مروری بر کارت هوشمند

علی محمودی

چکیده

کارت هوشمند[1]، یکی از مهم‌ترین ابزارهای تصدیق کاربر و ذخیره اطلاعات محرمانه است و در طراحی آن از الگوریتم‌های رمزنگاری استفاده می‌شود. امروزه در بسیاری از کاربردهایی که نیاز به نگهداری و انتقال امن اطلاعات و داده‌ها، کنترل دسترسی به سیستم‌های رایانه‌ای و نیز کنترل دسترسی فیزیکی به محیط‌های خاص به‌عنوان کلید الکترونیکی وجود دارد، از کارت‌های هوشمند استفاده می‌شود. مهم‌ترین علل محبوبیت کارت‌های هوشمند اندازه کوچک، مقاوم بودن در برابر دست‌کاری[2] و قابل حمل بودن آن‌هاست.

مقدمه

تاریخچه استفاده از کارت‌های پلاستیکی برای شناسایی افراد به حدود سال 1950 بر می‌گردد. در آن زمان فقط از بدنه پلاستیکی کارت به سادگی برای نوشتن نام و مشخصات دارنده کارت به‌صورت حروف برجسته[3] استفاده می‌شد و کارت نقشی شبیه به کارت‌های اعتباری امروزی ایفا می‌کرد. پیشرفت در زمینه استفاده از کارت‌ها، با ایجاد نوار مغناطیسی[4] بر روی کارت که توسط ماشین مخصوصی قابل خواندن و نوشتن بود، سرعت گرفت و وارد مرحله جدیدی شد [1]. با وجود محبوبیت این نوع کارت‌ها در صنعت بانکداری و امور مالی- اعتباری، سطح امنیتی ارائه شده توسط کارت‌های مغناطیسی پایین بود. در نتیجه با پیشرفت تکنولوژی نیمه هادی، نسل سوم کارت‌ها یعنی کارت‌های هوشمند پا به عرصه وجود نهاد.

انواع کارت‌های هوشمند

بر اساس نوع تراشه به کار رفته در کارت و نحوه ارتباط بین کارت و کارت‌خوان[5]، رده بندی‌های مختلفی برای کارت هوشمند وجود دارد [1].

الف) تقسیم‌بندی کارت‌ها بر حسب نوع تراشه

1- **کارت‌های حافظه‌ای** (Memory Cards): در کارت‌های حافظه‌ای ، تراشه توانایی پردازش و مدیریت اطلاعات را ندارد و فقط داده‌ها، از طریق پروتکل‌های هم‌زمان با کارت‌خوان، انتقال داده می‌شوند. کارت تلفن، کارت پارک اتومبیل، کارت بلیط الکترونیکی مترو و اتوبوس و ... نمونه‌ای از کارت‌های حافظه‌ای هوشمند هستند.

2- **کارت‌های ریزپردازنده‌دار** (Microprocessor Multifunction Cards): در این نوع از کارت‌های هوشمند، تراشه توانایی پردازش و مدیریت اطلاعات را دارد. برای این کار یک تابع یا نرم‌افزار خاص در تراشه ریزپردازنده، برای مدیریت داده‌ها از طریق سیستم عامل کارت[6] قرار می‌گیرد. کارت‌های بانکی، کارت سوخت و سیم‌کارت، نمونه‌های بارز از این کارت‌ها هستند.

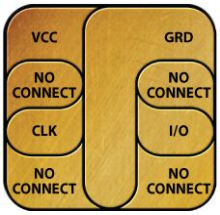
ب) تقسیم‌بندی کارت‌ها بر حسب روش ارتباط بین کارت و کارت‌خوان:

1- **کارت هوشمند تماسی** (Contact Smart Card):در این نوع کارت‌ها، ارتباط کارت با کارت‌خوان از طریق اتصالات الکتریکی که روی بدنه کارت وجود دارد برقرار می‌شود. استانداردهای ISO/IEC 7816 و ISO/IEC7810 استانداردهای

---

[1] Smart Cards
[2] Tamper-Proof
[3] Embossed
[4] Magnetic Stripe
5 Reader
6 Card OS

تدوین شده برای این نوع کارت‌ها هستند. کارت سوخت، گواهی‌نامه‌های هوشمند و سیم‌کارت نمونه‌ای از کارت‌های تماسی هستند.



2- **کارت هوشمند غیرتماسی** (Contactless Smart Card): در این نوع کارت‌ها، سیگنال لازم و تغذیه تراشه کارت به جای اینکه از اتصالات روی بدنه کارت تأمین شود با القاء سیگنال‌ها از طریق امواج الکترومغناطیسی و رادیویی (Radio Frequency Identification : RFID) به کارت صورت می‌گیرد و بین کارت و کارت‌خوان اتصال فیزیکی برقرار نمی‌شود. کارت‌های غیرتماسی اغلب از دو نوع استاندارد ISO/14443 و ISO693 استفاده می‌کنند و در کاربردهایی چون کنترل ترافیک در بزرگراه‌ها، پارکینگ‌ها و بلیط الکترونیکی اتوبوس و مترو به‌کار گرفته می‌شوند.

استانداردهای کارت هوشمند

1- استانداردهای ISO/IEC : مهم‌ترین استانداردها در زمینه کارت هوشمند توسط سازمان بین‌المللی استاندارد، (ISO) با همکاری کمیسیون بین‌المللی صنایع الکترونیکی، IEC تدوین شده‌اند. استانداردهای ISO/IEC موجود در مورد کارت‌های تماسی به‌طور خلاصه شامل بندهای یکم الی شانزدهم استاندارد ISO/IEC 7816 بوده و در مورد کارت‌های غیرتماسی شامل سه استاندارد ISO/IEC 10536، ISO/IEC 14443 و ISO/IEC 15693 است.

