Rishi Ranjan

| | | | |

Summary

My experience/interests lie in software and hardware fuzzing, vulnerability research and compiler theory. I have developed fuzzers for various platforms including UNIX and Windows, which have found bugs in various open and closed source softwares for which I have been credited with multiple CVEs. I have participated and won many CTFs, where I solved binary exploitation and reverse engineering challenges. My current focus is on leveraging compiler instrumentation techniques for faster and more efficient fuzzing.

Education

Virgina Tech *August 2022 - Present*
M.S. Computer Science, Advisor: Dr. Matthew Hicks

Indian Institute of Technology, Roorkee *July 2018 - May 2022*
B.Tech. Computer Science and Engineering GPA : 9.1/10

Publications

Published

Leo Stone, **Rishi Ranjan**, Matthew Hicks and Stefan Nagy. No Linux, No Problem: Fast and Correct Windows Binary Fuzzing via Target-embedded Snapshotting. ***USENIX Security 2023***.

In Review

Rishi Ranjan, Ian Peterson and Matthew Hicks. In Submission. ClosureX: Transforming Source Code for Correct Persistent Fuzzing. ***USENIX Security 2024***.

Work Experience

Research Assistant | FoRTE Research, Virginia Tech August 2022 - Present

Advisor: Dr. Matthew Hicks

- My work focuses on systems security and novel vulnerability research techniques.
- Designed new compile-time techniques to perform program state restoration at IR level for better fuzzing performance.
- Found **0-day bugs** in popular software like Linux Kernel's BPF library, GoPro's metadata parser and other popular open-source projects like c-blosc2 and md4c.

Security Research Intern | FoRTE Research, Virginia Tech October 2021 - February 2022

Advisor: Dr. Matthew Hicks

- Designed and implemented, state-of-the-art fuzzer WinFuzz for Windows.
- Found **0-day bugs** in popular open-source software such as GoPro's metadata parser, audiofile, pdf2json and jhead.
- Work published in the top security conference **USENIX Security 2023**.

Security Research Intern | HexHive, Summer@EPFL May 2021 - October 2021

Advisor: Dr. Mathias Payer

– Selected among 10,000 applicants for a research internship at École Polytechnique Fédérale de Lausanne under Dr Mathias Payer in collaboration with Huawei.

– Worked on a project for designing a stateful network protocol fuzzer, designed and implemented a new structured input generator for the fuzzer.

Student Developer @AFL++ | Google Summer of Code May 2020 - August 2020

Advisor: Dominik Maier, Heiko Eißfeldt

– Google Summer of Code is a global internship program focused on bringing student developers into open source software development.

– Designed and implemented the initial version of famous multithreaded scalable library for fuzzing called LibAFL in C. (Paper in ACM CCS 2022).

Projects

False-nine - A Compile-time memory optimisation project | Virginia Tech Github

– Implemented a compiler pass to automatically free dead memory objects on the heap.

– Reduces both the average and peak memory usage of a program significantly.

– Tech stack includes C++, LLVM and cmake.

LLVM based Compiler Optimizations | Virginia Tech Github

– Implemented LLVM passes to perform optimizations like Dead Code elimination, LICM on IR Code.

– Developed a generic framework to implement all kinds of Dataflow analysis compile-time passes.

– Tech stack includes C++ and LLVM toolchain.

Chakra, Content Management System | IMG, IIT Roorkee IITR Website

– As Chief Technical Coordinator of Information Management Group, IIT Roorkee, I designed and developed an in-house, modular Content Management System for hosting and maintaining **IIT Roorkee's official website**.

– Chakra is a RBAC based CMS to control access to webpages for the institute administration.

– It is used to maintain over **10,000** static webpages and **50** dynamic web services of the institute,

– The tech stack includes Scala, Django, NextJS, PostgreSQL and Docker.

Omniport | IMG, IIT Roorkee Documentation

– Omniport is the official all-purpose portal for IIT Roorkee student, faculty and administration.

– It hosts over 20 different official applications of IIT Roorkee which are used by students and administration alike, and has a userbase of over 15,000 users.

– As Chief Technical Coordinator of IMG, IIT Roorkee, I lead the development, maintainence and security of the backend, frontend and server-side for the portal.

– The tech stack includes Django, ReactJS, PostgreSQL, redis and Docker.

Achievements

CVEs credited	CVE-2023-37185, CVE-2023-37186, CVE-2023-37187, CVE-2023-37188.

Capture The Flag competitions (CTFs)

CSAW CTF 2020	Ranked **2nd** in India and **14th** globally as part of InfoSecIITR.
CISCO SecCon A&D CTF 2020	Ranked **1st** as a part of InfoSecIITR.
AISS 2020 CTF	Ranked **2nd** in India as part of team inv4sion
WhiteHat CTF 2020	Qualified for finals in Vietnam.
CSAW CTF 2019	Ranked **2nd** in India and **13th** globally as part of InfoSecIITR.

Other Awards

James Thomason Scholarship Awardee	Ranked among the top candidates selected at IIT Roorkee.
Joint Entrance Examination 2018 (Advanced)	Ranked in top 0.3 percentile with a rank of **280** among 150,000 candidates.

Relevant Technical Coursework

Graduate	Network Security, System and Software Security, Compiler Optimizations
Undergraduate	Information Security, Advanced Computer Architecture, Operating Systems, Compiler Design, Machine Learning

Skills

Languages	C, C++, Python, Scala, Javascript, Bash, x86 Assembly
Software Packages	LLVM, AFL++, LibAFL, Git, GDB, Ghidra, IDA Pro, SymCC, pwntools, QEMU, Django, ReactJS, NextJS
Platforms/Architectures	Linux, Windows, WSL, Docker

Outreach and Professional Development

Chief Technical Coordinator, IMG IIT Roorkee *May 2021 - May 2022*
Led the team of 40 students in development and maintainence of official software and services ecosystem of IIT Roorkee.
Responsible for maintaining and deploying protective measures at the software and server level to enhance the security of these services.

Coordinator, InfoSecIITR *July 2020 - August 2021*
Led the CTF team InfoSecIITR to popular CTF victories and contributed toward fostering a security culture in IIT Roorkee through talks and workshops.

Mentor, Student Mentorship Program IIT Roorkee *August 2020 - May 2021*
Mentored five freshman students in Computer Science, IIT Roorkee.