Vadayath Jayakrishna Menon

PH.D. · COMPUTER SCIENCE

✉ jkrshnmenon@asu.edu | ⌂ https://jkrshnmenon.github.io/ | ⊙ github.com/jkrshnmenon | in linkedin.com/in/jkrshnmenon/

Education

Arizona State University   *Arizona, USA*
Doctor of Philosophy in Computer Science   *Aug 2019 - Current*
- GPA: 4.0
- Research in Cyber Security

Amrita University   *Kerala, India*
Bachelor of Technology in Computer Science and Engineering   *July 2014 - May 2018*
- GPA: 9.27/10.0
- Graduated with Distinction

Research Experience

SEFCOM Lab at Arizona State University   *Arizona, USA*
Research Assistant   *Aug 2019 - Current*
- Working with Dr. Yan Shoshitaishvili and Dr. Ruoyu "Fish" Wang
- Research topics: Binary Exploitation, Fuzzing, Symbolic Execution, Static Binary Analysis, Reverse Engineering

ForAllSecure   *Pennsylvania, USA*
Intern   *May - Aug (2022) & May - Aug (2023)*
- Worked with Thanassis Avgerinos and Maxwell Koo
- Worked on implementing a snapshot fuzzer for virtual machines

SEFCOM Lab at Arizona State University   *Arizona, USA*
Research Scholar   *Oct 2018 - May 2019*
- Worked under the supervision of Dr. Yan Shoshitaishvili and Dr. Ruoyu "Fish" Wang
- Analyzing binary application software for identifying vulnerabilities

ISI at University of Southern California   *California, USA*
Research Scholar   *Feb 2018 - Oct 2018*
- Worked under the supervision of Dr. Christophe Hauser
- Identifying potential leak of pointers through static binary analysis and symbolic execution

Research Publications

Fuzz to the Future: Uncovering Occluded Future Vulnerabilities via Robust Fuzzing   *Salt Lake City, UT*
31st ACM Conference on Computer and Communications Security (CCS 24)   *2024*
Arvind S Raj, Wil Gibbs, Fangzhou Dong, **Jayakrishna Menon Vadayath**, Michael Tompkins, Steven Wirsz, Yibo Liu, Zhenghao Hu, Chang Zhu, Gokulkrishna Praveen Menon, Brendan Dolan-Gavitt, Adam Doupé, Ruoyu Wang, Yan Shoshitaishvili and Tiffany Bao,

Operation Mango: Scalable Discovery of Taint-Style Vulnerabilities in Binary Firmware Services   *Philadelphia, PA*
33rd USENIX Security Symposium (USENIX Security 24)   *2024*
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, and Ruoyu Wang

"Watching over the shoulder of a professional": Why hackers make mistakes and how they fix them   *San Francisco, CA*
45th IEEE Symposium on Security and Privacy (S&P 24)   *2024*
Irina Ford, Ananta Soneji, Faris Bugra Kokulu, **Jayakrishna Vadayath**, Zion Leonahenahe Basque, Gaurav Vipat, Adam Doupé, Ruoyu Wang, Gail-Joon Ahn, Tiffany Bao, and Yan Shoshitaishvili,

Greenhouse: Single-Service Rehosting of Linux-Based Firmware Binaries in User-Space Emulation   *Anaheim, CA*
32nd USENIX Security Symposium (USENIX Security 23)   *2023*
Hui Jun Tay, Kyle Zeng, **Jayakrishna Menon Vadayath**, Arvind S Raj, Audrey Dutcher, Tejesh Reddy, Wil Gibbs, Zion Leonahenahe Basque, Fangzhou Dong, Zack Smith, Adam Doupé, Tiffany Bao, Yan Shoshitaishvili, and Ruoyu Wang

Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs *Massachusetts, USA*

31st USENIX Security Symposium (USENIX Security 22) *2022*

Jayakrishna Vadayath, Moritz Eckert, Kyle Zeng, Nicolaas Weideman, Gokulkrishna Praveen Menon, Yanick Fratantonio, Davide Balzarotti, Adam Doupé, Tiffany Bao, Ruoyu Wang, Christophe Hauser and Yan Shoshitaishvili

Sleak: Automating Address Space Layout Derandomization *Puerto Rico, USA*

The 35th Annual Computer Security Applications Conference *2019*

Christophe Hauser, **Jayakrishna Menon**, Yan Shoshitaishvili, Ruoyu Wang, Giovanni Vigna and Christopher Kruegel

Professional Activities

ACM Conference on Computer and Communications Security *Utah, USA*

Artifact Evaluation Committee Member *Oct 2024*

18th USENIX WOOT Conference on Offensive Technologies (WOOT '24) *Pennsylvania, USA*

Artifact Evaluation Committee Member *Aug 2024*

Teaching Experience

CSE545: Software Security at Arizona State University *Arizona, USA*

Teaching Assistant *Aug 2021- Dec 2021*

- Assisted Dr. Ruoyu "Fish" Wang
- Primary duties were helping students with assignments and coursework

CSE365: Information Assurance at Arizona State University *Arizona, USA*

Teaching Assistant *Aug 2020- Dec 2020*

- Assisted Dr. Ruoyu "Fish" Wang
- Primary duties were helping students with assignments and coursework

Projects

Arbiter

A scalable and precise hybrid vulnerability analysis framework

- A hybrid vulnerability analysis framework that can be used to vulnerabilities that satisfy a given vulnerability description in binaries in a scalable and precise manner.
- Source code available on GitHub

PuzzIL

An intermediate language fuzzer for PHP

- An intermediate language fuzzer for the PHP JIT engine based on top of PhpIL.
- Found 2 bugs in the JIT engine of PHP 8.0
- Source code available on GitHub

Vulnerability Research

2023	**Wyze Camera 0-day**, Pwn2Own	*Vancouver*
2022	**Synology NAS 0-day**, Pwn2Own	*Vancouver*
2018	**CVE-2018-18311**, Heap overflow in Perl interpreter, CVSS 3.0 score: 9.8	

Extracurricular Activities

2024	**AIxCC Finalist with Shellphish**, DARPA AI Cyber Challenge	*Las Vegas, USA*
2024	**Small Business Track Competition Winners with Shellphish**, DARPA AI Cyber Challenge	
2023	**11th rank globally with team Shellphish**, DEFCON CTF Finals	*Las Vegas, USA*
2022	**13th rank globally with team Shellphish**, DEFCON CTF Finals	*Las Vegas, USA*
2021	**10th rank globally with team Shellphish**, HITB Pro CTF	*Abu Dhabi, UAE*
2020	**7th rank globally with team Shellphish**, DEFCON CTF Finals	*Las Vegas, USA*
2019	**11th rank globally with team Pwndevils**, Dragon CTF	*Warsaw, Poland*
2019	**First runners up with team Pwndevils**, CSAW Embedded Security Challenge	*New York, USA*
2016	**First runners up with team bi0s**, CSAW CTF 2016 (India)	*Uttar Pradesh, India*