسعه بایستی به یک شبکه کاملاً مجزا متصل باشد به نحوی که اجازه هیچ گونه دسترسی از خارج به آن وجود نداشته باشد. همانند توسعه سخت‌افزار، هیچ قابلیت مستند نشده‌ای نباید در نرم‌افزار گنجانده شود. برای پیشگیری از حملات ناخواسته، نباید در سیستم‌عامل امکان رونوشت گرفتن از حافظه فراهم شود، هر چند که باعث افزایش زمان تولید سیستم‌عامل گردد. با این وجود پیچیدگی در حال رشد سیستم‌عامل‌های کارت‌های هوشمند، موجب شده تا این قانون به درستی اجرا نگردد. برای اطمینان از در دسترس نبودن توابع مورد استفاده در زمان توسعه، بایستی در هنگام تکمیل توسعه سیستم‌عامل، این موارد در تست‌های ویژه‌ای بررسی شوند.

همچنین یک برنامه‌نویس به خاطر دلایل امنیتی، نباید به تنهایی بر روی یک پروژه کار کند، علت اصلی آن پیشگیری از خطاهای برنامه‌نویسی و کاهش احتمال حمله نفوذگران است. ضمناً پس از پایان توسعه سیستم‌عامل، تمامی کد بایستی توسط یک عامل تست کننده‌ی مستقل بررسی شود تا امکان مخفی‌سازی اسب‌های تراوا را در کد از بین ببرد.

- **توزیع دانش،**

اگر چند نفر روی یک موضوع کار کنند، نتیجه به دلیل نظرات و تجارب گوناگون افراد مختلف، در برابر حمله بسیار مقاوم‌تر خواهد بود. همچنین بهتر است هیچ فردی به همه اطلاعات دسترسی نداشته باشد. همین شرایط در هنگام بارگذاری کد برنامه، جداول و تنظیمات بر روی EEPROM وجود دارد و باعث می‌شود که سازنده تراشه که نسخه نهایی را برای ساختن ماسک دریافت می‌کند، اطلاعات کاملی را در مورد سیستم‌عامل به‌دست نیاورد و قسمت‌هایی از سیستم‌عامل که بر روی EEPROM قرار گرفته است، برای سازنده تراشه ناشناخته است. بنابراین سازنده نمی‌تواند مکانیسم‌های امنیتی سیستم‌عامل را با تحلیل کد ROM کشف نماید.[2]

۹.۲. حملات در هنگام تولید کارت و معیارهای دفاعی

از آنجا که محیط‌های تولید غالباً بسته هستند، حمله‌ها در حین تولید تراشه‌ها و یا کارت‌های هوشمند معمولاً حمله‌های درونی هستند. از آنجایی که در این محیط‌ها دسترسی‌ها و هویت‌ها کنترل می‌شوند و معمولاً معیارهای امنیتی در این مرحله باطل نمی‌شود، تنها برخی ازحمله‌های بسیار فنی در این مرحله ممکن است رخ دهد. در ادامه محافظت مورد نیاز در این مرحله آمده است.

احراز هویت در هنگام پایان یافتن هر مرحله

در مرحله ساخت، از ویفر میکروکنترلرهای کارت‌های هوشمند با استفاده از شماره‌های تراشه مجزا شده و کدهای انتقال محافظت می‌شود. در سیستم‌عامل‌های اخیر کد انتقال توسط تراشه تعریف می‌شود و تایید هویت یک نیازمندی اجباری برای هر دسترسی است.

تایید هویت‌های اجباری که پیش از پایان هر مرحله میان کارت هوشمند و بخش امنیتی ماشین اجرا کننده‌ی مراحل پایانی تولید، انجام می‌گیرد، امکان جابجایی تراشه‌ها و کارت‌ها را از میان خواهد برد. بدین ترتیب اجرای حملاتی که از طریق جایگزینی یک تراشه یا کارت هوشمند ساختگی با نمونه واقعی در انتهای مرحله تولید صورت می‌گیرد، معمولاً قابل اعمال نیستند.

از آنجا که مرحله تولید یک کارت هوشمند منحصرا" در اختیار کارخانه تولید کننده کارت است, اگر حمله‌ای در این مرحله طرح‌ریزی شود، این حمله توسط عوامل درونی کارخانه سازنده سازماندهی می‌گردد. از مهمترین تهدیدهای این مرحله می‌توان به جایگزینی تراشه کارت هوشمند با یک نمونه تراشه‌ی دیگر اشاره کرد. این جابجایی می‌تواند در شرایط خاص عملکردهای نامتعارفی را به‌دنبال داشته باشد. در شرایط مخاصمه و جنگ که حوزه‌های تهدید مختلفی ممکن است روی دهد نیز مبحث برقراری امنیت کارت هوشمند در مرحله تولید نقش به‌سزایی پیدا می‌کند.[2]

۹.۳. حملات در هنگام استفاده از کارت و معیارهای دفاعی

از آنجا که دسترسی به اجزای کارت پس از صادر شدن آن از سایر مراحل چرخه عمر آن ساده‌تر است، احتمال اجرای حملات نیز در زمان بکارگیری کارت از بقیه زمان‌ها بیشتر است.

معیارهای امنیتی بسیاری در ماژول‌هایی که کاربردهای امنیتی دارند، بکار گرفته می‌شود که در مورد کارت هوشمند قابل بکارگیری نیستند. به دلیل عدم وجود هرگونه منبع ذخیره‌سازی انرژی در کارت هوشمند، امکان اعمال مکانیزم‌های دفاعی فعال و همچنین تشخیص یک حمله بالقوه، بدون حضور یک منبع توان خارجی در کارت هوشمند وجود ندارد[۳۲]. به‌علاوه پاک شدن کلیدهای امنیتی و یا بسته شدن کارت می‌تواند کفایت نماید.

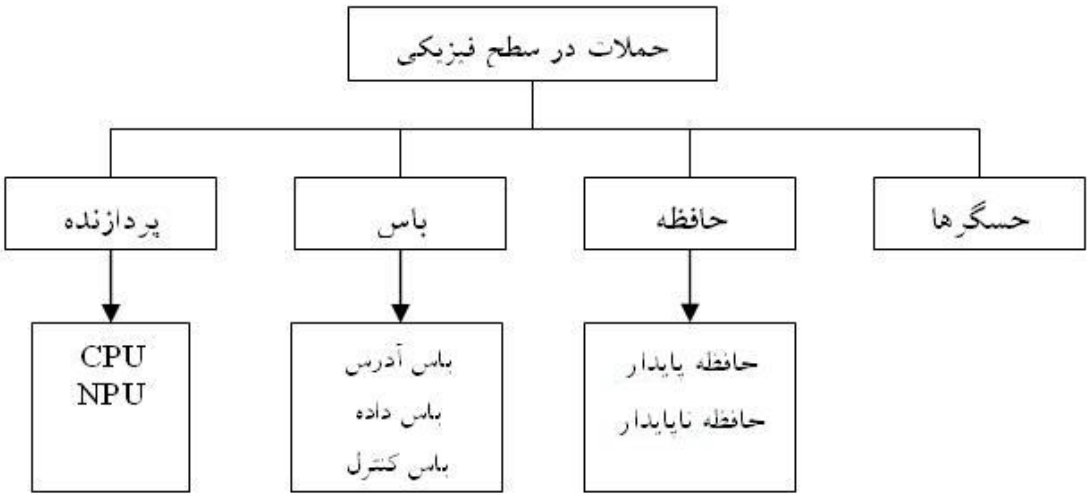
[۳۲] به دلایل قانونی نیز امکان اعمال خود تخریبی بر دارندگان کارت وجود ندارد.

در ادامه برخی از تکنیک‌های اعمال شده و شناخته شده‌ی حمله را معرفی می‌نماییم که هر چند معیارهای دفاعی در برابر آنها پس از مدتی از انتشار آنها شناخته شده است، اما برای تشخیص تهدیدهای اعمال شده بر روی کارت هوشمند باید در نظر گرفته شوند. لازم به ذکر است که در برابر برخی از حملات، راه مناسب دفاع شناخته نشده است.

حمله‌ها به دو دسته تقسیم می‌شوند که گونه اول در سطح فیزیکی و دسته دوم در سطح منطقی بر روی سیستم کارت هوشمند اعمال می‌گردند. حمله‌های فیزیکی به دو بخش فعال و غیرفعال تقسیم می‌شوند که تمامی این حملات در دو حالت ایستا و پویا قابل اجرا هستند. در نوع ایستا ریز تراشه در حال عمل نیست (فعال نیست) هرچند که روشن است و توان و ولتاژ به آن اعمال می‌گردد و در نوع پویا که بسیار دشوارتر اجرا می‌گردد، ریزتراشه با تمامی توابع و عملگرهایش تحلیل می‌گردد (فعال است). حمله‌های منطقی، حملاتی هستند که بر روی پروتکل‌ها و الگوریتم‌های به‌کار رفته در سیستم اجرا می‌شوند.[2]

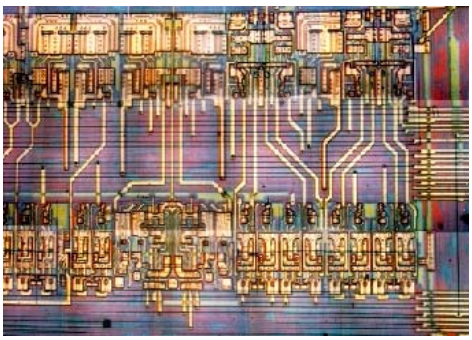
حملات در سطح فیزیکی و روش‌های مقابله

بهره‌برداری در سطح نیمه‌هادی و بخصوص در حمله‌های فعال، نیاز به دانش فنی فراوان و تجهیزات دقیقی نظیر میکروسکوپ برش دهنده‌ی لیزری، اشعه‌های یونی و کامپیوترهای بسیار دقیق دارد که تنها در اختیار سازمان‌های خاص قرار دارد و همین موضوع، احتمال حمله‌های فیزیکی را کاهش می‌دهد. دسته‌بندی حملات در سطح فیزیکی در شکل ۸ آمده است. حملات غیرفعال به اندازه حملات فعال نیاز به تجهیزات خاص نیست و با استفاده از دانش فنی بالا و تجهیزات معمولی قابل اجرا است. اما در هر حال برای مقابله با این حملات می‌بایست حفاظت‌های مورد نیاز در سخت‌افزار اعمال شود.



شکل ۸ : تصویر دسته بندی حملات در سطح فیزیکی

از جمله مخرب‌ترین حملات فیزیکی برداشتن تراشه از روی کارت و انجام فعالیت‌های مهندسی معکوس بر روی طرح‌بندی آن است. برای شکل‌دهی این حملات، ابتدا باید تراشه کارت از روی بدنه پلاستیکی آن جدا شود. برای حل نمودن لاک[۳۳] استفاده شده، می‌توان از اسید نیتریک (بالای ۹۸ درصد)، استفاده نمود. سپس تراشه را درون استون انداخته و تکان داده تا سطح سیلیکونی آن پیدا شود. حال تراشه می‌تواند مستقیماً مورد تجزیه و تحلیل قرار گیرد.



راه‌های زیادی برای طرح حملات فیزیکی وجود دارد. برای مثال پاک نمودن قفل امنیتی حافظه EEPROM با تابانیدن نور ماوراء بنفش به آن، کاوش عملکرد مدار با استفاده از پراب‌های[۳۴] بسیار ریز یا استفاده از میکروسکوپ‌های لیزری برای جستجو درون تراشه ، نمونه‌هایی از این روش‌ها هستند.

البته باید ذکر گردد که این نوع حملات بسیار پرهزینه بوده و نیاز به آزمایشگاه‌های مجهز دارند. برخی از این روش‌ها عبارتند از:

- روش‌های شیمیایی،
- روش‌های تحقیقی،
- پرتو الکترونیکی،
- FIB،
- IR.
- تنش‌های خارجی مثل تشعشع.

انواع روش‌های حمله فیزیکی شامل تحلیل‌های غیرفعال می‌باشند که مهمترین نوع آنها تحلیل‌های کانال جانبی است. انواع حمله‌های زمانی، توان مصرفی و تشعشعات الکترومغناطیسی سخت‌افزار از جمله حملات کانال جانبی است.

در ادامه مکانیزم‌های حفاظتی ریزتراشه در دو بخش تحلیل‌های ایستا و پویا بیان می‌شود.

[33] Resin

[34] Probes

تحلیل ایستا ریزتراشه کارت هوشمند

در ادامه معیارهای عمومی که برای محافظت در برابر تحلیل‌های ایستای ریزتراشه کارت شناخته شده‌اند، معرفی می‌گردد.

- انتخاب مناسب فناوری نیمه هادی،

ابعاد ساختارهای بکار رفته روی تراشه همانند پهنای خطوط، اندازه ترانزیستورها و... محدودیت‌های فناوری را مشخص می‌نماید. از آنجایی که پهنای ساختاری معمولا در اندازه‌های ۳۵/. میکرومتر تا ۱۳/. میکرومتر قرار می‌گیرند، فناوری نیمه هادی در حدود ۱ میکرومتر برای جلوگیری از اقتباس اطلاعات از تراشه امن مناسب است.

- طراحی تراشه به روش‌های خاص،

سلول‌های استانداردی که برای تولید مدارهای مجتمع نیمه‌هادی بکار می‌روند المان‌های پردازنده و یا حافظه را شکل می‌دهند که در اکثر محصولات بکار گرفته می‌شوند. کارخانه‌های سازنده تراشه کارت‌های هوشمند می‌بایست از روش‌های خاص استفاده کنند، بگونه‌ای که اطلاعات مدارهای درونی آنها به طور گسترده و عمومی وجود نداشته باشد.

- محل قرارگیری باس‌های تراشه،

باس‌های درونی تراشه نباید به گونه‌ای قرار گرفته باشند که امکان هرگونه اتصال به آنها و دریافت اطلاعات از آنها وجود داشته باشد. باس‌ها معمولاً در لایه‌های پایین‌تر قطعه نیمه‌هادی قرار می‌گیرند و در حالت تعریف شده برای آن تراشه درهم‌ریخته[۳۵] می‌شود.

- محل استقرار حافظه،

ROM، حافظه میانی به کار رفته برای اکثر برنامه‌ها است که محتویات آن را می‌توان بیت به بیت توسط یک میکروسکوپ اپتیکی بازخوانی نمود. بنابراین تبدیل کردن[۳۶] این بیت‌ها به بایت و تنظیم آنها برای حصول کد کامل ROM دشوار نیست. پس برای جلوگیری از این نوع آنالیز و دشوار نمودن تحلیل اپتیکی، ROM می‌بایست در پایین‌ترین لایه سیلیکون قرار گیرد.

- لایه‌های محافظ[۳۷]،

آنالیز فعالیت‌های سطح تراشه توسط اسکن با کیفیت بالا می‌تواند تهدیدی را درباره به‌دست آوردن محتویات RAM تراشه در حال عملکرد ایجاد نماید. با قرار دادن لایه‌های فلزی حامل جریان در بالای ناحیه‌ی حافظه و یا کل سطح تراشه می‌توان در برابر این تحلیل مقاومت نمود. از آنجا که این لایه‌های محافظ برای توزیع توان الکتریکی تراشه مورد نیاز هستند، برداشتن آنها توسط روش‌های شیمیایی موجب تخریب تراشه می‌شود.

- دفاع در برابر خواندن غیرمجاز حافظه فرار،

[35] Scramble

[36] Assemble

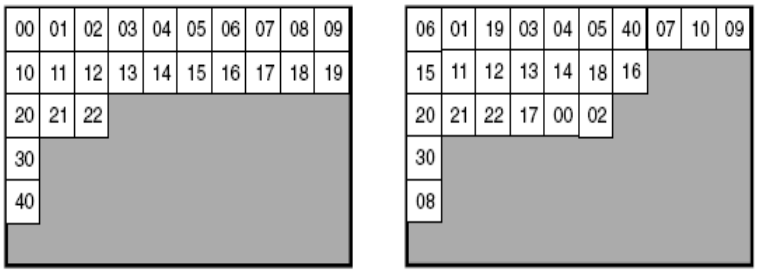
[37] Shields

محتویات RAM زمانی که توان سیستم قطع می‌شود از بین می‌رود. این موضوع زمانی که سلول‌های حافظه تا دمای منهای ۶۰ درجه سلسیوس سرد شوند، اتفاق نمی‌افتد.

