Prashast Srivastava

Email: prashast.srivastava@gmail.com
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.
GPA: 3.62 *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

Research Projects

Data-Driven Seed Filtering for Effective Fuzzing — Jun 2022 - Present
Purdue University - Graduate Research Assistant — *West Lafayette, IN*

- Formulate and conceptualize the probabilistic strategy for seed filtering
- Engineered the evaluation pipeline to aid in fine-tuning the filtering strategy
- Can outperform state-of-the-art corpus minimization tool while using drastically lesser seeds

Hybrid Path Analysis to Uncover Deserialization Vulnerabilities — Jun 2021 - Present
Purdue University - Graduate Research Assistant — *West Lafayette, IN*

- Engineered a framework to identify gadget chains for exploiting deserialization vulnerabiities
- Formulated a hybrid program analysis methodology to create concrete payloads for gadget chains
- Uncovered 38 new exploitable gadget chains across seven popular Java libraries

Optimizing Directed Fuzzing via Target-tailored Program State Restriction — Dec 2019 - Jun 2021
Purdue University - Graduate Research Assistant — *West Lafayette, IN*

- Built a directed fuzzing framework to test specific target locations in software applications
- Devised a methodology based on preemptive termination of infeasible program states
- Is more consistent and faster at uncovering bugs than existing state-of-the-art directed fuzzers

Effective Grammar-Aware Fuzzing using Grammar Automatons — Oct 2018 - Aug 2020
Purdue University - Graduate Research Assistant — *West Lafayette, IN*

- Built a framework for guided fuzzing of targets taking in structured input eg. interpreters
- Used formal language theory techniques to build an effective grammar-aware fuzzer
- Found 10 previously undiscovered vulnerabilities and has been integrated into AFL++ and LibAFL

Identification of Library Components in Stripped Binaries May 2018 - Dec 2018
GrammaTech - Research Internship *Ithaca, NY*

- Developed a framework for library component detection in statically linked stripped binaries.
- Built the evaluation framework for the initial prototype in Python
- Deployed as a product by GrammaTech now as CodeSentry

Automated IoT Firmware Introspection and Analysis Mar 2017 - May 2018
Purdue University - Graduate Research Assistant *West Lafayette, IN*

- Developed an automated dynamic analysis framework for the firmware of embedded devices.
- Built a generational fuzzer in Python and C with a Selenium backend.
- Found 7 previously undisclosed vulnerabilities across 6 different devices and assigned 4 CVE-ID

Publications

[In review] **Agustin M.***, **Prashast S.***, Alejandro R., Mathias P., *"Data-Driven Seed Filtering for Effective Fuzzing"*

[In review] **Prashast S.**, Flavio T., Kostyantyn V., Francois G., Antonio B., Mathias P., *"Probabilistic Path Exploration to Uncover Deserialization Vulnerabilities"*

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 (Oakland '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

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

Teaching

CS354 - Operating Systems Fall 2016, Fall 2017
Purdue University - Graduate Teaching Assistant *West Lafayette, IN*

- 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.

Mentorship

Henry Poggie, *Game Engine Fuzzing*, Purdue Undergraduate Project 2019
Wermeille Bastien, *Java-based Gadget Chain Classification*, EPFL Masters Project 2021
Jack Locascio, *Binary-level Directed Fuzzing*, Purdue Undergraduate Project 2021-2022

Service

ACSAC Artifact Evaluation Committee 2017
NDSS, Usenix Security Subreviewer 2021
EuroS&P External Reviewer 2022
IEEE LangSec Workshop Program Committee 2023

Invited Talks

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

Skills

Languages - Python, C, C++, Java
Frameworks - QEMU, AFL, AFL++, Jazzer, Soot, Selenium, Honggfuzz, Radare, IDA, Docker