عنوان مقاله:
حملات جانبی بر روی کارت های هوشمند و بررسی راهکاری ارائه شده برای جلوگیری از نشت اطلاعات محرمانه کارت

محل انتشار:
کنفرانس پدافند غیرعامل و توسعه پایدار (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
هادی اسکندری سبزی - *کارشناس ارشد مخابرات، مرکز تحقیقات صنایع انفورماتیک*

مهری یحیایی - *کارشناس ارشد فناوری اطلاعات، مرکز تحقیقات صنایع انفورماتیک*

خلاصه مقاله:
اغلب طراحان سامانه های رمزنگاری بر این باورند که مطالب رمز شده خود را در یک محیط بستهو امن ذخیره سازی و اداره کردهاند که قابل تحلیل و حمله نیست. یکی از این سامانه های رمزنگاریبر روی کارت های هوشمند پیاده سازی شده، که یکی از مهمترین ابزارهای تصدیق کاربر و ذخیرهاطلاعات محرمانه است که امروزه کاربرد وسیعی پیداکرده است. کارت های هوشمند دارای تراشهالکترونیکی و مغناطیسی می باشند که محیط مناسبی برای پیاده سازی الگوریتم های رمزنگاری وذخیره سازی اطلاعات هستند. این تراشه های الکترونیکی در حین انجام عملیات رمزنگاری ورمزگشایی جریان الکتریکی لازم را از منبع دریافت می کنند که این کار باعث به وجود آمدنفرآیندهای متفاوتی در تراشه میگردد. این فرآیندها می تواند از چندین نظر موردبررسی وتجزیه وتحلیل اطلاعات قرار گیرد، که استفاده کردن از این اطلاعات برای رسیدن به کلیدرمزنگاری را به اصطلاح حملات جانبی کانال گویند. یکی از قدرتمندترین و معمول ترین نوعحملات جانبی کانال استفاده از تجزیه وتحلیل توان مصرفی برای حمله است. در این نوع از حملاتسعی بر پیدا کردن یک راهحل و رابطه مناسب بین مصرف لحظه ای توان و وضعیت داخلی آن درزمان اجرای الگوریتم رمزنگاری است. ازآنجاییکه پیاده سازی الگوریتم های رمزنگاری در سامانه-هایی مانند کارت هوشمند، منجر به نشت اطلاعات حساسی از طریق مقادیر میانی الگوریتم می-گردد، پس اطلاعات حساس از طریق کمیت های فیزیکی موسوم به کانال جانبی نشت می کند، بهمراه اطلاعات در دسترس از ساختار ریاضی الگوریتم رمز پیاده سازی شده در سیستم، به منظوراستخراج کلید محرمانه به کاررفته، استفاده می شود و می توانند اطلاعات مخفی سامانه را آشکارسازند. ما در این مقاله به بررسی حمله های موفقی که با استفاده از نشت اطلاعات جانبی بر روی کارت هوشمند اعمال شده اند پرداخته و درنهایت با ارائه راهکارهایی که می تواند برای جلوگیری از حملات احتمالی بر روی کارت های هوشمند اعمال گردد می پردازیم.

کلمات کلیدی:
حملات جانبی کانال، کارت هوشمند، رمزنگاری، تجزیه تحلیل توان، نشت اطلاعات