

Richard Chaaya

✉ abouchaaya.richard@gmail.com • 🌐 Richard-AC.github.io

Education

- Brown University** 2021 – 2022
M.S in Computer Science
- Operating Systems
 - Networks
 - Compilers and Program Analysis
 - Formal Proof and Verification
 - Software Security
- CentraleSupélec** 2018 – 2021
M.S in Engineering
- Software Engineering
 - Computational complexity theory
 - Algebra and Cryptography
- Paris-Saclay University** 2018 – 2019
B.S in Fundamental Mathematics
- Preparatory classes at Janson de Sailly, Paris** 2016 – 2018
Undergraduate courses in Mathematics, Computer Science and Physics

Projects - Richard-AC.github.io

- Hypervisor Development for Security Research and Fuzzing** August 2022 -
- Wrote a Hypervisor in Rust using Intel VT-x optimized for fuzzing with up to 4 million VM resets per second
 - Fuzzed and discovered vulnerabilities in VirtualBox (CVE-2023-22002) and Avira Antivirus' Windows driver (CVE-TBA)
 - Wrote a PDF parser to generate and mutate PDFs and fuzz various readers
- Sysfilter** <https://gitlab.com/Egalito/sysfilter> October 2021 - April 2022
- Worked on the generation of system call filtering policies as part of the Secure Systems Lab of Brown University
 - Implemented an enforcement strategy for temporal system call policies based on seccomp
 - Analyzed 30K programs which showed an average reduction in indirect call targets numbers by 35% and syscalls by 5%
- Course Projects** January 2021 - April 2022
- OS: Wrote a UNIX inspired kernel with processes, threads, TTY and disks drivers, a file system and virtual memory
 - Networks: Wrote a TCP/IP stack in Rust. Analyzed VirtualBox's E1000 emulated device and reproduced a known CVE
 - Formal Proof: Formalized the Eudoxus Reals construction: <https://github.com/Richard-AC/EudoxusReals-Lean>

Skills

- Languages**
- Native French
 - Fluent English (IELTS 8.0/9.0)
 - Fluent Lebanese Arabic
- Programming**
- Rust / C / Python
 - x86 assembly
 - IDA Pro / WinDbg / gdb
 - Lean
 - OCaml
 - HTML / CSS / JavaScript

Work experience

- Security Research intern, L3Harris Trenchant, USA** February 2023 -
- JavaScript engine vulnerability research and fuzzer development
- Automated program analysis intern, QuarksLab, France** June 2022 - November 2022
- Developed a tool that uses fuzzing and symbolic execution for vulnerability research
 - The combination outperforms fuzzers by up to 20% in terms of coverage on popular targets like LibPNG and OpenThread
 - Got 1st at the SBFT'23 fuzzing competition and won Google's reward for "significant improvement over existing fuzzers"
- Teaching assistant at Brown University, Providence, USA** 2022
- CSCI1670/1690 - Operating systems teaching assistant
- Penetration testing intern, CGI Consulting, France** September 2020 - January 2021
- Conducted network and web application penetration tests and simulated phishing campaigns for a wide variety of clients
- Teaching assistant at Janson de Sailly, Paris, France** 2019-2020
- Teaching undergraduate level mathematics

Extracurriculars

- Capture The Flag**
- Plays CTF competitions with SHRECS, the student team of CentraleSupélec
 - FCSC 2023: 1st/2000+ in reverse engineering. FCSC 2022: 15th/1500+. THCon 2022: 1st. ImperialCTF 2022: 1st. CSAW 2021 Quals: 9th Europe. CSAW 2021 Finals: 4th Europe. Orange CTF 2021: 1st. NorzhCTF 2021: 3rd.

Vulnerability Research

- Discovered vulnerabilities through fuzzing (WinAFL, AFL, custom tooling) and code review and disclosed them to vendors
- VirtualBox (CVE-2023-22002), Avira Antivirus (CVE-TBA), CycloneTCP (CVE-2022-46078), OpenText (ZDI-21-1444)

Publications

- PASTIS - A Collaborative Approach to Combine Heterogeneous Software Testing Techniques** 2023
Robin David, Richard Abou Chaaya, Christian Heitman
SBFT2023 - The 16th Intl. Workshop on Search-Based and Fuzz Testing
- Symbolic Execution the Swiss-Knife of the Reverse Engineer** 2022
Robin David, Richard Abou Chaaya, Christian Heitman
3rd International KLEE Workshop on Symbolic Execution