1. Testing for Hardware Trojans: A Game-Theoretic Approach

Accession number: 14636191
Authors: Kamhoua, C.A. (1); Rodriguez, M. (1); Kwiat, K.A. (1)
Author affiliation: (1) Inf. Directorate, Air Force Res. Lab., Rome, NY, United States
Source: Decision and Game Theory for Security. 5th International Conference, GameSec 2014. Proceedings: LNCS 8840
Publication date: 2014
Pages: 360-9
Language: English
ISBN-13: 978-3-319-12600-5
Document type: Conference article (CA)
Conference name: Decision and GameTheory for Security. 5th International Conference, GameSec 2014
Conference date: 6-7 Nov. 2014
Conference location: Los Angeles, CA, USA
Publisher: Springer International Publishing
Place of publication: Cham, Switzerland
Material Identity Number: YXB4-1901-839
Abstract: The microcircuit industry is witnessing a massive outsourcing of the fabrication of ICs (Integrated Circuit), as well as the use of third party IP (Intellectual Property) and COTS (Commercial Off-The-Shelf) tools during IC design. These issues raise new security challenges and threats. In particular, it brings up multiple opportunities for the insertion of malicious logic, commonly referred to as a hardware Trojan, in the IC. Testing is typically used along the IC development lifecycle to verify the functional correctness of a given chip. However, the complexity of modern ICs, together with resource and time limitations, makes exhaustive testing commonly unfeasible. In this paper, we propose a game-theoretic approach for testing digital circuits that takes into account the decision-making process of intelligent attackers responsible for the infection of ICs with hardware Trojans. Testing for hardware Trojans is modeled as a zero-sum game between malicious manufacturers or designers (i.e., the attacker) who want to insert Trojans, and testers (i.e., the defender) whose goal is to detect the Trojans. The game results in multiple possible mixed strategy Nash equilibria that allow to identify optimum test sets that increase the probability of detecting and defeating hardware Trojans in digital logic.
Number of references: 9
Inspec controlled terms: circuit complexity - decision making - game theory - industrial property - integrated logic circuits - invasive software - logic testing
Uncontrolled terms: mixed strategy Nash equilibria - zero-sum game - intelligent attackers - decision-making process - digital logic circuit testing - IC complexity - integrated circuit testing - IC development lifecycle - malicious logic insertion - IC design - commercial off-the-shelf tools - COTS - third party IP - intellectual property - IC fabrication - microcircuit industry - game-theoretic approach - hardware trojans
Inspec classification codes: B1265B Logic circuits - B0240E Game theory - B1265A Digital circuit design, modelling and testing - C5120 Logic and switching circuits - C1140E Game theory - C6130S Data security
Treatment: Practical (PRA); Theoretical or Mathematical (THR)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1007/978-3-319-12601-2_22
IPC Code: G06F11/25 - G06F21/00 - H03K19/00 - G01R31/3183
Database: Inspec

Data Provider: Engineering Village