Prashast Srivastava

Email: prashast.srivastava@gmail.com
Phone: +1-510-693-0372 Website: prashast.github.io

Dept. of Computer Science,
Purdue University

Education

Computer Science at Purdue University — MS, Ph.D.
GPA: 3.62 *Research Domain*: Cybersecurity *Advisors*: Mathias Payer — 2016 - Present

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

Research Projects

Efficient Coverage-guided Structured Fuzzing — Oct 2018 - Dec 2019
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 a fast grammar-aware fuzzer on top of AFL
- Evaluated against state-of-the-art grammar-aware fuzzer and showed its effectiveness

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 in Python
- Promising results delivered across different compilers and optimizations.

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 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

Protecting Bare-metal Embedded Systems with Privilege Overlays — Aug 2016 - Dec 2016
Purdue University - Graduate Research Assistant — *West Lafayette, IN*

- Built a verifier for the compiled programs to ensure the correctness of the framework.
- Used Python to parse the assembly level executables and verify the instrumentations.
- Validated the security measures implemented by the compiler and pointed out data leaks.

Lightweight Self-verification code for IoT Devices — Aug 2015 - Dec 2015
BITS - Pilani, Hyderabad Campus - Research Internship — *Hyderabad, India*

- Developed lightweight techniques written in C for code self-verification on IoT devices.
- Employed Return Oriented Programming along with Code Checksumming
- Evaluated its efficacy by deploying it on applications running on an IoT testbed

Publications

[In review] **Prashast S.**, Mathias P., "*Gramatron: Efficient grammar-aware fuzzing*"

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, 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
Details: https://seclists.org/fulldisclosure/2018/Dec/21 **Avg. CVSS Score**: 8.32

Posters

"*Automated IoT Firmware Introspection and Analysis*" in 19th Annual CERIAS Research Poster Competition, Purdue University, 2018 (**Best Poster Award** -- 41 participants)

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.

Service

ACSAC Artifact Evaluation Committee 2017

Skills

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