1. Hardware Trojans: current challenges and approaches

Accession number: 14738830
Authors: Jacob, N. (1); Merli, D. (1); Heyszl, J. (1); Sigl, G. (1)
Author affiliation: (1) Fraunhofer AISEC, Garching, Germany
Source title: IET Computers & Digital Techniques
Abbreviated source title: IET Comput. Digit. Tech. (UK)
Volume: 8
Issue: 6
Publication date: Nov. 2014
Pages: 264-73
Language: English
ISSN: 1751-8601
CODEN: ICDTA6
Document type: Journal article (JA)
Publisher: IET
Country of publication: UK
Material Identity Number: DW19-2014-005
Abstract: More and more manufacturers outsource parts of the design and fabrication of integrated circuits (ICs) for cost reduction. Recent publications show that such outsourcing can pose serious threats to governments and corporations, as they lose control of the development process. Until now, the threat of hardware Trojans is mostly considered during fabrication. Third party intellectual properties (IPs) are also gaining importance as companies wish to reduce costs and shorten the time-to-market. Through this study, the authors argue that the threat of Trojans is spread throughout the whole IC development chain. They give a survey of both hardware Trojan insertion possibilities and detection techniques. Furthermore, they identify the key vulnerabilities at each stage of IC development and describe costs of hardware Trojan insertion and detection. This way, the threat level based on feasibility of Trojan insertion and the practicability of Trojan detection techniques is evaluated. Lately, detection techniques address the issue of including third party IP. However, those techniques are not sufficient and need more research to effectively protect the design. In this way, the authors' analysis provides a solid base to identify the issues during IC development, which should be addressed with higher priority by all entities involved in the IC development.
Number of references: 48
Inspec controlled terms: integrated circuits - invasive software
Uncontrolled terms: Trojan detection techniques - Trojan insertion - detection techniques - IC development chain - IP - intellectual properties - cost reduction - manufacturers outsource parts - Hardware Trojans
Inspec classification codes: B2220 Integrated circuits - C6130S Data security
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1049/iet-cdt.2014.0039
IPC Code: G06F21/00
Database: Inspec

Data Provider: Engineering Village