1. Interacting with Hardware Trojans over a network

Accession number: 12821760
Authors: Farag, M.M. (1); Lerner, L.W. (1); Patterson, C.D. (1)
Author affiliation: (1) Bradley Dept. of Electr. & Comput. Eng., Cyber at VT, Virginia Tech, Blacksburg, VA, United States
Source: Proceedings 2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2012)
Publication date: 2012
Pages: 69-74
Language: English
ISBN-13: 978-1-4673-2341-3
Document type: Conference article (CA)
Conference name: 2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2012)
Conference date: 3-4 June 2012
Conference location: San Francisco, CA, USA
Sponsor: IEEE Comput. Soc.
Publisher: IEEE
Place of publication: Piscataway, NJ, USA
Material Identity Number: YXB2-1901-210
Abstract: Hardware Trojan horses (HTHs) are emerging threats to integrated circuits (ICs) outsourced to a global supply chain or developed with untrusted tools and intellectual property (IP). HTHs are stealthy in nature, and covert communication is their usual means of interaction and information transfer. Previous research has focused on short-range interaction via side-channels and existing IC interfaces, while remote interaction with HTHs across wired computer networks has received less attention. Generalized and non-local HTH interaction can support attacks normally associated with software Trojans. We investigate remote communication with HTHs and provide partial methods to exploit vulnerabilities in media layers of the protocol stack. Specifically, we focus on covert communication over point-to-point physical links in 10 gigabit Ethernet (10GbE) networks by exploiting loose specifications in physical- and link-layer protocols. The developed HTHs are assessed in terms of resource overhead and achieved bit rate, and demonstrate the potential for establishing high bandwidth covert channels using lightweight implanted circuits. We also describe a PUF-based IC or IP tracking attack enabled by HTH interaction across a network.
Number of references: 15
Inspec controlled terms: integrated circuits - invasive software - local area networks
Uncontrolled terms: hardware trojan horses - HTH - integrated circuits - IC - global supply chain - untrusted tools - intellectual property - IP - short-range interaction - side-channels - wired computer networks - software trojans - remote communication - covert communication - point-to-point physical links - Etherne - link-layer protocols - physical-layer protocols
Inspec classification codes: B6210L Computer communications - C6130S Data security - C5620L Local area networks
Treatment: Practical (PRA)
Discipline: Electrical/Electronic engineering (B); Computers/Control engineering (C)
DOI: 10.1109/HST.2012.6224323
IPC Code: G06F21/00 - H04L12/28
Database: Inspec

Data Provider: Engineering Village