

عنوان مقاله:

دسته بندی و پیاده سازی تروجان های سخت افزاری و ارائه راهی نوین برای کشف آن ها

محل انتشار:

دوفصلنامه فناوری اطلاعات و ارتباطات ایران، دوره 9، شماره 31 (سال: 1398)

تعداد صفحات اصل مقاله: 20

نویسنده:

محمدباقر غزنوی قوشچی

خلاصه مقاله:

در سال های اخیر نوعی حمله سخت افزاری به نام تروجان سخت افزاری مطرح شده است که فرد متخاصم با تغییرات بدخواهانه بر روی تراشه، آن را برای رسیدن به مقصود خود آماده می کند. هدف از این حملات از کار انداختن تراشه، تغییر مشخصات و بدست آوردن اطلاعات حساس می باشد. در این مقاله ابتدا دسته بندی مناسبی از انواع تروجان های سخت افزاری و روش های کشف و مقابله با آن ها انجام شده است. در ادامه چهار نمونه عملی تروجان بر روی الگوریتم رمزنگاری DES پیاده سازی شده و نتایج آن مورد بررسی قرار گرفته است. سپس سخت افزاری بر پایه مشخصه تاخیر مدار پیشنهاد شده است که ورودی آن فرکانس حلقه های نوسانگر تعبیه شده در مدار تحت تست و خروجی آن یک رشته بیت متناظر با چالش اعمال شده می باشد. سخت افزار پیشنهادی به گونه ای طراحی شده است که در صورت تغییر در مدار اصلی، با تغییر در فرکانس حلقه های نوسانگر و در نتیجه رشته بیت مورد انتظار، وجود سخت-افزار تروجان را مشخص می کند. از طرفی با بررسی عوامل موثر بر فرکانس حلقه نوسانگر از جمله دما، ولتاژ و تغییرات پروسس، حلقه های نوسانگری برای تعبیه درون مدار توصیه شده است که باعث کاهش تغییرات فرکانس در برابر این عوامل شده و تغییرات فرکانس ناشی از این عوامل به منزله تغییر فرکانس ناشی از حمله به سخت افزار تلقی نمی شود و در نتیجه با حذف عوامل تاثیرگذار منفی محیطی در مدار طراحی شده، سخت افزار پیشنهادی با دقت بالایی برای کاربرد کشف تروجان پیشنهاد شده است.

کلمات کلیدی:

امنیت، تغییرات خرابکارانه، تروجان سخت افزاری، کشف تروجان، حلقه نوسانگر

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1859460>

