بسمه تعالی

☐ دفاع از رساله دکتری ☐ سمینار عمومی (Colloquium)

■ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ سمینار تخصصی (Seminar)

☐ سمینار تخصصی و مشورتی (Informal Seminar)

عنوان : طراحی و پیاده‌سازی مدارات جمع‌کننده دهدهی کارآمد در منطق سه‌مقداری با استفاده از تکنولوژی CNFET

سخنران : مریم طولابی نژاد

چکیده:

از ابتدای علم پردازش، پردازنده‌ها سهم بسیار بزرگی از بازار بسترهای سخت‌افزاری را در اختیار داشته‌اند. در واقع نقش حیاتی این دسته از تراشه‌ها در جنبه‌های مختلف دنیای امروز، از سیستم های نظامی و صنعتی و حفظ سلامت تا سیستم‌های مسیریابی غیرقابل انکار است. از طرفی وابستگی انسان به نتایج پردازش و وجود انگیزه خراب‌کاری در سیستم‌های کامپیوتری، نگرانی را در مورد صحت عملکرد و نیاز به امکان اطمینان را بوجود می‌آورد. عامل دیگری که مشخصاً خطر حمله به سخت افزار را جدی می‌کند، مدل تجاری فعلی در تولید تراشه‌های نیمه‌هادی است که با برون‌سپاری ساخت تمام اطلاعات طراحی و اجزای چینش در اختیار فرد سوم قرار می‌گیرد که تشخیص امانت داری او بعد از تحویل تراشه فیزیکی سخت و یا ناممکن است. از این رو روش هایی برای محافظت سخت‌افزارها در مقابل دست‌کاری‌های بدخواهانه‌ی فیزیکی ارائه شده‌است.

ایده‌های طراحی پردازنده امن در مراحل مختلف از طراحی تا ساخت و بسته به نوع حمله‌ی درنظر گرفته‌شده، در اجزای مختلف سیستم ارائه شده‌اند. این پژوهش به مقابله با حمله‌ی درج تروجان در پردازنده در مرحله‌ی ساخت فیزیکی می‌پردازد. روش ارائه شده امکانی را فراهم می‌کند تا با بررسی روند تغییر مقادیر سیگنال‌های کنترلی پردازنده در حین اجرای برنامه، بتوان صحت اجرای آن را تحلیل و تضمین کرد. این روش با انعطاف‌پذیری در مقابل انتخاب نواحی مورد پایش و تعریف تحلیل‌های متنوع از گزارش بدست‌آمده در حین اجرا، حملات بسیار زیادی را مورد پوشش و کشف قرار می‌دهد.

یکی از نقاط آسیب‌پذیر روش‌های قبلی در مقابل خطر درج تروجان، تصمیم‌گیری در مورد قابلیت اعتماد در سطح سخت‌افزار بوده‌است که با وجود افزایش ایمنی تشخیص، خود در مقابل خطر دست‌کاری خراب‌کارانه آسیب‌پذیر هستند. روش ارائه شده در این پژوهش با جدا کردن واحد تشخیص حمله از لایه‌ی سخت‌افزاری و انتقال آن به نرم‌افزار تحلیل‌گر امن، امکان دسترسی به نتایج تحلیل را از حمله کننده دور می‌کند و توان تحلیل‌های پیچیده‌تری را به استفاده‌کننده می‌دهد. در عین حال این گزارش‌های ویژگی‌های تروجان‌ها به عنوان یک پایگاه داده جهانی قابل به اشتراک‌گذاری بین تمام مصرف‌کنندگان این پردازنده می‌باشد و راهنمای طراحان و برنامه‌نویسان برای مراقبت از پردازش در مقابل حملات شناخته‌شده می‌شود.

برای ارزیابی عملکرد این روش دسته تروجان‌های گزارش شده‌ی مشخصی به بستر پردازنده ARM۷ تزریق شده‌است و با اجرای برنامه‌های آزمون معتبر و برنامه‌های معمول اجرا شده روی پردازنده، این آلودگی‌ها در گزارش دیده شده و توسط تحلیل‌گر کشف شده‌اند. با انتخاب درست سیگنال‌های مورد پایش، ٪ ۱۰۰حملات هدف قابل شناسایی هستند. سربار پیاده‌سازی این روش در سخت-افزار ٪ ۵ و بسیار کمتر از ایده‌های مشابه بوده‌است و تاثیر قابل مشاهده‌ای بر تاخیر و کارایی پردازنده نداشته‌است

زمان برگزاری: ۹۶/۱۲/۰۹

مکان برگزاری: دانشکده مهندسی و علوم کامپیوتر