RAHUL KANDE

4402 Boyett St, Apt. C Bryan, Texas 77801 https://www.rahulkande.com/

EDUCATION

Texas A&M University, College Station, Texas Ph.D. in Computer Engineering

Indian Institute of Technology, Guwahati, India Bachelor of Technology in Electronics and Communication Engineering (Minor in Computer Science and Engineering)

Related Coursework :

Advanced Computer ArchitectureIntro. to Formal VerificationAdvanced Design VerificationMicroprocessor System DesignSecure Computer Systems and ArchVLSI laboratory

July 2018 - Present GPA: **3.90** on scale of **4**

May 2013 – May 2017 GPA: **8.91** on scale of **10**

Software Security Microarchitecture Prediction Design Laboratory

TECHNICAL SKILLS

Languages: Verilog, C, C++, Python, Shell script Methodologies: Universal Verification Methodology (UVM) Tools: vcs (Synopsis), Modelsim (Siemens), irun (Cadence), Jaspergold (Cadence), Vivado (Xilinx)

PUBLICATIONS

- P. Borkar, C. Chen, M. Rostami, N. Singh, R. Kande, A.-R. Sadeghi, C. Rebeiro, and J. Rajendran, <u>WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors</u>, in USENIX Security, 2024 (accepted)
- **R. Kande**, H. Pearce, B. Tan, B. Dolan-Gavitt, S. Thakur, R. Karri, and J. Rajendran, <u>(Security) Assertions by</u> <u>Large Language Models</u>, in IEEE Transactions on Information Forensics and Security, 2024 (accepted)
- M. Rostami, C. Chen, **R. Kande**, H. Li, J. Rajendran and A.-R. Sadeghi, *Fuzzerfly Effect: Hardware Fuzzing for Memory Safety*, in IEEE Security & Privacy Special Issue on Memory Safety, 2024 (accepted)
- M. Rostami, S. Zeitouni, **R. Kande**, C. Chen, P. Mahmoody, J. Rajendran and A.-R. Sadeghi, *Lost and Found in Speculation: Hybrid Speculative Vulnerability Detection*, in Design Automation Conference, 2024 (accepted)
- V. Gohil*, R. Kande*, C. Chen, A.-R. Sadeghi, and J. Rajendran, <u>MABFuzz: Multi-Armed Bandit Algorithms for</u> <u>Fuzzing Processors</u>, Design, Automation and Test in Europe Conference (DATE) 2024 (accepted) (* indicates equal contribution)
- M. Rostami, M. Chilese, S. Zeitouni, **R. Kande**, J. Rajendran, and A.-R. Sadeghi, *Beyond Random Inputs: A Novel ML-Based Hardware Fuzzing*, Design, Automation and Test in Europe Conference (DATE) 2024 (accepted)
- C. Chen, V. Gohil, **R. Kande**, A.-R. Sadeghi, and J. Rajendran, *PSOFuzz: Fuzzing Processors with Particle Swarm Optimization*, IEEE/ACM International Conference on Computer-Aided Design (ICCAD) 2023
- C. Chen, **R. Kande**, N. Nguyen, F. Anderson, A. Tyagi, A.-R. Sadeghi, and J. Rajendran, <u>HyPFuzz: Formal-Assisted Processor Fuzzing</u>, USENIX Security Symposium 2023 (Acceptance rate: 29%)
- R. Kande, A. Crump, G. Persyn, P. Jauernig, A.-R. Sadeghi, A. Tyagi, and J. Rajendran, <u>TheHuzz: Instruction</u> <u>Fuzzing of Processors Using Golden-Reference Models for Finding Software-Exploitable Vulnerabilities</u>, USENIX Security Symposium 2022 (Acceptance rate: 18%)
- C. Chen, R. Kande, P. Mahmoody, J. Rajendran, A.-R. Sadeghi, <u>Trusting the Trust Anchor: Towards Detecting</u> <u>Cross-Layer Vulnerabilities with Hardware Fuzzing</u>, in 2022 59th ACM/IEEE Design Automation Conference (DAC)

 A.-R. Sadeghi, J. Rajendran, R. Kande, <u>Organizing The World's Largest Hardware Security Competition:</u> <u>Challenges, Opportunities, and Lessons Learned</u>, in the Proceedings of the 2021 on Great Lakes Symposium on VLSI, pp. 95-100

EXPERIENCE

Hardware Security Group, Texas A&M UniversitySeGuide: Dr. Jeyavijayan Rajendran, Department of Electrical and Computer EngineeringGraduate Research Student

- I am developing hardware fuzzing tools to detect security vulnerabilities in processor designs.
- As an organizer of Hack@EVENT, a set of hardware security CTF competitions (1000+ participants so far), I
 added security features (like AES crypto engine, register locks and FUSE memory) and inserted more than
 200 security bugs in open source RISC-V SoCs like Ariane, OpenPiton, and OpenTitan.

Intel, Hillsboro, Oregon

Intern as Offensive Security Researcher

- Worked in the Offensive Security Research (OSR) team of the Intel Product Assurance and Security (IPAS) organization.
- Developed an automated static analysis tool to aid the design and verification engineers in detecting the vulnerabilities in the reset logic of Intel processors using Synopsys Verdi Interoperable Apps (VIA) interface.

