SaTC 2019 PI meeting breakout group report summary: *Trust and Security Opportunities and Challenges in Hardware Security*

Co-leads: Jim Plusquellic, Swaroop Ghosh, Rashmi Jha

Room: Poplar, Hilton Mark Center, Alexandria, VA

Problem/domain summary

- What is the topic?
  - **Hardware Security**
    - System-level security: Hardware-Software interface, cross-layer security, non-interference, Firmware, Subsequent layers, Lots of ways to attack
    - Design: Verifying trust in 3rd Party IP
    - Supply chain: Defending against counterfeiting
    - Manufacturing: Establishing trust
    - In-field System Security: side-channel attacks, detecting tamper
- Data-driven Quantifiable Assurance, Zero Trust
- Deploy-ability: PPACT (Power, Performance, Area, Cost, Trust), practicality of solutions, *Triangle representation (efficiency vs. security vs. flexibility).*
- Hardware support for Software Security: Hardware security features that provide primitives for enhancing software security beyond TRNG.
- Metric for Security: Benchmarking at various layers.

Problem/domain summary (Continued…)

- Why is it important to society? to a secure and trustworthy cyberspace? in other ways?
  - It impacts correctness, privacy, and safety
  - Unlike software, patching hardware is difficult
  - How can we build trusted systems with untrusted hardware?
    - Hardware is the root-of-trust, software security depends on trusted and secure hardware

Problem/domain summary (Continued…)

- Is there is an existing body of research and/or practice? What are some highlights or pointers to it?
  - Each of the layers has some level of work done, cross layer integration is missing
  - Materials/Devices: Process Monitoring Structures, Reverse Engineering of layouts
  - Circuits: Embedded security primitives, PUFs, obfuscations, logic locking/encryption, TRNG
  - Architectures: Noise injection in communication channel, memory encryption, deterministic guarantees of latency, information-flow, non-interference
  - Hardware-software integration: Hardware and software open sources, TPM, DSA, security property propagation
  - Firmware: Elephant in the room, hardware-security community owns it, authenticating firmware updates, integral part of secure-boot process

Key research challenges

- What are important challenges that remain? Are there new challenges that have arisen based on new models, new knowledge, new technologies, new uses, etc?
- *Tools and metrics for measuring security and trust within and across layers is missing.*
  - *Whole idea of quantifying security is missing.*
  - *Support provided in EDA tools*
  - *Cross-layer verification capabilities: Verification complexity, tool efficiency*
  - *How to express and propagate the security/trust specifications in every layer?*
    - *Spectre Meltdown for example*

Key research challenges (Continued...)

- *Lack of adversarial attack models and vulnerability evidence*
  - *Models for real-world critical exploits for hardware are not well-defined*
    - *Hardware honeypots? Educational value for students*
  - *Always ON vulnerability vs. sporadic triggering vulnerabilities.*
  - *Push for opensource architecture will provide opportunities for investigating vulnerabilities.*
- *Security-aware abstraction at various layers and CAD tool support*
  - *Obfuscation of logic and memory access patterns at architecture level*
  - *Non-interference in Microarchitecture*
    - *What data has to be non-interfering?*
    - *Addressing a regime of leakage.*
    - *Intra/Cross-layer support for security context-sensitive data*

Key research challenges (Continued...)

- *Security in Specialized Architectures (Neuromorphic, Cryptographic, Quantum, Accelerators…)*
- *Hardening ASICs/FPGA technologies and architectures*
- *Materials/Devices:*
  - *Physical Assurance to detect and prevent tampering/fault injections.*
  - *Studying interplay between reliability, fault-tolerance, and security and trust.*
    - *E.g. Phase Change Memory (PCM): Encryption makes wear-out in PCM problem even worse.*
- *Circuits:*
  - *Payloads (kill-switches, leakage, and beyond), issue of trigger (not much reported on trigger)*
  - *fault-injection attacks*
  - *side channel, leakage*
- *Hardware acceleration of post-quantum cryptography*

Potential approaches

- Are there promising directions to addressing them? What kinds of expertise and collaboration is needed (disciplines and subdisciplines)?
- Within/Across abstraction layer security and specification issues
  - Materials/Devices: Lack of security specifications
  - Circuits: Quantifying benefits vs. Cost, PPACT, security metrics.
  - Architectures: Cross-layer security, security metrics (within and cross-layer), benchmarks to test.
    - *Classifying bits leaked based on rate and sensitivity*

- FPGA: Moving target architectures, leveraging co-design as a security feature, managing the resources, re-defining architecture for multi-tenant
- New behavioral design language constructs for secure designs, HLS support
- New analog design methodologies

Long-term significance

- Will this domain/problem remain relevant in 10 years? if so, why?
  - Will become more important in 10 years
  - Societal dependence on autonomy: Hardware has to make decisions in real-time with no down-time
    - Big driver for security in future
    - Trust and Reputation management
    - Edge computing in untrusted fields
  - Post CMOS devices, 3D ICs,Quantum : Attack models are undefined and untested.
  - Security Automation throughout the design process.
    - Design Aids for security.
    - Evolving security metric beyond PPA.
  - Incorporation of security into Undergraduate education