Nikhilesh Kumar Singh

CONTACT INFORMATION

SSB 421,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras,
Chennai 600036, India

Email: mailme.nikhilesh@gmail.com
Web: https://nikhileshksingh.github.io

EDUCATION

Ph.D., Department of Computer Science & Engineering
IIT Madras, 2019-present
Expected Thesis Submission: April 2024

MS by Research, Department of Computer Science & Engineering
IIT Madras, 2017-2019

B.Tech., Department of Computer Science & Engineering
BIT Sindri, 2013-2017

RESEARCH INTERESTS

Micro-architectural Security, Hardware Security, Real-time Safety,
AI for System Security

PUBLICATIONS (* equally contributing authors)

Pallavi Borkar, Chen Chen*, Mohamadreza Rostami,* **Nikhilesh Singh**, *Rahul Kande, Ahmad-Reza Sadeghi, Chester Rebeiro, and Jeyavijayan (JV) Rajendran*
WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors, In 33rd Usenix Security Symposium (pre-print) 2024

Nikhilesh Singh*, *Shagnik Pal*, Rainer Leupers, Farhad Merchant, and Chester Rebeiro*
ProMiSE: A Programmable Hardware Monitor for Secure Execution in Zero Trust Networks, In IEEE Embedded Systems Letters [Paper] 2024

Nikhilesh Singh, *Karthikeyan R, Chester Rebeiro, Jithin Jose, and Ralph Mader*
Kryptonite: Worst-Case Program Interference on Multi-Core Embedded Systems, In ACM TECS (EMSOFT 2023) [Paper] 2023

Anirban Chakraborty,* **Nikhilesh Singh***, *Sarani Bhattacharya, Chester Rebeiro, and Debdeep Mukhopadhyay*
Timed Speculative Attacks exploiting Store-to-Load Forwarding bypassing Cache-based Countermeasures, In 59th DAC [Paper] [Code] 2022

***Nikhilesh Singh**, Vinod Ganesan, and Chester Rebeiro*
Secure Processor Micro-architecture,
In Handbook of Computer Architecture, Springer (Book) (Paper) 2022

Sareena KP, ***Nikhilesh Singh**, Chester Rebeiro, and Kamakoti V*
RaDaR: A Real word Dataset for AI powered Run-time Detection of Cyber Attacks
In 31st ACM International Conference on Information and Knowledge Management (CIKM) [Paper] 2022

*Sareena KP, **Nikhilesh Singh**, Chester Rebeiro, and Kamakoti V*
JUGAAD: Comprehensive Malware Behavior-as-a-Service
In 15th Cyber Security Experimentation and Test Workshop (CSET)@Usenix Security Symposium [Paper] 2022

*Sareena KP, **Nikhilesh Singh**, Chester Rebeiro, and Kamakoti V*
SUNDEW: An Ensemble of Predictors for Case-Sensitive Detection of Malware
Under review, (pre-print) 2022

***Nikhilesh Singh** and Chester Rebeiro*
LEASH: Enhancing Micro-architectural Attack Detection with a Reactive Process Scheduler, (pre-print) 2021

PATENTS

***Nikhilesh Singh** and Chester Rebeiro*
Method and Electronic Device for Mitigating Micro-architectural Side-channel Attack by Dynamic Resource Allocation
IN Patent 495535 Granted: 2024

*Sareena KP, **Nikhilesh Singh**, Chester Rebeiro, and Kamakoti V*
System And Method for Malware Detection by Cross-dimensional Behavioural Analysis, IN Patent Application 452897 Granted: 2023

***Nikhilesh Singh**, Karthikeyan R, and Chester Rebeiro*
System and Method of Estimating Realizable Maximum Runtime Interference on Multi-Core Platforms
IN Patent Application 202341061438 Published: 2023

*Vinayak Honkote, **Nikhilesh Singh** and Rajesh Poornachandran*
Safety and Integrity Violation Detection System, Device and Method
US Patent Application US20220219324A1 [Intel Labs] Published: 2022

PROJECTS

Whitebox Fuzzing to Detect and Locate Side-Channel Timing Vulnerabilities in Processors Mar 2021 - Nov 2023

- A pre-silicon technique using fuzzing to detect timing vulnerabilities in processors and a graph representation of the design to locate to root cause of the detected vulnerabilities.
- 12 new timing vulnerabilities and their corresponding location in popular RISC-V processors such as BOOM, Rocket Core, and CVA6.
- To appear in Usenix Security Symposium 2024.

Post-Detection Response Strategies to Handle False-Positives in Attack Detection Jul 2022 - present

- Developed a solution to counter the impacts of false-positives in attack detection by using a reactive mechanism for resource allocation.
- Manuscript under review.

Co-processor Design for Configurable Runtime Monitoring in Zero-Trust Architecture (ZTA) Networks Jul 2022 - Nov 2023

- Developed a solution based on Shakti RISC-V processors that provides a periodic update on the security health of devices in a ZTA setup.
- Presented TASER@CHES 2023
- Published in IEEE ESL, 2024.

Studying Program Interference in Resource-Constrained Real-Time Systems Sep 2021 - Mar 2023

- Developed a framework to estimate the worst-case program interference in real-time systems such as automotive using Reinforcement Learning.
- Kryptonite is being ported to the AUTOSAR framework, which is an industry standard for automobiles.
- Patent under examination and published in ACM TECS (EMSOFT) 2023.

Novel Timing Channels in Load-Store Buffers Jun 2020 - Nov 2021

- Developed novel approaches for leakages using the internal processor buffers, mainly the Load-Store buffers.
- The attack can bypass existing cache-based attack prevention techniques.
- Published in DAC 2022.

