Prashast Srivastava

CONTACT INFORMATION

DSI 406
Department of Computer Science
Columbia University
New York, NY 10027 USA

Voice: (510) 693-0372
E-mail: ps3400@columbia.edu
WWW: https://prashast.github.io

RESEARCH INTERESTS

My research focuses on improving the state of system security through software testing. I aim to democratize testing by expanding the capabilities of automated solutions to uncover hard-to-detect bugs and streamlining their integration into the software development pipeline.

EDUCATION

Purdue University, USA

Ph.D., Computer Science, **Aug. 2016 - May 2023**

- Dissertation Topic: "Practical Methods for Fuzzing Real-World Systems"
- Advisors: Prof. Mathias Payer, Prof. Antonio Bianchi

M.S., Computer Science

BITS-Pilani, UAE

B.E. (Hons.), Computer Science, **Aug. 2012 - Aug. 2016**

ACADEMIC EXPERIENCE

Columbia University, USA

Postdoctoral Research Scientist **Jun. 2023 - Present**
Conduct software testing research and mentor students under the supervision of Prof. Suman Jana.

Purdue University, USA

Graduate Student **Aug. 2016 - May 2023**
Built automated dynamic analysis frameworks to uncover vulnerabilities across a wide range of application domains, from low-level firmware running on embedded devices and off-the-shelf user-space utilities to libraries used in high-level enterprise applications.

Graduate Teaching Assistant **Aug. 2016 - Dec. 2017**
Served as Teaching Assistant (Fall 2016) and then Head Teaching Assistant (Fall 2017) for the undergraduate Operating Systems class with class strength of over 140 students.

PROFESSIONAL EXPERIENCE

GrammaTech, USA

PhD Research Internship **May 2018 - Dec 2018**
Implement ML-based software pipeline to perform binary similarity

PUBLICATIONS

Dongdong She, Adam Storek, Yuchong Xie, Seoyoung Kweon, **Prashast Srivastava**, and Suman Jana. "FOX: Coverage-guided Fuzzing as Online Stochastic Control." In Proceedings of the of the 31st ACM SIGSAC Conference on Computer and Communications Security, 2024.

Prashast Srivastava, Flavio Toffalini, Kostyantyn Vorobyov, François Gauthier, Antonio Bianchi, and Mathias Payer. "Crystallizer: A Hybrid Path Analysis Framework to Aid in Uncovering Deserialization Vulnerabilities." In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2023.

Prashast Srivastava, Stefan Nagy, Matthew Hicks, Antonio Bianchi, and Mathias Payer. "One Fuzz Doesn't Fit All: Optimizing Directed Fuzzing via Target-Tailored Program State Restriction."

In Proceedings of the 38th Annual Computer Security Applications Conference, 2022.

Prashast Srivastava, and Mathias Payer. "Gramatron: Effective Grammar-aware Fuzzing." In Proceedings of the 30th ACM Sigsoft International Symposium on Software Testing and Analysis, 2021.

Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, and Mathias Payer. "Firmfuzz: Automated IoT Firmware Introspection and Analysis." In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, 2019.

Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab, **Prashast Srivastava**, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer. "Protecting bare-metal embedded systems with privilege overlays." In Proceedings of the 38th IEEE Symposium on Security and Privacy, 2017.

Open-source Artifacts

`https://github.com/HexHive/FirmFuzz`*
`https://github.com/HexHive/Gramatron`*
`https://github.com/HexHive/Crystallizer`*
`https://github.com/HexHive/SieveFuzz`*
`https://github.com/FOX-Fuzz/FOX`

** Primary developer for the project*

Mentorship

Madalina Stoicov (Barnard B.S.) *OSS Fuzzer Development*	2024
Robert Boada (Columbia B.S.) *Visualizing Fuzzer Progress*	2024
Carol Zhang (Columbia Masters') *Modularizing Fuzzers*	2024
Adam Storek, (Columbia PhD) *Control-theory guided Fuzzing*	2023-2024
Seoyoung Kweon (Columbia Masters' → UCSD PhD) *Control-theory guided Fuzzing*	2023-2024
Farhan Saif (IUT Dhaka → UIC PhD) **SIGPLAN-M Mentee** *Probabilistic Seed Selection*	2023-2024
Jack Locascio (Purdue B.S. → Northrop Grumman) *Binary-level Directed Fuzzing*	2021-2022
Wermeille Bastien (EPFL Masters' → LIIP) *Java Deserialization Vulnerabilities*	2021
Henry Poggie (Purdue B.S. → UIUC) *Game Engine Fuzzing*	2019
Jiahao Li (MIT B.S → Hudson River Trading) *Embedded Firmware Fuzzing*	2017

Service

NDSS Program Committee	2025
DIMVA Program Committee	2025
ISC Program Committee	2025
ISSTA Tool Demonstrations Program Committee	2024, 2025
IEEE LangSec Workshop Program Committee	2023,2024, 2025
SIGPLAN-M Mentor	2023,2024
EuroSP External Reviewer	2022

	NDSS, Usenix Security Subreviewer	2021
	ACSAC Artifact Evaluation Committee	2017

Honors and Awards	ACSAC Best Poster Award	2022
	ACSAC Student Travel Grant	2022
	CCS Student Travel Grant	2019
	CERIAS Research Poster Competition (1st Place)	2018

Vulnerabilities Discovered	CVE-2018-19239, CVE-2018-19240, CVE-2018-19241, CVE-2018-19242 CVE-2020-15866 • **Avg. CVSS Score:** 8.62 • **Targets:** Routers, IP Cameras, Language Interpreters

Invited Talks	FOX: Coverage-guided Fuzzing as Online Stochastic Control (Seminar at Boston University)	2024
	Threat Modeling (Guest Lecture at Columbia)	2024
	Crystallizer: Java Deserialization Vulnerability Discovery (Conference talk at FSE)	2023
	Crystallizer: Java Deserialization Vulnerability Discovery (Security Seminar at Columbia)	2023
	One Fuzz Doesn't Fit All (Conference talk at ACSAC)	2022
	Challenges with Fuzzing Complex Systems (Guest lecture at Purdue University)	2021, 2022
	Gramatron: Efficient grammar-aware fuzzing (Conference talk at ISSTA)	2021
	Fuzzing IoT/CPS Devices (Guest Lecture at Purdue University)	2020
	FirmFuzz:Automated IoT Firmware Introspection (Conference Talk at IOTS&P)	2019