عنوان مقاله:
حمله کانال جانبی به منظور مهندسی معکوس کد برنامه درحال اجرا بر روی یک میکروکنترلر

محل انتشار:
چهارمین کنفرانس ملی و دومین کنفرانس بین المللی پژوهش های کاربردی در مهندسی برق، مکانیک و مکاترونیک (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
عاطفه فلاح - *دانشجوی کارشناسی ارشد مخابرات رمز دانشگاه صنعتی مالک اشتر،تهران*

علیرضا قهرمانیان - *مجتمع دانشگاهی فناوری اطلاعات ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران*

حسین بهرامگیری - *استادیار، گروه مخابرات، دانشگاه صنعتی مالک اشتر، تهران*

خلاصه مقاله:
حملات کانال جانبی تقریبا به مدت یک دهه تنها برای استخراج کلید در الگوریتم های رمزنگاری استفاده می شد که در همان زمان مشخص شد از اطلاعات کانال جانبی می توان اطلاعات بسیار دیگری استخراج کرد. یکی از این کاربردها استخراج کد در حال اجرا بر روی میکروکنترلر می باشد. این مساله با حمله الکترومغناطیس به انجام رسیده است، و ما در این مقاله با استفاده حمله را مبتنی بر تحلیل توان مصرفی اجرا می کنیم. تا کنون تکنیک های مختلفی ارایه شده است، که ما نیزدر این مقاله پیرو کارهای انجام شده مسیله استخراج کد را به یک مسیله طبقه بندی تبدیل می کنیم، بدین صورت که هر دستورالعمل میکروکنترلر را به عنوان یک کلاس در نظر می گیریم و با استفاده از الگوریتم های کاهش ابعاد مانندPCA وLDA اطلاعات منحصر به فرد هر کلاس را استخراج کرده و سپس با استفاده از الگوریتم KNN طبقه بندی را انجام می دهیم. در اینجا از روش های مختلف کاهش ابعاد استفاده نموده ایم و در نهایت با استفاده از الگوریتم LDA برای 4 دستور به بیشترین نرخ استخراج برابر 80.75 درصد رسیدیم.

کلمات کلیدی:
حمله تحلیل توان، میکروکنترلر، مهندسی معکوس،SCANDAL، KNN، PCA، LDA