****

**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **نام استاد راهنما:**  **جناب آقای دکتر علی جهانیان** | | | **نام دانشجو:**  **زهرا اطهاری نیکوروان** | |
| **گرایش: معماری کامپیوتر** | **رشته: مهندسی کامپیوتر** | | | **مقطع: کارشناسی ارشد** |
| **تاریخ: 27/7/1401** | | | **نوع دفاع:**   * **دفاع پروپوزال □** * **دفاع پایان نامه 🗷** * **دفاع رساله دکترا □** | |
| **ساعت: 10:30 تا 12:00** | | |
| **مکان: دانشکده مهندسی کامپیوتر – کلاس 200** | | |
| **عنوان: ارائه یک معماری مقاوم در برابر حمله مبتنی بر معماری شبح** | | | | |
| **داوران داخلی: جناب آقای دکتر مقصود عباسپور** | | **داوران خارجی: جناب آقای دکتر بیژن علیزاده** | | |
| **چکیده:**  با گسترش روزافزون سیستم‌های کامپیوتری، حفظ امنیت این سیستم‌ها بیش‌ازپیش موردتوجه قرار گرفته است. امنیت می‌تواند در لایه‌های مختلفی، از امنیت قطعات استفاده‌شده در مدار، تا کدهای سطح بالای نرم‌افزاری، موردمطالعه قرار گیرد. در این میان، امنیت سخت‌افزار از اهمیت بالایی برخوردار است. یکی از مباحث حوزه امنیت سخت‌افزار که در سال‌های اخیر به‌شدت موردتوجه قرار گرفته است، بحث حملات مبتنی بر اجرای گذرا است. حملات شبح، گونه‌ای از این حملات هستند که با نفوذ در رفتار پردازنده‌های مدرن، روی طیف زیادی از پردازنده‌ها موفق عمل می‌کنند.  از زمان معرفی این حملات، شاهد ارائه روش‌های مقابله با آنها در سطوح مختلف بوده‌ایم. در این پایان‌نامه، به ارائه یک روش مقابله نوین و مؤثر در برابر این حملات در سطح معماری پرداخته‌ایم. برای نیل به این هدف، تمرکز اصلی روی تحلیل چگونگی نشت اطلاعات مخفی از حافظه نهان است. روش پیشنهادی، با تحلیل دقیق چگونگی رفتار حملات شبح، به ارائه یک روش رمزگذاری برای پنهان کردن اطلاعات مخفی از دید مهاجم می‌پردازد، به‌طوری اطمینان حاصل شود که مهاجم تنها قادر به دسترسی به اطلاعات مخفی به‌صورت رمزشده ‌است. اساس این روش، رمزگذاری داده‌ها در گذرگاه ارتباطی بین حافظه و پردازنده است.  روش پیشنهادی با استفاده از شبیه‌ساز Gem5 روی معماری X86 پیاده شد. نتایج نشان داد که با اعمال این روش محافظتی، جلوی نشت اطلاعات سری از طریق حمله شبح گرفته می‌شود. معماری پیاده‌سازی‌شده دارای سربار زمانی 5.7% نسبت به معماری غیر امن بود که نتیجه موفقی قلمداد می‌شود. سنتز کد سخت‌افزاری معماری پیشنهادی نشان داد که پیاده‌سازی این معماری باعث افزایش مساحت به میزان تنها 120 میکرومتر مربع می‌گردد. این عدد در مقایسه با مساحت معماری X86، بسیار ناچیز و قابل چشم‌پوشی است. همچنین افزایش توان به میزان 105 میکرووات خواهدبود که این عدد نیز بسیار کوچک است. | | | | |