PIETRO BORRELLO

Systems-Security Ph.D. Student

linkedin.com/in/pietro-borrello
github.com/pietroborrello
twitter.com/borrello_pietro
+39 340 998 1143
pietro.borrello95@gmail.com

EDUCATION

Ph.D. in Engineering in Computer Science - *Sapienza University of Rome* 2019 – exp. Dec 2022
Master's Degree in Engineering in Computer Science - 110 cum Laude. GPA 30/30 2019
Bachelor's Degree in Engineering in Computer Science - 110 cum Laude. GPA 29.95/30 2017

TECHNICAL SKILLS

Proficient: C, C++, Python, x86-64 & ARM asm, LLVM, Kernel dev, Java, Javascript, SQL, docker, qemu
Familiar: Rust, Go, AVR asm, Scala, Ruby, OCaml, Win32 programming, IDA & ghidra scripting

EXPERIENCE

DEFCON CTF 26, 27, 28, 29/ *Las Vegas, USA* Aug 2018 – 2021

As a member of the team **mhackeroni**, which I cofounded, I participated 4 times in **DEFCON CTF**.

VISITING Ph.D. STUDENT at TU GRAZ – CoreSec group/ *Graz, Austria* Oct – Dec 2021

Lead project on reverse engineering + exploitation of the Intel Microcode via undocumented instructions. Held lecture on *Advanced Linux Kernel Exploitation* at the University at the end of my visiting period.

HONORS PROGRAM / *Sapienza University of Rome* 2015 – 2019

Enrolled in the **Honors Program** of my department working on automating exploitation techniques.

RELEVANT PROJECTS

Fuzzing: *(c++, llvm, docker)*

- **Predictive Context Fuzzing:** LLVM passes to enhance AFL++ fuzzer for collision-free context sensitivity.

Side-Channels: *(c, c++, python, llvm, pyshark)*

- **Constantine:** an LLVM compilation framework to automatically protect against side channels attacks.
- **Memory Compression Fuzzer:** a genetic fuzzer to automatically analyze compression algorithms for side-channels that found remotely exploitable vulnerabilities in Postgres, Memcached and Linux Kernel.

Microarchitectural Attacks: *(c, assembly, javascript, wasm, v8)*

- **Spectre, Meltdown & RIDL:** I provided open-source PoCs of attacks such as Spectre, Meltdown & RIDL.
- **Spectre Mitigations:** new attacks and defenses for Spectre vulnerabilities in the Cloudflare Workers. Cloudflare integrated our *Dynamic Process Isolation* in its production system.

CPU Introspection: *(c, assembly, ghidra, sleigh)*

- **CPU monitor:** a system to sniff data in flight in the CPU to observe speculative execution taking place.
- **Intel Atom Microcode Decompiler:** a Ghidra processor module to reverse engineer Intel microcode.

Code Reuse Techniques: *(c, ptrace, python, angr, javascript, html, css, d3.js)*

- **raindrop:** a binary obfuscator that transforms program functions into obfuscated ropchains.
- **RopMate:** the first Visual Analytics system specifically designed to assist humans in crafting ropchains.
- **RopGun:** transparent ROP mitigation based on anomaly detection on hardware performance counters.

LEADERSHIP AND COMMUNICATION SKILLS

Cybersecurity Tutor – CyberChallenge.IT / *Sapienza University of Rome* 2018 – 2021
Low-Level Systems Teaching Assistant / *Sapienza University of Rome* 2019 – 2021
Co-Founder of Roman DEFCON group / *Rome, Italy* 2018 – Today
Co-Founder of mhackeroni and TheRomanXpl0it CTF teams / *Italy* 2017 – Today
European CyberChallenge 3rd classified / *ENISA - Malaga, Spain* October 2017

SCIENTIFIC CONTRIBUTIONS

Predictive Context-sensitive Fuzzing
P. Borrello, A. Fioraldi, D.C. D'Elia, D. Balzarotti, L. Querzoni, C. Giuffrida. (Under Review)

Practical Timing Side Channel Attacks on Memory Compression
M. Schwarzl, **P. Borrello**, G Saileshwar, H. Mueller, D. Gruss, M. Schwarz. (Under Review)

Robust and Scalable Process Isolation against Spectre in the Cloud
M. Schwarzl, **P. Borrello**, A. Kogler, T. Schuster, K. Varda, D. Gruss, M. Schwarz. (Under Review)

Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization
P. Borrello, D.C. D'Elia, L. Querzoni, C. Giuffrida. ACM CCS 2021

Hiding in the Particles: When Return-Oriented Programming Meets Program Obfuscation
P. Borrello, E. Coppa, D.C. D'Elia. IEEE DSN 2021

The Rop Needle: Hiding Trigger-Based Injection Vectors via Code Reuse
P. Borrello, E. Coppa, D.C. D'Elia, C. Demetrescu. ACM SAC 2019

Boosting Virtualization Obfuscation with Return Oriented Programming
P. Borrello, E. Coppa, D.C. D'Elia, C. Demetrescu. Poster @ ACSAC 2018

Ropmate: Visually Assisting the Creation of ROP-Based Exploits
M. Angelini, G. Blasilli, **P. Borrello**, E. Coppa, D.C. D'Elia, S. Ferracci, S. Lenti, G. Santucci.
Best paper Award @ IEEE VizSec 2018

I authorize the use of my personal data in compliance with GDPR (EU) 2016/679 of April 27,2016.