Saket Upadhyay

Charlottesville, VA

saket@virginia.edu | saketupadhyay.com | github.com/Saket-Upadhyay | linkedin.com/in/saketupadhyay/ | Saket Upadhyay

Personal Profile

I am a Ph.D. candidate in Computer Science at the University of Virginia, specializing in memory compartmentalization and privilege isolation. My research leverages compiler infrastructure (LLVM) to automate software partitioning into isolated compartments, enforce fine-grained access policies, and verify correctness while maintaining efficient execution on physical hardware. As a Ph.D. intern at Google, I optimized large-scale cloud workloads under hardware constraints and multi-objective trade-offs, experience I apply to evaluating the performance overhead of isolation. My prior work includes object-level memory profiling of Chromium, threat intelligence, malware analysis, and reverse engineering. I am dedicated to expanding access to STEM education for individuals from diverse backgrounds.

Education

University of Virginia *Virginia, USA*

Ph.D. in Computer Science *Aug 2022 - Current*

- GPA 3.8/4
- Graduate Student Representative '25-26, '26-27
- International Student Citizen Leaders Fellowship '24-25
- Steering committee member in Computer Architecture Student Association (CASA) '23-24
- Teaching Assistant: Compilers CS4620, Network Security and Privacy CS6501/ECE6502

Vellore Institute of Technology *Bhopal, India*

BTech in Computer Science *May 2018 - May 2022*

- CGPA 8.5/10
- Established and led the student research and development group in the cybersecurity department.
- Conducted cybersecurity workshops for high school students and faculty training, including live demonstrations of security concepts.

Publications

Conference Proceedings

Shiny Objects: Object-Centric Characterization of Chromium. Saket Upadhyay, Ashish Venkat
ACM SIGMETRICS 2026, 2026, Ann Arbor, MI, USA

Special Session: Detecting and Defending Vulnerabilities in Heterogeneous and Monolithic Systems: Current Strategies and Future Directions. Venkat Nitin Patnala, Sai Manoj Pudukotai Dinakarrao, Guru Venkataramani, Jie Chen, Milos Doroslovacki, Fan Yao, Hongyu Fang, Meron Demissiea, Todd Austin, Lauren Biernacki, Saket Upadhyay, Arnabjyoti Kalita, Ashish Venkat
2024 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), 2024, Raleigh, NC, USA

PACE: Platform for Android Malware Classification and Performance Evaluation. Ajit Kumar, Vinti Agarwal, Shishir K. Shandilya, Andrii Shalaginov, Saket Upadhyay, Bhawna Yadav
2019 IEEE International Conference on Big Data (Big Data), 2019, Los Angeles, CA, USA

Journal Articles

Modified Firefly Optimization Algorithm-Based IDS for Nature-Inspired Cybersecurity. Shishir Kumar Shandilya, Bong Jun Choi, Ajit Kumar, Saket Upadhyay
Processes 11.3 (2023). 2023

AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. Shishir Kumar Shandilya, Saket Upadhyay, Ajit Kumar, Atulya K. Nagar
Future Generation Computer Systems 127 (Feb. 2022) pp. 297–308. 2022

PACER: Platform for Android Malware Classification, Performance Evaluation and Threat Reporting. Ajit Kumar, Vinti Agarwal, Shishir Kumar Shandilya, Andrii Shalaginov, Saket Upadhyay, Bhawna Yadav
Future Internet 12.4 (Apr. 2020) p. 66. 2020

Book Chapters

Nature-Inspired Malware and Anomaly Detection in Android-Based Systems. Saket Upadhyay
Advances in Nature-Inspired Cyber Security and Resilience, 2022

Archive

FuzzDistill: Intelligent Fuzzing Target Selection using Compile-Time Analysis and Machine Learning. Saket Upadhyay
arXiv, 2024

Projects

Compartmentalization and Privilege Management

DARPA, University of Virginia *2024 – Present*

- Designed and implemented LLVM compiler passes to automate software compartmentalization, using annotations from other collaborators.
- Developed compiler passes for verification of a multi-stage, multi-collaborator compartmentalization pipeline, to ensure correctness of access policies.
- Investigating and designing strategies for efficient compression of access matrices to optimize resource usage.
- Developed an instrumentation pass to inform gate-call placements for hardware enforcement by other collaborators.

Object-Centric Characterization of Large-Scale Software Systems

University of Virginia *August 2023 – Present*

- Developed a scalable, low-overhead instrumentation design for object lifetime profiling.
- Investigated the memory management strategies employed within the Chromium web browser.
- Implemented a compiler pass to instrument object tracking gadgets, enabling collection of object-level runtime data.
- Designed a framework for processing raw trace data and generating comprehensive lifetime analysis reports, supporting in-depth performance investigations.

