دانشکده مهندسی

گروه برق

پایان‌نامه کارشناسی

گرایش: الکترونیک

عنوان: بررسی امنیت کارت های هوشمند

استاد راهنما: دکتر شهرام محمدی

نگارش: مریم خلفی

شهریور 91

چکیده :

این پایان نامه راجع به امنیت کارت های هوشمند می باشد. در فصل اول پس از بررسی تاریخچهٔ کارت های هوشمند، به انواع این کارت ها پرداخته شده و ساختار آن ها بررسی شده است. در فصل دوم به راه های شناسایی و نحوهٔ شناخت کاربر اشاره شده و راه های شناسایی امن معرفی می شوند. در نهایت در فصل آخر به انواع حملات ممکن به کارت های هوشمند و زمان بندی انواع حملات پرداخته شده است و پس از بررسی، راه های مقابله با آن ها و حفاظت کارت های هوشمند شناخته شده است.

فهرست مطالب

مقدمه

یکی از مزایای مهم کارت های هوشمند در مقایسه با دیگر رسانه های ذخیره سازی اطلاعات مانند کارت های نوار مغناطیسی و دیسکت ها، این است که می توانند اطلاعات را به طوری که محرمانه بماند ذخیره کنند. یک نیاز ضروری برای این منظور، سخت افزار تراشهٔ مناسب و بهینه همراه با روش های پنهانی مناسب برای محرمانه نگه داشتن اطلاعات است. اما، امنیت به عواملی بیش از سخت افزار میکروکنترلری ویژه و الگوریتم های پیاده شده در نرم افزار سیستم عامل وابسته است. امنیت برنامهٔ کارت هوشمند و اصول طراحی استفاده شده توسط توسعه دهنده های آن نیز از تقاضاهای بنیادی اند. این پروژه خلاصه ای از نکات مهم، روش ها و استراتژی های تولید کارت های هوشمند امن و برنامه های کارت هوشمند امن را در بر می گیرد.

فصل اول: معرفی کارت هوشمند

1-1) تاریخچهٔ کارت هوشمند (Smart Card)

بر اساس گزارش های منتشر شده، اولین کارت هوشمند حاوی یک ریزپردازنده، در سال 1967 میلادی و توسط دو مهندس آلمانی ابداع شد. این اختراع منتشر نشد تا این که یک روزنامه نگار فرانسوی در سال 1974 م، اختراع کارت هوشمند را در فرانسه به ثبت رسانیده و خبر ظهور این فناوری را منتشر کرد. بنابراین کارت هوشمند، توسط فردی فرانسوی با نام رولاند مورنو در سال 1974 ثبت شد. از آن زمان به بعد، شرکت هایی نظیر Bull، Honeywell و Motorola در این زمینه به فعالیت پرداختند و در نتیجهٔ فعالیت های آن ها، در سال 1979 اولین کارت هوشمند ریزپردازنده ای ساخته شد. اولین استاندارد برای کارت هوشمند در سال 1986 و با عنوان ISO 789116/1 مطرح شد.

استفاده از کارت هوشمند در سطح ملی، برای نخستین بار در فرانسه و در سال 1986 انجام گرفت. در این سال، شرکت مخابرات فرانسه برای اولین بار به جای سکه در تلفن های عمومی از کارت هوشمند استفاده کرد که این اقدام، سبب رفع بسیاری از مشکلات استفاده از تلفن های عمومی، سوء استفاده ها و خراب کاری ها شد. پس از آن، از اوایل دههٔ 90 میلادی، استفاده از کارت های هوشمند در کشور های مختلف رواج پیدا کرد و به تدریج، کاربردهای جدیدی برای آن پیدا شد.

در کشور جمهوری اسلامی ایران نیز چند سالی است که بعضی شرکت ها مانند شرکت لاله کامپیوتر، اقدام به تولید کارت های هوشمند می کنند.

2-1) سخت افزار کارت هوشمند

کارت هوشمند، کارتی پلاستیکی با ابعاد کارت های اعتباری (حدود 5.5 در 8.5 سانتی متر) است که بر روی آن یا در بین لایه های آن، تراشه های حافظه و ریزپردازنده برای ذخیره سازی داده ها و پردازش آن

ها قرار داده شده است. یک کارت هوشمند، کامپیوتر کوچکی است که بر روی یک کارت پلاستیکی نصب شده است. این قبیل کارت ها به راحتی در جیب جای می گیرند و کاربردهای مختلفی دارند.