2- استانداردهای CEN (کمیته اروپایی استاندارد)

3- استانداردهای EMV

4- استانداردهای ETSI

5- استانداردهای GSM : بیشتر مربوط به استانداردهای سیم کارت SIM

6- استاندارد Global Platform

مباحث رمزنگاری

الف- زیرساخت کلید عمومی PKI

یکی از موارد بهره‌گیری از کارت‌های هوشمند، استفاده از آن‌ها برای فعال‌سازی سازوکارهای مرتبط با ارائه اعتماد مبتنی بر زیرساخت کلید عمومی در سازمان و نیز نگهداری زوج کلیدهای کاربران است. از این رو، این دسته از کارت‌ها باید امکانات مورد نیاز برای تولید کلیدهای رمزنگاری، انجام فرایندهای رمزنگاری، تولید امضای دیجیتال و ارتباط با نرم‌افزارهای مجهز به زیرساخت کلید عمومی را در اختیار کاربران قرار دهند.

برای ارائه سطح مطلوب کارکردی و امنیتی در حوزه رمزنگاری مورد استفاده در زیر ساخت کلید عمومی، استانداردهای FIPS 140-2 و بخش پانزدهم ISO/IEC 7816 باید توسط کارت‌های هوشمند پشتیبانی شوند.

ب- الگوریتم‌های رمزنگاری

از طرفی برای رمزنگاری اطلاعات در کارت‌های هوشمند از الگوریتم‌های رمزنگاری از قبیل RSA، DES، AES و ... که در آن‌ها مولدهای اعداد تصادفی و توابع یک‌طرفه چکیده‌ساز به‌کار گرفته شده است، استفاده می‌شود. برای اطلاع بیشتر به [2] رجوع شود.

ج - حملات کانال جانبی

پیاده‌سازی الگوریتم‌های رمزنگاری در سامانه‌هایی مانند کارت هوشمند، منجر به نشت اطلاعات حساسی از مقادیر میانی الگوریتم می‌شود. این اطلاعات حساس از طریق کمیت‌های فیزیکی موسوم به کانال جانبی نشت می‌کند و می‌تواند اطلاعات مخفی سامانه را آشکار سازد. کارت هوشمند و سایر سامانه‌های رمزنگاری باید به‌گونه‌ای طراحی شوند که در برابر این تحلیل‌ها مقاوم باشند. از انواع حملات کانال جانبی، می‌توان به موارد زیر اشاره کرد[2]:

1- حمله تحلیل خطا
2- حمله تحلیل زمانی
3- حمله تحلیل توان
4- حمله تحلیل تشعشعات مغناطیسی و ....

چالش‌های استفاده از کارت هوشمند در کشور

با توجه به گسترش روز افزون استفاده از کارت‌های هوشمند در داخل کشور، تقریباً هر روز شاهد ارائه سرویس‌های جدید امنیتی مبتنی بر کارت هوشمند هستیم. اما آنچه که در حال حاضر، فرایند رشد و گسترش استفاده از کارت‌های هوشمند را مورد تهدید قرار می‌دهد، عدم وجود نظارت نظام‌مند و سازمان یافته بر فرایند تولید، توزیع و بهره‌گیری از این دسته محصولات است.

باید توجه داشت که برای اطمینان از ارائه سطح مطلوب امنیتی توسط کارت‌های هوشمند، علاوه بر انجام آزمون‌های فیزیکی و کارکردی، بایستی آزمون‌های امنیتی مختلفی نیز بر روی آن‌ها انجام شود. از جمله آزمون‌های مهمی که باید بر روی کارت‌های هوشمند انجام شوند و هم اکنون هیچ مرجعی در کشور، متولی انجام آن‌ها نیست، عبارتند از:

- آزمون‌های کارکرد کارت هوشمند مبتنی بر استانداردهای ISO/IEC
- آزمون‌های امنیت ماژول‌های رمزنگاری برای کارت هوشمند.
- آزمون ارزیابی امنیتی کارت‌های هوشمند
- ارزیابی مقاومت کارت‌های هوشمند در برابر حملات کانال جانبی

در حال حاضر، مرکز تحقیقات صنایع انفورماتیک، به‌عنوان متولی تدوین شاخص‌های ارزیابی کارت‌های هوشمند و انجام آزمون‌های مزبور، آمادگی ارائه مشاوره‌های لازم برای نیل به سطح مطلوب امنیتی و کارکردی در حوزه کارت‌های هوشمند را به سازمان‌ها و فعالان حوزه فناوری اطلاعات دارد.

نتیجه‌گیری

کارت‌های هوشمند از جمله متداول‌ترین و در عین حال حساس‌ترین ابزارهای تصدیق کاربر و ذخیره‌سازی اطلاعات سری هستند. استفاده از کارت‌های هوشمند در حوزه‌های بسیاری افزایش چشمگیری داشته است. سیم‌کارت و کارت‌های بانکی، نمونه‌هایی هستند که نشان می‌دهند تا چه حد این فناوری زندگی امروزه مردم جهان را تحت تأثیر قرار داده است. در این مقاله، به اختصار به معرفی کارت‌های هوشمند، دسته بندی، استانداردها و مباحث رمزنگاری مربوط به آن پرداختیم.

مراجع

[1] م. ریحانی تبار، "حمله به کارت‌های هوشمند با استفاده از اطلاعات نشتی"، کارشناسی ارشد: دانشگاه صنعتی شریف، 1381.
[2] ج. باقر زاده، "تحلیل توانی کارت هوشمند"، کارشناسی ارشد: دانشگاه صنعتی شریف، 1391.