SAND2018-7536D

The Center for Cyber Defenders

Expanding computer security knowledge

Microarchitectural Diversity

Disabling Trojans with Automated Digital Circuit Modification

Jonathan Cruz, PhD Student, University of Florida

Project Mentor: Jason Hamlet

Problem Statement:

- Globalization of the semiconductor industry has fostered wide-spread adoption of a horizontal business model.
- Untrusted third-party IP (3PIP) vendors can introduce malicious functionality known as Hardware Trojans.
- It is infeasible to exhaustively test circuits to detect malicious modifications.

Objectives and Approach:

- *Goal*: Disable or eliminate Trojans in digital circuits.
- Given 3PIP:
  1. Convert IP into graph and simulate to estimate signal probabilities.
  2. From suspect nodes, enumerate k-bit slices.
  3. Identify suspect slices by comparing BDD of k-bit slice to known comparator structures.
  4. Diversify (add/remove/ invert) suspect slice and simulate circuit.
  5. Keep changes if resulting circuit satisfies comprehensive test vectors.

Results

- We ran our approach on three Trojan-inserted RTL benchmarks publicly available on Trust-Hub.
- From Table I, we observe that all Trojans comparators were successfully identified.

Benchmark	No. Gates	Identified Structures	FN	% Troj.
RS232-T400	322	20	0	1/20
RS232-T700	363	26	0	3/26
RS232-T800	304	20	0	1/20

TABLE I: Analysis of Identification on Trust-Hub Benchmarks

Impact and Benefits:

- Our approach can successfully identify Trojans structures in a 3PIP.
- Next steps are to disable the Trojans by modifying the gate structure of the comparator trigger, simulate the design, and verify the effects.
- Along with standard verification techniques, diversification can be used for defense-in-depth for protecting against hardware Trojans.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.