همچنین اگر داده ذخیره شده برای مدت زمان طولانی بدون تغییر بماند، محتوای RAM به طور کامل پاک نمی‌شود. اما کلیدهای سری درون RAM ثابت نمی‌مانند و با سایر مقادیر جایگزین می‌شوند که این امکان اجرای حمله با تغییر دمای محیط را کاهش می‌دهد. خواندن سلول‌های RAM هرچند بسیار دشوار است و نیاز به تشخیص حالات سوئیچ نمودن ترانزیستورهای درون قطعه دارد، اما توسط میکروسکوپ‌های الکترونی و روش‌های پیشرفته قابل اجرا است که مراحل برداشتن لایه‌های غیرفعال و فلزی از نیازمندی‌های این حمله است.

- پیچیده نمودن حافظه،

درهم‌ریختگی و پیچیده نمودن حافظه بر روی میکروکنترلر تراشه، بسیار پرکاربرد است؛ این تکنیک به امنیت طرح پیچیده‌سازی که برای سلول‌های حافظه بکار رفته است، بسیار بستگی دارد. این روش به سادگی پیاده می‌شود و نیاز به فضای اضافی روی تراشه ندارد. تحلیل‌گر، بدون اطلاعات پیچیده‌سازی نمی‌تواند نحوه آدرس‌دهی سلول‌های حافظه را کشف نماید.EEPROM نیز می‌تواند توسط نرم‌افزاری درهم‌ریخته شود. شکل سمت راست شکل ۹ آدرس‌دهی درهم ریخته شده حافظه را نشان می‌دهد که آدرس‌دهی خطی آن در سمت چپ شکل ۹دیده می‌شود.



شکل ۹ : تصویرآدرس دهی سلول های حافظه

- رمزگذاری حافظه

در کنار پیچیده‌سازی حافظه، می‌توان از رمزگذاری ویژه حافظه و برخی از ثبات‌های پردازنده استفاده نمود. برای این منظور می‌توان برای افزایش فضای کلید، در کنار کلید از برخی از آدرس‌های حافظه در پروسه رمزگذاری و رمزگشایی نیز استفاده نمود.

برای جلوگیری از خوانده شدن EEPROM می‌بایست از امکان شناسایی داده‌های محرمانه همانند کلید و یا PIN، توسط تحلیل‌گر جلوگیری به عمل آید. برای این منظور می‌بایست PIN توسط یک تابع یکطرفه و یک کلید ویژه (تعریف شده برای هر کارت) رمز شود.

تحلیل پویا ریزتراشه کارت هوشمند

یک بخش اساسی از حملات فیزیکی در حالت پویا، بر روی سخت‌افزار کارت صورت می‌گیرد. روش‌های تحلیل و مکانیزم‌های دفاعی به اختصار در ادامه آورده شده است.

- نظارت[۳۸] بر لایه غیرفعال،

لایه غیرفعال توسط روش‌های شیمیایی قابل برداشتن است؛ امکان اجرای یکسری از حملات فیزیکی مانند پراب‌گذاری با برداشتن لایه غیرفعال آغاز می‌شود، بنابراین می‌بایست از یک مدار سنسوری که با اندازه‌گیری مقاومت و ظرفیت خازنی تراشه، حضور مدار را بررسی می‌نماید، استفاده نمود. در این صورت تخریب این لایه می‌تواند توسط سنسور وقفه‌ای[۳۹] به نرم‌افزار تراشه داده یا کل سخت‌افزار را غیرفعال نماید.

- نظارت بر ولتاژ،

نظارت بر ولتاژ می‌بایست در هر ریزتراشه‌ی کارت هوشمند وجود داشته باشد و در صورت بیشتر و یا کمتر شدن منابع تغذیه از حدود مجاز، تراشه را غیرفعال نماید. این ویژگی به نرم‌افزار این اطمینان را می‌دهد که تراشه در محدوده‌ای از ولتاژ که ممکن است به درستی عمل نکند، قرار نخواهد گرفت. در غیر این صورت، تراشه ممکن است پرش‌های کنترل نشده یا خطاهای محاسباتی داشته باشد که این رفتار پر از نقص ممکن است در تعیین کلیدهای سری توسط تکنیک‌های تحلیل نقص تفاضلی[۴۰] به کار رود. به طور مثال در صورتی که محدوده ولتاژ ۳-۵ ولت باشد، آستانه‌های خاموش شدن ۲/۳ تا ۶/۳ ولت می‌باشد.

- نظارت بر فرکانس،

یک کارت هوشمند توسط یک کلاک پالس خارجی عمل می‌نماید که اجرای عمل ریزتراشه را در حالات تک مرحله‌ای نیز ممکن می‌سازد. این موضوع امکان تحلیل را با اندازه‌گیری جریان‌های مصرفی عملگرها و پتانسیل الکتریکی سطح تراشه فراهم می‌سازد. به منظور جلوگیری از تحلیل، اجزایی برای تشخیص شرایط فوق فرکانس و زیرفرکانس در تراشه ساخته می‌شود که احتمال کاهش نرخ کلاک به سطوح غیرمجاز را نشان می‌دهد.

حداقل نرخ کلاک یک مگاهرتز است و تراشه معمولاً در حوالی ۵۰۰ KHZ متوقف می‌شود و حد بالای آن پنج مگاهرتز است و آشکارسازها[۴۱] تراشه را در فرکانس تقریباً هفت مگاهرتز از کار می‌اندازند.

- نظارت بر حرارت،

[38] Monitoring

[39] Intrrupt

[40] Differential Fault Analysis (DFA)

[41] Detector

حسگر حرارت برای دماهای بسیار بالا، تنها در برخی از تراشه‌ها به کار گرفته می‌شود، زیرا معمولاً میکروکنترلر در محدوده عملکرد نامتعارف دما آسیب نمی‌بیند اما ممکن است خطاهایی در این مورد صورت بگیرد.

- درهم‌ریختگی باس داده،

در بسیاری از میکروکنترلرها، باس‌های درونی متصل به حافظه درهم‌ریخته می‌شوند. شکل سمت راست شکل ۱۰، باس پیچیده شده و شکل سمت راست آن یک طرح باس معمولی را نشان می‌دهد.

شکل ۱۰: تصویر باس پیچیده و باس معمولی

- یکسان‌سازی جریان مصرفی CPU

در یک پردازنده کارت هوشمند مصرف جریان برای همه دستورالعمل‌های ماشین می‌بایست یکسان باشد، در غیر این صورت بخشی از اطلاعات محرمانه را می‌توان به‌دست آورد. این حمله‌ها که به تحلیل‌های توان مصرفی[۴۲] معروف هستند، انواع ساده و تفاضلی دارند که انواع متغیرهای وابسته به داده روی برنامه‌های در حال اجرا توسط پردازنده را نیز همانند تابش‌های الکترومغناطیسی[۴۳] تراشه شامل می‌شوند. این حمله دفاع مناسبی ندارند اما در ادامه چند نکته بر مبنای روش‌های سخت‌افزاری و نرم‌افزاری بهینه شده بیان می‌شود.

ساده‌ترین راه‌حل سخت‌افزاری بکارگیری رگولاتور ولتاژ سریع‌العمل در تراشه است که از یک مقاومت حسگر برای نظارت کردن بر جریان تراشه استفاده می‌کند تا استقلال آن را از دستورالعمل‌ها و داده‌ها بسنجد. مولدهای جریان نویز مصنوعی بر روی تراشه نیز راه‌حل موثر دیگری است؛ یک راه حل فنی و پیچیده نیز استفاده از طراحی پردازنده‌های بهینه شده با یک جریان خروجی ثابت است. یک روش دفاعی ساده‌تر فعال ساختن بخش‌هایی از ریزتراشه است که در حین اجرای SPA[۴۴] یا DPA[۴۵] نیازی به اجرای آنها نیست که برای اینکار با استفاده از داده‌های تصادفی در مقادیر ورودی به تولید نویزهای مصنوعی در جریان مصرفی پرداخته می‌شود.[2]

[42] Power Consumption Attack

[43] Electromagnetic Emanation

[44] Simple Power Analysis

[45] Differential Power Analysis

۹.٤. حمله‌ها در سطح منطقی و روش‌های مقابله

مهمترین پیش‌نیاز حمله بر روی امنیت کارت هوشمند در سطح منطقی، آگاهی از جریان ارتباطات و اطلاعات میان ترمینال و کارت هوشمند است. در این حمله نیازی به درک پروسه اتفاق افتاده در سطح سخت‌افزار نیست و به جای آن نرم‌افزارها، الگوریتم‌ها و پروتکل‌های در حال اجرا مورد توجه هستند. به همین دلیل این حملات تنها در حالت پویا قابل اجرا هستند. اما در مواردی نیز ممکن است مکانیسم‌های محافظتی در نرم‌افزارهای کاربردی در کارت هوشمند وابستگی زیادی به مکانیسم‌های امنیتی فراهم شده در سیستم‌عامل و سخت‌افزار کارت داشته باشند. به عنوان مثال اگر بتوان محتویات EEPROM کارت را با استفاده از روش‌های تحلیلی به‌دست آورد، پیچیده‌ترین و امن‌ترین روش‌های رمزنگاری بی‌فایده خواهند بود، زیرا حمله‌کننده می‌تواند کلیدها را از روی محتویات حافظه به‌دست آورد. در ادامه انواع شناخته شده حمله‌ها و معیارهای دفاعی صورت گرفته در سطح منطقی ارائه شده است.

حملات و روش‌های دفاعی در نرم‌افزارها و الگوریتم‌های کارت هوشمند

در این بخش مباحث امنیتی مرتبط با سیستم‌عامل، نرم‌افزارها و الگوریتم‌های کارت هوشمند ارائه شده است. این مباحث که در قالب نکات امنیتی لازم الاجرا در نرم‌افزارها و الگوریتم‌ها مطرح می‌شود، در ادامه ذکر شده است.

- مکانیسم‌های ساده

برای مقابله با حملات، مکانیسم‌های به کار رفته در برنامه کاربردی می‌بایست تا حد امکان ساده باشند تا هم پیاده‌سازی آنها راحت باشد و هم بررسی و تست آنها سخت صورت نپذیرد. استفاده از کد پیچیده نه تنها باعث امنیت بیشتر نمی‌شود بلکه باعث وجود حفره‌های امنیتی می‌گردد که عمل حمله را ساده‌تر می‌کند. به عنوان مثال، مکانیسم‌های امنیتی موجود در سیستم‌عامل بایستی در برنامه‌های کاربردی مورد استفاده قرار گیرند چون امنیت را در لایه پایین‌تری فراهم می‌کنند و به اندازه لازم، تست شده‌اند و در کنار آنها می‌توان از مکانیسم‌های امنیتی در سطح نرم‌افزار استفاده کرد.

- سطوح دسترسی محافظه‌کارانه،

سطوح دسترسی به فایل‌ها و منابع و فرمان‌های مورد استفاده در کارت هوشمند بایستی تا حد امکان به صورت محافظه‌کارانه اعطا شود. بجز مواردی که نیاز حتمی وجود دارد، سایر دسترسی‌ها به منابع باید محدود شود. زیرا در این صورت تلاش بیشتری برای حمله به سیستم مورد نیاز است و احتمال اعطای حق دسترسی به اطلاعات حساس به صورت ناخواسته به صورت چشمگیری کاهش پیدا می‌کند.

- استفاده از ماشین‌های حالت برای ترتیب دستورات و دسترسی به فایل‌ها،

در صورتی که نتوان دستور دلخواه را در زمان دلخواه و به تعداد دفعات دلخواه اجرا کرد، حمله به برنامه کاربردی مورد استفاده در کارت هوشمند بسیار دشوارتر می‌گردد. این امر با استفاده از یک ماشین حالت برای تعریف ترتیب مجاز

دستورات قابل اجرا، محقق می‌گردد. به عنوان مثال اگر تصدیق اصالت دوجانبه[۴۶] (دو طرفه) به عنوان اولین قدم تایید هویت مورد نیاز است، یک حمله کننده در قدم اول برای اجرا کردن دستورات دیگر مجبور باشد که از این سد بگذرد.

در صورتی که فایل‌های موجود در کارت هوشمند علاوه بر حفاظت شدن به‌وسیله سطوح دسترسی ذخیره شده در داخل اشیاء، توسط یک ماشین حالت که دستورات و پارامترهای مجاز آنها را تعریف می‌کند، محافظت شوند کار حمله کننده بسیار دشوارتر خواهد گشت. اگر از یک ماشین حالت استفاده شود، تنها دستورات تعریف شده در برنامه کاربردی بر روی کارت هوشمند قابل اجرا خواهند بود.

- سطوح مختلف ارزیابی،

هر شخص یا هر تجهیزاتی نیاز نیست بتواند تمامی ویژگی‌های امنیتی کارت را بررسی کند. مثلاً یک پایانه (ترمینال) خرده‌فروشی در یک سیستم خرید و فروش الکترونیکی، ممکن است تنها تعدادی کلید برای بررسی امضاهای دیجیتال در اختیار داشته باشد نه کل کلیدها را. این کار باعث می‌شود که حمله کننده با به‌دست آوردن کلید اصلی یک پایانه نتواند امنیت کل سیستم را به مخاطره بیاندازد.

- ویژگی‌های امنیتی،

برخی از ویژگی‌های اضافی جاسازی شده در داخل تراشه‌ها که توسط پایانه قابل ارزیابی باشد، می‌تواند در کنار تست‌های نرم‌افزاری به افزایش امنیت کارت کمک کند. برای این منظور می‌توان هم از مولفه‌های آنالوگ و هم از مولفه‌های دیجیتال استفاده کرد. امنیت فراهم شده توسط این خصوصیات به میزان پنهان‌سازی آنها بستگی دارد و برای برنامه‌های کاربردی مختلف، متفاوت است و این نشان‌دهنده این امر است که تراشه‌ها بسته به برنامه‌های کاربردی، متفاوتند.

- انتقال داده‌ها به صورت امن،

ریسک‌های متعددی در هنگام انتقال داده‌ها در یک محیط غیرامن وجود دارد و یک حمله کننده با دستکاری در واسطه‌های بین کارت و پایانه می‌تواند داده‌های مورد نظر را در یک جلسه، حذف کرده یا اطلاعات مورد نظر را وارد کند.

در کارت‌های هوشمند جهت انتقال داده‌ها به صورت امن می‌توان از یک روش پیغام‌رسانی امن استفاده نمود. با این وجود می‌بایست از رمز نمودن تمامی اطلاعات انتقالی پرهیز شود و تنها بایستی برای انتقال کلیدها از رمزنگاری استفاده شود. تقریباً تمامی اطلاعاتی که در حافظه کارت هوشمند نوشته می‌شود جنبه عمومی دارد و در صورت رمزنگاری، هیچ کس نمی‌تواند بفهمد که چه اطلاعاتی در داخل کارت نوشته یا از آن خوانده می‌شود بنابراین برای بر طرف کردن هر گونه شبهه، بایستی اطلاعات حتی‌الامکان به صورت رمز نشده انتقال پیدا کنند.

[46] Mutual Authentication

- استفاده از توابع تصحیح خطا،

اگر یک جلسه در یک شرایط تعریف شده و به صورت ناگهانی خاتمه پیدا کند، یا در مورد جلسات قبلی اطلاعاتی مورد نیاز باشد، بهتر است که از ثبت وقایع[۴۷] ویژه برنامه کاربردی استفاده شود. این فایل‌های ثبتی معمولاً توسط سیستم‌عامل فراهم می‌شوند و در هنگام یک جلسه، به‌روز می‌شوند تا حالات جاری برنامه‌های کاربردی یا امضاها یا اطلاعات دریافت شده توسط پایانه را ثبت کنند و برای این منظور معمولاً از فایل‌های چرخشی استفاده می‌شود.