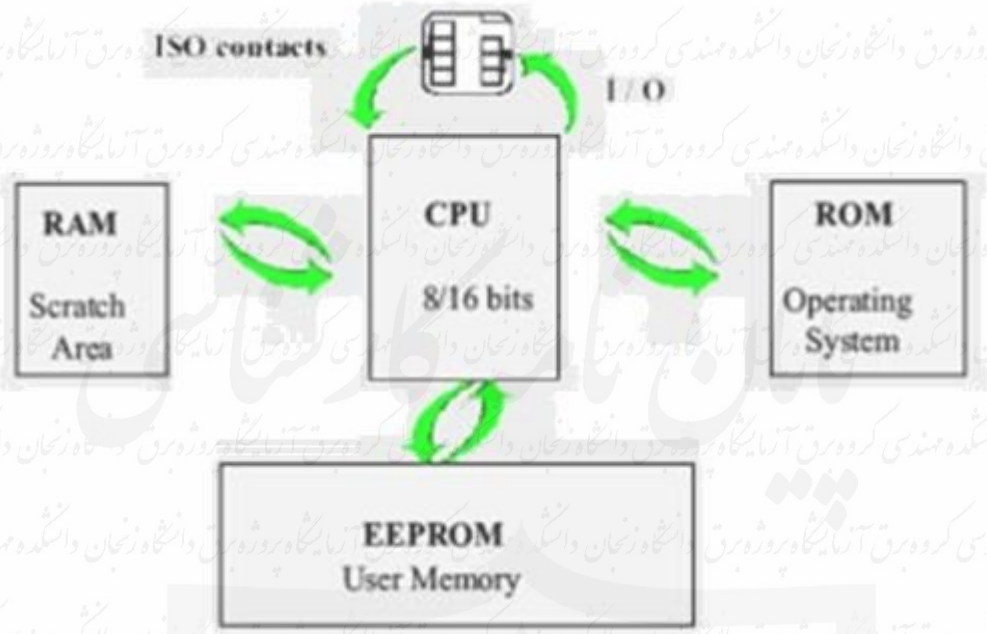
کارت هوشمند که با نام های « کارت چیپ دار» یا «کارت با مدار مجتمع» هم شناخته می شود کارتی است که بر روی آن، مدار مجتمع نصب شده است. از این نوع کارت می توان به جای کارت اعتباری و کارت پول یا در سیستم های امنیتی کامپیوتری، سیستم های تشخیص هویت و بسیاری موارد دیگر استفاده کرد.

کارت های هوشمند از نظر اندازه و شکل ظاهری، شبیه به کارت های مغناطیسی معمولی هستند. ولی درون این کارت ها کاملا با کارت های معمولی، متفاوت است. کارت های مغناطیسی معمولی، یک تکه پلاستیک ساده هستند با یک نوار مغناطیسی، در حالی که کارت های هوشمند، درون خود یک ریزپردازنده دارند. این ریزپردازنده چون بیش از اندازه کوچک است با تکنولوژی خاصی کشت می شود (تبدیل یک ترانزیستور اندازهٔ یک نخود به سایزی معادل کوچک تر از نوک سوزن). ریزپردازنده معمولا در زیر یک اتصال طلایی، در یک طرف کارت قرار دارد. این ریزپردازنده در کارت های هوشمند، در حقیقت جایگزین نوار مغناطیسی در کارت های معمولی شده است. اطلاعاتی را که روی نوار مغناطیسی کارت های معمولی وجود دارد می توان به راحتی خواند، روی آن نوشت، آن را حذف کرد و یا تغییر داد. به علت وجود همین مشکل، نوار مغناطیسی محل خوبی برای نگه داری اطلاعات نیست. به همین دلیل هم، برای استفاده از چنین کارت هایی، نیاز به طراحی شبکه های کامپیوتری گسترده برای تایید صحت و دریافت و پردازش اطلاعات وجود دارد. کارت هوشمند، بدون نیاز به چنین امکاناتی به دلیل امنیت خود می تواند اطلاعات را در خود ذخیره کرده تا در صورت لزوم در محل های مختلف بتوان از این اطلاعات، بدون نیاز به اتصال به شبکه استفاده کرد. ریزپردازنده در کارت هوشمند، برای امنیت مورد استفاده قرار می گیرد. در واقع کارت هوشمند، یک کامپیوتر کوچک است که با کامپیوتری که به دستگاه کارت خوان متصل است ارتباط برقرار می کند و تا ریزپردازندهٔ کارت، از معتبر بودن دسترسی به کارت مطمئن نشود، به کارت خوان اجازهٔ دسترسی نمی دهد. پس از صدور مجوز دسترسی، کارت خوان می تواند با کارت که دارای یک RAM است کار کند و اطلاعات را بخواند، پردازش کند و تغییر دهد. کارت های هوشمند می توانند تا 8 کیلو بایت RAM (حافظه با دسترسی تصادفی برای خواندن و نوشتن اطلاعات)، 364

