Arturo Villacañas : Curriculum Vitae

me@arturovillacanas.com

last updated: May 2024

WORK EXPERIENCE

Research Experience

For those who may not be familiar with the security or the machine learning scene:

"sec-ranking": author's position in the global ranking for security authors (2023)
"⋆": affiliation's global position in csrankings.org, machine learning (2023)
"†": affiliation's global position in csrankings.org, security (2023)

University of Cambridge Mar 2024 - ongoing
Research Intern — On-site (United Kingdom) (⋆45) Age: 23 years old
Supervisors: Ekdeep Singh Lubana, Usman Anwar, Prof. David Krueger
Study of safety training in VLMs (TBP)

CISPA Helmholtz Center for Information Security Jul 2023 - Dec 2023
Research Intern — On-site (Germany) (†1, ⋆76) Age: 22 years old
Supervisors: Prof. Thorsten Holz (sec-ranking: 7), Prof. Lea Schönherr
Study of what makes for safe multi-agent interactions in LLM systems (TBP)

IMDEA Software Institute Sep 2021 - Dec 2022
Research Intern — On-site (Spain) (†32) Age: 20 - 21 years old
Supervisor: Prof. Juan Caballero (sec-ranking: 81)
Study of data selection and annotation of APT-related tokens in large text corpus for their use as actionable intelligence for cyberattack authorship attribution

Industry Experience

Innotec Security 2019
Security Engineer — On-site (Spain) Age: 18 years old
R&D engineer. Improved the accuracy of detection systems by at least 150%, enhancing REYES (CCN-CERT) correlation rules by clustering different sources of forensic data (Sysmon, Zeek, pcaps) coming from the systems that were being monitored. Implemented a distributed ETL (Kafka, Hadoop) that handles over 1M daily logs

CCN-CERT 2017
Security Engineer — On-site (Spain) Age: 16 years old
Deployment of world-class infrastructure to secure classified systems. All my activities in this role are protected under a military Non-Disclosure Agreement (NDA)

EDUCATION

Graduate Education

(Currently applying to programs for 2024-2026)

Undergraduate Education

Universidad Politécnica de Madrid (UPM), Spain 2019 - 2024
- BSc in Computer Science
- BSc in Business Management and Administration
360 ETCS (65 courses). Solid background in: Mathematics (12 courses), Systems (11), Programming (9), Quantitative Economics (20), Policy Analysis (12)

PUBLICATIONS

Peer-Reviewed

∗ stands for equal contribution

The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction Tools
Future Generation Computer Systems, v. 144 — Published in 2023
Juan Caballero*, Gibran Gomez*, Srdjan Matic*, Gustavo Sánchez*, Silvia Sebastián*, and **Arturo Villacañas***
https://arxiv.org/abs/2208.00042

FATR: a Framework for Automated Analysis of Threat Reports
JNIC 2022
Juan Caballero*, Gibran Gomez*, Srdjan Matic*, Gustavo Sánchez*, Silvia Sebastián*, and **Arturo Villacañas***
https://dialnet.unirioja.es/servlet/articulo?codigo=9206603

SELECTED AWARDS

Grant and Scholarship Awards

Travel Grant for IEEE SaTML 2024, Toronto: $2,500 **2024**
Financial award to help fund attendance of IEEE SaTML conference

QueerinAI's Grad App Aid for LGBTQ+ ML scholars: $850 **2023**
Financial aid and feedback from senior scientists on applying to graduate programs

European Lighthouse on Secure and Safe AI Travel Grant: 500€ **2022**
Financial award to help fund attendance of CISPA Summer School 2022

Academic Excellence Scholarship: 800€ **2020**
For performance in first year of undergraduate studies

Global Honours in Baccalaurate: 2,200€ **2019**
The regional government of Madrid subsidized my first year of college

Awards for Papers and Competitions

Best Work in Progress, JNIC'22 **2022**
Award for our extended abstract in JNIC'22

ACADEMIC SERVICE

Security

Context: Security currently unfolds in four tier-1 venues: IEEE S&P (acceptance rate in 2022: 14.52%), USENIX Security (18%), CCS (22.4%), and NDSS (16.2%). Reviewing is limited to PC members, and being a PC member is considered a proxy for prestige among Faculty members. PhD students may either act as external reviewers on behalf of a known supervisor or apply to the Artifact Evaluation PC

Artifact Evaluation PC: USENIX Security (2024)

COURSES

KU Leuven Summer School in AI Security & Privacy **2023**
Five-day program centered on AML, problem-space attacks, privacy in deep learning (DP), and the exploration of diverse failure modes (e.g., adversarial malware samples) in ML-based platforms within the domain of cybersecurity

CISPA Summer School in System Security **2023**
Five-day program co-hosted with Intel Research centered on bringing together the state of the art in exploit development and offensive security, with each day focused on one domain: system security (fuzzing, instrumentation), trusted computing (TEEs), microarchitectures,

embedded/drone/space security, and cyber-physical systems

CISPA Summer School in Trustworthy ML **2022**
Five-day program focused on mathematics for privacy (DP), fairness, and causality, featuring tutorials on how to analyze algorithms in these domains and their trade-offs. It also included tutorials on conducting research to audit real-world systems (Alexa, self-driving cars), as well as on the privacy of genomic data

LANGUAGES

English: CEFR level: C1, certified by Cambridge English (overall score: 196/210).
Spanish: Native.

TECHNICAL PROGRESS

Programming Languages

Expert: Python (including effortless use of asyncio, functools, dataclasses, metaclasses, memoryviews, optimization via integration of C/C++ code; packages like numpy, sympy, pandas, scikit), C
Strong: C++, Rust (as a proxy: reading the Rustonomicon), Java
Small familiarity: Matlab, Fortran, Scala, VHDL (FPGA), R, Javascript

Machine Learning Frameworks

Average: PyTorch, CUDA (PyCUDA, CUDA C++)
Small familiarity: JAX, Gym

Data Architectures

Strong: Hadoop, HDFS, Kafka, Airflow, Spark, Mongo, SQL Server
Small familiarity: Logstash, Dagster, GraphQL