یک علت برای استفاده از فایل‌های ثبت کننده، امکان استفاده از توابع تصحیح خطا به‌واسطه آنها است و بدین وسیله می‌توان کارت را به حالت اولیه قبل از روی دادن خطا بازگرداند.

- تصدیق اصالت،

تصدیق اصالت یک طرفه که توسط کارت‌های مغناطیسی قابل انجام است تنها قابلیت تصدیق اصالت کارت توسط پایانه را فراهم می‌کند و یک کارت مغناطیسی نمی‌تواند پایانه مورد استفاده را تصدیق اصالت کند. با بکارگیری کارت‌های هوشمند می‌توان به صورت فعال از دسترسی پایانه غیرمجاز به محتویات کارت، جلوگیری به عمل آورد. استفاده از تصدیق اصالت دوطرفه مانع از تحلیل سیستم‌عامل کارت به صورت شخصی می‌گردد.

- رفتار برخط[۴۸]،

جهت upload و download کردن برنامه‌ها و اطلاعات مورد نیاز، لازم است که کارت با سیستم پیش‌زمینه ارتباط داشته باشد. هر چه اندازه سیستم بزرگتر شود و میزان سود حاصل از جعل هویت حمله کننده افزایش یابد، اهمیت قابلیت برقراری ارتباط برخط با سیستم پیش‌زمینه بیشتر می‌گردد و با این ارتباط می‌توان اطلاعات کارت را با پایگاه داده مرکزی تطبیق داد و در صورت نیاز، کارت را مسدود کرد. یکی از روش‌های کارا برای ارتباط برخط، استفاده از یک شمارنده برای التزام کارت برای برقراری ارتباط برخط پس از تعداد مشخصی ارتباط برون خط[۴۹] است و بعد از این ارتباط، سیستم پیش‌زمینه می‌تواند شمارشگر را بازنشانی کند.

- استفاده از لیست‌های سیاه[۵۰]،

از آنجایی که هیچ‌گاه نمی‌توان احتمال استفاده از کارت‌های جعلی را به طور کل از بین برد، مکانیسمی مورد نیاز است تا به‌واسطه آن بتوان کارت‌های جعلی یا دزدیده شده را مسدود کرد. روش‌های پایه‌ای که می‌توان برای این منظور به کار برد استفاده از لیست‌هایی است که با یک سری مشخصات یکتا، کارت را تشخیص می‌دهند (مانند شماره کارت).

- مقابله در برابر ویروس‌های کامپیوتری و اسب‌های تراوا،

[47] Log

[48] On-Line

[49] Off-Line

[50] Black List

در کارت‌های هوشمند جدید، قابلیت بارگذاری برنامه‌های جدید، پس از صادر کردن کارت برای کاربر وجود دارد و بنابراین به صورت بالقوه امکان بارگذاری ویروس یا اسب تراوا در کارت‌های هوشمند وجود دارد ولی با وجود سیاست‌های امنیتی لحاظ شده در سیستم عامل کارت‌های هوشمند، امکان بارگذاری برنامه‌ها به صورت کنترل نشده و غیر مجاز در حافظه کارت‌های هوشمند وجود ندارد و همچنین معمولاً در این سیستم‌عامل‌ها، مکانیسم‌هایی برای جلوگیری از دسترسی به برنامه‌های کاربردی به اطلاعات یکدیگر پیش‌بینی شده است.

- جستجوی تمام فضای حالت کلید،

یک روش برای جلوگیری از جستجوی کلید، بزرگ‌تر در نظر گرفتن فضای جستجوی کلید با افزایش طول کلید و یا افزودن کاراکترهایی به آن است. روش دیگر جلوگیری از امکان یافتن یک زوج مقدار رمز نشده و معادل رمز شده آن در نرم‌افزار کاربردی کارت به منظور عدم امکان اجرا جستجوی فضای جامع است. در واقع در بسیاری از موارد در برنامه‌های کاربردی نیازی به رمز کردن اطلاعات نیست و تنها کافی است که با استفاده از یک MAC[51]، از صحت اطلاعات، اطمینان حاصل شود که حمله جستجوی جامع برای یافتن کلید و مقادیر مورد نیاز حمله جستجو ، از روی MAC دشوارتر است. در واقع در روند اجرای یک تابع MAC، یک مقدار تصادفی تولید شده و در کنار سایر داده های ورودی به تابع اعمال می‌گردد. در صورتی که مقدار تصادفی به متن رمز نشده کارت هوشمند اضافه شود، اطلاعاتی که می‌بایست رمز شود در هر بار بکارگیری تابع متفاوت خواهد بود و این جستجوی فضای جامع را دشوارتر می‌سازد.

در بسیاری از موارد مقدار تصادفی علنی نبوده و می‌تواند یک راز تقسیم شده میان ماژول امنیتی و کارت هوشمند باشد. علاوه بر این، استفاده از اعداد تصادفی، حتی اگر علنی باشد مقاومت مناسبی در برابر حملاتی همچون DFA و SPA/DPA فراهم می‌کند.

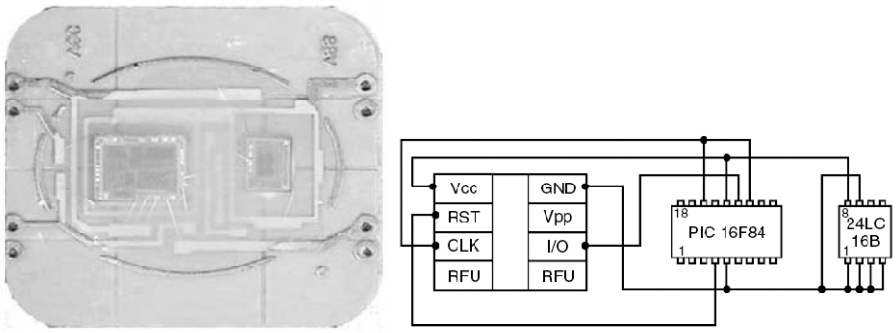
استفاده از کلیدهای پویا برای جلسات مختلف نیز برای مقاومت در برابر چنین حملاتی موثر است؛ چون در صورت یافتن کلید به صورت تصادفی، این کلید برای جلسه‌های دیگر قابل استفاده نخواهد بود.

- جلوگیری از جعل کارت‌های هوشمند،

شایع‌ترین حمله علیه کارت هوشمند، به کارگیری کارت هوشمندی است که مهاجم آن را به صورت دلخواه برنامه‌ریزی نموده و شامل توابع تحلیلی اضافه است. به طور مثال فناوری جاوا امکان تولید برنامه و بارگذاری آن به کارت ساختگی را فراهم می‌آورد. شکل۱۱ نشان دهنده درون یک کارت هوشمند است که ریزتراشه PIC[52] کارت و حافظه EEPROM EEPROM دیده می‌شوند، در اینجا مدار جایگزین (نشان داده شده در سمت چپ شکل ۱۱) به صورت داده شده، همان عمل کارت را انجام خواهد داد.

[51] Massage Authentication Code

[52] Programmable Intelligent Computer



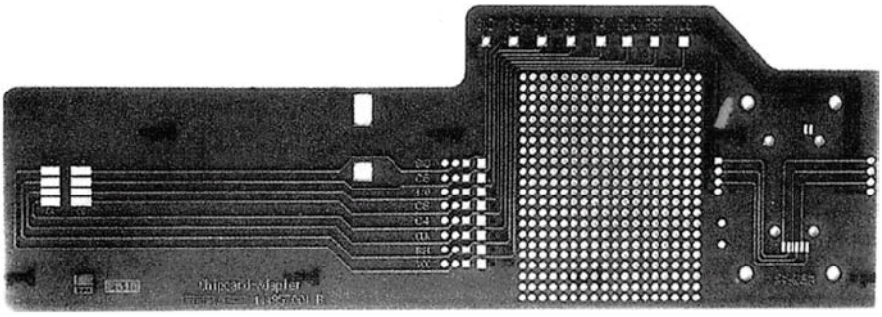
شکل ۱۱: تصویر اجزای داخلی کارت هوشمند

در صورتی که بتوان برنامه‌های یک کارت هوشمند را جعل نمود و بر روی یک کارت جعلی بارگذاری کرد، ممکن است بتوان بخشی از ارتباطات میان ترمینال و کارت را ثبت نمود و اطلاعات آن را ارزیابی کرد. از طرفی چون که مکانیزم‌های ارتباطی معمولا از رمزنگاری استفاده می‌کنند؛ برای امکان اجرای یک حمله نیاز به دانستن کلید رمز و یا از کاراندازی محافظت های رمزنگاری کاربردها است.

معمولا به منظور جلوگیری از جعل کارت، دستورالعمل‌ها و دستورات بکار رفته توسط کارت منتشر نمی‌شوند اما روال‌هایی برای تشخیص آنها وجود دارد.

- دفاع در برابر حمله بهره‌برداری از داده‌های در حال عملکرد،

می‌توان از یک کارت هوشمند ساختگی برای استفاده از داده در حین یک جلسه بهره گرفت. تغییرات مورد نیاز شامل یک اتصال اضافی به بالای I/O است که توسط یک کامپیوتر سریع و برنامه‌نویسی مناسب می‌توان هر داده دلخواه را درون ارتباط میان ترمینال و کارت هوشمند وارد و یا حذف نمود. آداپتوری که امکان اندازه‌گیری بر روی کارت در خارج ترمینال را می‌دهد در شکل ۱۲ دیده می‌شود.



شکل ۱۲: تصویر آداپتور اندازه گیری در خارج ترمینالل

- جلوگیری از وقفه‌گذاری در توان[۵۳]،

[53] Power Intrruption

در یک زمان مشخص که دستوری بر روی کارت در حال اجرا است وقفه در توان ورودی به کارت می‌تواند گونه‌ای از حمله‌های نوین را شکل دهد. این نوع از حمله بر مبنای این واقعیت شکل می‌گیرد که در برنامه‌نویسی تمامی دستورالعمل‌های نوشتن در EEPROM به صورت پشت سر هم و منطبق بر یک استاندارد برنامه‌نویسی قراردادی اجرا می‌شود و اگر برنامه‌نویس در مرتب نمودن این دستورالعمل‌ها دقت نکند، تحلیل‌گر می‌تواند با قطع توان در لحظه‌ای خاص مزایایی را به دست آورد.

ساده‌ترین روش پیشگیری از حمله، مرتب نمودن دستورالعمل‌های نوشتن EEPROM می‌باشد که در استاندارد EN1546 برای این زمینه توضیحات لازم را شامل می‌شود.

- جلوگیری از تحلیل جریان در حین مقایسه PIN،

انواع حمله روی ویژگی‌های مقایسه‌ای مانند PINها می‌تواند با ترکیب اندازه‌گیری‌های فیزیکی یک پارامتر و تغییر مقادیر منطقی صورت بگیرد. این نوع حمله مبتنی بر مکانیزم‌هایی است که در آن داده‌ها به کارت ارسال شده و با مقادیر متناظر مقایسه می‌شوند و شمارنده‌ای[۵۴] بر مبنای نتیجه‌ی مقایسه، افزایش می‌یابد. حمله مبتنی بر اصول اندازه‌گیری جریان کارت عمل می‌کند. اگر دستورالعمل مناسب شامل مقایسه داده به کارت ارسال شود، امکان بررسی افزایش شمارنده از طریق مقایسه جریان اندازه‌گیری شده وجود خواهد داشت.

دو روش دفاعی در برابر این حمله وجود دارد، ساده‌ترین دفاع معمولاً مشتمل بر افزایش شمارنده پیش از انجام مقایسه است و پس از انجام کار کاهش می‌یابد. در روش دوم در صورت عدم انطباق مقدار مورد مقایسه، شمارنده افزایش می‌یابد و در غیر این صورت مقدار شمارنده در یک سلول استفاده نشده EEPROM نوشته می‌شود.

- جلوگیری از تحلیل زمانی مقایسه PIN،

در صورتیکه یک PIN برای مقایسه به کارت فرستاده شود، برنامه مقایسه،PIN دریافتی را بایت به بایت با مقادیرPIN ذخیره شده مقایسه می‌کند. در یک برنامه معمولی و بدون ملزومات امنیتی اولین تفاوت در مقادیر مقایسه، برنامه‌ی مقایسه را به پایان می‌برد و این امکان حدس PIN را برای تحلیل‌گر به صورت بایت به بایت فراهم می‌کند. برای دفاع در برابر این تهدید می‌بایست روتین مقایسه ارقام به صورت یکباره انجام شود.

- استفاده از الگوریتم‌های رمزنگاری عاری از نویز برای جلوگیری از حمله زمانی،

امنیت کارت به کلیدهای سری الگوریتم‌های رمز، بستگی زیادی دارد و برای دسترسی به کارت در ابتدای هر مرحله‌ای، ترمینال می‌بایست هویت خود را بوسیله کلید سری به اثبات برساند. بنابراین احراز هویت ترمینال توسط کارت یک هدف جذاب برای تحلیل‌گر است. در حالی که احراز هویت کارت توسط ترمینال نسبت به حمله‌های روی کارت جذابیت اجرای حمله ندارد و کارایی آن نسبت به جعل هویت ترمینال کمتر است.

[54] Counter

کارت هوشمند ترمینال را با یک پروسه مقایسه‌ای همانند روند MAC[55] یا کد احراز هویت پیام بررسی و محرز می‌نماید. یک تحلیل‌گر با پردازش زمان ارسال دستور و دریافت پاسخ از کارت می‌تواند نتایجی را در ارتباط با MAC و کلید در حال استفاده، به‌دست آورد.

حمله‌های زمانی یک تهدید جدی برای کارت‌های هوشمند هستند که استفاده از الگوریتم‌های رمزنگاری که تفاوت‌های روشنی در زمان اجرا برای کلیدها و مقادیر ورودی و خروجی مختلف دارند، می‌تواند منشاء اجرای این حمله باشد؛ بنابراین سطح نویز در الگوریتم بسیار مهم است. الگوریتم‌های رمز عاری از نویز که زمان رمزگذاری و رمزگشایی آنها مستقل از مقادیر ورودی است و هیچ الزامی برای اضافه نمودن مقادیر نویز تصادفی به داده‌ها در آن وجود ندارد، یک راه حل مناسب برای ایجاد مقاومت در برابر حمله‌های زمانی می‌باشند.

- جلوگیری از تحلیل تفاضلی نقص،

حمله تفاضلی نقص یا DFA بر روی رمز DES برای اولین بار اعمال شد که در بسیاری از کارت‌های هوشمند استفاده می‌شوند. این حمله با اعمال پروسه رمز روی داده‌های تعیین شده و ایجاد خطا در رمز در حین محاسبه موجب تغییراتی در برخی از بیت‌های کلید شده(بهتر شود) و در نتیجه متن رمزی نادرست تشکیل می‌گردد. خطا در اثر میدان‌های فرکانس بالا و یا تابش‌های یونیزه شده ایجاد می‌گردد.

ساده‌ترین روش دفاع، محاسبه‌ی دوباره الگوریتم رمز و مقایسه نتایج است. در صورتی که مقایسه‌ها با یکدیگر منطبق بود تلاشی برای تغییر هیچ‌کدام از بیت‌ها از خارج کارت صورت نگرفته است. این دفاع فرض می‌کند خطاهای تصادفی شدید موجب تغییر بیت‌ها دو مرتبه پیاپی نخواهند شد که می‌تواند فرض صحیحی باشد هر چند که این دفاع عیب اضافه نمودن زمان پردازش را خواهد داشت.

- دفاع در برابر مشغول نمودن پردازنده،

حمله دیگری که به مثابه DFA عمل می‌نماید و سعی در بازیابی کلید سری الگوریتم رمز می‌نماید تلاش برای تاثیر بر روی کد روتین‌های برنامه بوسیله مشغول نمودن عملکرد پردازنده می‌باشد. انواع حمله‌هایی نظیر حمله نوری از سال ۱۹۹۸ برای کارخانه‌های سازنده کارت و ریزتراشه‌ها شناخته شده است و از سال ۲۰۰۲ نیز روش‌های مختلف حمله‌های القای خطای اپتیکی[56] مطرح شده است.

