Hasini Witharana

Gainesville, Florida, USA
witharana.hasini@ufl.edu
hasini-witharana

Education

2020 – Present — **Ph.D. University of Florida**, Computer Science.
Thesis title: *Design of Trustworthy Systems using Security Assertions.*
Advisor: *Prof. Prabhat Mishra*

2020 – 2023 — **M.Sc. University of Florida**, Computer Science and Engineering.

2014 – 2018 — **B.Sc. University of Moratuwa Sri Lanka**, Computer Science and Engineering.

Work Experience

2020 – Present — **Research Assistant**, University of Florida.

May 2021 – Aug 2021 — **Security Research Intern**, Intel Corporation, USA.

2019 – 2020 — **Software Engineer**, WSO2, Sri Lanka.

Apr 2018 – Aug 2018 — **Google Summer of Code Contributor**, Apache Foundation, USA.

Jun 2017 – Dec 2017 — **Software Engineering Intern**, WSO2, Sri Lanka.

Research Interests

Security — CPU Side-Channel Attacks, Trusted Execution Environments, Confidential Computing

Verification — Assertion-Based Verification, Test Generation, Pre-Silicon Verification.

Quantum — Quantum Device Verification

Research Publications

Journal Articles - Accepted

1. H. Witharana, A. Jayasena, A. Whigham, and P. Mishra, "Automated generation of security assertions for rtl models," *ACM Journal on Emerging Technologies in Computing Systems*, 2023.
2. A. Jayasena, B. Kumar, S. Charles, H. Witharana, and P. Mishra, "Network-on-chip trust validation using security assertions," *Journal of Hardware and Systems Security*, 2022.
3. H. Witharana, Y. Lyu, S. Charles, and P. Mishra, "A survey on assertion-based hardware verification," *ACM Computing Surveys (CSUR)*, 2022.
4. H. Witharana, Y. Lyu, and P. Mishra, "Directed test generation for activation of security assertions in rtl models," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2021.

Journal Articles - Under Review

1. H. Witharana, A. Jayasena, and P. Mishra, *Incremental concolic testing of memory rtl models, ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2023 - Major Revision.
2. S. Sanjaya, H. Witharana, and P. Mishra, *Assertion-based validation using clustering and dynamic refinement of hardware checkers, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2023.

Conference Proceedings - Accepted

1. H. Witharana, D. Chatterjee, and P. Mishra, "Verifying memory confidentiality and integrity of intel tdx trusted execution environments," in *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2024.
2. H. Witharana, D. Volya, and P. Mishra, "Qcassert: Quantum device testing with concurrent assertions," in *Asia and South Pacific Design Automation Conference (ASPDAC)*, 2024.
3. H. Witharana, S. Sanjaya, and P. Mishra, "Dynamic refinement of hardware assertion checkers," in *2023 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2023.
4. H. Witharana and P. Mishra, "Speculative load forwarding attack on modern processors," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2022.

Conference Proceedings - Under Review

1. H. Witharana and P. Mishra, *Adversarial assertions*, 2024 61st ACM/IEEE Design Automation Conference (DAC), 2024 - Under Review.

Patent

1. P. Mishra, H. Witharana, and S. Sanjaya, "Dynamic refinement of hardware assertion checkers," U.S. Provisional Patent Application No. 63/489,020, filed March 8 2023.
2. P. Mishra, H. Witharana, and D. Volya, "Quantum device testing using concurrent assertions," Invention Disclosure November 1 2023.

Other Publications

1. H. Witharana and P. Mishra, *Scalable assertion-based validation of trusted execution environments*, SRC TECHCON, 2023.
2. H. Witharana and P. Mishra, *Security validation of trusted execution environments*, GOMACTech, 2023.
3. H. Witharana and P. Mishra, *Side-channel attack on modern processors*, SRC TECHCON, 2022.
4. H. Witharana and P. Mishra, *Automated generation of security assertions*, SRC TECHCON, 2021.
5. H. Witharana and P. Mishra, *Directed test generation for activation of assertions*, SRC TECHCON, 2020.