Intelligent Fuzzing Target Selection via Compile-Time Analysis and Machine Learning

University of Virginia *August 2024 – December 2024*

- Designed and implemented a modular, open-source infrastructure for feature extraction, model training, and prediction for fuzzing target selection using compile-time analysis and machine learning.
- Achieved a PoC accuracy of 86% in identifying optimal fuzzing targets, demonstrating the effectiveness of the approach.
- Developed an LLVM compiler pass for efficient extraction of function-level and basic block features.
- Designed a Python framework to evaluate and train over ten ML algorithms, to find optimal approach for target selection.
- Created Python-based back-end APIs and a web front-end to visualize results.
- Project repository available at: https://github.com/Saket-Upadhyay/FuzzDistill

Teaching

CS6501/ECE6502 Network Security and Privacy *University of Virginia*

Graduate Teaching Assistant *Spring 2024 / Spring 2025*

- Delivered a guest lecture on ”Leveraging Compilers for Static Software Profiling,” exploring binary security techniques through compiler modifications, enhancing student understanding of low-level analysis. [llvm-obfuscation-edu]
- Graded assignments and projects.
- Conducted office hours.

CS4620 Compilers *University of Virginia*

Graduate Teaching Assistant *Fall 2023 / Fall 2024*

- Modernized the teaching compiler’s (tipc) optimizer by integrating a new pass manager within LLVM 15+.
- Implemented opaque pointers within the tipc’s CodeGen routine.
- Successfully migrated the tipc’s codebase from LLVM14 to LLVM17.
- Delivered an ‘explainer lecture’ to explain project details, code sections, and deliverable expectations.
- Graded assignments and projects.
- Conducted office hours.

Work Experience

Google *Hyderabad, India*

PhD SWE Intern *July 2026 - Nov 2026*

- Optimizing large-scale cloud systems for Google Cloud Platform.
- Designed and productionized a framework to automatically optimize multi-objective high-performance cloud workloads using evolutionary search , applied to diverse workloads on x86 and ARM VMs.
- Achieved an 8x improvement in zero-loss throughput of a network workload on multi-NIC VMs by treating CPU and DRAM as first-class optimization targets.
- Conducted experiments and reasoned about hardware constraints and tradeoffs in high-performance cloud systems, using custom C and Python probes for memory latency and per-packet timing.
- Fixed measurement bugs in PerfKit Benchmarker and contributed two merged fixes to the open-source Pktgen-DPDK benchmark.
- Built and used agentic tools to reduce developer toil.
- Presented the work to Google Cloud leadership.
- **Technical Skills:** Python, C, DPDK, Pktgen-DPDK, PerfKit Benchmarker, Linux VMs (x86 and ARM), Linux tools, NUMA and memory profiling, evolutionary optimization, workload analysis, data analysis, research documentation.

University of Virginia *Charlottesville, VA*

Research Assistant *Aug 2022 - Current*

- Low-level software and hardware security research with Dr. Ashish Venkat.
- **Technical Skills:** C++, Linux/Windows VMs, Linux tools, LLVM, LLVM IR, Python, x86 assembly, *nix scripting, Git, software build systems (CMake, ninja, makefiles), development on HPC clusters, data analysis, research documentation (LaTeX).

Uptycs *Bangalore, India (Remote)*

Security Research Intern *Jul 2021 - Jan 2022*

- Collaborated with a small team to expand the existing threat intelligence database that enables cloud-native application protection platform (CNAPP) and extended detection and response (XDR) solutions.
- Wrote and validated YARA rules for new malware families for the XDR platform.
- Validated detection rules for CNAPP and XDR deployment (development).
- Learned advanced malware reverse engineering and AV evasion techniques from renowned and experienced malware researchers.
- Gave a talk on 'Automating malware process scanning with Python3' in PyCode2021 Conference.
- **Technical Skills:** C++, Linux/Windows VMs, Linux tools, YARA, Python, x86 assembly, Scripting, Git., Debuggers, IDA Pro, Ghidra
- **Soft Skills:** Teamwork, Time Management, Communication, Presentation skills.

Skills

Core	x86, ARM, Operating Systems (Threads, Process Control, Memory/Resource Management, Virtual Memory), Systems Performance (NUMA and Memory Tuning, Cloud Benchmarking), Compilers (AST, Grammars, State Machines, Optimizations), LLVM, Bash/Shell Scripting, Security Testing, Reverse Engineering (GDB, Ghidra, IDA Pro, x32dbg, LLDB), Threat Analysis, Threat Models (OWASP, MITRE Att&ck).
Programming	C, C++, Python, x86 and ARM Assembly.
Miscellaneous	*nix systems, LaTeX, Microsoft Office, Git, Adobe Creative Cloud suite (Photoshop, PremierePro, Aftereffects, Lightroom)

Achievements

2024	**International Student Citizen Leaders Fellowship**, UVA	*USA*
2021	**1st Runner-up**, HackDSC Hackathon, Google DSC	*India*
2020	**Winner ,** Ultimate Secure Code Tournament	*Global*
2020	**Winner**, TrendMicro Cloud Security CTF	*Global*
2020	**Winner**, DEFCON 28 Secure Code Tournament	*USA*
2019	**Best Paper Award**, IEEE International Conference on Big Data 2019	*USA*

Interests

Motorcycles, Cooking, Mountain biking, Hiking, Swimming, Community Service.

Languages

English	Full professional proficiency (ILR level 4)
Hindi	Native proficiency (ILR level 5)
Marathi, Gujarati, Punjabi	Elementary proficiency (ILR level 1)
Russian, Dutch	(ILR level 0)

** ILR = Interagency Language Roundtable scale.*