دفاع در برابر این حمله در سطوح مختلف تعریف می‌شود. در سطح سخت‌افزار برای ریزتراشه کارت هوشمند مهم است که حسگرهای مناسب داشته باشد که بتوانند مزاحمت‌های پردازنده را آشکار نمایند. این حسگرها شامل آشکارسازهای ولتاژ ناگهانی و تعداد زیادی از حسگرهای نوری مناسب می‌باشند.

[55] Message Authentication Code

[56] Optical Fault Injection

سطح بعدی در دفاع‌ها پیاده‌سازی در نرم‌افزار است. در این حالت فلوچارت برنامه می‌بایست قوی‌تر باشد و به ازای تمامی شرایط، یک دستور مجزا ارائه شده باشد. مثلاً اگر در یک بخش فلوچارت یک شرط کوچکتر و مساوی وجود دارد، می‌بایست هر یک از این شروط کوچکتر و یا مساوی به صورت مجزا آورده شده باشد. پیشگیری دیگر اجرای دوبار متوالی یک پرسش و پاسخ و تنها با یک تاخیر تصادفی میان دو بخش است. علاوه بر آنچه بیان شد، تمامی داده‌های محرمانه ذخیره شده درRAM پس از استفاده می‌بایست حذف شوند و یا به طور موقت رمز گردند.

حملات و روش‌های دفاعی در سیستم‌عامل کارت هوشمند

در این بخش مباحث امنیتی مرتبط با سیستم‌عامل کارت هوشمند ارائه شده است. این مباحث که در قالب نکات امنیتی لازم‌الاجرا در سیستم‌عامل مطرح می‌شوند در ادامه ذکر شده‌اند.

- تست‌های سخت‌افزاری و نرم‌افزاری،

پایه و اساس مکانیسم‌های محافظتی در سیستم‌عامل، روش‌های محافظتی اعمال شده در سخت‌افزار است. سه دسته مکانیسم‌های محافظتی که عبارتند از سیستم‌عامل، سخت‌افزار و نرم‌افزار با هم رابطه تنگاتنگی دارند و مانند دانه‌های زنجیرمتصل به هم، ضعیف‌ترین حلقه تعیین کننده میزان امنیت کل سیستم است. سیستم‌عامل مبنا و پایه برنامه کاربردی واقعی را تشکیل می‌دهد که باید از اطلاعات و پروسس‌های آن محافظت شود.

وقتی سیستم‌عامل راه‌اندازی می‌شود، باید تمامی اجزای مهم سخت‌افزار بررسی شود. به عنوان مثال بررسی RAM یک از کارهای ضروری سیستم‌عامل است، زیرا تمام شرایط دسترسی در RAM ذخیره می‌شوند و هرگونه خطا در دسترسی به حتی یک بیت هم می‌تواند باعث یک رخنه امنیتی گردد. همچنین لازم است که checksum مربوط به قسمت‌های مهم ROM و EEPROM بررسی گردند و CPU نیز باید حداقل با فرمان ATR[۵۷] آزمایش شود.

در صورت مشاهده خطا در سخت‌افزار یا checksum، سیستم‌عامل می‌تواند فوراً وارد یک حلقه بی‌پایان شود که باعث می‌شود پیغام ATR پاسخ داده نشود و دستورات بعدی دریافت نشوند. اشکالی که در این روش وجود دارد، آن است که این حالت از خارج کارت قابل بررسی و پیگری نیست. روش دیگر ارسال یک ATR خاص توسط CPU قبل از وارد شدن به حلقه بی‌پایان است ولی باید توجه داشت که ارسال یک ATR خطای ساده، مستلزم عملکرد تقریباً کامل CPU، چندین بایت در RAM و چند صد بایت از کد در ROM است.

- تفکیک به صورت لایه‌ای در سیستم‌عامل،

عوارض ناشی از خطاهای طراحی و برنامه‌نویسی در سیستم‌عامل، با استفاده از تمایز مناسب بین لایه‌های مختلف در سیستم‌عامل تا حد زیادی قابل جبران است و طراحی لایه‌ای مانع می‌شود تا خطای به‌وجود آمده در یک لایه به سایر لایه‌ها منتشر شود.

[57] Answer To Reset

- نظارت بر انتقال داده‌ها،

در کارت هوشمند، تمامی ارتباطات ورودی و خروجی باید توسط سیستم‌عامل نظارت شوند تا از دسترسی غیرمجاز جلوگیری شود. همچنین در لایه انتقال اطلاعات، تمامی ورودی‌های غیرمجاز باید در نظر گرفته شوند تا از طریق دستکاری بلوک‌های داده‌ای منتقل شده به کارت، نتوان اطلاعات محرمانه کارت را استخراج کرد.

- استفاده از checksum برای محتوای با اهمیت در حافظه،

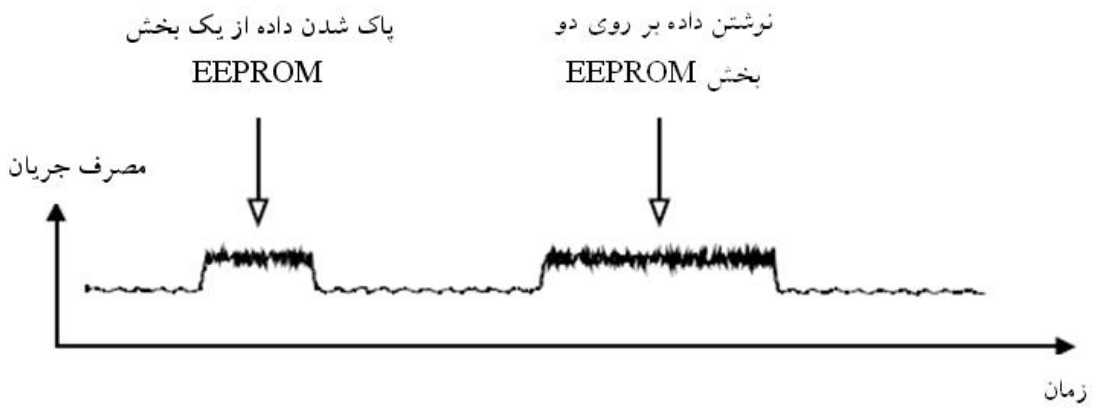
با استفاده از این روش می‌توان از تغییرات ناخواسته محتویات حافظه مطلع شد. همچنین قبل از دسترسی یا اجرای برنامه از روی حافظه، باید معتبر بودن checksum مورد بررسی قرار گیرد.

- پنهان‌سازی برنامه‌های کاربردی،

بدینوسیله سیستم‌عامل می‌تواند یک DF[58] را که شامل برنامه‌های کاربردی و فایل‌های مربوطه است، پنهان کند به صورتی که برنامه‌های مختلف نسبت به هم ایزوله شوند. البته در صورتی که یک واحد مدیریت حافظه در سخت‌افزار موجود باشد، برنامه‌ها را می‌توان به صورت کامل از هم ایزوله کرد.

- مخفی‌نگه داشتن فعالیت‌های سیستم‌عامل

در هنگام نوشتن بر روی EEPROM، پمپ شارژ داخل تراشه باید فعال شود تا جریان مصرفی تراشه افزایش پیدا کند. این کار باعث می‌شود تا حمله کننده نتواند از روی جریان مصرفی تراشه، به عملکرد آن پی ببرد. در شکل ۱۳ میزان جریان مصرفی تراشه را در صورت استفاده از پمپ شارژ نشان می‌دهد.



شکل ۱۳: تصویر میزان جریان مصرفی تراشه در هنگام استفاده از پمپ شارژ

[58] Dedicated Files

- استفاده از شرایط دسترسی به صورت شی‌گرا،

در گذشته نرم‌افزارهای کاربردی در کارت هوشمند بر اساس یک مکانیسم دسترسی با مدیریت متمرکز بنا شده بودند که باعث می‌شد تا خطاهای حافظه یا یک نرم‌افزار، امنیت کلی کارت هوشمند را تحت تاثیر قرار دهد. در صورتی که در سیستم‌های نوین مدیریت فایل به صورت شی‌گرا، شرایط دسترسی در فایل‌های جداگانه ذخیره می‌شود و در صورت وقوع خطا در حافظه، تنها یک فایل تحت ثاتیر قرار می‌گیرد.

- غیرفعال‌سازی کارت هوشمند،

سیستم‌عامل باید بتواند کارت هوشمند را در انتهای چرخه حیات کارت، به صورت کامل غیرفعال کند تا تحلیل نرم‌افزاری کارت‌های از رده خارج شده که از لحاظ فیزیکی سالم هستند، امکان پذیر نگردد.

- مولد اعداد تصادفی،

در تایید هویت از اعداد تصادفی برای تمیز دادن جلسات از یکدیگر مورد استفاده می‌شود. هر جلسه باید نسبت به جلسات قبلی و بعدی متفاوت باشد تا از اطلاعات به‌دست آمده از جلسات گذشته نتوان برای تکرار داده‌ها استفاده کرد. یک روش دیگر حمله درخواست تعداد زیادی عدد تصادفی از کارت است تا از اطلاعات جمع شده بتوان ترتیب اعداد را پیش‌بینی کرد یا درخواست اعداد تصادفی را آنقدر ادامه داد تا حافظه EEPROM کارت پر شود و یک عدد به صورت متوالی تکرار گردد.[2]

۱۰. استانداردهای کارت هوشمند

۱۰.۱. استاندارد ISO7810

استاندارد ISO 7810 یک استاندارد بین‌المللی است که برای تعریف ابعاد و مشخصات فیزیکی کارت‌های هوشمند مورد استفاده قرار می‌گیرد. این استاندارد چهار قالب برای کارت‌های شناسایی تعریف می‌کند که عبارتند از: ID-1، ID-2، ID-3 و ID-000.

- ID-1: فرمت ID-1، اندازه کارت را برابر با 85.60*53.60 mm تعریف می‌کند و عموماً برای کارت‌های بانکی و ATM از این قالب استفاده می‌شود. همچنین در بسیاری از کشورها برای کارت گواهینامه نیز از این قالب استفاده می‌شود. نسبت طول به عرض در این قالب تقریباً برابر با نسبت عدد طلایی (1.618:1) در نظر گرفته شده است. استانداردهای ISO 7811، ISO 7813 و ISO7816 بر پایه این قالب تعریف شده‌اند.
- ID-2: اندازه کارت در فرمت ID-2 برابر با 74 mm * 105 است. این قالب فضای بیشتری برای نمایش عکس فراهم می‌کند، طوری که کاملاً قابل شناسایی باشد ولی با این وجود هنوز به اندازه‌ای کوچک است که بتوان آن را در کیف پول جای داد.
- ID-3: اندازه کارت در فرمت ID-3 برابر با 88 mm * 125 است و عموماً برای ویزا و پاسپورت مورد استفاده قرار می‌گیرد.

- ID-000: اندازه کارت در فرمت ID-000 برابر با 15 mm * 25 تعریف می‌کند که برای سیم‌کارت‌ها مورد استفاده قرار می‌گیرد.[1]

۱۰.۲. استاندارد ISO7816-x

استاندارد ISO7816-x تکمیل شده استاندارد ISO 7810 بوده و شامل اجزای زیر است:

۱. 7816-1: مشخصات فیزیکی,
۲. 7816-2: کارت‌های تماسی – مشخصات و محل قرارگیری اتصالات,
۳. 7816-3: مشخصات الکتریکی و نشان دادن کلاس‌ها برای مدارهای مجتمع کارت‌هایی که با ولتاژهای ۵ ولت، ۳ ولت و ۱/۵ ولت کار می‌کنند,
۴. 7816-4: سازمان، امنیت و دستورات تبادلی,
۵. 7816-5: نحوه ثبت کردن سازندگان برنامه‌های کاربردی,
۶. 7816-6: المان‌های داده‌ای مبادله‌ای بین صنایع,
۷. 7816-7: فرمان‌های میان صنعتی برای زبان پرسجوی ساختیافته کارت (SCQL),
۸. 7816-8: فرمان‌های عملیات امنیتی,
۹. 7816-9: فرمان‌های مدیریتی کارت,
۱۰. 7816-10: سیگنال‌های الکترونیکی و پاسخ فرمان بازنشانی (ATR) برای کارت‌های سنکرون,
۱۱. 7816-11: تصدیق هویت با استفاده از روش‌های بیومتریک,
۱۲. 7816-12: کارت‌های تماسی واسط الکتریکی USB و رویه‌های عملیاتی,
۱۳. 7816-13: فرمان‌های مدیریت برنامه‌های کاربری در محیط‌های چند منظوره,
۱۴. 7816-15: برنامه کاربردی اطلاعات رمزنگاری.

استاندارد ISO 7816-1: مشخصات فیزیکی

استاندارد ISO 7816-1 مشخصات فیزیکی کارت را در مواردی از قبیل ابعاد، تشعشعات الکترومغناطیسی، تنش مکانیکی، محل قرارگیری تراشه مجتمع در کارت، محل قرار گرفتن نوار مغناطیسی و مقاومت در برابر الکتریسیته ساکن تعریف می‌کند.

استاندارد ISO 7816-2: مشخصات و محل قرارگیری اتصالات

استاندارد ISO 7816-2 محل و ابعاد دقیق نقاط اتصال را در کارت‌های تماسی مشخص می‌کند. همچنین در این بخش محل قرارگیری و مشخصات الکتریکی هر یک از اتصالات فلزی کارت تعریف می‌شود.

استاندارد ISO 7816-3: مشخصات و محل قرارگیری اتصالات

در این بخش از استاندارد ۷۸۱۶، میزان توان، ساختارهای سیگنال و اطلاعات مبادله شده بین کارت‌های تراشه‌دار و ادوات واسطه مثل ترمینال کارت برای مدارهای مجتمعی که با ولتاژهای ۵ ولت، ۳ ولت و ۱/۵ ولت کار می‌کنند، تعریف می‌شود. همچنین سرعت سیگنال‌ها، سطوح ولتاژ و مقادیر جریان، محاسبه پریتی[۵۹]، روال عملکردی و مکانسیم‌های ارتباطی و مخابراتی مشخص می‌شود.

استاندارد ISO 7816-4: سازمان، امنیت و دستورات تبادلی

مسأله امنیت در استاندارد ISO 7816-4 به دو بخش "امنیت کارت" و "امنیت پیام" تقسیم می‌شود. بخش اول اقدامات و ساختارهای طراحی شده برای محافظت از اطلاعات ذخیره شده در کارت را پوشش می‌دهد. بخش دوم روی محافظت پیام‌ها از کارت و به کارت، تمرکز می‌کند و شامل رمزنگاری، بررسی صحت داده و مخفی نمودن داده‌ها می‌شود. این استاندارد در مورد نحوه پیاده‌سازی داخلی کارت با دنیای خارج، بحث نمی‌کند و مستقل از واسطه فیزیکی کارت است و فقط در مورد واسطه‌ها بحث می‌کند.

این استاندارد موارد زیر را مشخص می‌کند:

- محتویات زوج دستورات و پاسخ‌های تبادلی با دستگاه واسط,
- روش‌های دسترسی به اجزا و اشیاء داده‌ای درون کارت,
- روش‌های دسترسی به فایل‌ها و داده‌های دورن کارت,
- ساختار و محتویات بایت‌هایی که برای نگهداری سابقه عملکرد کارت مورد استفاده قرار می‌گیرند,
- ساختار برنامه‌های کاربردی و داده‌های موجود در کارت به آن صورت که از طرف واسطه در هنگام پردازش دستورات مشاهده می‌شوند,
- ساختار امنیتی برای تعریف سطوح دسترسی به فایل‌ها و داده‌های موجود در کارت,
- روش‌ها و مکانیسم‌های موجود برای مشخص کردن و آدرس‌دهی برنامه‌های کاربردی در کارت هوشمند,
- روش‌های تبادل پیغام به صورت امن,
- روش‌های دسترسی برای الگوریتم‌های مورد استفاده در کارت.

استاندارد ISO 7816-5: نحوه ثبت کردن سازندگان برنامه‌های کاربردی

در این بخش یک سیستم شماره‌گذاری برای شناسه نرم‌افزارهای کاربردی و روندی برای ثبت شناسه فراهم‌کنندگان تعریف می‌شود. شناسه برنامه (AID) برای آدرس‌دهی یک برنامه کاربردی در کارت مورد استفاده قرار می‌گیرد. این بخش از استاندارد، نحوه کدینگ[۶۰] شناسه برنامه را همزمان با روش‌هایی برای آدرس‌دهی اجزای آن در داخل کارت مشخص می‌کند.

