Research Needs: Trustworthy and Secure Semiconductors and Systems (T3S)

April 1, 2019

Semiconductor Research Corporation (SRC), Durham, NC 27703

Overview

Thank you for your interest in reviewing research needs for *Trustworthy and Secure Semiconductors and Systems (T3S)*, a research program of Global Research Collaboration (GRC) at Semiconductor Research Corporation (SRC). The mission of the T3S research program is to develop designs, analysis strategies, processes and tools for secure, trustworthy, reliable and privacy preserving chips, systems, computing and communications.

The GRC typically focuses on research in a timeframe 5 – 8 years ahead of technology release. This timeframe represents the "sweet spot" for pre-competitive collaborative research, after which the industry focuses on proprietary development for technology differentiation by each company. Successful research proposals should match this timing.

Research Needs

The T3S research program is focused on developing architectures, strategies, techniques, software/firmware, and tools to provide assurance that electronic systems will perform as intended. Such assurance is a function of processes and tools integrated across all steps of design, manufacturing, and distribution. The program supports research to develop designs, analysis strategies, processes and tools for secure, trustworthy, reliable and privacy-preserving integrated circuits for computing and communications systems. Some examples of research outcomes are to decrease the likelihood of unintended behavior or access, to increase resistance and resilience to tampering, and to improve the ability to provide authentication throughout the supply chain and in the field. We highlight the key strategic challenges divided into five categories:

1. **Trust architectures and hardware designs**
2. **Advanced security techniques**
3. **Security aspects of embedded software and firmware**
4. **Security assurance and verification**
5. **Authentication and attestation**

This document is not intended to cover the complete landscape of the required research, but rather to identify the most critical areas for university research to address.

Contributors include:

Analog Devices	Doug Gardner
Arm	Prakash Ramrakhyani, Supreet Jeloka
IBM	Peilin Song
Intel	Claire Vishik, Sohrab Aftabjahani, Rosario Cammarota
Mentor, A Siemens Business	Michael Chen
Texas Instruments	Ariton Xhafa
Semiconductor Research Corporation	John Oakley, David Yeh

Research Needs: Trustworthy and Secure Semiconductors and Systems (T3S)

April 1, 2019

Semiconductor Research Corporation (SRC), Durham, NC 27703

The following are representative of relevant research needs without priority ordering:

1	**Trust architectures and hardware designs**
1.1	Quantifying impact of security at the level of circuits and processors in terms of system-wide functionality, performance, and power goals
1.2	Innovative defense mechanisms against "side channel attacks"; for example developing on-die sensors to monitor attacks in real time and mitigate them
1.3	Cryptographic architectures optimized for highly constrained devices
1.4	Security architectures for heterogeneous systems including protection of AI/ML enabled sub-systems
1.5	Novel approaches for self-healing/self-reconfiguring features for robust long term secure operations to protect against failures such as maliciously induced transient or aging effects
2	**Advanced security techniques**
2.1	Protecting IP in a world of 3D and 2.5D packaging and split manufacturing
2.2	Hardware design strategies and cryptography methods for Post-Quantum devices
2.3	Developing robust AI/ML models and reasoning methods to predict attack and defense mechanisms
2.4	Approaches, models and frameworks for reasoning about and specifying hardware-specific security properties to realize a Security by Design paradigm
2.5	Identifying and defining metrics for evaluating and comparing secure designs with privacy preserving properties and trust worthiness as needed and for ability to provide trust evidence at the system level
3	**Security aspects of embedded software and firmware**
3.1	Strategies and techniques to avoid/reduce vulnerabilities in embedded software and firmware
3.2	Methods to provide updates to address system vulnerabilities discovered after deployment to enable field upgradable security
4	**Security assurance and verification**
4.1	Tools, techniques, and methodologies for verifying hardware-specific security properties and enforcing security design principles
4.2	Establishment of safety properties without knowing all aspects of the design, and thereby providing strong provable assurance
4.3	Approaches to increase automation of security verification and analysis of IP beyond functional analysis
4.4	Security analysis and verification methods for robustness of non-deterministic systems like ones with long term learning
4.5	Novel approaches to highly accurate, non-destructive, and low cost physical analysis techniques
5	**Authentication and attestation**
5.1	Novel approaches to design elements that enable authentication/attestation during design and throughout the product life cycle
5.2	Generation, protection and establishment of trust models for hardware and firmware interacting with the software stack
5.3	Multi-dimensional assurance approaches to protect microelectronic supply chain and enable counterfeit detection and avoidance