

ADRIAN HERRERA

EXPERIENCE

Defence Science and Technology Group (DSTG)

Technical Team Lead

Canberra, Australia

Feb. 2021 – Present

- Lead a team of computer science and software security professionals undertaking software security research and development for clients across the Department of Defence
- Build relationships with operational clients, international partners, and academia to shape the team's research

DSTG

Senior Software Security Researcher

Canberra, Australia

Aug. 2017 – Feb. 2021

- Research on automated binary analysis and fuzzing for vulnerability discovery
- Develop and teach "Software Security" undergraduate subject at the Australian National University

École polytechnique fédérale de Lausanne (EPFL)

Research Engineer (Dependable Systems Lab)

Lausanne, Switzerland

Jul. 2016 – Aug. 2017

- Develop the S²E binary analysis platform
- Supervision of undergraduate student projects

Australian Cyber Security Centre (ACSC)

Malware Analyst and Researcher

Canberra, ACT

Feb. 2015 – Jul. 2016

- Secondment to the malware analysis team
- Reverse engineering, software development, and research activities for malware analysis

DSTG

Software Security Researcher

Adelaide, SA / Canberra, ACT

Jan. 2012 – Jul. 2016

- Researching, developing, and deploying new malware detection and analysis capabilities for clients
- Supervision of undergraduate summer vacation student projects

Commonwealth Scientific and Industrial

Research Organisation (CSIRO)

Summer Intern and Thesis Student

Brisbane, QLD

Nov. 2010 – Nov. 2011

- Research project on "Supporting Sensor Network Security with Trusted Platform Modules (TPM)"
- Sponsorship of undergraduate thesis project

EDUCATION

Australian National University (ANU)

PhD (Computer Science)

Canberra, ACT

Mar. 2019 – Present

- Dissertation: "State Space Search in Fuzzing" (expected submission Apr. 2023)

University of Wollongong (UOW)

Bachelor of Engineering (Computer) (Honours I)

Wollongong, NSW

Mar. 2006 – Nov. 2011

- 3.72/4 Grade Point Average (GPA)
- Honours project: "A Key Distribution Protocol for Wireless Sensor Networks"

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

- **A. Herrera**, M. Payer, A. Hosking, “DATAFlow: Toward a Data-Flow-Guided Fuzzer”, *ACM Transactions on Software Engineering and Methodology (TOSEM)*, Jan. 2023
- Z. Jiang, S. Gan, **A. Herrera**, F. Toffalini, L. Romero, C. Tang, M. Egele, C. Zhang, M. Payer, “EVOCATIO: Conjuring Bugs from a Single PoC”, *ACM Computer and Communications Security (CCS)*, Nov. 2022
- **A. Herrera**, M. Payer, A. Hosking, “Registered Report: DATAFlow – Towards a Data-Flow-Guided Fuzzer”, *Fuzzing Workshop (FUZZING)*, Apr. 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)*, Jul. 2021
- A. Hazimeh, **A. Herrera**, M. Payer, “Magma: A Ground-Truth Fuzzing Benchmark”, *ACM SIGMETRICS*, Jun. 2021
- **A. Herrera**, “Optimizing Away JavaScript Obfuscation”, *IEEE Source Code Analysis and Manipulation (SCAM)*, Sep. 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*, May 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*, May 2018
- **A. Herrera**, “Automated Analysis of Flash Malware”, *DST Group Report DST-Group-TN-1511*, Jul. 2016
- **A. Herrera**, B. Cheney, “JMD: A Hybrid Approach for Detecting Java Malware”, *Australasian Information Security Conference (AISC)*, Jan. 2015. **BEST PAPER AWARD**
- **A. Herrera**, “How Secure is the Next-Generation Internet? An Examination of IPv6”, *DSTO Report DSTO-GD-0767*, Oct. 2013
- **A. Herrera**, W. Hu, “A Key Distribution Protocol for Wireless Sensor Networks”, *IEEE Local Computer Networks (LCN)*, Oct. 2012

TALKS

- “Hot Fuzz: ‘We’ve got grey, or... white[-box fuzzers]”, Australian Reverse Engineering and Vulnerability Research (AUREVR) Conference, 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