Akshay Ajayan

Tempe, Arizona

✉ iamakshayajayan@gmail.com | ⌂ akshayajayan.com | r00tus3r

Personal Profile

Security researcher and CTF player. Arizona State University graduate student. Member of CTF team Shellphish. Experienced in binary analysis, fuzzing, vulnerability research, software reverse engineering and 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
- Research Topics: Binary Analysis, Symbolic Execution, Fuzzing, Taint Analysis, Reverse Engineering, Binary Exploitation

Microsoft Corporation *Redmond, Washington*

Research Intern *June 2024 - August 2024*

- Used LLMs to automatically fix C/C++ security warnings reported by PREFast static analysis tool
- Developed a fully automated pipeline and evaluated it on windows source code
- Collaborated with MORSE (Microsoft Offensive Research & Security Engineering) and MSECAI (Microsoft Security & Artificial Intelligence)

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
- Wrote a Windows kernel driver and a userspace program to directly interface with ntfs.sys driver
- 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 - May 2026 (Expected)*

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*

Publications

Operation Mango: Scalable Discovery of Taint-Style Vulnerabilities in Binary Firmware Services

Wil Gibbs, Arvind S Raj, Jayakrishna Menon Vadayath, Hui Jun Tay, Justin Miller, **Akshay Ajayan**, Zion Leonahenahe Basque, Audrey Dutcher, Fangzhou Dong, Xavier Maso, Giovanni Vigna, Christopher Kruegel, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang
33rd USENIX Security Symposium (USENIX Security 24), 2024, Philadelphia, PA

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

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*

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, Qemu, IDA Pro, Ghidra, angr, radare2, pwntools, Intel PIN, Git