IranArze.ir

بخشی از ترجمه مقاله

عنوان فارسی مقاله :

تحلیل حساسیت روشهای سیگنال توان به منظور آشکارسازی سخت افزار تروجان در شرایط محیطی و فرایند واقعی

عنوان انگلیسی مقاله :

A Sensitivity Analysis of Power Signal Methods for Detecting Hardware Trojans Under Real Process and Environmental Conditions

Reza Rad, *Member, IEEE*, Jim Plusquellic, *Member, IEEE*, and Mohammad Tehranipoor, *Senior Member, IEEE*

ایران عرضه
مرجع مقالات
ترجمه شده

توجه !

این فایل تنها قسمتی از ترجمه میباشد.

برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انکلیسی مقاله، اینجا کلیک نمایید.

پیشینه

ظهور مدل تجاری نیمه هادی افقی جهانی مجموعه نگرانیهایی در ارتباط با امنیت و اعتماد سیستم های اطلاعاتی خلق نموده است که جامعه مدرن همواره به خاطر تابعیت حساس برآن تکیه می کند. موضوعات امنیت و اعتماد سخت افزاری طیف وسیعی داشته و تهدیدهای وابسته به تعبیه خرابکارانه مدارهایTrojan تعبیه شده به منظور کارهای زیر را در برمی گیرد: عمل کردن به صورت kill switch جهت از کار انداختن تراشه، دزدی مدار مجتمع (IC) ، حملات طراحی شده به منظور استخراج کلیدهای رمزگشایی و IP از تراشه و وقفه در سیستم و انحراف آن. از میان تهدیدهای مذکور، تعبیه خرابکارانه سخت افزار Trojan در IC نگرانی نسبتاً جدیدی در زمینه اعتماد به شمار می رود که به همراه سایر ریسک های امنیتی سخت افزار می بایست به آن رسیدگی شو د.

در بخش بعدی شیوه های پیشنهاد شده در پاسخ به نیاز به روش های تشخیص و آشکارسازی Trojan جمع بندی می گردد. تحلیل کمبودهای شیوه های پیشنهاد شده اعلان شیوه های مطلوب به عنوان راه حل مسئله را با مشکل مواجه می کند. اگرچه استراتژی بکاررفته نسبت به سایر روشهای تحلیل سیگنال توان محاسن منحصر به فردی دارد، اما راه حل کاملی برای این مسئله به شمار نمی رود، مثلاً روش معرفی شده موضوع محرک تست را در نظر نمی گیرد. بنابراین بهترین راه حل احتمالاً ترکیبی از شیوه تحلیل سیگنال و ویژگیهای سایر روشهای پیشنهاد شده در قسمت ذیل می باشد .

II. ROUNDoqBACKG

The emergence of a globalized, horizontal semiconductor business model raises a set of concerns involving the security and trust of the information systems on which modern society is increasingly reliant for critical functionality. Hardware security and trust issues span a broad range including threats related to the malicious insertion of Trojan circuits designed, e.g., to act as a “kill switch” to disable a chip, to integrated circuit (IC) piracy, to attacks designed to extract encryption keys and IP from a chip, and to malicious system disruption and diversion. Of these threats, the malicious insertion of hardware Trojans in ICs is a relatively new trust concern that must now be addressed in combination with other hardware security risks.

The following briefly summaries the approaches proposed by others in response to the need for Trojan detection methods. An analysis of the deficiencies of each of the proposed approaches makes it difficult to declare any one of these approaches as a solution to the problem. Although our strategy provides several unique advantages over other power signal analysis methods, it is not a complete solution for this problem, e.g., our method does not address the test stimulus issue. Therefore, the best solution is likely a combination of our signal analysis approach with features from other proposed methods as described below.

ایران عرضه
مرجع مقالات
ترجمه شده

توجه !

این فایل تنها قسمتی از ترجمه میباشد.

برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

همچنین برای مشاهده سایر مقالات این رشته اینجا کلیک نمایید.