1. Hardware Trojans classification for gate-level netlists based on machine learning

Accession number: 16410066
Authors: Hasegawa, K. (1); Oya, M. (1); Yanagisawa, M. (1); Togawa, N. (1)
Author affiliation: (1) Dept. of Comput. Sci. & Commun. Eng., Waseda Univ., Tokoyo, Japan
Source: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)
Publication date: 2016
Pages: 203-6
Language: English
ISBN-13: 978-1-5090-1507-8
Document type: Conference article (CA)
Conference name: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)
Conference date: 4-6 July 2016
Conference location: Sant Feliu de Guixols, Spain
Sponsor: IEEE Council on Electron. Design Autom.
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXB6-1902-553
Abstract: Recently, we face a serious risk that malicious third-party vendors can very easily insert hardware Trojans into their IC products but it is very difficult to analyze huge and complex ICs. In this paper, we propose a hardware-Trojan classification method to identify hardware-Trojan infected nets (or Trojan nets) using a support vector machine (SVM). Firstly, we extract the five hardware-Trojan features in each net in a netlist. Secondly, since we cannot effectively give the simple and fixed threshold values to them to detect hardware Trojans, we represent them to be a five-dimensional vector and learn them by using SVM. Finally, we can successfully classify a set of all the nets in an unknown netlist into Trojan ones and normal ones based on the learned SVM classifier. We have applied our SVM-based hardware-Trojan classification method to Trust-HUB benchmarks and the results demonstrate that our method can much increase the true positive rate compared to the existing state-of-the-art results in most of the cases. In some cases, our method can achieve the true positive rate of 100%, which shows that all the Trojan nets in a netlist are completely detected by our method.
Number of references: 11
Inspec controlled terms: invasive software - learning (artificial intelligence) - pattern classification - support vector machines
Uncontrolled terms: hardware Trojans classification - gate-level netlists - machine learning - malicious third-party vendors - IC products - hardware-Trojan infected nets - support vector machine - five-dimensional vector - learned SVM classifier - SVM-based hardware-Trojan classification - trust-HUB benchmarks
Inspec classification codes: C5480 Security aspects of hardware - C6130S Data security - C6170K Knowledge engineering techniques
Treatment: Practical (PRA)
Discipline: Computers/Control engineering (C)
DOI: 10.1109/IOLTS.2016.7604700
IPC Code: G06F15/18 - G06F21/00 - G06N5/04
Database: Inspec
Copyright 2016, The Institution of Engineering and Technology
Data Provider: Engineering Village