

Akul Pillai

Curriculum Vitae

📍 West Lafayette, IN, USA

☎ +1 (765) 746-9668

@ contact@akulpillai.com

🌐 akulpillai.com

🐙 github.com/akulpillai

🐦 @akulpillai

Education

- 2022 – present **PhD Student** **CGPA: 4.0/4.0**
Electrical and Computer Engineering, Purdue University
- 2017 – 2021 **Bachelor of Technology** **CGPA: 8.58/10**
Computer Science and Engineering, Amrita School of Engineering, Amritapuri.
Graduated in June 2021

Experience

- August 2021
- present **Visiting Research Scholar** **Purdue University**
Conducting research with Prof. Aravind Machiry at the School of Electrical and Computer Engineering on various aspects of systems security.
- 2017 – 2021 **Team biOs member** **Academic CTF Team, Amrita School of Engineering, Amritapuri**
Reverse engineering and binary analysis of Linux, OS X and Windows binaries, kernel modules, and Android applications.
Familiarized with multiple architectures, obfuscation & Anti-analysis techniques, fuzzing and binary exploitation of x86-64 Linux binaries / kernel modules.
Part of the core team, responsible for mentoring junior members and leading projects.
- May 2019
summer **Google Summer of Code** **The NetBSD Foundation**
Completed the project "Adapting TriforceAFL for NetBSD Kernel Fuzzing", adding a new fuzzer to the NetBSD security tools arsenal.

Projects

- Aug 2021 **Cornucopia** **Developer**
A framework for feedback-guided generation of binaries
C++ / Python / Linux
- April 2020 **biOs-ADF** **Developer and Maintainer**
An optimized and automated Attack Defence CTF Framework written in Rust, developed in-house by team biOs with a focus on eliminating setup-difficulty, used in multiple national level CTFs.
Rust / Linux
- Nov 2020 **mad_monkey** ([Gitlab](#)) **Developer and Maintainer**
Fuzzer for FreeBSD's libalias module, which can be fuzzed on Linux.
C / Linux
- Aug 2020 **concrete** ([Github](#)) **Developer and Maintainer**
Get coverage data for compiled binaries. Currently supports x86-64 ELF.
Rust / Linux
- Jun 2020 **secREtary** ([Github](#)) **Developer and Maintainer**
A Reverse Engineering Toolkit developed by team biOs. Contributed to the TaintTracker Module which can taint input and print backtraces for functions where tainted input was accessed, modified or compared.
C++ / Intel PIN / Linux
- April 2020 **rustyrop** ([Github](#)) **Developer and Maintainer**
ROP gadget scanner in Rust. Currently supports x86-64 ELF/Mach-O binaries.
Rust
- Feb 2020 **lizardmap** ([Github](#)) **Developer and Maintainer**
A script that generates an interactive treemap visualisation of cyclomatic complexities from the results of *lizard*. This visualisation can aid in target selection for software assessment and fuzzing.
Python

- Jun 2019 **TriforceNetBSDSyscallFuzzer** ([Github](#)) **Developer and Maintainer**
 A syscall fuzzer for NetBSD built on top of TriforceAFL which is a modified version of AFL that supports fuzzing using QEMU's full system emulation.
C / Python / x86-64 / NetBSD
- Jan 2019 **Contributions to NetBSD** **Community Contributor**
 Authored an example Kernel Module - *mapper* which is a basic implementation of mmap.
 Submitted patches for several undefined behaviour bugs triggered while booting the NetBSD kernel allowing for fuzzing with the UB sanitizer enabled.
 Created pkgsrc packages [wip/triforceafl](#) and [wip/triforcenetbsdsyscallfuzzer](#).
C / Python / x86-64 / Linux
- Nov 2018 **How2Kernel** ([Github](#)) **Developer and Maintainer**
 A repository to get started with kernel exploitation in Linux with exploitable kernel modules, kernel images, exploits and documentation detailing the mitigations and bypasses.
C / Python / x86-64 / Linux

Technical Skills

Languages: Python, Rust, C, x86, ARM
Tools: GDB, radare2, IDA Pro, Ghidra
Frameworks: Intel PIN, FRIDA, Capstone, angr

Research Interests

Reverse Engineering
 Binary Analysis
 Operating Systems
 Fuzzing
 Vulnerability Research

Achievements

- April 2020 **Champions, International** **IJCTF**
 Finished the online CTF emerging as the winner, as a part of team biOs.
- April 2020 **Runners Up, International** **Byte Bandits CTF**
 Played as part of team biOs's reversing team.
- Aug 2019 **Runners Up, International** **Onsite Finals, ISITDTU CTF, Da Nang, Vietnam**
 Champions in the online qualifiers round, finished runners up in the onsite finals.
- Mar 2019 **Student Scholarship Awardee and Packet Wars Winner** **Troopers 19, Heidelberg, Germany**
 Selected to attend with scholarship for completing technical challenge.
 Subsequently won onsite CTF event.
- Oct 2018 **Champions, International** **Hack.lu CTF, Ruhr-Universität, Bochum, Germany**
 Crowned the winner in the online CTF organised at the Hack.lu Conference at Luxembourg.

Technical Talks

- Mar 2019 **A Look into the Sanitizer Family** ([Slides](#)) **Cysinfo Community Meetup, Bengaluru**
 Detailing the usage and working of the Address Sanitizer (ASan) and the Undefined Behaviour Sanitizer (UBSan) and how they can aid in fuzzing and vulnerability detection.

Events Organised

- 2018 - 2021 **InCTF Events** **Team biOs**
 Core Organiser and Challenge Author
- InCTF Junior**
 Reverse Engineering challenge creation team lead for InCTFj, a CTF conducted by team biOs for School Students in India with a focus on Cyber Security awareness.
- InCTF Nationals**
 Challenge Author and Reversing team lead for the National edition of InCTF, a CTF conducted for University Students in India.
- InCTF International**
 Challenge Author and Reversing team lead for the international edition of InCTF, a 68.89 rated CTF on cftime.org