Samsung Research Institute, Delhi, India

RTL Design and Verification Engineer

- CODEC IP project:
 - Enhanced the Verilog RTL design to reduce the design area. The gate count has been reduced by 10%.
 - Upgraded a bash script and a Verilog based test bench to automate the process of design verification.
- Security IP project:
 - Modified a C model of the IP to obtain a reference model for verification.
 - Developed a UVM based verification environment to verify the IP; Identified the functional coverage points, generated the corresponding test cases and verified the IP for all the test cases.

Department of Electronics and Communication Engineering, IIT Guwahati July 2016 – May 2017 Undergraduate Research Student

- Designed a 5-stage 32-bit Microprocessor with support for Co-processor, burst mode memory transfer, separate Instruction and Data cache, branch prediction and early branch evaluation.
- Verified the working of the processor design on a Xilinx based Virtex-6 FPGA evaluation kit for 100 programs each having 50-100 instructions.

Semi-Conductor Laboratory, Punjab, India

Intern

• Developed a hardware design IP for the UDP and Ethernet internet protocols with support for ARP protocol and an internal cache for temporary MAC address storage using Xilinx ISE Design and simulation tool.

AWARDS & ACHIEVEMENTS

- TheHuzz paper got shortlisted for Top Picks in Hardware and Embedded Security, 2023.
- Quality Graduate Student Award, Department of Electrical and Computer Engineering, TAMU, 2023.
- Third place, in Hardware Demonstration, IEEE Hardware Oriented Security and Trust, 2022.
- IEEE Hardware Oriented Security and Trust Student Travel Grant in 2020, 2022, and 2023.
- ACM/IEEE Design Automation Conference, Young Fellowship award in 2020 and 2021.
- USENIX Security Symposium Student Grant award in 2020 and 2021.
- ACM/IEEE Design Automation Conference, best Research Video Award in 2020.
- Department Graduate Merit scholarship, TAMU 2018.
- Qualified the 'Professional' programming test organized by Samsung (Only around 20% of the Samsung employees are Professional qualified world-wide).

Sept. 2018 – Present

May 2016 – June 2016

July 2017 – Aug. 2018

Dec. 2020 – May 2021

TALKS/TOOL DEMONSTRATIONS/WORKSHOPS

- Invited talk on Hardware Fuzzing at Indian Institute of Technology, Guwahati in Nov 2023.
- TheHuzz, Hardware Fuzzer to Detect Security Vulnerabilities in Processors, poster presentation at the Network and Distributed System Security Symposium (NDSS), 2023.
- TheHuzz, Hardware Fuzzer to Detect Security Vulnerabilities in Processors, CAD Tool Demo at 1st edition of CAD4SEC Workshop, 2022.
- *TheHuzz, Hardware Fuzzer to Detect Security Vulnerabilities in Processors,* Hardware Demonstration at IEEE Hardware Oriented Security and Trust, 2022.
- Insights and Lessons Learnt during Hack@DAC 2021, special session, ACM/IEEE Design Automation Conference, 2022.

LEADERSHIP & ACTIVITIES

Mentorship Activities at Texas A&M University

- Assisted junior PhD student, Aneesh Dixit, with setting up the FPGA experiments for his project.
- Mentored junior PhD students, Nicholas Heinrich-Barna and Saichand Samudrala with their "PLC Fuzzing", "Black-box Fuzzing", and "Hardware Architectures for Zero Knowledge Proof" projects.
- Assisted masters students, Georges Alsankary, Arjun Muralidharan, and Garrett Persyn with their thesis projects on fuzzing processors to detect security vulnerabilities.

Academic Activities at Texas A&M University

Assisted my advisor with teaching and managing the *Hardware Security* and *Introduction to Digital Design* courses during Fall'19, Spring'20, Spring'21, Fall'21, Fall'22, Fall'23.

- Designed class projects Logic Locking Processors, Identifying Hidden Instructions in Processors, & Hardware Fuzzing; class demonstrations Hacking into coffee-maker & Exploiting the vulnerabilities in hardware designs.
- Mentored 100+ undergraduate and graduate students.

Samsung Research Institute

Great Work Place (GWP) Agent

• Planned and organized various fun and team building activities on monthly and quarterly basis aimed to make Samsung a better work place.

Indian Institute of Technology, Guwahati

Head of Entrepreneurship Development Cell

- Lead a team of around 150 members to organize various lecture series and workshops in our campus including *UDGAM*, the Annual E-summit of IIT Guwahati.
- Organized TEDx for the first time in IIT Guwahati along with a team of Post Graduate students.

SERVICE

- Volunteer at Aggieland Humane Society, TX, USA
- Member of National Sports Organization (NSO), Athletics.
- Volunteered in LED (Learn.Explore.Discover) an initiative by the Annual Tech Festival of IITG in which we demonstrated simple experiments to the school students nearby our campus so as to explain them the basic principles of science.
- Volunteered as a member of Academic Initiatives club of our college to conduct remedial classes for the freshers of our department.

WORK AUTHORZATION

Eligible to work in the U.S for a period of 12 months under Curricular Practical Training (CPT) program.

April 2015 – April 2016

Aug. 2017 – Aug. 2018

Dec. 2022 to Present