****

**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **نام استاد راهنما:**  جناب آقای دکتر علی جهانیان | | | D:\Important Info\Personal Pic\vahhab_samadi-320.png**نام دانشجو:**  وهاب صمدی بخارائی | |
| **مقطع:** دکتری | **گرایش:** معماری سیستم‌های کامپیوتری | | | **رشته:** مهندسی کامپیوتر |
| **تاریخ: سه شنبه - 24/12/۱۴۰۰** | | | **نوع دفاع:**   * دفاع نهائی رساله | |
| **ساعت: ۱۵:00 الی 17:00** | | |
| **مکان:**  <http://194.225.24.96/defa-computer-3/> | | |
| **عنوان**  **ارائه روند طراحی آگاه از امنیت کانال جانبی برای تراشه‌های خاص‌منظوره** | | | | |
| **داوران داخلی:**  جناب آقای دکتر مقصود عباسپور  جناب آقای دکتر حمیدرضا مهدیانی | | **داوران خارجی:**  جناب آقای دکتر مرتضی صاحب الزمانی  جناب آقای دکتر بیژن علیزاده ملفه | | |
| **چکیده:**  حملات کانال جانبی توان مصرفی گروهی مهم از حملات کانال جانبی هستند که تلاش دارند از آسیب‌پذیری‌های موجود در پیاده‌سازی فیزیکی مدارها، جهت استخراج اطلاعات محرمانه و تهاجم به آنها استفاده کنند. یکی از چالش­های مهم از منظر طراحان سخت‌افزار در روند خودکار طراحی، نبود سنجه‌‌ها، ابزارها و روش­هایی است که به صورت خودکار بتوانند سطح امنیت یک مدار را در خلال روند طراحی استخراج کنند. علاوه بر آن، ابزارهای فعلی مورد استفاده مهندسان هیچ رهنمود یا گزارشی را به آنها در مورد موقعیت یا منشأ آسیب‌پذیری‌های کانال جانبی در مراحل قبل ازساخت طراحی بر روی سیلیکون ارائه نمی‌دهند.  در این رساله ما قصد داریم تا بر محدودیت­های موجود در این حوزه فائق آییم و روشگانی را ارائه کرده‌ایم تا بتواند منشأ ناامنی‌های کانال جانبی یک تراشه خاص منظوره را در خلال روند طراحی آن شناسایی و موقعیت‌یابی کند. پیش از آن، ما تلاش خواهیم کرد تا به این پرسش پاسخ دهیم که آیا می‌توان از سنجه‌های ارزیابی امنیت کانال جانبی که در مراحل بعد از ساخت بر روی سیلیکون استفاده می‌شوند، در مراحل قبل از سیلیکون استفاده نمود یا خیر؟ بدین منظور توانمندیهای پارامتر تی در آزمون تی مورد بررسی و ارزیابی درسنجش امنیت کانال جانبی در مراحل قبل از ساخت مورد بررسی قرار گرفته است. پس از آن، ما لیستی از ویژگی­هایی را ارائه کرده‌ایم که یک سنجه باید واجد آن باشد تا بتوان از آن در ابزارهای خودکار طراحی تراشه‌های خاص منظوره و روند سنجش امنیت کانال جانبی بهره برد.  در نهایت، ما روشگان پیشنهادی خود جهت سنجش یک طراحی از منظر امنیت کانال جانبی را مطرح کرده‌ایم. این روشگان در قالب یک چارچوب به نام «Patch» پیاده‌سازی شده‌است که می‌تواند نشت کانال جانبی را با دقت یک سیگنال در سطح یک طراحی شناسایی و مکان‌یابی کند. این چارچوب با ابزاری به نام «Injection» همراهی می‌گردد که این ابزار توانایی درج خودکار مقاوم‌سازی در نقاط آسیب‌پذیر طراحی را دارا می‌باشد. نتایج بدست‌آمده نشان می‌دهد که با درج مقاوم‌سازی‌های انجام‌شده، با توجه به سطوح حساسیت‌ مختلف در مراحل تشخیص آسیب‌پذیری، تعداد حداقل دنباله‌های توان برای کشف کلیدرمزنگاری در مدار AES مورد آزمون، بین 14% الی 437% افزایش داشته‌است. این میزان از امنیت در قبال سربار فضای سیلیکون مصرفی بین %8/1 الی %‌5/49 حاصل شده‌است. مدت زمانی که به صورت خاص برای انجام پردازشهای لازم برای تحلیل و بهینه‌سازی امنیت جانبی به روند طراحی تحمیل شده است، کمتر از 6 دقیقه برای یک مدار AES-128 بوده است. | | | | |