Zion Leonahenahe Basque

zionbasque.com
zionbasque@asu.edu
LinkedIn: zion-basque
GitHub: mahaloz
Tempe, Arizona

Education

Arizona State University — Tempe, AZ
Ph.D. in Computer Science, Security (expected), GPA: 4.00 — Fall 2021–Spring 2025

Arizona State University — Tempe, AZ
B.S. in Computer Science, GPA: 4.00 — Fall 2017–Fall 2020

- Capstone: "Semantic Fuzzing of Autonomous Systems"

Experience

Arizona State University, SEFCOM Lab — Tempe, AZ
Senior Cybersecurity Research Assistant — 2017–Pres.

- Advisers: Dr. Ruoyu "Fish" Wang, Dr. Yan Shoshitaishvili
- Research Topics: Binary Analysis/Exploitation, Fuzzing, CFG Recovery, Decompilation
- Worked as project lead; Independent work; Technical Reading/Writing

ForAllSecure — Palo Alto, CA
Fuzzing Research Intern — Summer 2019

- Worked in a team of two; Vulnerability discovery on open-source projects
- Lead development on Fuzzer seed sharing system (2k LoC Python)
- Development on the Mayhem Fuzzing System; Continuous Fuzzing

Arizona State University, Fulton Schools — Tempe, AZ
Fulton Undergraduate Researcher — Fall 2018, Fall 2020

- Machine Learning Applied to Fuzzing Mutation Strategies
- Advanced CFG Recovery of Binaries

Vulnerability Discovery

- **CVE-2019-10028: Netflix DIAL Server**
  - Publicized on Axios; Discovered at ForAllSecure
- **CVE-2019-13103, CVE-2019-13104, CVE-2019-13105, CVE-2019-13106: Das-Uboot**
  - Publicized on Threat Post; Discovered at ForAllSecure
  - RCE in largely used bootloader code

Projects

- **Open-source Reverse Engineering Tools**
  - angr: Symbolic Execution Engine; Dev; Python & C; *5.6k GitHub Stars*
  - Decomp2GEF: GDB-Decompiler Interaction Server; Lead dev; Python; *137 GitHub Stars*

  - phuzzer: Fuzzing Management System; Dev; Python; *125 GitHub Stars*
  - BinSync: Cross-Disassembler Collaboration Tool; Lead dev; Pytohn; Grant: DARPA Award F8750-19-C-0003

- **Academic Systems Security Research**
  - FlakJack: Finding Occluded Vulnerabilities with Exploit Patching and Fuzzing; Co-author; In-Submission
  - SPARTACUS: Proactively Protecting Users From Phishing by Triggering Cloaking; Co-author; In-Submission
  - Ali'i CFG: Resolving Indirect Jumps in Binary CFG Recovery; First Author; Writing

Extracurricular Activities

Shellphish CTF Team

Co-captain 2018–Pres.

- Co-captain since 2020; Managed team of 20-40 hackers in competitions
- Organized weekly meetings; Maintained team's global ranking and U.S. ranking (3rd)
- Captained two DEF CON CTF Finals, competed in three total
- Competed in over *124* 48-hour CTFs since 2018; Specialized in Binary Exploitation
- Organized yearly team CTF "iCTF", played by 200+ teams each year

ASU Hacking Club

Lecturer 2017–2021

- Taught program exploitation techniques; Lectured to 700+ students since joining
- Helped develop pwn.college, a free, online, learning platform for systems exploitation
- Created online ctf-based education resources used by thousands of students
- Hosted 2018 DEF CON Finals CTF with the Order of the Overflow

Scholarships and Awards

Computing Research Association Undergrad Research Award (Honorable Mention)	2021
ASU Graduate Impact Award	2020
ASU FURI Distinguished Researcher	2020
Center for Cyber Safety and Education Scholarship	2020–Pres.
THINK STEM Scholarship Fund	2018–Pres.
ASU New American Deans Award	2017–Pres.

Skills

- **Disassemblers:** Modern Decompiler Design, IDA Pro, Binary Ninja
- **Programming:** Python, C, CI Design
- **Reverse Engineering:** GDB, angr (Symbolic Execution), Program Tracing, Containerization
- **Program Exploitation:** Modern Heap Attacks, Kernel Exploitation, Stack-based exploitation
- **Vulnerability Discovery:** Fuzzing, Static Analysis
- **Soft Skills:** Leadership, Focus, Empathy