[59] Parity

[60] Coding

این استاندارد مشخص می‌کند که چگونه شناسه‌های نرم‌افزاری یکتا را بوسیله ثبت قسمتی از شناسه به صورت بین‌المللی تعریف کرد و موارد زیر را در بر می‌گیرد:

- فرایند ثبت کردن،
- مسئولین درگیر این فرآیند،
- موجود بودن انطباقی بین بخش‌های ثبت شده توسط شناسه و فراهم‌کنندگان برنامه‌های کاربردی مربوطه.

استاندارد ISO 7816-6: المان‌های داده‌ای مبادله‌ای بین صنایع

در استاندارد ISO 7816-6 المان‌های داده‌ای (DEs) که برای تبادلات بین صنعتی مبتنی بر ICCهای تماسی و غیرتماسی مورد استفاده قرار گیرند، تعریف شده‌اند. این ICCها ممکن است برای عملیات رمزنگاری هم مورد استفاده قرار بگیرد. در این قسمت شناسه، نام، توصیف، قالب، کدینگ و چینش هر DE و روش‌های بازیابی آن در کارت، تعریف شده است.

در این استاندارد نحوه پیاده‌سازی داخلی یا خارجی المان‌های داده‌ای آورده نشده است.

استاندارد ISO7816-7: فرمان‌های میان صنعتی برای زبان پرس‌وجوی ساخت‌یافته کارت[۶۱]

در استاندارد ISO 7816-7 پارامترهای مورد نیاز برای کارت‌های هوشمند تماسی جهت استفاده در مبادلات بین‌المللی تعریف شده است. از این کارت‌های شناسایی برای تبادل اطلاعات مذاکره شده بین کارت و دنیای خارج استفاده می‌شود و طی این عمل، کارت اطلاعات مورد نیاز را فراهم می‌کند (نتایج محاسباتی، داده ذخیره شده) یا محتویاتش را تغییر می‌دهد (ذخیره کردن اطلاعات، به خاطر سپردن رویدادها).

استاندارد ISO 7816-8: فرمان‌های عملیات امنیتی

در استاندارد ISO 7816-8، دستورات بین صنعتی که برای عملیات رمزنگاری در کارت‌های تماسی یا غیر تماسی مورد استفاده قرار می‌گیرند، تعریف می‌شوند. این دستورات تمامی چرخه حیات کارت را پوشش می‌دهند و بعضی قبل از صادر شدن و بعضی در زمان استفاده و بعضی بعد از دوره انقضای کارت مورد استفاده قرار می‌گیرند.

[61] SCQL

همچنین در این استاندارد پیوست‌هایی به عنوان مثال جهت عملیات مرتبط با امضای دیجیتال، گواهی‌ها و وارد کردن و صادر کردن کلیدهای نامتقارن آورده شده است. انتخاب و شرایط استفاده از مکانیسم‌های رمزنگاری ممکن است قابلیت صدور کارت را تحت تاثیر قرار دهند ولی در این استاندارد در این مورد بحث نشده است.

استاندارد 9-7816: فرمان‌های مدیریتی کارت

در استاندارد 9-7816 فرامین بین صنعتی برای کارت‌های هوشمند تماسی و غیرتماسی جهت مدیریت کارت مانند ساختن یا پاک کردن فایل‌ها، مورد استفاده قرار می‌گیرد. این فرامین تمامی چرخه حیات کارت را در برمی‌گیرند و بنابراین بعضی از این فرمان‌ها ممکن است قبل از صدور کارت یا بعد از انقضای کارت مورد استفاده قرار گیرند.

یک پیوست در این استاندارد فراهم شده است تا نحوه کنترل ذخیره اطلاعات در داخل کارت را (بارگذاری به صورت امن)، با استفاده از بررسی سطوح دسترسی موجودیت بارگذار کننده و محافظت از داده‌ها به وسیله پیغام‌رسانی امن نشان دهد. اطلاعات بارگذاری شده ممکن است به عنوان مثال محتوی کد، کلید یا برنامک‌ها باشد.

استاندارد 10-7816: سیگنال‌های الکترونیکی و پاسخ فرمان بازنشانی برای کارت‌های سنکرون

استاندارد 10-7816 توان ساختار سیگنال و ساختار ATR را بین یک کارت هوشمند با ارتباط سنکرون و یک دستگاه واسط مانند مانند ترمینال مشخص می‌کند.

استاندارد 11-7816: تصدیق هویت با استفاده از روش‌های بیومتریک

استاندارد 11-7816 دستوارت بین صنعتی برای تصدیق اصالت فردی با استفاده از روش‌های بیومتریک را در کارت‌های هوشمند مشخص می‌کند. دستورات مورد استفاده در استاندارد 4-7816 تعریف شده اند. همچنین قسمتی از اشیاء داده‌ای مورد استفاده از ISO/IEC 19785-1 استخراج شده‌اند. همچنین این استاندارد مثال‌هایی برای ثبت کردن[۶۲] و تصدیق کردن[۶۳] ارائه می‌کند و مسایل امنیتی را نشان می‌دهد.

[62] Enrollment

[63] Verification

استاندارد 12-7816: کارت‌های تماسی – واسط الکتریکی USB و رویه‌های عملیاتی

استاندارد 12-7816 شرایط عملیاتی یک کارت هوشمند را که از واسط USB استفاده می‌کند تعریف می‌کند. کارت هوشمندی که از واسط USB استفاده می‌کند، USB-ICC نامیده می‌شود. استاندارد 12-7816 موارد زیر را مشخص می‌کند:

- شرایط الکتریکی هنگامی که یک USB-ICC در یک دستگاه واسط مورد استفاده قرار می‌گیرد. برای اتصالاتی که هنگام استفاده از واسط USB مورد استفاده قرار نمی‌گیرند.
- مشخصات استاندارد USB و مشخصه ویژه کلاس USB-ICC,
- تبادل اطلاعات بین میزبان و USB-ICC با استفاده از تبادلات حجیم[۶۴] یا تبادلات کنترلی[۶۵] ,
- تبادلات کنترلی که از دو پروتکل متفاوت با نام‌های نسخه A و نسخه B استفاده می‌کند,
- تبادلات وقفه‌ای (اختیاری) برای مشخص کردن رویدادهای آسنکرون,
- حالت و شرایط خطا.

این استاندارد دو پروتکل را برای تبادلات کنترلی فراهم می‌کند. این عمل به منظور حمایت از پروتکل T=0 (نسخه A) یا تبادلات در سطح APDU (نسخه B) صورت گرفته است. این استاندارد در USB-ICC برای هر یک از تبادلات یک ماشین حالت فراهم می‌کند (تبادلات حجیم، تبادلات کنترلی نسخه A و نسخه B). نمونه‌هایی از ترتیب‌های احتمالی که USB-ICC باید بتواند اداره کند در پیوست استاندارد 12-7816 آورده شده است.

استاندارد 13-7816: فرمان‌های مدیریت برنامه‌های کاربری در محیط‌های چند منظوره

استاندارد 13-7816 همچنان در حال توسعه است و بنا است که روش‌هایی از استاندارد[۶۶] را مانند پروتکل‌های کانال امن[۶۷]، با یکدیگر مجتمع کند.

استاندارد 15-7816: برنامه کاربردی اطلاعات رمزنگاری

این استاندارد یک برنامه کاربردی در کارت هوشمند را تعریف می‌کند.این برنامه اطلاعاتی در مورد عملکرد رمزنگاری را شامل می‌شود. همچنین این استاندارد یک شکل مشترک گرامری و قالب اطلاعات رمزنگاری و اطلاعات و مکانیسم‌های به اشتراک گذاری این اطلاعات در زمان مناسب را تعریف می‌کند. این استاندارد قابلیت‌های زیر را در بر می‌گیرد:[1]

[64] Bulk Transfers

[65] Control Transfers

[66] Global Platform

[67] Secure Channel Protocols

- ذخیره کردن چند نمونه از اطلاعات رمزنگاری در داخل یک کارت،
- استفاده از اطلاعات رمزنگاری،
- بازیابی اطلاعات رمزنگاری،
- ارجاع میانی به اطلاعات رمزنگاری بواسطه DOهای تعریف شده در زمان لزوم،
- روش‌های متفاوت تصدیق اصالت.

۱۰.۳. استاندارد EMV

EMV استانداردی است که به منظور سازگاری میان کارت‌های IC دار و پایانه‌های POS سازگار با IC و ATM و برای تصدیق اصالت پرداخت بوسیله کارت‌های اعتباری و نقدی به کار می‌رود و نام آن برگرفته از سه حرف اولیه Europay، MasterCard و VISA می‌باشد که در ابتدا برای توسعه این استاندارد با هم همکاری کردند. این استاندارد تبادلات در سطح فیزیکی، الکتریکی، داده و برنامه کاربردی را بین کارت‌های IC دار و ادوات پردازنده آنها را جهت تراکنش‌های مالی تعریف می‌کند. بخش‌هایی از این استاندارد کاملاً بر مبنای واسط کارت IC دار که در استاندارد ۷۸۱۶ موجود است تعریف شده است. کارت‌های مبتنی بر این استاندارد "Chip and PIN" و "IC Credit" هم نامیده می‌شوند. دو نمونه معروف پیاده‌سازی EMV عبارتند از SDV – VISA و MChip – MasterCard.

MasterCard یک برنامه تصدیق اصالت تراشه (CAP) برای تجارت الکترونیکی امن دارد که با نام EMV-CAP شناخته می‌شود.

هدف و انگیزه استفاده از EMV، سازگاری میان انواع کارت‌های مبتنی بر EMV با پایانه‌های پرداخت بوسیله کارت اعتباری در سراسر دنیاست که این کار بوسیله تعریف API سطح بالا میان کارت و پایانه صورت می‌پذیرد و باعث کاهش هزینه و زمان مورد نیاز جهت تولید نرم‌افزارهای مورد نیاز می‌شود.

نسخه اولیه EMV در سال ۱۹۹۹ انتشار پیدا کرد و در حال حاضر این استاندارد توسط EMVCo تعریف و مدیریت می‌شود و گواهی سازگاری با این استاندارد توسط این شرکت بعد از بررسی نتایج بررسی‌های انجام شده توسط یک آزمایشگاه معتبر، صادر می‌شود. بعد از پذیرفته شدن در آزمایش‌های مشترک EMVCo، نرم‌افزار باید برای سازگاری با EMV بررسی شود.[1]

۱۰.۳.۱ فهرست مستندات و استانداردهای EMV

Book1: از ICC مستقل از برنامه کاربردی تا نیازمندی‌های واسط پایانه

Book2: امنیت و مدیریت کلید

Book3: مشخصات برنامه‌های کاربردی

Book4: ملزومات دارنده، حمل کننده و فراهم کننده کارت

٤.١٠. استاندارد FIPS 140-1, -2

استاندارد FIPS نیازمندی‌های امنیتی مورد نیاز یک ماژول رمزنگاری را که برای حفاظت از اطلاعات با ارزش به کار می‌رود، تعریف می‌کند. این استاندارد چهار سطح امنیتی را بر اساس سطوح کیفی امنیتی تعریف می‌کند که عبارتند: سطح ۱، ۲، ۳ و ۴. این چهار سطح، بخش نسبتاً وسیعی از برنامه‌های کاربردی و انواع محیط‌هایی را که ماژول‌های رمزنگاری در آنها مورد استفاده قرار می‌گیرند، پوشش می‌دهد. نیازهای امنیتی سطوح مربوط به طراحی به صورت امن و مسائل مربوط به پیاده‌سازی ماژول‌های رمزنگاری را پوشش می‌دهد و شامل مواردی از قبیل مشخصات ماژول رمزنگاری، درگاه‌ها و واسطه‌های ماژول رمزنگاری، نقش‌ها، سرویس‌ها و تصدیق اصالت، مدل حالت محدود[68]، امنیت فیزیکی، محیط عملیاتی، مدیریت کلیدهای رمزنگاری، تداخل/سازگاری مغناطیسی (EMI/EMC)، تست‌های توسط خود دستگاه، اطمینان از طراحی و نهایتاً مقابله جهت رسیدن حداقل خسارت در برابر سایر حملات را پوشش می‌دهد.

البته سازگاری با این استاندارد برای اطمینان از امنیت فراهم شده برای ماژول مورد نظر کافی نیست و کاربر ماژول رمزنگاری مسئول است تا از انطباق امنیت فراهم شده توسط ماژول رمزنگاری با نیازمندی‌های امنیتی مورد نظر صاحب اطلاعات، اطمینان حاصل کند. همانطور که استفاده از یک ماژول رمزنگاری معتبر امنیت کل سیستم را تامین نمی‌کند، اطمینان از امنیت ماژول رمزنگاری نیز امنیت کل سیستم را تضمین نخواهد کرد.

- امنیت سطح ۱،

این سطح، پایین‌ترین سطح امنیتی را دارا است و در آن نیازمندی‌های پایه‌ای امنیتی برای یک ماژول رمزنگاری تعریف می‌شود. در این سطح، هیچ مکانیسم مشخصی برای امنیت فیزیکی ماژول رمزنگاری در نظر گرفته نمی‌شود. امنیت سطح ۱ اجازه می‌دهد که مولفه‌های نرم‌افزار و سفت‌افزار[69] در یک ماژول رمزنگاری، تحت یک سیستم محاسباتی همه منظوره و یک سیستم‌عامل ارزیابی نشده اجرا شوند. این گونه پیاده‌سازی‌ها برای برنامه‌های کاربردی با نیازمندی‌های امنیتی محدود و در شرایطی که سایر روش‌های نظارتی مانند امنیت فیزیکی، امنیت شبکه، روال‌های مدیریتی وجود ندارند و یا در سطح محدودی وجود دارند، مناسب است. در این گونه موارد ممکن است پیاده‌سازی‌های نرم‌افزاری الگوریتم‌های رمزنگاری، از معادل سخت‌افزاری آنها به صرفه‌تر باشد.

- امنیت سطح ۲،

امنیت سطح ۲، مکانیسم حفاظت فیزیکی ماژول رمزنگاری را با افزودن قابلیت تشخیص دستکاری[70] ارتقاء می‌دهد.این امنیت شامل روکش یا قفل‌های آشکارساز دستکاری و ... است. این پوشش‌ها طوری روی ماژول رمزنگاری قرار می‌گیرند که برای دسترسی فیزیکی به کلیدهای رمزنگاری یا پارامترهای امنیتی حساس (CSP[71]) ماژول، باید آنها را شکست یا ازبین برد.

[68] Finite Sate Model

[69] Firmware

[70] Tamper Evident

[71] Critical Security Parameters

امنیت سطح ۲ اجازه می‌دهد تا مولفه‌های نرم‌افزار و سخت‌افزار یک ماژول رمزنگاری بر روی یک سخت‌افزار همه منظوره اجرا شود. البته سیستم‌عامل مورد استفاده باید با پروفایل محافظتی مربوط به معیار مشترک که در پیوست B استاندارد موجود است، سازگار باشد و حداقل دارای سطح اطمینان EAL2 یا بیشتر باشد.

یک سیستم‌عامل مورد اطمینان، سطحی از امنیت را فراهم می‌کند که ماژول‌های امنیتی که بر روی سیستم‌های همه منظوره مورد استفاده قرار می‌گیرند را با سیستم‌های سخت‌افزاری اختصاصی قابل مقایسه می‌سازد.

- امنیت سطح ۳،

در سطح امنیتی علاوه بر موارد در نظر گرفته شده در سطح ۲، امنیت فیزیکی در سطحی مورد نیاز است که از دسترسی فرد نفوذگر به اطلاعات حساس پارامترهای رمزنگاری(CSP) موجود در ماژول رمزنگاری جلوگیری به عمل آید. در این سطح، باید بتوان با احتمال بالا، عمل نفوذ در سطح فیزیکی را تشخیص داد و نسبت به آن عکس‌العمل نشان داد مانند صفر کردن تمامی اطلاعات رمز نشده CSP که در ماژول قرار دارند.

