

عنوان مقاله:

تحلیلی بر روش های کشف حمله ی سخت افزاری در سیستم های توکار

محل انتشار:

همایش ملی مهندسی کامپیوتر و فناوری اطلاعات (سال: 1392)

تعداد صفحات اصل مقاله: 6

نویسنده:

علی دری - دانشگاه آزاد اسلامی واحد مشهد، انجمن علمی کامپیوتر، مشهد، ایران

خلاصه مقاله:

سیستم های توکار، کامپیوتر های کوچکی هستند که عضوی از سیستم یا ماشین بزرگ تر بوده و وظیفه یا کار خاصی را انجام می دهند. این سیستم ها معمولا برنامه های محدودی را اجرا می کنند که غالبا از نوع کنترلی هستند، به همین دلیل امنیت در این سیستم ها به یکی از مهمترین چالش ها تبدیل شده است. کشف حمله یکی از چالش های امنیتی این نوع سیستم هاست. با توجه به اینکه سیستم های کشف حمله نرم افزاری دارای تاخیر در کشف حمله هستند و حمله را پس از وقوع کشف می کنند، گزینه ی مناسبی برای سیستم های توکار نیستند. در سیستم توکار با توجه به کاربرد های این سیستم لازم است حمله در لحظه ی وقوع کشف شود. از جمله بهترین راه کارهای دفاع در برابر حمله، کشف حمله ی سخت افزاری است که با کمترین تاخیر و قبل از اجرای کد مخرب، آن را کشف می کند. در این مقاله مروری بر انواع روش های کشف حمله در سیستم های توکار خواهیم داشت و پس از آن با تمرکز بر روش های سخت افزاری، انواع روش های سخت افزاری ارائه شده را بررسی و مزایا و کاستی های آن ها را بر خواهیم شمرد و با ارزیابی روش ها در پارامترهای متفاوت که دارای اهمیت هستند، نحوه ی عملکرد آن ها را مقایسه خواهیم کرد.

کلمات کلیدی:

سیستم های توکار، امنیت، حملات هکری، سیستم کشف حمله، سیستم کشف حمله سخت افزاری

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/254277>

