

Akshay Ajayan

Tempe, Arizona

✉ iamakshayajayan@gmail.com | 🏠 akshayajayan.com

Personal Profile

Security researcher and CTF player. Arizona State University graduate student. Member of CTF team Shellphish. Experienced in binary analysis, software reverse engineering and linux application development in Python and C.

Work Experience

SEFCOM Lab, Arizona State University

Tempe, Arizona

Research Assistant

August 2020 - Present

- Current project focuses on improving fuzzing using target specific seed compression
- Found and reported multiple bugs in linux filesystem drivers
- Collaborated with researchers in multiple projects to improve the security of real world programs
- Research Topics: Binary Analysis, Symbolic Execution, Fuzzing, Taint Analysis, Reverse Engineering, Binary Exploitation

SEFCOM Lab, Arizona State University

Tempe, Arizona

Research Apprentice

February 2019 - April 2020

- Project: Improving ntfs-3g using differential symbolic execution
- Developed a framework for concolic tracing FUSE API based linux filesystem drivers for NTFS, FAT and VFAT
- Applied techniques like symbolic execution and reverse engineering for this project
- Wrote a Windows kernel driver and a userspace program to directly interface with ntfs.sys driver
- Contributed to open source projects like angr and claripy
- Advised by Dr. Ruoyu "Fish" Wang and Dr. Yan Shoshitaishvili

Teaching Experience

- | | | |
|------|--|------------|
| 2023 | Teaching Assistant at ASU , CSE 545: Software Security, Assisted Dr. Ruoyu "Fish" Wang | Tempe, USA |
| 2022 | Teaching Assistant at ASU , CSE365: Introduction to Information Assurance, Assisted Dr. Ruoyu "Fish" Wang | Tempe, USA |
| 2022 | Teaching Assistant , ForAllSecure Hackathon held at ASU | Tempe, USA |

Education

Arizona State University, Tempe Campus

Arizona, USA

Ph.D. in Computer Science

August 2020 - Present

Advisors: Dr. Ruoyu "Fish" Wang and Dr. Yan Shoshitaishvili

Amrita Vishwa Vidyapeetham, Amritapuri Campus

Kerala, India

B.Tech. in Computer Science

July 2015 - May 2019

Achievements

- | | | |
|------|---|-------------------|
| 2021 | 10th Place at HITB PRO CTF Finals , Team Shellphish | Abu Dhabi, UAE |
| 2019 | Runners-up at CSAW Embedded Security Challenge , Team Pwndevils | New York, USA |
| 2019 | Black Hat Student Scholarship , Black Hat USA | Las Vegas, USA |
| 2018 | Finalist at CSAW CTF , Team bi0s | IIT Kanpur, India |
| 2018 | Winner of Battle Underground CTF , NullCon International Security Conference | Goa, India |
| 2018 | Student Excellence Award , Amrita Vishwa Vidyapeetham | Kollam, India |
| 2017 | Second runners-up at Tux of War , Tathva - National level Techfest | NITC, India |
| 2017 | Student Excellence Award , Amrita Vishwa Vidyapeetham | Kollam, India |

Vulnerability Research

- | | |
|----------------|--|
| XFS | CVE-2023-2124 |
| NTFS-3G | CVE-2021-39251, CVE-2021-39252, CVE-2021-39253, CVE-2021-39254, CVE-2021-39255, CVE-2021-39256, CVE-2021-39257, CVE-2021-39258, CVE-2021-39259, CVE-2021-39260, CVE-2021-39261, CVE-2021-39262, CVE-2021-39263 |
| Pillow | CVE-2021-27921, CVE-2021-27922, CVE-2021-27923 |

Projects

Platform Independent Programs (PIP-64)

Final year Undergraduate Project

- Made platform independent programs for aarch64 and x64 with focus on it's security implications.
- Successfully created multiple programs valid on both architectures.
- Program can have the same or different behavior depending on the architecture.
- Created a single shellcode valid on multiple architectures.

Open-source Contribution

Binary analysis and CTF tools

- angr - Binary analysis framework. Made multiple bug fixes, added support for control registers and wrote a few function summaries.
- radare2 - Reverse engineering framework for Unix. Added support for recovering class structure information from gcc compiled binaries.
- r00tEmu - Unicorn engine based emulator for x64 programs. Has basic support for tracing and generating memory/register dumps.
- Differential Debugging: Helper tool for debugging large binaries. Records and highlights executed instructions in IDA.

Extracurricular Activities

Shellphish CTF Team

Tempe, USA

Member

2019 - Present

- Participated in and won multiple CTF events
- Entered DEF CON CTF finals from 2019 to 2023
- Developed automated tools for attack defense CTFs

bi0s CTF Team

Kollam, India

Member

2016 - 2019

- Mentored and lead a team of undergraduates
- Reverse engineered binaries of different architectures and languages
- Participated in and won multiple CTF events
- Organized yearly CTF events InCTF and InCTF Junior
- Hosted workshops for college and school students

Skills

Languages Python, C, C++, Assembly (x86, x64, MIPS, ARM), Bash

Tools GDB, IDA Pro, Ghidra, angr, radare2, pwntools, Intel PIN, Git