

Andrés Sánchez Marín

andres.sanchez@epfl.ch andsanmar.github.io

PROFESSIONAL EXPERIENCE

HEXHIVE GROUP, EPFL	Lausanne, Switzerland
PhD Student/Research Assistant	Sep 2019 – present
Compartmentalization techniques evaluation. Automating the detection of Speculative ROP chains. Software analysis of side-channel attacks exploitation	
IBM RESEARCH	Zürich, Switzerland
Research Assistant	Jun 2020 – Sep 2020
Taxonomy of kernel code reuse attacks, KASLR bypasses and mitigations in software and architectural level	
MASSACHUSETTS INSTITUTE OF TECHNOLOGY	Cambridge, United States
Visiting Researcher	Jun 2019 – Aug 2019
Security analysis of compressed cache architectures, demonstration of first data at rest microarchitectural leak	
IMDEA SOFTWARE INSTITUTE	Madrid, Spain
Research Intern	Sep 2018 – Jun 2019
Reasoning about speculative execution attacks and existing proposals for countermeasures. Automating the detection of speculative information flows in large code-bases	
DISTRIBUTED SYSTEMS LABORATORY, UPM	Madrid, Spain
Research Intern	Sep 2017 – Dec 2017
Integrating an Elastic Complex Event Processing for Static and Streaming Data and a NoSQL distributed database	

EDUCATION

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE	Lausanne, Switzerland
PhD in Computer Science	2021 – present
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE	Lausanne, Switzerland
Master of Science in Computer Science	2019 – 2021
MSc Thesis: Characterization of the overheads for comprehensive compartmentalization of software	
UNIVERSIDAD POLITÉCNICA DE MADRID	Madrid, Spain
Bachelor of Science in Mathematics and Computing	2015 – 2019
Obtained honors in 10 courses. Member of ACM UPM chapter	
Final Degree Project: Detecting speculative information flows on large code-bases	

AREAS OF INTEREST

My main research interest is the development of reliable and optimized software systems, focusing on systems security. Concerning the complete and correct system's specification, and in case of a leaky implementation, to detect how software is able to exploit it, detect the code patterns that perform the exploit and, aim to be secure by circumventing the flaws while keeping its efficiency. All the next topics are of my interest:

Computer Systems	Security	Privacy
Programming Languages & Paradigms	Software Optimizations & Synthesis	Compilers
Algorithms and Data Structures	Hardware Architecture	Operating Systems
Formal Verification	Theoretical Foundations of Computer Science	Quantum computing

HONORS & AWARDS	IEEE Micro Top Picks Award, 2021 MSc Research Scholar, EPFL, 2019 — 2021
LANGUAGES	Spanish (mother tongue), English (fluent) – 90 TOEFL iBT, French (basic)
PROGRAMMING	C, Rust, Prolog, Haskell, C++, Assembly, \LaTeX , Python, Scala, Lisp, Linux, Git, LLVM
CERTIFICATIONS	CCNA 1 & 2, Free Time Monitor Certification
NBA NETACAD DREAM TEAM	In the NBA Global Games (2016, Madrid). Working with Cisco and NBA team on the network infrastructure for the event and helping on its installation.
VOLUNTEER EXPERIENCE	CIRCA-MAS's Sumac Wasi enhancement project during 2018 summer; recreational and learning activities for a 40 kids group of a marginal Arequipa neighbourhood.

PROCEEDINGS PUBLICATIONS

- [1] M. Guarnieri, B. Koepf, J. F. Morales, J. Reineke, and A. Sánchez, "SPECTECTOR: Principled detection of speculative information flows," in *Proceedings of the 41st IEEE Symposium on Security and Privacy*, IEEE, 2020.
- [2] P.-A. Tsai, A. Sanchez, C. Fletcher, and D. Sanchez, "Safecracker: Leaking secrets through compressed caches," in *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS '20*, ACM, 2020.
- [3] A. Bhattacharyya, A. Sánchez, E. M. Koruyeh, N. Abu-Ghazaleh, C. Song, and M. Payer, "Specrop: Speculative exploitation of ROP chains," in *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, (San Sebastian), pp. 1–16, USENIX Association, Oct. 2020.