همچنین امنیت سطح ۳ نیازمند تصدیق اصالت هویت-محور[۷۲] است که نسبت به تصدیق اصالت نقش-محور[۷۳] بهبود یافته است. همچنین برای رسیدن به این سطح از امنیت، تمامی ورودی و خروجی‌های CSPهای رمز نشده باید از طریق درگاه‌هایی صورت پذیرد که از لحاظ فیزیکی، از سایر درگاه‌ها یا واسطه‌هایی که به صورت منطقی از سایر واسطه‌ها بواسطه یک مسیر اطمینان[۷۴] جدا شده‌اند، مجزا باشد. CSP ها ممکن است به صورت رمز شده یا رمز نشده وارد یا خارج شوند. همچنین سطح امنیتی ۳ اجازه می‌دهد که مولفه‌های نرم‌افزار و سفت‌افزار تحت یک سخت‌افزار همه منظوره اجرا شوند ولی باید از سیستم‌عاملی استفاده شود که علاوه بر سازگاری با PPهای ارائه شده در پیوست B، با نیازمندی‌های عملکردی مسیر اطمینان ارائه شده در FTP_TRP.1 سازگار باشد و همچنین با معیار ارزیابی EAL3 در معیار مشترک (یا بیشتر) و همچنین نیازمندی اطمینان پذیری اضافی مدل سیاستگذاری امنیتی یک هدف ارزیابی غیر فرمال یا(ADV_SPM.1) informal Target of Evaluation سازگار باشد.

پیاده‌سازی مسیر اطمینان، CSP های رمز نشده و نرم‌افزار و سفت‌افزارهای ماژول امنیتی را از دسترسی نرم‌افزارها یا سفت‌افزارهای ناامنی که ممکن است بر روی سیستم اجرا شوند، محافظت می‌کند.

- امنیت سطح ۴،

امنیت سطح ۴ بیشترین سطح امنیت را در این استاندارد فراهم می‌کند و مناسب استفاده در محیط‌های غیر محافظت شده هستند. این سطح امنیتی علاوه بر تامین نیازهای امنیتی سطح ۳، از افشای امنیتی ماژول رمزنگاری در برابر شرایط و نوسانات محیطی در خارج محدوده عملکردی عادی ماژول، جلوگیری می‌کند. برای این منظور، ماژول باید نوسانات خارجی را تشخیص دهد و CSP ها را صفر کند.

[72] Identity-Based

[73] Role-Based

[74] Trust Path

در سطح امنیتی ۴، مولفه‌های سفت‌افزار و نرم‌افزاری می‌توانند بر روی یک سیستم محاسباتی همه منظوره مورد استفاده قرار گیرند ولی سیستم‌عامل مورد استفاده باید علاوه بر تامین نیازمندی‌های امنیتی مطرح شده در سطح ۳، با معیار مشترک سطح اطمینان EAL4 یا بیشتر ارزیابی شود.[1]

۱۰.٤.۱ اهداف امنیتی کارکردی

نیازهای امنیتی مورد نیاز برای ماژول رمزنگاری از اهداف امنیتی کارکردی سطح بالای زیر استخراج می‌شوند که عبارتند از:[1]

- به‌کار گیری و پیاده‌سازی صحیح توابع امنیتی تایید شده برای حفاظت از داده‌های حساس،
- حفاظت از ماژول رمزنگاری در برابر عملیات یا استفاده غیر مجاز،
- حفاظت در برابر افشای غیر مجاز محتویات ماژول رمزنگاری که شامل کلیدهای رمزنگاری رمز نشده و CSP ها است.

محافظت در برابر تغییرات غیرمجاز و غیرمحسوس ماژول رمزنگاری که شامل مواردی از قبیل تغییر غیرمجاز، جایزنی وارد کردن و یا پاک کردن کلیدهای رمزنگاری و CSPها است،

نشان دادن حالت عملیاتی ماژول رمزنگاری،

اطمینان از عملکرد صحیح ماژول رمزنگاری در حالت عملکرد در شرایط تایید شده،

کشف خطا در عملکرد ماژول رمزنگاری و جلوگیری از افشای اطلاعات حساس و CSPها به علت این خطاها.

۱۰.٤.۲ نیازمندی‌های امنیتی

در این بخش نیازمندی‌های امنیتی ماژول‌های رمزنگاری برای سازگاری با این استاندارد در حوزه‌های طراحی و پیاده‌سازی، آورده شده‌اند که شامل مواردی از قبیل مشخصات ماژول رمزنگاری، درگاه‌ها و واسطه‌های ماژول رمزنگاری، نقش‌ها، سرویس‌ها و تصدیق اصالت، مدل حالت محدود، امنیت فیزیکی، محیط‌های عملیاتی، مدیریت کلیدهای رمزنگاری، تداخل و سازگاری مغناطیسی، تست کردن خود۷۵ و اطمینان از طراحی است. کاهش خطر در برابر سایر حملات هنوز تست نشده است ولی فراهم کننده باید کنترل‌های اعمال شده را مستند کند (مانند حمله تحلیل توان تفاضلی یا TEMPEST). خلاصه این ملزومات امنیتی در جدول ۱ آورده شده است.[1]

[75] Self-Test

	سطح ۱ امنیتی	سطح ۲ امنیتی	سطح ۳ امنیتی	سطح ۴ امنیتی
مشخصات ماژول رمزنگاری	مشخصات ماژول رمزنگاری، محدودیت‌های رمزنگاری، الگوریتم‌های تایید شده، حالات تصدیق شده عملکرد. توصیف عملکرد ماژول رمزنگاری شامل شامل تمامی مولفه‌های سخت‌افزار، نرم‌افزار و سفت‌افزار، شرح سیاست امنیتی ماژول			
درگاه‌ها و واسطه‌های ماژول رمزنگاری	مشخصات تمامی واسطه‌ها و تمامی مسیرهای ورود و خروج اطلاعات		درگاه‌های اطلاعات برای پارمترهای محافظت نشده حساس امنیتی به طور فیزیکی یا منطقی از سایر درگاه‌های داده‌ای مجزا باشد.	
نقش‌ها، سرویس‌ها و تصدیق اصالت	جداسازی منطقی نقش‌ها و سرویس‌های الزامی و اختیاری	تصدیق اصالت کاربر به صورت نقش-محور یا هویت محور	تصدیق اصالت کاربر به صورت هویت-محور	
مدل حالت محدود	مشخصات مدل حالت محدود. حالات الزامی و اختیاری، دیاگرام حالات گذرا و مشخصات گذار حالات			
امنیت فیزیکی	تجهیزات در سطح محصول	قفل‌ها و آشکارسازی دستکاری	تشخیص دستکاری و واکنش متقابل برای پوشش‌ها و درها	تشخیص دستکاری و بسته پاسخ، EFP یا EFT
محیط‌های عملیاتی	یک کاربر، کد قابل اجرا، روش بررسی صحت تصدیق شده	PP های مرجع بایستی با EAL2 ارزیابی شده باشند با مکانیسم‌های کنترل دسترسی و بازبینی	PP های مرجع بایستی با EAL3 ارزیابی شده باشند به‌علاوه مدلسازی سیاست‌های امنیتی	PPهای مرجع بعلاوه مسیرهای اعتماد بایستی در سطح EAL4 ارزیابی شده باشند.
مدیریت کلیدهای رمزنگاری	مکانسیم‌های مدیریت کلید: اعداد تصادفی، تولید کلید، استقرار کلید، توزیع کلید، رورود/خروج، ذخیره سازی و صفر کردن کلید			
	رمز و کلیدها خصوصی که به صورت دستی استقرار پیدا کرده‌اند ممکن است به صورت رمز نشده وارد یا خارج شوند.		رمز و کلیدها خصوصی که به صورت دستی استقرار پیدا کرده‌اند ممکن است به صورت رمز نشده وارد یا خارج شوند.	
تداخل و سازگاری مغناطیسی	سازگار با 47CFR FCC بخش ۱۵، قسمت B کلاس A (استفاده تجاری)		سازگار با 47CFR FCC بخش ۱۵، قسمت B کلاس B (استفاده خانگی)	

	سطح ۱ امنیتی	سطح ۲ امنیتی	سطح ۳ امنیتی	سطح ۴ امنیتی
تست کردن خود	تست زمان روشن شدن، تست الگوریتم‌های رمزنگاری، تست صحت نرم‌افزار، سفت‌افزار، تست توابع حساس، تست‌های شرطی			
اطمینان از طراحی	مدیریت تنظیمات (C`M)	نصب و تولید به صورت امن، انطباق طراحی و سیاست‌ها، مستندات راهبردی	پیاده‌سازی با زبان‌های سطح بالا	مدل فرمال، شرح جرئی (اثبات غیر فرمال)، پیش شرط‌ها و پس شرط‌ها
کاهش خطر در برابر سایر حملات	مشخصات پیشگیری در برابر حمله‌هایی که در حال حاضر نیازمندی‌های امنیتی در دسترسی ندارند.			

شکل ۱۴: جدول۱- خلاصه نیازمندی‌های امنیتی

یک ماژول رمزنگاری برای تمامی نیازمندی‌های امنیتی، امتیاز و توضیحات جداگانه‌ای دریافت می‌کند و علاوه بر آن یک امتیاز سراسری کسب می‌کند که مشخص کنند حداقل امتیاز کسب شده در حوزه‌های مستقل است.

۱۰.٤.۳ مشخصات ماژول رمزنگاری

در سطوح امنیتی ۱ و ۲ ممکن است سیاست امنیتی در ماژول رمزنگاری، زمان عملکرد ماژول در حالت تایید شده را مشخص کند ولی سطوح امنیتی ۳ و ۴، یک ماژول رمزنگاری، انتخاب عملکرد در حالت تایید شده را مشخص می‌کند.

مستندات زیر برای تمامی سخت‌افزار، نرم‌افزار و سفت‌افزارهای ویژه امنیت در ماژول رمزنگاری الزامی است:

- مستند مشخص کننده مولفه‌های سخت‌افزار، نرم‌افزار و سفت‌افزار موجود در ماژول رمزنگاری و محدوده این مولفه‌ها
- مستند مشخص کننده مولفه‌های سخت‌افزار، نرم‌افزار و سفت‌افزار موجود در ماژول رمزنگاری که از ملزومات این استاندارد مستثنی شده‌اند و منطق علت این عمل.
- مستند مشخص کننده تمامی درگاه‌های فیزیکی و واسطه‌های منطقی و تمامی مسیرهای داده‌های تعریف شده در ورودی و خروجی‌های ماژول رمزنگاری.
- مستندی که در آن تمامی توابع امنیتی تایید شده و تایید نشده به کار رفته در ماژول رمزنگاری فهرست شده‌اند و تمامی حالت‌های عملیاتی تایید شده و تایید نشده را مشخص می‌کنند.
- مستندی که شامل بلوک دیاگرام تمامی اجزای اصلی سخت‌افزاری و ارتباطات بین اجزای ماژول رمزنگاری باشد که شامل تمامی ریزپردازنده‌ها، بافرهای ورودی/خروجی، محل ذخیره کردن کلید، حافظه برنامه و حافظه مورد استفاده در برنامه می‌شود.

- مستندی که شامل طرح سخت‌افزار، نرم‌افزار و سفت‌افزار ماژول رمزنگاری باشد که برای توصیف طراحی از زبان‌های توصیفی سطح بالا استفاده یا شماتیک سخت‌افزار استفاده می‌شود.
- مستندی که تمامی اطلاعات امنیتی از قبیل راز و کلیدهای خصوصی رمزنگاری، داده‌های مورد استفاده در تصدیق اصالت مانند کلمه‌های عبور و PINها، CSPها و کلیه اطلاعات تحت حفاظت (مانند رویدادها و اطلاعات ثبت شده و ...) را که افشا یا تغییر آنها، امنیت سیستم را مختل می‌کند، مشخص می‌کند.
- مستندی که سیاست‌گذاری امنیتی ماژول رمزنگاری را مشخص می‌کند که از قوانین ناشی از نیازمندی‌های استاندارد یا ملزومات اعمال شده توسط سازنده تشکیل شده است.

۱۰.٤.٤ درگاه‌ها و واسطه‌های ماژول رمزنگاری

یک ماژول رمزنگاری از چهار واسطه منطقی تشکیل شده است که عبارتند از واسط ورودی داده‌ها واسط خروجی داده‌ها واسط ورودی‌های کنترلی و واسط خروجی حالت. همچنین در صورت نداشتن تغذیه درونی، از یک درگاه توان برای ورودی توان[۷۶] استفاده می‌شود.

تمامی اطلاعات ورودی به ماژول رمزنگاری تنها باید از طریق مسیر ورودی و تمامی اطلاعات خروجی باید تنها از طریق مسیر خروجی، خارج شوند و مسیر خروجی داده‌ها باید هنگام تولید کلید و صفر کردن کلید به صورت منطقی از مدارماژول رمزنگاری مجزا باشد. در سطوح امنیتی ۱ و ۲ ممکن است درگاه‌های فیزیکی و واسطه‌های منطقی مورد استفاده در ورودی و خروجی کلیدهای رمزنگاری رمزنشده، مولفه‌های کلید رمزنگاری، داده‌های مورد استفاده در تصدیق اصالت و CSPها ممکن است به صورت فیزیکی یا منطقی با سایر درگاه‌ها یا واسطه‌های ماژول رمزنگاری مشترک باشد ولی در سطوح امنیتی ۳ و ۴، درگاه‌های فیزیکی باید به صورت فیزیکی و درگاه‌های منطقی باید به صورت منطقی از یکدیگر مجزا باشند.[1]

۱۰.٤.٥ نقش‌ها، سرویس‌ها و تصدیق اصالت

هنگامی که کلیدهای رمزنگاری و CSPها تغییر نمی‌کنند، افشا نمی‌شوند یا جایگزین نمی‌شوند، کاربر نیاز به دریافت نقش تصدیق شده ندارد. تصدیق اصالت در یک ماژول رمزنگاری به منظور تصدیق کردن کاربر برای دسترسی به ماژول و بررسی مجاز بودن کاربر برای دریافت نقش مورد نظر انجام سرویس مربوط به نقش مورد نظر است.

یک ماژول رمزنگاری باید از سه نقش کاربر[۷۷]، مدیر رمزنگاری[۷۸] و نگهداری[۷۹] حمایت کند. کاربر می‌تواند از سرویس‌های عمومی رمزنگاری و سایر توابع امنیتی تصدیق شده استفاده نماید. مدیر رمزنگاری می‌تواند عملیات مربوط به دادن مقادیر

[76] Power Port

[77] User Role

[78] Crypto Officer Role

[79] Maintenance Role

اولیه در رمزنگاری یا اعمال مدیریتی مانند وارد کردن یا خارج کردن کلیدهای رمزنگاری، CSPها و ... را اجرا نماید. مسئول نگهداری می‌تواند سرویس‌های مربوط به نگهداری فیزیکی یا منطقی را اجرا نماید که با ورود به این حالت و هنگام خروج از آن، تمامی کلیدهای خصوصی و رازهای رمز نشده و CSPهای محافظت شده، صفر می‌شوند. البته ممکن است ماژول رمزنگاری از نقش‌های دیگری هم علاوه بر سه نقش فوق حمایت کند که در این صورت این نقش‌ها باید در مستندات آورده شوند.

یک ماژول رمزنگاری برای کابران سه سرویس نشان دادن حالت ماژول رمزنگاری، اجرای تست ماژول توسط خود ماژول و اجرای دستورات تایید شده را فراهم می‌کند.

مستندات باید مواردی از قبیل: سرویس‌ها، عملیات یا توابع فراهم شده توسط ماژول رمزنگاری (تصدیق شده یا نشده) ورودی‌ها و خروجی‌های مربوط به هر سرویس و نقش تایید شده مورد نیاز برای اجرای سرویس و سرویس‌های فراهم شده توسط ماژول رمزنگاری که نیاز به نقش تصدیق شده ندارند و چگونگی عدم تغییر، افشا و یا جایگزینی کلیدهای رمزنگاری و CSPها توسط این سرویس‌ها باشند.