Micro-architectural Leakage Attack-Aware Scheduling Jan 2019 - Jun 2021

- Designed an OS scheduler for Linux that deploys hardware performance counters to detect micro-architectural attacks such as L1-data & instruction cache attacks, Rowhammer, and L3-cache attacks.
- Developed a kernel-based solution for micro-architectural attack mitigation and a per-thread performance monitoring module. (pre-print)

Feasibility Analysis of Various Light-Weight Ciphers on Renesas R-Car M3 Board (Code) May 2019 - June 2019

Industrial Project, Prof. Chester Rebeiro

- Performed analysis of tradeoffs among light-weight ciphers for alternatives to vulnerable CAN bus protocol used in automobiles.

Open Malware Research: An IIT Madras Initiative Jan 2018 - present

- Co-designed a testbed consisting of more than 500 heterogeneous devices such as Intel-i7, Intel-atom, Galileo, and Raspberry Pi boards.
- Built classification models based on the collected data.
- JUGAAD Testbed appeared in CSET'22, RaDaR Dataset in CIKM'22, SUNDEW solution has a patent granted, and the manuscript is under review.
- Part of the Open Malware Research Initiative at IIT Madras. (link)

Lynx: A Modified Cipher Based on 128-bit AES (Code) Jan 2018 - May 2018

Course Project, Applied Cryptography, Prof. Chester Rebeiro

- Designed a variant of AES with different S-Box and performed analysis on efficiency and security against timing attacks.

A 5-Stage Microprocessor Implementing RISC-V RV32I Base + RV32C Instruction Set (Code) Aug 2017 - Nov 2017

Course Project, CAD for VLSI, Prof. Kamakoti V.

- Implemented a 5-stage pipelined, in-order processor supporting a broad subset of RISC-V RV32I/C instructions using Bluespec System Verilog with basic logic for handling control and data hazards.

WORK EXPERIENCE

Project Officer Aug 2022 - present

C-HERD, IIT Madras

- Working on multiple Hardware Security projects at the Centre on Hardware Security Entrepreneurship Research & Development (C-HERD), IIT Madras, funded by the Ministry of Electronics and IT, Govt. of India.

Graduate Intern Technical Oct 2021 - June 2022
Intel Labs, Bangalore

- Worked with the Bangalore Design Lab in collaboration with the Internet-of-Things Group (IoTG) on anomaly detection in industry-scale operations.
- Patent pending on a framework for safety, security, and efficiency of industrial IoT devices.

Visting Researcher Feb 2021 - July 2021
RWTH Aachen University, Aachen, Germany

- Worked with Prof. Rainer Leupers and Dr. Farhad Merchant at the Institute for Communication Technologies and Embedded Systems, funded by the AROP fellowship.
- Worked towards Security-aware Silicon designs and performed vulnerability evaluation of TrentOS by Hensoldt Cyber based on the seL4 micro-kernel.

MS Project Associate Jun 2017 - Aug 2019
Information Security Education and Awareness (ISEA) initiative, Govt. of India.

- Designed efficient profiling and detection techniques for malware using machine learning.

Teaching Assistant Jun 2017 - Nov 2021
Teaching Assitant for various courses at IIT Madras.
Operating Systems (Aug-Nov 2021) | Operating Systems (Aug-Nov 2020) | Secure Processor Design (Jan-July 2020) | Operating Systems (June-Nov 2019) | Network Security (Jan-May 2019) | Secure Systems Engineering (Jun-Nov 2018) | Introduction to Programming (Jun 2017-May 2018).

Mentorship Jan 2018 - present
IIT Madras

- Mentored 9 UG/PG students and 2 summer interns for multiple projects encompassing Malware Detection using ML/DL techniques, Hardening the Android Kernel with HPC-based Security Features, and Cryptanalysis.

Teaching Assistant Jan 2019 - Mar. 2019
NPTEL

- Teaching assistant for a MOOC with more than 4000 enrolments: Information Security-V by Prof. Chester Rebeiro, hosted by NPTEL.

ACHIEVE -MENTS

Keshav-Rangnath (KR) Excellence in Research Award 2023
A biannual award across all disciplines at IIT Madras for Ph.D. research.

First prize, *Robert Bosch Centre for DS and AI Annual Research Showcase* 2023
Poster on the use of RL in interference estimation on multi-core systems.

Semi-finalists, *Swadeshi Microprocessor Challenge 2020* 2021
Selected in the Top 100 out of 6K participating teams for our proposed design of a secure and versatile framework for Unmanned Aerial Vehicles (UAVs) which includes deploying ROS on RISC-V Shakti processors.

Advanced Research Opportunities Program Fellowship 2020
RWTH Aachen University, Aachen, Germany

Winners, *Embedded Security Challenge, CSAW (India Region)* 2019
Organized by the New York University.

ISEA Research Fellowship 2017
Information Security Education and Awareness, MeiTy, Govt. of India

99.5 percentile, GATE CS 2017
Council of Indian Institutes of Technology

SKILLS

Programming Languages
C/C++, Assembly, Python, MATLAB, BlueSpec System Verilog

Tools and Frameworks
Linux Perf Tool, Intel Pin, Linux Kernel, gem5, Cuckoo Sandbox, Synopsis VCS Simulator, Tensorflow, OpenAI gym, LaTeX

REFERENCES

Prof. Chester Rebeiro (Ph.D. Advisor)
Associate Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras, Chennai, India

Email: chester@cse.iitm.ac.in
Web: http://www.cse.iitm.ac.in/chester/