

Prashast Srivastava

Email: ps3400@columbia.edu
Phone: +1-510-693-0372 Website: prashast.github.io

Dept. of Computer Science,
Columbia University

Work Experience

Postdoctoral Research Scientist at Columbia University Jun 2023 - Present
Supervisor: Suman Jana New York, NY

Research internship at GrammaTech May 2018 - Dec 2018
Supervisor: Vineeth Kashyap Ithaca, NY

Education

Computer Science at Purdue University MS, Ph.D.
Advisors: Mathias Payer, Antonio Bianchi Aug 2016 - May 2023

Computer Science at BITS-Pilani Dubai Campus B.E. (Hons.)
CGPA: 9.29 Aug 2012 - Aug 2016

Publications

Dongdong S., Adam S, Yuchong X., Seoyoung K., **Prashast S.**, Suman J., “*FOX- Coverage-guided Fuzzing as Online Stochastic Control*”, in ACM SIGSAC Conference on Computer and Communications Security (CCS’24), 2024

Prashast S., Flavio T., Kostyantyn V., Francois G., Antonio B., Mathias P., “*Crystallizer: A Hybrid Path Analysis Framework to Aid in Uncovering Deserialization Vulnerabilities*”, in ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE’23), 2023

Prashast S., “*Practical Methods for Fuzzing Real-World Systems*”, Ph.D. Thesis, Purdue University, 2023

Prashast S., Stefan N., Matthew H., Antonio B., Mathias P., “*One Fuzz Doesn’t Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction*”, in Annual Computer Security Applications Conference (ACSAC ’22), 2022

Prashast S., Mathias P., “*Gramatron: Efficient grammar-aware fuzzing*”, in ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA ’21), 2021

Prashast S., Hui P., Jiahao L., Hamed O., Howard S., Mathias P., “*FirmFuzz: Automated IoT Firmware Introspection and Analysis*”, in ACM CCS Workshop on IoT Security and Privacy (IoT S&P ’19), 2019

Abraham C., Naif A., Khaled S., **Prashast S.**, Jinkyu K., Saurabh B., Mathias P., “*Protecting Bare-metal Embedded Systems With Privilege Overlays*”, in IEEE Symp. On Security and Privacy (IEEE S&P ’17), 2017

Rajesh S., C. Hota, **Prashast S.**, “*Roppery: Protection against code exploitation using ROP and Checksumming in IoT environment*” in International Conf. on Communication and Info. Technology, 2017

Mentorship

Henry Poggie, <i>Game Engine Fuzzing</i> , Purdue Undergraduate Project	2019
Wermeille Bastien, <i>Java-based Gadget Chain Classification</i> , EPFL Masters Project	2021
Jack Locascio, <i>Binary-level Directed Fuzzing</i> , Purdue Undergraduate Project	2021-2022
Adam Storek, Control-theory guided Fuzzing, Columbia PhD Project	2023-2024
Seoyoung Kweon, Fuzzing Progress Quantification, Columbia Masters' Project	2023-2024
Farhan Saif, <i>Probabilistic Seed Selection</i> , SIGPLAN-M Mentorship program	2023-2024

Teaching

CS354 - Operating Systems	Fall 2016, Fall 2017
<i>Purdue University - Graduate Teaching Assistant</i>	<i>West Lafayette, IN</i>
<ul style="list-style-type: none">• TA for a class of 123 students (Fall 2016) and Head TA for a class of 148 students (Fall 2017)• Created a lab assignment around a FUSE-based filesystem used in both terms.	

Service

ACSAC Artifact Evaluation Committee	2017
NDSS, Usenix Security Subreviewer	2021
EuroS&P External Reviewer	2022
IEEE LangSec Workshop Program Committee	2023, 2024
ISSTA Tool Demonstrations Program Committee	2024
SIGPLAN-M Program Mentor	2023, 2024
NDSS Program Committee	2025

Awards

CERIAS Symposium Research Poster Competition (1st Place)	2019
Best Poster Award at ACSAC'22	2023

Vulnerabilities discovered

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

Invited Talks

<i>FirmFuzz: Automated IoT Firmware Introspection and Analysis</i> , Conference talk at IOT S&P'19	2019
<i>Fuzzing IoT/CPS devices</i> , Guest lecture at CS department, Purdue University	2020
<i>Gramatron: Efficient grammar-aware fuzzing</i> , Conference talk at ISSTA '21	2021
<i>Challenges with Fuzzing Complex Systems</i> , Guest lecture at CS department, Purdue University	2021, 2022
<i>One Fuzz Doesn't Fit All</i> , Conference talk at ACSAC '22	2022
<i>Crystallizer: Deserialization Vulnerability Discovery</i> , Conference talk at FSE '23	2023