یک ماژول برای تصدیق اصالت کاربر می‌تواند از دو روش تصدیق اصالت نقش محور[۸۰] یا روش تصدیق اصالت هویت محور استفاده کند. همچنین ممکن است یک ماژول رمزنگاری به یک کاربر تصدیق اصالت شده برای یک نقش، اجازه اجرای تمامی سرویس‌های مربوط به آن نقش را بدهد یا ممکن است کاربر برای اجرای هر سرویس نیازمند تصدیق اصالت به صورت جداگانه باشد.

همچنین در صورت خاموش شدن ماژول، اطلاعات مربوط به تصدیق اصالت‌های قبلی، معتبر نخواهند بود.

از لحاظ قدرت، تصدیق اصالت باید با موارد زیر سازگار باشد:

- برای هر مورد استفاده از تصدیق اصالت، احتمال موفقیت یک تلاش تصادفی (مانند حدس زدن کلمه عبور یا پین) باید کمتر از ۱ در ۱۰۰۰۰۰۰ باشد.
- برای تلاش‌های متوالی برای استفاده از مکانیسم تصدیق اصالت در طول مدت یک دقیقه، احتمال موفقیت یک تلاش تصادفی باید کمتر از ۱ در ۱۰۰۰۰۰ باشد.
- بازخورد اطلاعات مورد استفاده در تصدیق اصالت باید مخفی نگاه داشته شود (هنگام وارد کردن کلمه عبور، مقدار آن نشان داده نشود).
- بازخورد دریافت شده توسط کاربر هنگام تلاش برای تصدیق اصالت، موجب کاهش قدرت مکانسیم مورد استفاده در تصدیق اصالت نگردد.

مستندات باید شامل مواردی از قبیل: مکانیسم‌های تصدیق اصالت حمایت شده توسط ماژول رمزنگاری، انواع داده‌های مورد استفاده جهت تصدیق اصالت و قدرت مکانیسم‌های تصدیق اصالت مورد حمایت ماژول رمزنگاری باشد.

[80] Role-Based Authentivation

در سطح امنیتی ۱، نیازی به تصدیق اصالت جهت کنترل دسترسی به ماژول نیست ولی در سطح ۲، از تصدیق اصالت نقش محور برابر کنترل دسترسی به ماژول استفاده می‌شود. در سطوح ۳ و ۴ نیز برای کنترل دسترسی ماژول رمزنگاری، از تصدیق اصالت هویت محور استفاده می‌شود.

۱۰.٤.۶ مدل حالت محدود

هر عملیات صورت گرفته در ماژول رمزنگاری باید با یک جدول یا دیاگرام حالت‌گذار ارائه شود که دارای موارد زیر است که این موارد باید در مستندات مربوطه نیز آورده شوند.

- تمامی شرایط عملیاتی و خطای ماژول رمزنگاری،
- تحولات صورت گرفته از یک حالت به حالت دیگر،
- رویدادهای ورودی که باعث گذار از حالتی به حالت دیگر می‌شود،
- رویدادهای خروجی ناشی از انتقال از یک حالت به حالت دیگر.

یک ماژول رمزنگاری داری شرایط عملیاتی و خطایی از قبیل حالت‌های قطع بودن با وصل بودن تغذیه، حالت‌های مدیر رمزنگاری، حالت ورود کلید یا CSP، حالات کاربری، حالت تست خود[۸۱] و حالت‌های خطا. همچنین ممکن است یک ماژول رمزنگاری حالت‌های دیگری مانند حالت عبوری[۸۲] که در آن سرویس‌ها بدون پردازش رمزنگاری اجرا می‌شوند و حالت‌های نگهداری و سایر حالت‌ها باشد.

۱۰.٤.۷ امنیت فیزیکی

یک ماژول رمزنگاری که به تماماً به صورت نرم‌افزاری پیاده‌سازی شده و امنیت فیزیکی آن صرفاً بوسیله میزبان تامین می‌گردد با این استاندارد سازگار نیست.

امنیت فیزیکی، برای سه نوع درج فیزیکی ماژول رمزنگاری مشخص شده است که عبارتند از: ماژول‌های تک تراشه‌ای، چند تراشه‌ای و چند تراشه‌ای مجزا. بر اساس سطح امنیت فیزیکی اعمال شده، تلاش برای حمله آشکار سازی می‌شود[۸۳] یا ماژول رمزنگاری در برابر نفوذ عکس‌العمل نشان می‌دهد و از کلیدها و CSPهای رمز نشده محافظت می‌کند[۸۴].

لیست نیازمندی‌های امنیتی برای سطوح مختلف در جدول ۲ آورده شده است.

---

[81] Self-Test

[82] Bypass States

[83] Tamper Evidence

[84] Tamper Response

	نیازمندی‌های کلی برای تمامی جاسازی‌ها	ماژول‌های رمزنگاری تک تراشه‌ای	ماژول‌های رمزنگاری چند تراشه‌ای تعبیه شده	ماژول‌های رمزنگاری چند تراشه‌ای مستقل
امنیت سطح ۱	مولفه‌های دارای مشخصه یک محصول	نیازمندی خاصی ندارد	در صورت امکان، بسته‌بندی یا پوشش قابل برداشتن	بسته‌بندی در سطح محصول
امنیت سطح ۲	مشهودبودن دستکاری (مانند پوشش، محفظه یا قفل)	پوشش مات نشان‌دهنده دستکاری روی تراشه یا محفظه	ماده پنهان‌ساز مات نشان‌دهنده دستکاری یا محفظه با قفل‌های نشان‌دهنده دستکاری و یا قفل‌های مقاوم در برابر بازشدن برای درها و یا پوشش‌های قابل برداشتن	محفظه مات با قفل‌های نشان‌دهنده دستکاری و یا قفل‌های مقاوم در برابر بازشدن برای درها و یا پوشش‌های قابل برداشتن
امنیت سطح ۳	صفر کردن خودکار در هنگام دسترسی به واسطه نگهداری. مدار صفرکننده و واکنشی در برابر دستکاری. هواکش‌های محافظت شده.	پوشش مات سخت و آشکارساز دستکاری روی تراشه یا محفظه محکم در برابر نفوذ یا برداشتن	ماده سخت و مات پنهان‌ساز مدار چند تراشه‌ای یا ملزومات قابل اعمال برای مدارهای چند تراشه‌ای مستقل در سطح ۳	ماده سخت و مات پنهان‌ساز مدار چند تراشه‌ای یا محفظه محکم که برداشتن آن یا تلاش برای نفوذ به آن باعث آسیب‌های جدی گردد.
امنیت سطح ۴	EFP و EFT برای دما و ولتاژ	پوشش سخت و مقاوم در برابر برداشتن بر روی تراشه	بسته آشکارساز دستکاری با قابلیت واکنش و مدار صفر کننده.	بسته آشکارساز و واکنشی در برابر دستکاری و مدار صفر کننده

شکل ۱۵: جدول ۲- خلاصه لیست ملزومات امنیت فیزیکی

۱۱. پدافند غیرعامل در کارت هوشمند

در این جا به طور خلاصه به برخی ملاحظات پدافند غیرعامل که در سیستم کارت هوشمند باید به آن ها توجه کرد، می پردازیم:

- در حال حاضر رویکرد کلی گنجاندن چند کاربرد در یک کارت است. باید توجه داشت کاربردهایی که ایمنی بالایی نیاز دارند، مثل مسائل مالی در کنار کاربردهایی چون حمل و نقل که امنیت از اهمیت بالایی برخوردار نیست قرار نگیرد.
- سیستم عامل کارت هوشمند باید ترجیحا بومی باشد. اگر امکان پذیر نیست، باید سیستم عاملی انتخاب شود که دانش و امکان بومی کردن آن وجود داشته باشد. مثلا بتوان یک تکنیک امنیتی کشف نشده در آن گنجاند.
- ماشین مجازی جاوا، به علت محدود کردن دسترسی غیر مجاز به حافظه، عدم استفاده از اشاره گر، تشخیص خطاهای رایج برنامه سازی و ...، دارای نقاط قوت زیادی به لحاظ امنیتی است که باید آن ها را مد نظر قرار داد.
- اگر از کارت های هوشمند چند کاربرده استفاده می شود، بایست از فضای کارت حداکثر استفاده ی بهینه را کرد. مثلا اگر داده ای میان چند برنامه مشترک است، باید فرایند به اشتراک گذاشتن در فاز تولید نرم افزار مورد بررسی قرار بگیرد.
- برای کشورهایی که به علت محدودیت‌های فناوری، مجبور هستند به تولید تراشه کارت در خارج از کشور اعتماد نمایند, توجه به تهدیدهایی نظیر آنچه که در جنگ‌های اطلاعاتی روی می‌دهد و یا برنامه‌های تخریبی دشمنان در هنگام جنگ، بسیار مهم است. از این رو از دیدگاه شرایط جنگی یک رویکرد بهینه برای مرحله تولید کارت, انتقال فناوری تولید وساخت تراشه‌های کارت هوشمند در داخل کشور است.
- جهت عدم وابستگی به یک فراهم کننده ماژول کارت هوشمند باید حداقل از چند فراهم‌کننده‌ی مختلف که تامین کننده نیازهای امنیتی ماژول مورد نظر باشند استفاده کرد. تا در صورت اجرای تحریم توسط یک فراهم کننده برای کشور، نسبت به آن فراهم کننده وابستگی به‌وجود نیاید و بتوان ماژول‌های تهیه شده از فراهم‌کنندگان دیگر را جایگزین این ماژول فعلی نمود.
- یک کارت هوشمند نیاز به مکانیزمی برای تشخیص حمله دارد تا در موقع لزوم در برابر آن واکنش نشان داده و به طور مثال کلیدهای محرمانه را پاک نماید که این مکانیزم می‌تواند پروسه‌ای را ایجاد نماید که غیر از شرایط نرمال عملکرد باشد؛ به طور مثال ولتاژ بالاتر و یا تغییر نرخ کلاک پالس؛ از آنجایی که این شرایط در زمانی که خطایی در سامانه اتفاق بیافتد نیز ممکن است رخ دهد، معمولاً از مکانیزم اتوماتیکی برای بلوکه نمودن و یا پاک کردن کلیدها استفاده نمی‌شود ولی در کاربردهای خاص کارت هوشمند در حوزه‌های سری و خیلی محرمانه می‌بایست از این قابلیت استفاده نمود.
- برای ماژول‌های کارت هوشمندی که در سطح ملی استفاده می‌شوند، می‌بایست از ماژول چند لایه استفاده شود و در لایه فوقانی و تحتانی نباید اطلاعاتی ذخیره شود. این انتخاب در جلوگیری از دسترسی آسان به محتویات داخلی حافظه کارت بخصوص EEPROM تاثیر به‌سزایی خواهد داشت.
- لایه‌های فلزی می‌توانند مانعی برای اسکن نمودن تراشه به منظور تعیین جزئیات تراشه باشند. در هنگام طراحی بر روی سطح تراشه می‌بایست لایه‌های فلزی برای توزیع توان در نظر گرفته شوند که به نوعی محافظت از تراشه را نیز به عهده داشته باشند.

- می‌بایست در کنار RAM حسگر دمایی وجود داشته باشد تا در صورت پایین آمدن دما (تغییر ناگهانی دما) از حد مجاز تمام محتویات RAM (یا کلیدهای سری) پاک شود. همچنین می‌بایست در صورت مقیم شدن طولانی مدت

- کلیدها یا پارامترهای سری درون RAM، مکانیزمی برای پاک شدن کلیدها یا پارامترهای سری درون RAM وجود داشته باشد.
- فضای آدرس‌دهی سلول‌های حافظه درون تراشه با یک طرح درهم‌ریختگی منحصر به تراشه می‌بایست پیچیده‌سازی شود. بنابراین حافظه EEPROM می‌بایست با یک طرح درهم‌ریختگی به طور نرم‌افزاری آدرس‌دهی شود. در کنار درهم‌ریختگی می‌توان از رمزگذاری حافظه نیز استفاده نمود.
- ماژول مورد استفاده در کارت هوشمند ملی بایستی دارای حسگر نوری جهت تشخیص نفوذ و حمله فیزیکی به تراشه باشد و در صورت حمله، بایستی اقدامات لازم جهت جلوگیری از دسترسی مهاجم به اطلاعات حساس صورت پذیرد.
- تراشه می‌بایست مجهز به یک مدار ناظر بر ولتاژ باشد تا در صورتی که ولتاژ تراشه از محدوده تعریف شده‌ای تجاوز نمود، آن را خاموش نماید.
- تراشه می‌بایست مجهز به مداری برای نظارت بر فرکانس عملکرد تراشه باشد تا اگر فرکانس از نرخ کلاک تعریف شده‌ای کمتر یا بیشتر شد، عکس‌العمل نشان دهد.
- برای افزایش سطح امنیت، بایستی ارزیابی کارت در سطوح مختلف امکان پذیر باشد و نباید کلیه کلیدهای مورد نیاز جهت ارزیابی را تنها در یک پایانه نگهداری کرد.
- حالات و شرایط فعلی عملکردی نرم‌افزار کارت باید به صورت امنی ثبت شود تا در صورت بروز خطا بتوان کارت را بدون نیاز به دخالت انسان و به صورت خودکار به حالت اولیه برگرداند.
- برای امنیت بیشتر بایستی تصدیق اصالت دوطرفه صورت گیرد و هم بایستی اصالت کارت توسط پایانه و هم اصالت پایانه توسط کارت بررسی شود و از آنجایی که تصدیق اصالت دوطرفه در کارت‌های مغناطیسی امکان پذیر نمی‌باشد، در کاربردهای حساس بایستی از کارت هوشمند استفاده شود.
- روتین دستورات و کلاس دستورالعمل‌های درون نرم‌افزار کارت نباید آشکار و عمومی باشد و همچنین نباید توسط روال‌های کشف دستورالعمل‌ها قابل بازسازی باشد.
- اجرای مکانیزم‌های امنیتی نظیر رمزنگاری و احراز هویت می‌بایست مستقل از زمان پردازش داده‌ها و کلیدهای مختلف باشد تا حملات زمانی که با تحلیل زمان اجرای داده‌های مختلف کلید را حدس می‌زنند، قابل اجرا نباشد.
- الگوریتم‌های رمزنگاری بکاررفته باید عاری از نویز باشند و زمان اجرای رمزگذاری و رمزگشایی برای داده‌های مختلف با طول‌های متفاوت و کلیدهای مختلف باید یکسان باشد.
- کارت هوشمند را باید بتوان به صورت کامل در انتهای چرخه حیات توسط سیستم عامل، غیر فعال کرد و اطلاعات غیر ضروری در پایان چرخه حیات کارت بایستی حذف شوند.
- جهت تولید زوج کلید در رمزنگاری نامتقارن، بایستی از الگوریتم بومی که برای این منظور طراحی شده است، استفاده شود. البته قبل از استفاده بایستی از کارایی و امنیت مورد نیاز برخوردار باشد.
- بایستی از الگوریتم درهم‌سازی (Hash) بومی جهت تولید ورودی مورد نیاز جهت تولید امضای دیجیتال، استفاده شود. البته قبل از استفاده بایستی از کارایی و امنیت مورد نیاز برخوردار باشد.

