Topic: OSD141-IA2

Chip Scan, Inc.

Detecting Malicious Circuits in IP-Core using Boolean Functional Analysis

A key to securing any DoD weapon or computational platform is being assured of the functionality provided by the microelectronics that underlies that platform. If the microelectronics contains hidden functionality, malicious or benign, that functionality can be discovered and exploited by a adversary to achieve catastrophic effects such as disabling the system, causing malfunction or exfiltrating confidential information. Chip Scan's products precisely address these problems: they help identify and mitigate hardware backdoors, or undocumented functionality, in systems that use FPGAs or Custom ASICs. Chip Scan's underlying technology is based on novel, peer-reviewed, award winning research that has been successfully tested using open red teaming exercises. This technology is currently at TRL 7. The Chip Scan team provides expert strategic advice, and works with partners to identify risk and implement mitigations to minimize the dangers of unassured microelectronic supply chains.

Technology Category Alignment:

Cyber
Trust Foundations
Trust Foundations
Electronic Warfare (EW)
Modular/Open/Reconfigurable Architectures

Contact:
sales@chipscan.us
(646) 593-7274
http://www.chipscanllc.com/
SYSCOM: ONR
Contract: N00014-16-C-2036

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-3252-17

Topic # OSD141-IA2

Detecting Malicious Circuits in IP-Core using Boolean Functional Analysis

Chip Scan Inc

WHO

SYSCOM: ONR

Sponsoring Program: ONR

Transition Target: PMW-130

TPOC:
Dr. Sukarno Mertoguno
sukarno.mertoguno@navy.mil

Other transition opportunities:
Commercial chip provider/manufacturers have interest in ensuring that their product is free of malicious circuits. If successful the tool developed within this SBIR should find its market in the commercial sector as well as military sector.

Notes:
SoC: System of Chips
IP: Intellectual Property
NSS: Network System Security
FPGA: Field Programmable Gate Arrays
ASIC: Application Specific Integrated Circuits

WHAT

Operational Need and Improvement: Critical infrastructure systems in the defense, aerospace, telecommunications, and automotive sectors extensively use digital microelectronic components, such as Field Programmable Gate Arrays (FPGAs), Application Specific Integrated Circuits (ASICs) or System on Chips (SoCs) sourced from a very large number of vendors through a cost competitive process. These FPGAs, ASICs and SoCs are created using collaborative, international processes using very complex software and hardware design steps. Consequently these devices embed vulnerabilities, intentionally or unwittingly, leaving them open to attacks that can catastrophically compromise confidentiality, integrity or availability of entire systems that utilize these products. There is a need to supplement qualitative controls with deep technical analysis in NSS programs of record.

Specifications Required: An important requirement for tools that provide deep technical analysis for undocumented features is that they should be able to identify malicious behaviors before the system is fielded. A further requirement is that it should be minimally invasive to developers and should not require developers to (re)write specifications, code, or even write properties.

Technology Developed: Chip Scan's revolutionary first-of-a-kind security product, ESPY, addresses the risk from compromised hardware supply chains early during manufacturing where these problems can be identified and eliminated before a system is fielded. Backed by award-winning university research and real-world red teaming, ESPY has a proven ability to identify backdoors, aka undocumented features or hardware trojans, in FPGA, ASIC and SoC designs. ESPY has broad coverage against backdoor risk from multiple sources from compromised designs, to third-party IP, and even Electronic Design Automation tools.

Warfighter Value: Digital microelectronics is the computational bedrock on which mission critical, defense and infrastructure platforms are built and it is hard to overstate the risk of a compromised supply chain. Compromised supply chains are often the only remaining or feasible threat vector for highly controlled national security systems. The analysis performed by ESPY provides higher assurance that systems will work as intended without surprise supply chain attacks from an adversary.

WHEN

Contract Number: N00014-16-C-2036 **Ending on:** September 4, 2018

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Capability demonstration of typical components	Low	Identification of backdoors in fielded IP blocks.	7	March 2018

HOW

Projected Business Model: ESPY can be flexibly deployed to suit customer needs. ESPY can be run on a single machine or elastically parallelized across a private cloud or FedGov cloud. ESPY also includes a clean, drag-and-drop, modern web interface, and a command line interface for power users.

ESPY integrates with Chip Scan's security-as-a-service attestation and cloud locker service. All validated IP blocks and certification provided by Chip Scan can be stored securely for easy distribution and access of the IP within and across projects.

Every purchase of ESPY product includes one year of support services which provides access to Chip Scan's premier support and all product updates during that time. Chip Scan premier support provides online access to ESPY security practitioner guide, training materials and documentation. Customer requirement specific training is also available.

Company Objectives: Chip Scan provides deep, practical technical solutions to supply chain risk management. Chip Scan has already tested these designs through red teaming activities and is actively seeking engagement to address supply chain risk problems.

Potential Commercial Applications: looking for partners to expand its trust and security offerings. Chip Scan has developed technology for mitigating risk of backdoors in already deployed systems (e.g., network switches).

Contact: , VP Sales
sales@chipscan.us (646)593-7274