Jose Antonio Zamudio Amaya

Controllable Automated Testing for Security-Critical Software

joszamama@gmail.com · linkedin.com/in/joszamama · jzamudio.com · github.com/joszamama · Google Scholar

SUMMARY

Ph.D. candidate at CISPA Helmholtz Center for Information Security, developing controllable automated testing for security-critical software under Prof. Andreas Zeller. Creator of Fandango, a language-based fuzzer that has found vulnerabilities in heavily tested targets, adopted by Bosch and Volkswagen, and downloaded over 100,000 times on PyPI. Author of 6 peer-reviewed publications with 8 papers under review, all at top venues.

EXPERIENCE

CISPA Helmholtz Center for Information Security
Oct 2023 - Oct 2027

Doctoral Researcher · Saarbrucken, Germany

- 2.5 years into PhD research on controllable automated testing under Prof. Andreas Zeller. Author and lead developer of Fandango, which has found vulnerabilities in security-critical software. Extended it to stateful protocol testing, feature-focused generation, and LLM-based constraint extraction.

Max Planck Institute for Security and Privacy (MPI-SP)
Sep - Nov 2025

Internship · Bochum, Germany

- Visited Dr. Marcel Böhme's group to investigate statistical methods and theoretical foundations for improving precision and efficiency of coverage-guided fuzzing.

Universidad Pablo de Olavide
Feb - Oct 2023

Student Researcher · Seville, Spain

- Designed metaheuristic optimization algorithms for NP-hard combinatorial problems under Prof. Alfredo Garcia Hernandez-Diaz.

Universidad de Sevilla
Jan 2022 - Oct 2023

Student Researcher · Seville, Spain

- Researched software product line optimization under Prof. David Benavides Cuevas. Developed WebSPL and XatKitSPL, awarded both Bachelor's Thesis and Master's thesis Honors Distinctions.

EDUCATION

Universitat des Saarlandes · Ph.D. in Computer Science (Systems Security) — Oct 2023 - Oct 2027

National University of Singapore · Fuzzing and Software Security Summer School 2024 — May - Jun 2024

Universita degli Studi di Bergamo · TAROT 2024 Summer School on Software Testing, Verification & Validation — Jul 2024

Universidad de Sevilla · M.Sc. Software Engineering: Big Data, ML, Data Science & AI. Honors Distinction. — 2022 - 2023

Universidad de Sevilla · B.Sc. Software Engineering. Honors Distinction. — 2018 - 2022

ACCEPTED PUBLICATIONS

[2025] **J.A. Zamudio Amaya**, M. Smytzek, A. Zeller. *Fandango: Evolving Language-Based Testing.* Proceedings of the ACM on Software Engineering (ISSTA), 2025.

[2025] P. Kalbitzer, **J.A. Zamudio Amaya**, A. Zeller. *XAVIER: Grammar-Based Testing for XML Injection Attacks.* ISSTA 2025.

[2025] S. Neuhaus, **J.A. Zamudio Amaya**, A. Zeller. *Personalized Fuzzing: A Case Study with Fandango on a GNSS Module.* ISSTA 2025.

[2024] **J.A. Zamudio Amaya**. *Shaping Test Inputs in Grammar-Based Fuzzing.* ISSTA 2024.

[2024] E. Barrena, S. Bermudo, A.G. Hernandez-Diaz, A.D. Lopez-Sanchez et al., **J.A. Zamudio Amaya**. *Finding the Minimum k-Weighted Dominating Sets Using Heuristic Algorithms.* Mathematics and Computers in Simulation, 2024. (Author order alphabetical.)

[2023] S. Lubos, A. Felfernig, V.M. Le, T.N.T. Tran, D. Benavides, **J.A. Zamudio** et al. *Analysis Operations on the Run: Feature Model Analysis in Constraint-Based Recommender Systems.* SPLC 2023.

PROJECTS

Fandango
Aug 2024 - Present

Lead Developer · github.com/fandango-fuzzer/fandango

- Open-source language-based fuzzer combining formal grammars with Python constraints to generate semantically valid test inputs via evolutionary search.
- Supports black-box fuzzing, input mutation, and stateful protocol testing (FTP, DNS). Published at ISSTA 2025. 100+ GitHub stars. 100k+ downloads on PyPI.

