Luca Borzacchiello

Curriculum Vitae

✉ borzacchiello@diag.uniroma1.it
🖝 borzacchiello.github.io

Ph.D. student in computer engineering. My research interests include program analysis, symbolic execution, fuzzing, reverse engineering.

Education

2018 – now	**Ph.D. in Engineering in Computer Science**, *Sapienza University of Rome*, Rome. *Advisor: Prof. Camil Demetrescu*
2016 – 2018	**Master of Science in Engineering in Computer Science**, *Sapienza University of Rome*, Rome, *110 cum laude*. GPA: 29.64/30. *Thesis Advisor: Prof. Camil Demetrescu*. Cybersecurity curriculum. Courses held in English.
2013 – 2016	**Ingegneria Informatica e Automatica**, *Sapienza University of Rome*, Rome, *110 cum laude*, GPA: 29.19/30. *Thesis Advisor: Prof. Camil Demetrescu*

Teaching Experiences

from Sep 2018 to Jul 2021	**Teaching assistant of "Functional and Parallel Programming" course**, *Sapienza University of Rome*, Rome.
from Mar 2017 to Jul 2018	**Teaching assistant of "Computer Systems" course**, *Sapienza University of Rome*, Rome.

Educational Experiences

Sep 2019	**Summer School**, *System Security School*, Padua. 2019 International Summer School on "System Security" (S3).
Jul 2019	**Summer School**, *Summer School on Hot Topics in Cybersecurity*, Rome. International Cybersecurity Summer School.
from Mar 2017 to June 2017	**Cybersecurity Course**, *CyberChallenge.IT*, Rome, 66 h. Italian training program in cybersecurity for talented students of age 17-23, organized by CINI and Sapienza.

Notable Software Projects

- **Fuzzolic** *A QEMU fork that implements a concolic executor for automatic vulnerability detection.*
  Available online at `https://github.com/season-lab/fuzzolic`

- **SENinja** *A symbolic execution plugin for BinaryNinja. It can be used to analyze binary programs.*
  Available online at `https://github.com/borzacchiello/seninja`

- **SymNav** *A tool to visualyze the internal state of a symbolic execution engine.*
  Available online at `https://github.com/season-lab/symnav`

Publications

- Luca Borzacchiello, Emilio Coppa, Camil Demetrescu. **FUZZOLIC: mixing fuzzing and concolic execution.** *Computers & Security (COSE)*, 2021.

- Luca Borzacchiello, Emilio Coppa, Camil Demetrescu. **Fuzzing Symbolic Expressions.** *International Conference on Software Engineering (ICSE)*, 2021.

- Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. **Memory Models in Symbolic Execution: Key Ideas and New Thoughts.** *Software Testing, Verification and Reliability*, 2019.

- Marco Angelini, Graziano Blasilli, Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu, Simone Lenti, Simone Nicchi, Giuseppe Santucci. **SymNav: Visually Assisting Symbolic Execution**. *IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2019.

- Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu. **Reconstructing C2 Servers for Remote Access Trojans with Symbolic Execution.** *International Symposium on Cyber Security Cryptology and Machine Learning (CSCML)*, 2019.

Presentations

June 2021   **Hybrid Fuzzing**, *Presentation*, DEF CON group 11396 Rome, Online.

May 2021   **Fuzzing Symbolic Expressions**, *Presentation*, International Conference on Software Engineering (ICSE), Online.

Oct 2019   **SymNav: Visually Assisting Symbolic Execution**, *Presentation*, IEEE Symposium on Visualization for Cyber Security (VizSec), Vancouver, Canada.

June 2019   **Reconstructing C2 Servers for Remote Access Trojans with Symbolic Execution**, *Presentation*, 3rd International Symposium on Cyber Security Cryptology and Machine Learning (CSCML), Be'er Sheva, Israel.

Skills

Programming:	Advanced knowledge of C, python. Good experience with C++, Java, Scala
Operating Systems:	Good experience with GNU/Linux and Microsoft Windows
Tools:	BinaryNinja, Ghidra, IDA Pro, Radare2, QEMU, gdb, git, docker
Frameworks:	Intel PIN, angr, LLVM, KLEE, S2E

Languages

Italian: Mothertongue

English: Fluent

Awards

- Grant "Avvio alla Ricerca". 2020
- Grant "Avvio alla Ricerca". 2019
- Completed "flare-on 6" CTF. Organized by FireEye. 2019
- Third place in penetration testing at *CyberChallenge.IT*. Organized by Sapienza. 2017