کیلو بایت ROM (حافظهٔ فقط خواندنی)، 256 کیلوبایت PROM (حافظهٔ فقط خواندنی قابل برنامه ریزی) و یک ریزپردازندهٔ 16 بیتی داشته باشند. کارت هوشمند همچنین از یک واسط سریال برای نقل و انتقال اطلاعات استفاده کرده و انرژی خود را هم، از یک منبع بیرونی (مثلاً دستگاه کارت خوان) تامین می کند. ریزپردازنده هم، برای انجام یک مجموعه عملیات محدود، همانند رمزنگاری مورد استفاده قرار می گیرد. کارت های هوشمند می توانند برای کارت های اعتباری، کارت پول، سیستم های امنیتی کامپیوتری، سیستم های تشخیص هویت دولتی و بسیاری موارد دیگر مورد استفاده قرار گیرند. شکل1 یک نمونه کارت هوشمند را نشان می دهد:

شکل1) کارت هوشمند بیمهٔ پزشکی فرانسه

شکل 2، شمای داخلی کارت هوشمند را نشان می دهد:



شکل 2) شمای داخلی کارت هوشمند

شکل 3، قسمت های سخت افزاری کارت هوشمند را نمایش می دهد که شامل موارد زیر است:

1- بدنهٔ پلاستیکی کارت که در آن یک حفرهٔ مربع شکل وجود دارد، از انواع پلاستیک های ذیل ساخته می شود:

- ABS
- PVC
- PC-Polycarbonate

2- صفحهٔ فلزی Contact Disc برای اتصال پایه های کوچک chip به پایه های فلزی کارت خوان می باشد. این صفحهٔ فلزی به صورت شش و یا هشت پایه ساخته می شود و از روی شکل ظاهری صفحه معمولا نمی توان به نوع کارت پی برد.

3- Chip، همانند ریزپردازندهٔ یک کامپیوتر شخصی، از المان های سخت افزاری ذیل تشکیل شده است:

- پردازشگر مرکزی CPU
- حافظهٔ فقط خواندنی ROM
- حافظهٔ موقت جهت نوشتن و خواندن RAM
- حافظهٔ دائم جهت نگه داری داده ها از نوع EEPROM یا Flash-Memory

- درگاه سریال (Serial Port) جهت ارتباط با دنیای خارج

شکل 3) سخت افزار کارت هوشمند

3-1) دسته بندی کارت های هوشمند

کارت های هوشمند را بر حسب موارد مختلفی دسته بندی می کنند. در ادامه به دو مورد آن پرداخته می شود:

1-3-1) دسته بندی بر اساس نحوهٔ ارتباط با کارت خوان

کارت هوشمند که شبیه به یک کامپیوتر ساده و کوچک است می تواند از طریق دستگاه کارت خوان و اتصال طلایی خود، ارتباط برقرار کند تا بتوان به اطلاعاتی که درون حافظهٔ این کارت قرار دارد دسترسی پیدا کرد.