- بایستی از الگوریتم checksum بومی جهت بررسی صحت اطلاعات مورد نظر، استفاده شود. البته این الگوریتم بایستی از کارایی و امنیت مورد نیاز برخوردار باشد.
- بایستی از قالب بومی برای ذخیره‌سازی اطلاعات بیومتریک با نرخ تصادم مورد نیاز و متناسب با کاربرد مورد نظر استفاده شود. همچنین اطلاعات بیومتریک مورد انتخاب بایستی متناسب با عرف و پذیرش و کارایی در سطح جامعه انتخاب شود.
- بایستی در کاربردهای ملی به جای استفاده از مکانیسم‌های تصدیق اصالت متداول، از مکانیسم‌های تصدیق اصالت بومی شده استفاده کرد تا میزان امنیت افزایش یابد. البته استفاده از روش بومی برای تصدیق اصالت لزوماً موجب بالا بردن امنیت نمی‌شود و بایستی از استحکام و کارایی روش مورد استفاده، اطمینان حاصل شود.
- مدیران و پرسنلی که دارای سطح دسترسی ویژه در سیستم مبتنی بر کارت هوشمند در سطح ملی هستند، بایستی به نحو مطلوبی آموزش داده شده و توجیه شوند و که از لحاظ امنیتی مورد تایید باشند و صلاحیت آنان از مراجع ذیصلاح استعلام گردد.[1]

۱۲.کاربردهای مختلف کارت هوشمند

بیشترین کاربرد کارت های هوشمند در زمینه پرداخت الکترونیک است. به عنوان نمونه، در کاربردهایی مانند کارت-های نقدی و اعتباری، کیف پول الکترونیک، کارت های وفاداری (بن های سازمانی، تخفیف برای اعضاء و ...) و کارت-های پارکینگ و بلیط؛ از خدمات پرداخت استفاده می شود. در دیگر حوزه ها نیز، خدمات این کارت ها برای کارت بهداشت و درمان، حمل و نقل، تشخیص هویت، دسترسی و ورود به مکان های خاص و . . . ، مورد استفاده قرار گرفته است. گستره کاربرد و سرعت فراگیری کارت های هوشمند، امروزه آن را به یکی از الزامات زندگی شهری تبدیل کرده است و به همین دلیل بسیاری از کشورها در حال سرمایه گذاری وسیع در این زمینه هستند. در این سند به دلیل محدودیت، به پنج گروه اصلی از کاربردهای کارت اشاره شده و ضمن معرفی اجمالی کاربردها در هر گروه، یکی از آنها تشریح خواهد شد.

این گروه های خدمات عبارتند از[4] :

- حمل و نقل درون شهری و بین شهری؛
- گردشگری؛
- فرهنگی – رفاهی؛
- پرداخت شهروندان؛
- نیروی انسانی سازمان ها .

۱۲.۱. خدمات حمل و نقل درون شهری و بین شهری

در این گروه از خدمات، حداقل می توان به پانزده تنوع از کاربردهای کارت هوشمند اشاره کرد که ضمن ذکر نام آنها، یکی از خدمات حمل و نقل بطور اجمال تشریح خواهد شد. این خدمات پانزده گانه عبارتند از: استفاده از کارت های هوشمند بعنوان بلیط الکترونیکی در حمل و نقل مترو، بلیط الکترونیک برای اتوبوس های درون شهری، پرداخت کرایه ی تاکسی و آژانس، پرداخت هزینه توقف (پارک و پارکومترها)، توقف گاه های عمومی، مجوز ورود به توقف گاه های اختصاصی، رزرو مکان در توقف گاه های عمومی و اختصاصی، عوارض تردد در بزرگ راه ها، کنترل و نظارت بر رانندگان وسایط نقلیه عمومی و اختصاصی، بلیط الکترونیک برای اتوبوس های بین شهری، بلیط الکترونیک برای قطارهای مسافری، بلیط الکترونیک برای سفرهای هوایی، اخذ مستقیم جریمه یا ثبت تخلف توسط نیروی انتظامی، پرداخت هزینه های سوخت(کارت سوخت) و پرداخت هزینه های تعمیرات و نگهداری خودرو (معاینه فنی، تعمیرات، بازبینی های نوبه ای، نظافت، شستشو و ...)

نمونه ای از خدمات حمل و نقل: بلیط قطارهای مسافری

از کارت هوشمند می توان به عنوان بلیط چاپی قطارهای مسافری استفاده کرد. کارت خوان های مربوط را می توان در باجه صدور بلیط و نیز در سکوهای مسافرگیری نصب کرد. در هنگام تهیه بلیط از باجه صدور بلیط (در ایستگاه یا هر آژانس مسافرتی)،

مسافر ضمن پرداخت هزینه بلیط از طریق کارت، کد مجوز سوار شدن به قطار مربوطه را روی کارت خود دریافت می کند. قبل از سوار شدن به قطار در سکوی مسافرگیری، با استفاده از کارت خوان مربوطه تراکنش انجام شده و دو قبض صادر می گردد که یکی برای تحویل به مسئول مربوطه و دیگری به عنوان لاشه بلیط نزد مسافر باقی می ماند. اطلاعات تراکنش های انجام شده توسط کارت خوان ها، در پایان هر روز از طریق تجهیزات تخلیه اطلاعات دستی (مانند رایانه کیفی) ثبت شده و به مرکز گردآوری اطلاعات و از آنجا به شرکت صادر کننده کارت انتقال می یابد. در صورت امکان می توان از طریق خط سریال، اطلاعات کارت خوان ها را در دفتر ایستگاه دریافت و سپس کار ارسال به شرکت صادر کننده کارت را انجام داد. شرکت معادل مجموع مبالغ تراکنش های انجام شده را پس از کسر کارمزد به حساب سازمان مربوطه واریز خواهد کرد. با توجه به تعداد مسافران، بسته به نوع معماری کارت می توان از بخش تماسی یا بدون تماس کارت استفاده کرد. تکنولوژی ارتباطی در داخل ایستگاه به صورت برخط و در ارتباط با خارج از ایستگاه به صورت برون خط خواهد بود [4] .

معمولاً این نوع پرداخت ها از طریق حساب اعتباری یا کیف پول الکترونیک انجام می پذیرد. از جمله مزایای این کاربرد می توان به موارد زیر اشاره کرد :

- ✓ حذف هزینه های چاپ، توزیع، فروش و گرد آوری بلیط های کاغذی؛
- ✓ تسهیل و تسریع فرایند گردآوری پول؛
- ✓ فراهم آوردن بستر نظارتی ارزان و قابل اطمینان؛
- ✓ امکان گزارش گیری سریع و آسان.

۱۲.۲. خدمات کارت در حوزه گردشگری

استفاده از کارت هوشمند در حوزه گردشگری، عمدتاً به منظور پرداخت هزینه مراکز خرید کالا و خدمات، شناسایی و تقویت ارتباط با مشتریان وفادار و در موارد خاص، جهت کنترل دسترسی و نظارت می باشد که به عنوان نمونه، به کاربرد کارت در هتل ها و مراکز اقامتی اشاره می گردد .

۱۲.۳. استفاده در هتل ها و مراکز اقامتی

کارت هوشمند به عنوان ابزاری برای پرداخت هزینه و مجوز استفاده از خدمات مختلف در هتل ها می توان استفاده کرد. در این کاربرد می توان در قسمت پذیرش، رستوران، بوفه و دیگر نقاط ارائه خدمات در هتل، کارت خوان نصب کرد. دارنده کارت در هتل می تواند هزینه کلیه خدمات را با استفاده از آن پرداخت نماید. مجموعه کارت خوان هایی که در بخش های مختلف نصب شده اند به طور دائم اطلاعات خود را به کامپیوتر مرکزی هتل ارسال می کنند. این اطلاعات به صورت روزانه به شرکت صادر کننده کارت منتقل می گردد. شرکت نیز معادل مجموع مبالغ تراکنش های انجام شده را پس از کسر کارمزد، به حساب فرد یا سازمان مربوط واریز می کند.

استفاده از سیستم کارت امکاناتی را نیز در اختیار هتل قرار می دهد. این سیستم امکان شناسایی مشتریان وفادار را فراهم ساخته و در مواردی که هتل تمایل به ارائه تخفیف به این مشتریان را (به طور دائم یا در دوره های خاصی از سال) داشته باشد، انجام آن را تسهیل و ساده می کند. همچنین درصورت تجهیز هتل، می توان از کارت برای کنترل دسترسی دارنده به امکانات معینی در هتل، بهره گرفت[4].

از جمله مزایای این نوع خدمات، عبارتند از:

- تسهیل و تسریع فرایند گردآوری پول،
- فراهم آوردن بستر نظارتی ارزان و قابل اطمینان،
- امکان گزارش گیری سریع و آسان،
- امکان شناسایی و یا تعریف مشتریان وفادار،
- امکان ارائه تخفیف های ویژه به مشتریان وفادار و نیز، گروه های ویژه ای از دارندگان کارت، برای خدمات معین و در اوقات معینی از سال.

۱۲.٤. خدمات کارت هوشمند در حوزه فرهنگی – رفاهی

از جمله این خدمات می توان به زمینه هایی مانند: امانت کتاب در کتابخانه ها؛ پرداخت در مراکز تفریحی (شهربازی، سیرک و ...)؛ پرداخت در موزه ها؛ باشگاه های ورزشی و استادیوم ها، فرهنگسراها، سینماها و نمایشگاه ها؛ اشاره کرد. در این بخش بعنوان نمونه به روش استفاده از کارت در سینماها اشاره می گردد.

۱۲.۵. خدمات کارت در فرهنگ سراها، سینماها و نمایشگاه ها

از کارت هوشمند می توان به عنوان ابزاری برای پرداخت هزینه و کنترل تردد در مکان های فرهنگی نظیر فرهنگسراها، سینماها و نمایشگاه ها استفاده کرد. در این کاربرد لازم است در ورودی محل (یا در موارد خاص هر بخش از آن) دستگاه کارت خوان نصب شود. دارنده کارت هنگام ورود به مکان فرهنگی می تواند هزینه استفاده از امکانات یا بخش های مختلف آن را با استفاده از کارت پرداخت نموده و مجوز استفاده از آنها را به صورت کد مناسب روی کارت دریافت کند. هنگام استفاده از امکانات (مانند ورود به سالن نمایش در سینما یا سالن های مختلف نمایشگاه)، با انجام تراکنش، ورود فرد تأیید می گردد و در صورت لزوم، قبضی صادر می گردد که به متصدی مربوطه تحویل خواهد شد. از جمله مزایای این کاربرد می توان به موارد زیر اشاره کرد[4]:

- حذف هزینه های چاپ، توزیع، فروش و گردآوری بلیط؛
- تسهیل و تسریع فرایند گردآوری پول نقد؛
- فراهم آوردن بستر نظارتی ارزان و قابل اطمینان؛
- امکان گزارش گیری سریع و آسان؛
- امکان شناسایی و یا تعریف مشتریان وفادار؛
- امکان ارائه تخفیف های خاص به مشتریان وفادار و نیز گروه های ویژه ای از دارندگان برای خدمات معین و در اوقات معینی از سال.

۱۲.۶. خدمات کارت در حوزه پرداخت‌های شهروندان

پرداخت‌های شهروندان در قبال دریافت خدمات، هم‌اکنون از طریق مراجعه به بانک‌ها صورت می‌پذیرد. در بعضی از موارد (نظیر پرداخت قبض‌ها) شهروندان با مراجعه به بانک، قبض مربوطه را پرداخت می‌کنند و رسید پرداخت‌های انجام شده به سازمان مربوطه ارسال می‌گردد. در موارد دیگر، شهروند پس از مراجعه به اداره یا سازمان مربوطه، از مبلغ پرداختی مطلع شده و با مراجعه به بانک مبلغ مذکور را پرداخت می‌کند و قبض آن را به اداره یا سازمان مربوطه تحویل می‌دهد. قبض مذکور در پرونده شهروند بایگانی می‌گردد. در روش سنتی نه تنها منابعی مانند زمان، هزینه تردد، هزینه‌های آلودگی محیط و ...، را متحمل می‌شویم، بلکه سازمان ها همواره با مغایرت اطلاعات و شکایت شهروندان مواجه هستند. نظیر چنین روال‌هایی در مورد شرکت‌ها و مؤسسات نیز صادق است. با استفاده از فناوری کارت، تعداد جابجایی‌ها و عملیات کاغذی کاهش یافته و گزارش گیری از عملیات و جستجوی سوابق مربوط به شهروندان به صورت ماشینی و با سهولت و هزینه کمتری قابل انجام است. به عنوان مثال، با ایجاد کیوسک های خدمات شهری مجهز به کارت خوان، بخش قابل توجهی از خدمات شهری و پرداخت های مربوط به آنها با سریع ترین و کم هزینه ترین شیوه انجام می‌پذیرد. هر شهروند دارنده کارت یا هر فرد حقیقی که به نمایندگی رسمی یک شرکت یا مؤسسه کارت دریافت کرده است، می‌تواند از این خدمات استفاده کند. از جمله این خدمات می‌توان به مواردی همچون پرداخت عوارض شهرداری؛ هزینه‌های راهنمایی و

رانندگی، ثبت احوال؛ قبض‌های انرژی و تلفن؛ هزینه‌های گذرنامه و روادید؛ هزینه‌های گمرکی؛ هزینه‌های بیمه و ...، اشاره کرد. فرایند پرداخت در این حوزه نیز مانند بخش قبلی می‌باشد. بنابراین از تشریح مجدد عملیات و تراکنش‌ها اجتناب می‌گردد[4].

۱۲.۷. خدمات کارت در حوزه نیروی انسانی

یکی از معضلات سازمان ها، اعطای کمک های نقدی و غیر نقدی و پرداخت حقوق و مزایا به کارمندان است. در این زمینه به کارگیری کارت های هوشمند در قالب کارت های اعتباری، نقدی و کیف پول الکترونیک، موجب ایجاد سهولت و مزایای فراوان برای سازمان و کارکنان خواهد شد.

همچنین، به کارگیری کارت های متعدد برای کاربردهای متفاوت، یکی دیگر از معضلات و مسائل سازمان ها است. عدم وجود ارتباط بین این سیستم ها، امکان استفاده از برخی از مزایا و امکانات را سلب کرده و بعضاً موجب ایجاد فرایندها و روال های تکراری می گردد. با بکارگیری فناوری کارت هوشمند چند منظوره، امکان برخورداری از کلیه مزایای فوق در قالب یک کارت، امکان پذیر خواهد بود. از جمله خدمات قابل ارائه به کارکنان از طریق کارت هوشمند عبارت است از: پرداخت حقوق و مزایای ماهیانه، کمک های غیرنقدی و پرداخت هزینه های اداری (درمان، سفر، مأموریت و...)

۱۲.۸. پرداخت حقوق و مزایای ماهیانه

از کارت هوشمند جهت پرداخت حقوق پرسنل در سازمان ها استفاده می شود. در این کاربرد، حقوق و مزایا روی کارت پرسنل شارژ می‌شود و دارنده کارت می‌تواند با مراجعه به شعب بانکی پول نقد دریافت کرده و یا با مراجعه به سایر پذیرندگان کارت، مستقیماً اقدام به خرید کالا و خدمات کرده و هزینه آن را با استفاده از کارت پرداخت نماید. معادل مبلغ شارژ شده، بعلاوه درصدی به عنوان کارمزد، به حساب شرکت صادر کننده کارت واریز می‌گردد. با توسعه هر چه بیشتر شبکه پذیرندگان کارت و تجهیز آن‌ها به دستگاه‌های کارت خوان، نیاز پرسنل به دریافت وجه نقد کاهش می‌یابد. در این کاربرد، پرداخت حقوق به حساب نقدی دارنده کارت منتقل می‌گردد[4].

از جمله مزایای این نوع کاربرد می توان به موارد زیر اشاره کرد:

۱. کاهش مخاطرات حمل وجوه نقد،
۲. تسهیل و تسریع فرایند پرداخت،
۳. کاهش نیاز پرسنل به دریافت و استفاده از وجه نقد درصورت توسعه شبکه پذیرندگان.

فهرست منابع :

۱. سند مطالعه و طراحی نمونه کارت هوشمند از دیدگاه پدافند غیر عامل[1]

۲. WILEY, 2003 Wolfgang Rankl, Wolfgang Effing [2] Smart Card Handbook

۳.ADDISON-WESLEY, 2000 Zhiqun Chen [3] Java Card Technology for Smart Cards

۴.WILEY, 2007 Wolfgang Rankl [4] Smart Card Applications

۵. Artech House, 2001 Mike Hendry [5] Smart Card Security and Applications

۶. Keith Mayes, Konstantinos Markantonakis [6] Smart Cards, Tokens, Security and Applications Springer, 2008

۷. www.iso.org/ISO7816-X

۸. www.emvco.com/approvals.aspx

۹. خروجی پروژه امکان‌سنجی توسعه کارت هوشمند سلامت، وزارت بهداشت درمان و آموزش پزشکی-شرکت آشنا ایمن