Research Needs: Hardware Security (HWS)

April 4, 2022

Semiconductor Research Corporation (SRC), Durham, NC 27703

Overview

Thank you for your interest in reviewing research needs for *Hardware Security (HWS)*, a research program of *Global Research Collaboration (GRC)* at *Semiconductor Research Corporation (SRC)*. The mission of the HWS research program is to develop designs, analysis strategies, processes, and tools for secure, trustworthy, reliable and privacy preserving chips, packaging, 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.

Innovation in semiconductor technology is needed to advance information and communication technologies (ICT) critical to our economic growth and national security. Five seismic shifts that will define the future of semiconductors and ICT. SRC will continue to align our research needs, portfolio, and scope to the Decadal Plan for Semiconductors, https://www.src.org/about/decadal-plan/. The "ICT Security Challenges" seismic shift describes challenges in hardware security over the next decade and beyond.

Moving forward, the SRC is also embarking on an effort to broaden participation in its funded research programs. This aggressive agenda will help us drive meaningful change in advanced information and communication technologies that seem impossible today. In the programs we lead, we must increase the participation of women and under-represented minorities as well as strike a balance between U.S. citizens and those from other nations, creating an inclusive atmosphere that unlocks the talents inherent in all of us. Please visit, https://www.src.org/about/broadening-participation/, for more information about the 2030 Broadening Pledge.

Research Needs

The HWS research program is focused on developing architectures, strategies, methodologies, techniques, software/firmware, and tools to provide assurance that electronic systems will perform as intended. Such an assurance is a function of processes and tools integrated across all steps of design, manufacturing, testing, packaging, 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 systems' 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. **Trusted architectures and hardware designs**
2. **Security techniques for advanced technologies and packaging**
3. **Security aspects of embedded software, firmware, and soft IP**
4. **Security assurance, protection, and verification**
5. **Authentication, attestation, and provisioning**

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

Research Needs: Hardware Security (HWS)

April 4, 2022

Semiconductor Research Corporation (SRC), Durham, NC 27703

1	**Trusted architectures and hardware designs**
1.1	Quantifying impact of security at various levels of abstraction (such as circuits, components, sub-systems, systems, and systems of systems) in terms of system-wide functionality, performance, and power goals
1.2	Innovative defense mechanisms and methods against "side channel attacks" and elimination of attack vectors
1.3	Cryptographic architectures and designs for either classic security mechanisms or mechanisms to compute on encrypted data, optimized for area, power, energy, performance, latency, etc. usually targeted to highly constrained devices and high-performance computing systems
1.4	Security architectures for heterogeneous systems including protection of AI/ML enabled sub-systems and neuromorphic architectures
1.5	Hardware security specific design strategies, side-channel analysis, and cryptography methods (e.g. fully homomorphic encryption) for Post-Quantum and privacy-preserving devices
1.6	Quantify opportunities and challenges of new device materials (Beyond CMOS) to enhance system security and trusted architectures
2	**Security techniques for advanced technologies and packaging**
2.1	Developing robust AI/ML models and reasoning methods to predict attack and defense mechanisms
2.2	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
2.3	Security of disaggregated/heterogeneous systems, e.g., advance packaging technologies like heterogeneous integration
2.4	Security of emerging devices/architectures/systems/technologies, e.g., NVMs
3	**Security aspects of embedded software, firmware, and soft IP**
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
3.3	Generation, protection, and establishment of trust models for hardware and firmware interacting with the software stack
3.4	Strategies and techniques to avoid/reduce vulnerabilities in data center and cloud, including multi-tenancy
4	**Security assurance, protection, and verification**
4.1	Tools, techniques, and methodologies for verifying hardware-specific security properties (including algorithmic and formal verification) and enforcing security design principles (confidentiality, integrity, availability, etc.)
4.2	Approaches, models, and frameworks of pre-Silicon design for reasoning about and specifying hardware-specific security properties to realize a Security by Design paradigm
4.3	Security root of trust primitives, analysis, verification methods, and self-healing for robust long term secure operation of evolving systems over the product life cycle (5-20 years)
4.4	Novel approaches to highly accurate, non-destructive, and low-cost techniques to create secure/trustable designs and validation processes, establish trust, and protect IP in untrusted fab environments
5	**Authentication, attestation, and provisioning**
5.1	Novel approaches to design elements that enable authentication/attestation during design, operation, firmware, operating systems, and throughout the product life cycle (5-20 years), particularly in the cloud environment
5.2	Approaches and techniques to enable provable evidence device state and identity, e.g., postquantum, blockchain, etc.
5.3	Novel approaches to End-to-End Security Solutions that eliminates the diverse communication methods and inherent complexities, e.g. zero trust environments
5.4	Study of 6G wireless communication security features and physical layer security techniques