****

**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C:\Users\Mojtaba\Dropbox\Screenshots\pic.png**نام دانشجو:**  **مجتبی گزمه** | | | **نام استاد راهنما:**  **جناب آقای دکتر علی جهانیان** | |
| **رشته: مهندسی کامپیوتر** | **گرایش: معماری سامانه های کامپیوتری** | | | **مقطع: دکتری** |
| **نوع دفاع:**   * **دفاع پروپوزال ▪** * **دفاع پایان نامه □** * **دفاع رساله دکتری □** | **تاریخ: 10/05/1400** | | | |
| **ساعت: 15 الی 17** | | | |
| **مکان:** [http://194.225.24.96/defa-computer-](http://194.225.24.96/defa-computer-3)4 | | | |
| **عنوان: تشخیص تروجان سخت‌افزاری زمان اجرا در مدارهای مجتمع عام­منظوره مبتنی بر داده­های پیش از ساخت** | | | | |
| **داوران خارجی:**  **جناب آقای دکتر بیژن علیزاده**  **جناب آقای دکتر مرتضی صاحب الزمانی** | | **داوران داخلی:**  **جناب آقای دکتر مقصود عباسپور**  **جناب آقای دکتر دارا رحمتی** | | |
| چکیده:  **در سال‌های اخیر در طراحی مدارهای مجتمع، روند رو به رشدی وجود داشته است که توانسته جنبه‌های مختلفی از طراحی نیمه‌هادی و جریان تولید را در سراسر جهان پخش کند. درواقع، برای پایین آوردن هزینه طراحی و ساخت مدارهای مجتمع، زنجیره تأمین صنعت نیمه‌هادی در سراسر جهان توزیع‌شده است. با افزایش پیچیدگی IC‌ها، شرکت‌های بیشتری درگیر فرآیند ساخت IC می‌شوند تا کارایی و قابلیت تولید را بهبود بخشند. چنین برون‌سپاری باعث می‌شود که مهاجمان مدارهای مخربی را که به آن تروجان‌های سخت‌افزاری می‌گویند، به طرح اصلی اضافه کنند. تروجان‌های سخت‌افزاری با خطاهای ایجادشده در هنگام طراحی متفاوت هستند. درواقع خطاها با انجام آزمون‌هایی (اِعمال ورودی به مدار و ارزیابی خروجی آن) تشخیص داده می‌شوند، اما تروجان‌های سخت‌افزاری با این روند آزمون قابل‌تشخیص نیستند، چراکه تروجان‌ها توسط یک فرد متخصص در مکان‌ها یا زمان‌هایی فعال می‌شوند که تشخیص آن با روش‌های معمول آزمون ساده نیست. ازاین‌رو برای تشخیص تروجان‌های سخت‌افزاری باید به دنبال راهکارهایی باشیم که بتوان با احتمال بالا و در زمان و هزینه توجیه‌پذیر این تروجان‌ها را تشخیص دهیم. روش‌های مقابله با تروجان سخت‌افزاری متفاوتی وجود دارد که در سطوح متفاوتی از طراحی اعمال می‌شود. به‌عنوان‌مثال می‌توان با تحلیل کد سطح RTL منطق‌های مخرب را شناسایی کرد. یک دسته از روش‌های تشخیص تروجان، یافتن تروجان سخت‌افزاری در زمان اجرا است. در این روش، یافتن تروجان، به‌صورت هم‌زمان با کارکرد عادی سیستم است. در این روش‌ها می‌توان با استفاده از اندازه‌گیری ویژگی‌های پیش از ساخت و تحلیل و تجزیه و مقایسه آن‌ها با ویژگی‌های پس از ساخت برای تشخیص تروجان سخت‌افزاری استفاده کرد. از مزایای این روش نسبت به سایر روش‌ها می‌توان تشخیص تروجان‌های سالخوردگی را نام برد. همچنین تروجان‌هایی که توسط سیگنال‌های خارجی خاصی فعال می‌شوند نیز تنها با این روش شناسایی می‌شوند. یکی از معایب این روش افزایش مساحت اشغال‌شده و توان مصرفی سیستم است.**  **در این رساله هدف طراحی یک سیستم تشخیص تروجان سخت‌افزاری است که با اندازه‌گیری داده‌های پیش از ساخت و تحلیل و مقایسه آن‌ها با داده‌های پس از ساخت در زمان اجرا بتوان انواع تروجان‌های بعد از ساخت و همچنین تروجان‌هایی که فقط در زمان اجرا فعال می‌شوند را شناسایی کرد.** | | | | |