Presentations and Talks

2023 **DATE**, Dynamic refinement of post-silicon checkers (Antwerp, Belgium).
SRC TECHCON, Assertion based validation of trusted execution environments (Austin, Texas).
2022 **ICCAD**, Microarchitectural attacks on modern processors (San Diego, California)
SRC TECHCON, Timing side-channel attacks on modern processors (Austin, Texas).
2021 **SRC TECHCON**, Automated security assertion generation framework (Online).
2020 **SRC TECHCON**, Directed test generation for security assertions (Online).

Projects

Sep 2022 - Present
Compositional Security Verification of Trusted Execution Environments
Funding: *Semiconductor Research Corporation (SRC)*
Role: *Lead Researcher*
Description: Verifying Trusted Execution architectures using security properties

Jan 2020 - Dec 2022
Validation of System-on-Chip Vulnerabilities using Security Assertions
Funding: *Semiconductor Research Corporation (SRC)*
Role: *Lead Researcher*
Framework: `https://github.com/UFESL/ISV`
Description: An automated security verification framework for Register Transfer Level (RTL) designs using security assertions.

2022 - 2023
Design-for-Debug Architecture for Post-Silicon Security Validation
Funding: *National Science Foundation (NSF)*
Role: *Researcher*
Description: Dynamic refinement of hardware assertions for post silicon debug.

Awards and Achievements

2023 **Gartner Group Graduate Fellowship**, for Outstanding CISE PhD Students (UF).
2022 **Travel Grant**, sponsored by IEEE CEDA to attend ICCAD.
Gartner Group Graduate Fellowship, for Outstanding CISE PhD Students (UF).
2020 **Full Assistantship**, for PhD program in Computer Science (CISE) from UF.
2014 **Merit Scholarship**, to pursue undergraduate studies by the government of Sri Lanka.

Professional Services

Reviewer of Journals
- ACM Transactions on Embedded Computing Systems (**TECS**), 2023

Reviewer of Conferences
- International Symposium on Hardware/Software Codesign and System Synthesis (**CODES+ISSS**), 2022
- Design Automation and Test in Europe (**DATE**), 2023
- IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), 2023

Membership
- **Student Member**, Women in Cybersecurity
- **Student Member**, IEEE

Proposal Development Activities

Sep 2023
SAFETEE: Security Validation of Trusted Architectures
Organization: *National Science Foundation (NSF) | US - India Collaboration*
Description: A security validation framework to verify the trustworthiness of TEEs in the presence of side-channel and micro-architectural adversaries.

Sep 2022
Compositional Security Verification of TEEs
Organization: *Semiconductor Research Corporation (SRC)*
Description: A semi-automated validation framework to validate TEEs using security properties.

Jan 2022
Scalable Memory Verification
Organization: *Micron*
Description: Memory design verification using Concolic testing (simulation + symbolic).

Teaching and Advising Activities

Mentoring Junior Ph.D. Students

2022 - 2023 — Sahan Sanjaya (UF) | Assertion minimization using clustering.

2021 - 2023 — Aruna Jayansena (UF) | Automated security assertion generation.

Hansika Weerasena (UF) | Formal verification of VM-based TEE architectures.

Mentoring Undergraduate Researchers

2023 — Emmett Kogan (UF) | Abstracting Intel TDX architecture

Lydia Chung (UF) | Theorem proving from trusted computing

2022 — Miranda Overstreet (UF) | Reinforcement learning based Concolic testing

Sahan Sanjaya (University of Moratuwa) | Dynamic refinement of hardware checkers.

2021 — Andrew Whigham (UF) | Taint analysis to identify information leakage

2020 — Aruna Jayansena (University of Moratuwa) | Assertion-based network-on-chip validation.

Teaching

2022 — CPU side-channel attack basics - Penetration Testing

2021 — Remote Proof-of-Concept development for CPU side-channels - Intel Security Assurance Group

References

Dr. Prabhat Mishra
Professor (Advisor)
CISE Department, University of Florida
prabhat@ufl.edu

Dr. Sartaj Sahni
Distinguished Professor
CISE Department, University of Florida
sahni@ufl.edu

Dr. My T. Thai
Professor
CISE Department, University of Florida
mythai@cise.ufl.edu

Dr. Domenic Forte
Professor
ECE Department, University of Florida
dforte@ece.ufl.edu