انواع کارت های هوشمند از دیدگاه تکنولوژی ساخت و نحوهٔ ارتباط با کارت خوان به سه گروه کارت های تماسی (Contact)، کارت های بدون تماس (Contact-less) و کارت های با رابط دوگانه (Dual Interface) تقسیم می شوند.

1-1-3-1) کارت هوشمند تماسی (Contact)

برای استفاده از این قبیل کارت ها، باید اتصال فیزیکی بین کارت و دستگاه کارت خوان برقرار گردد. داده های موجود بر روی کارت، به صورت سریال به کارت خوان ارسال می شود و پس از پردازش، اطلاعات جدید از طریق همان پورت، به روی کارت منتقل می شود. به عنوان نمونه، کارت های تلفن عمومی،

جزو این دسته محسوب می شوند. مشکل اصلی این قبیل کارت ها، خراب شدن کنتاکت های فلزی (محل های تماس) بر اثر عوامل خارجی نظیر ضربه و شرایط فیزیکی محیط است. درشکل5، قسمت های موجود در کنتاکت های فلزی این نوع کارت، به تصویر کشیده شده است.

شکل 4) شمایی از کارت هوشمند تماسی

شکل 5) قسمت های مختلف کنتاکت های کارت هوشمند تماسی

2-1-3-1) کارت هوشمند غیر تماسی (Contact-less)

نسل جدید کارت های هوشمند، کارت های هوشمند بدون تماس هستند. این کارت ها بدون تماس و با تکنولوژی القاء (Identification Radio Frequency) با دستگاه کارت خوان ارتباط برقرار می کنند. فقط کافی است این کارت در نزدیکی دستگاه قرار گیرد. این نوع کارت در مواقعی که نیاز به برقراری ارتباط سریع و حتی بدون دخالت دست وجود دارد کاربرد بسیاری دارد. برای مثال برای ورود یک فرد به اتاق، کارت، ممکن است در جیب یا کیف شخص باشد و از همان محل و بدون نیاز به خارج کردن، با دستگاه کارت خوان، ارتباط برقرار کرده و مجاز بودن ورود، بررسی شده و در باز شود. همچنین در بسیاری از سیستم های حمل و نقل عمومی در دنیا به دلیل حجم زیاد مسافران و به خاطر سریع تر شدن

نتیجه گیری

کارت های هوشمند از جمله پرکاربردترین ابزارهای رمزنگاری هستند و لذا محافظت از آن ها در مقابل انواع حملات مختلف از جمله موارد بسیار مهم به شمار می رود. در این پایان نامه، پس از معرفی مختصر کارت های هوشمند و انواع روش های شناسایی، انواع حملات به کارت های هوشمند و راه های مقابله با آن ها را به طور اجمالی مورد بررسی قرار دادیم. با توجه به مطالب مطرح شده، موضوع حفاظت از کارت های هوشمند در مقابل چنین حملاتی می تواند از جمله موضوعات جذاب و مهم تحقیقاتی برای مراکز علمی و نیز صنعتی کشور باشد.

منابع و مراجع

[۱] اصفهانی، رضا، "کارت هوشمند"، دانشگاه امام حسین (ع)، قسمت اول تا سوم

[۲] معصومی، مسعود، "امنیت سخت افزاری کارت های هوشمند"، دانشگاه صنعتی خواجه نصیر

[3] Kenneth G. Paterson, Fred Piper and Matt Robshaw, "Smart Cards and the Associated Infrastructure Problem", Information Security Technical Report, Vol 7, No. 3 (2002) 20-29

[4] Tony Boswell, "Smart card security evaluation: Community solutions to intractable problems", information security technical report 14 (2009) 57 – 69

[5] Xuefei Leng, "Smart card applications and security", information security technical report 14 (2009) 36 – 45

[6] John Abbott, "Smart Cards: How Secure Are They? ", GSEC Practical v1.3, March, 2002

[7] Wolfgang Rankl and Wolfgang Effing, "Smart Card Handbook", John Wiley & Sons, Germany, 2002

[8] Marc Witteman, "Advances in Smartcard Security", Information Security Bulletin, 2002

[9] "What Makes a Smart Card Secure? ", Smart Card Alliance, 2008

[10] Wolfgang Rankl, "Overview about Attacks on Smart Cards", Munich, February 2003