Eliminating Timing Information Flows in a Mix-trusted System-on-Chip

Tech ID: 23220 / UC Case 2013-197-0

BACKGROUND

Modern computing systems continue to find themselves in control of applications

which we rely on for our personal health and safety. These systems which require high-assurance have a very high cost of failure. In order to build such a system with complete security, it must be built with a secure computing foundation. Creating such a secure hardware foundation is non-trivial for a number of reasons. One of which is due to the use of third-party intellectual property cores to reduce both the cost and design time of modern system-on-chips (SOC). Ensuring the integrity of trusted cores in these systems becomes difficult since the behavior of the third party cores is undefined.

TECHNOLOGY DESCRIPTION

The present invention shows how information can be monitored at the level of Boolean gates to isolate trusted and untrusted cores in a modern SoC. The method is evaluated on the Opencores WISHBONE cross-bar interconnect architecture with successful isolation of the trusted and untrusted cores demonstrated.

APPLICATIONS

The subject technology can be applied to any computing system wherein reliability and a high Evaluation Assurance Level (EAL) are a must. Achieving a high EAL is often costly and very difficult when designers utilize third party cores to save time. By applying the techniques of this research, undefined cores can be successfully isolated and a secure mix-trusted integration can be realized.

RELATED MATERIALS

- A Practical Testing Framework for Isolating Hardware Timing Channels; Jason Oberg, Sarah Meiklejohn, Timothy Sherwoody and Ryan Kastner - 12/16/2012

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	9,305,166	04/05/2016	2013-197

CONTACT

University of California, San Diego
Office of Innovation and Commercialization
innovation@ucsd.edu
tel: 858.534.5815.

OTHER INFORMATION

CATEGORIZED AS

- **Computer**
  - Hardware
  - Security

RELATED CASES

2013-197-0