Compás
Feb 2026 - Present

Lead Developer · Feature-focused test generation

- Grammar-based test generator guided by feature models, enabling targeted testing of specific software configurations and feature interactions.
- Combines software product line variability with Fandango's constraint-driven fuzzing to generate feature-focused test suites. Submitted to ASE 2026.

TALKS & PRESENTATIONS

[2026] *How to Test Complex Systems Automatically and Systematically.* Tutorial at FSE 2026, Montreal, Canada.

[2025] *Fandango: Evolving Language-Based Testing.* ISSTA 2025, Trondheim, Norway.

[2025] *XAVIER: Grammar-Based Testing for XML Injection Attacks.* ISSTA 2025, Trondheim, Norway.

[2025] *Personalized Fuzzing: A Case Study with Fandango on a GNSS Module.* ISSTA 2025, Trondheim, Norway.

SERVICE

Website Chair
2026

International Workshop on Search-Based and Fuzz Testing (SBFT 2026)

Reviewer
2024

Journal of Systems and Software · Elsevier · ISSN: 0164-1212

TEACHING

Universitat des Saarlandes
Oct 2023 - Feb 2024

Teaching Assistant, Security Testing (Advanced Course) · Saarbrucken, Germany

- Assisted in the advanced Security Testing course, designing exercises, projects, and exams for a cohort of 207 students.
- Covered topics including fuzzing, static analysis, and vulnerability discovery, bridging academic research with practical lab work.

Fuzzing with Fandango
2025 - 2026

Tutorial and Reference · Co-authored with M. Smytzek, A. Liggesmeyer, V. Huber, A. Zeller

- Co-author of a 300-page tutorial and reference guide on language-based fuzzing with Fandango.

Thesis Supervision
2024 - 2026

Advisor · CISPA Helmholtz Center for Information Security

- T. Scheckenbach (M.Sc.) — SSL/X.509 certificate fuzzing. Now Ph.D. student at CISPA.
- P. Kalbitzer (M.Sc.) — XML injection testing (XAVIER, published at ISSTA 2025). Now at InputLab.
- T. Speicher (M.Sc.) — JSON injection fuzzing. Now Cyber Security Consultant at REGLER CONNECT.
- N. Khalatiani (B.Sc.) — Property-based testing. Now in Elite Master's in Software Engineering.

SKILLS

Techniques	Grammar-based fuzzing, language-based testing, black-box and white-box fuzzing, coverage-guided fuzzing, evolutionary search, constraint solving, protocol testing, feature modeling
Domains	SSL/TLS certificates, network protocols (DNS, FTP), GNSS navigation, web APIs, XML/JSON processors, cryptographic libraries, compiler inputs, software product lines, LLM outputs
Programming	Python (expert), Rust, Java (proficient), C/C++, JavaScript
Tools	Fandango, AFL++, LLVM, libFuzzer, OSS-Fuzz, Wireshark, Z3, Git, Docker, Linux
Languages	Spanish (native), English (C2 full professional proficiency)

HONORS & AWARDS

Jul 2023	Master's Thesis Honors Distinction - Universidad de Sevilla. Selected to present at SISTEDES 2023.
Jun 2022	Bachelor's Thesis Honors Distinction - Universidad de Sevilla. Selected to present at SISTEDES 2022.

COLLABORATIONS

Max Planck Institute for Security and Privacy, IMDEA Software Institute, University of Sevilla, University of Graz, University of Passau, Universidad Pablo de Olavide, and Luxembourg Institute of Science and Technology (LIST).

INTERESTS

I believe publicly funded research should produce publicly available tools and data. Every artifact I build is open source, every experiment I run is designed to be reproducible, and every dataset I collect is published alongside the paper. Beyond my own work, I actively pursue industry transfer: collaborations with Bosch and Volkswagen showed me that academic tools can have real impact when they are built to be used, not just to be cited. I seek out collaborators across institutions and disciplines because the best ideas come from the intersection of different perspectives. Science should be open, reproducible, and built to last.