

ADRIAN HERRERA

Experience

Interrupt Labs Canberra, Australia
Principal Vulnerability Researcher *Feb. 2023 – Present*

- Develop tools (fuzzers, emulators, static analyzers) for vulnerability research and exploit development
- Software reverse engineering and auditing

Australian National University (ANU) Canberra, Australia
Adjunct Lecturer *Feb. 2020 – Present*

- “Software Security” lecturer, teaching automated vulnerability discovery

Defence Science and Technology Group (DSTG) Canberra, Australia
Technical Team Lead *Feb. 2021 – Feb. 2023*

- Led a team of computer scientists and security researchers undertaking cyber security R&D for the Australian Defence Organisation
- Build and manage relationships with operational clients, international partners, and academia

DSTG Canberra, Australia
Senior Software Security Researcher *Aug. 2017 – Feb. 2021*

- Research on automated vulnerability discovery (fuzzing, program analysis)

École polytechnique fédérale de Lausanne (EPFL) Lausanne, Switzerland
Research Engineer (Dependable Systems Lab) *Jul. 2016 – Aug. 2017*

- Develop the S²E binary analysis platform

Australian Cyber Security Centre (ACSC) Canberra, ACT
Malware Analyst and Researcher *Feb. 2015 – Jul. 2016*

- Reverse engineering, software development, and research for malware analysis

DSTG Adelaide, SA / Canberra, ACT
Software Security Researcher *Jan. 2012 – Jul. 2016*

- Research, develop, and deploy malware detection and analysis capabilities for the ACSC

Commonwealth Scientific and Industrial Research Organisation (CSIRO) Brisbane, QLD
Summer Intern and Honours Student *Nov. 2010 – Nov. 2011*

- Research on wireless sensor network security

Education

ANU Canberra, ACT
PhD (Computer Science) *Mar. 2019 – Dec. 2023*

- Dissertation: “State Space Search in Fuzzing”

University of Wollongong (UOW) Wollongong, NSW
Bachelor of Engineering (Computer) (Honours I) *Mar. 2006 – Nov. 2011*

Awards

- DSTG Achievement Award, Science Communication, 2020
- ANU Remote Teaching and Student Experience Award, COMP2710 Software Security, 2020
- DSTG Certificate of Recognition, ISSISP organisation, 2018

- DSTG Certificate of Recognition, University outreach, 2018

Publications

- S. Luo, **A. Herrera**, P. Quirk, M. Chase, D. Ranasinghe, S. Kanhere, “Make out like a (Multi-Armed) Bandit: Improving the Odds of Fuzzer Seed Scheduling with T-SCHEDULER”, *ACM Asia Computer and Communications Security (AsiaCCS)*, 2024
- **A. Herrera**, M. Payer, A. Hosking, “DATAFLOW: Toward a Data-Flow-Guided Fuzzer”, *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2023
- Z. Jiang, S. Gan, **A. Herrera**, F. Toffalini, L. Romerio, C. Tang, M. Egele, C. Zhang, M. Payer, “EVOCATIO: Conjuring Bugs from a Single PoC”, *ACM Computer and Communications Security (CCS)*, 2022
- **A. Herrera**, M. Payer, A. Hosking, “Registered Report: DATAFLOW – Towards a Data-Flow-Guided Fuzzer”, *Fuzzing Workshop (FUZZING)*, 2022
- **A. Herrera**, H. Gunadi, S. Magrath, M. Norrish, M. Payer, A. Hosking, “Seed Selection for Successful Fuzzing”, *ACM International Symposium on Software Testing and Analysis (ISSTA)*, 2021
- A. Hazimeh, **A. Herrera**, M. Payer, “Magma: A Ground-Truth Fuzzing Benchmark”, *ACM SIGMETRICS*, 2021
- **A. Herrera**, “Optimizing Away JavaScript Obfuscation”, *IEEE Source Code Analysis and Manipulation (SCAM)*, 2020
- **A. Herrera**, H. Gunadi, L. Hayes, S. Magrath, F. Friedlander, M. Sebastian, M. Norrish, A. Hosking, “Corpus Distillation for Effective Fuzzing: A Comparative Evaluation”, *arXiv:1905.13055*, 2019
- B. Zhang, C. Feng, A. Herrera, V. Chipounov, G. Candea, “Discover Deeper Bugs with Dynamic Symbolic Execution and Coverage-based Fuzz Testing”, *IET Software*, 2018
- **A. Herrera**, “Automated Analysis of Flash Malware”, *DST Group Report DST-Group-TN-1511*, 2016
- **A. Herrera**, B. Cheney, “JMD: A Hybrid Approach for Detecting Java Malware”, *Australasian Information Security Conference (AISC)*, 2015 (**BEST PAPER AWARD**)
- **A. Herrera**, “How Secure is the Next-Generation Internet? An Examination of IPv6”, *DSTO Report DSTO-GD-0767*, 2013
- **A. Herrera**, W. Hu, “A Key Distribution Protocol for Wireless Sensor Networks”, *IEEE Local Computer Networks (LCN)*, 2012

Talks

- “The Hitchhiker’s Guide to Fuzzer Coverage Metrics”, *Australasian Software Engineering Summer School(ASESS)*, Jan. 2024
- “Code Analysis with Databases”, *CSides Canberra*, Apr. 2023
- “Hot Fuzz: We’ve got grey, or... white[-box fuzzers]”, *Australian Reverse Engineering and Vulnerability Research (AUREVR)*, Jun. 2022
- “Seed Selection for Successful Fuzzing”, *CSIRO’s Data61 & DST Cyber Security Summer School (CSSS)*, Feb. 2022
- “Analyzing Trigger-Based Malware with S²E”, *Malware Reverse Engineering (MRE)*, Jul. 2019
- “Deobfuscating JavaScript Malware”, *BSides Canberra*, Mar. 2019 (**BEST SPEAKER AWARD**)
- “Optimizing Away JavaScript Obfuscation”, *CSides Canberra*, Jul. 2018
- “Program Analysis for Reverse Engineers: from \top to \perp ”, *BSides Canberra*, Mar. 2018

Service

- Artifact evaluation committee, *Workshop on Offensive Technologies (WOOT)*, 2023

- Technical reviewer, *Exploring and fuzzing IoTs Firmware with Qemu* book, 2022
- Artifact evaluation committee, *Fuzzing Workshop (FUZZING)*, 2022
- Organizing committee, *CSIRO's Data61 & DSTG Cyber Security Summer School (CSSS)*, 2022
- Organizing committee, *International Summer School on Information Security and Protection (ISSISP)*, 2018