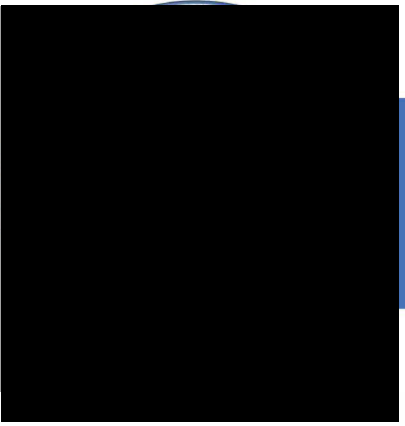

PIETRO BORRELLO

COMPUTER SCIENCE ENGINEER

INTERESTS

I'm an enthusiast for Binary Exploitation, Malware Analysis, Microarchitectural Attacks, Ethical Hacking, Secure Coding, Vulnerability Assessment and Penetration Testing.

SOFTWARE SKILLS

Fluent in C (Unix and Win32), Linux Kernel Programming, C++, Assembly x86-64, Python, Java, Scala, Ruby, OCaml, SQL, AMPL, HTML, CSS, JavaScript, ERB, JSON, Git, LaTeX.

CURRENT POSITION

I'm a first year Ph.D. student in Engineering in Computer Science at Sapienza University of Rome.

github.com/pietroborrello

EXPERIENCE

DEFCON CTF 26, 27 • LAS VEGAS, USA • AUGUST 2018, AUGUST 2019
As a member of the Italian team mHACKeroni, I went to Las Vegas for two years to participate to the most important hacking competition in the world: DEFCON CTF 26 and 27. This is the first time Italy qualifies since 2008, and the best obtained result ever. We gained 7th place among the strongest teams in the world in 26th, and 5th place in 27th.

EUROPEAN CYBERCHALLENGE • MALAGA, SPAIN • OCTOBER 2017
Awarded for the 3rd place with the Italian Team of cybersecurity at the European Cyber Security Challenge 2017 held in Malaga, by ENISA.

HONORS PROGRAM • SAPIENZA UNIVERSITY • 2015-2019
I am currently enrolled in the Honors Program of my department: with my research supervisors, we are working on automatizing advanced exploitation techniques as Return Oriented Programming.

EDUCATION

BACHELOR'S DEGREE IN ENGINEERING IN COMPUTER SCIENCE • SAPIENZA • JULY 2017
110 cum Laude, GPA: 29.95/30.

MASTER'S DEGREE IN ENGINEERING IN COMPUTER SCIENCE • SAPIENZA • OCTOBER 2019
110 cum Laude, GPA: 30/30.

LEADERSHIP AND COMMUNICATION SKILLS

CYBERSECURITY TUTOR • SAPIENZA • 2018-2019
Organized lectures and practical challenges on advanced exploitation techniques for the Italian CyberChallenge.IT 2018 and 2019 training program (Sapienza University of Rome).

CO-FOUNDER OF DEFCON GROUP • ROME • SEPTEMBER 2018 - TODAY
Organizer of monthly security talks for the DEFCON group in Rome, to provide a gathering point to people interested in security.

SECURITY INTERESTS

I regularly participate in CTFs with the TheRomanXpl0it team that I co-founded, currently one of the strongest Italian CTF team. I am also one of the founders of mHACKeroni CTF team that participated at DEFCON CTF 26 and 27, in Las Vegas.

RESEARCH INTERESTS

PROGRAM ANALYSIS
I started my research activities in 2016 investigating programming languages techniques, in particular program analyses such as symbolic execution.

CODE REUSE TECHNIQUES
I have a strong background in exploitation attacks through code reuse techniques, such as ROP and COOP, with an eye on how to automatize them. I explored how program analysis techniques, such as symbolic execution, may be used to extract an accurate semantic signature for ROP gadgets, which I used as a building block for a ROP compiler.

EXPLOIT MITIGATIONS
I explored exploit mitigations based on hardware facilities as branch predictors and return address stack, to provide one of the first open source and portable implementation of such technique to the security community.

SOFTWARE OBFUSCATION
I am investigating how to enhance existing code obfuscation techniques such as Virtualization Obfuscation, through the use of code reuse techniques.

MICROARCHITECTURAL ATTACKS
I studied how modern processor optimizations may lead to leak of secrets through the CPU's microarchitectural state, providing open source proof of concepts of attacks such as Spectre & Meltdown, described in various papers, or enhancing existing ones.

SCIENTIFIC CONTRIBUTIONS

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