Mathieu TARRAL

Email: mathieu.tarral@protonmail.com
Mobile: +33 6 31 66 30 78
Github: github.com/Wenzel

Executive Summary

Senior Software Security Engineer with 9 years of experience specialized in virtualization, virtual machine introspection, and fuzzing. Expertise spanning low-level systems programming to high-level cloud deployments. Passionate about bridging the gap between complex technical challenges and end-user protection. Seeking opportunities to leverage this diverse skillset to tackle cutting-edge problems in software security, with Open-Source at heart.

Experience

- **Intel** — Remote, FR
  Senior Software Security Engineer — *Jan 2022 - Present (2.5y)*
  - **kAFL**: Took ownership and transformed kAFL, a fast-guided fuzzer for x86 VMs based on QEMU/KVM, from IntelLabs PoC into an out-of-the-box internal product, bridging the gap and driving adoption for testing critical drivers and complex software stacks. Acted as Internal PM (customers, features, roadmap). Built extensive documentation and training courses.
  - **TSFFS**: Maintained coverage-guided fuzzer based on SIMICS for challenging targets (bootloaders, UEFI)
  - **VMsifter**: Co-led and developed an enhanced Sandsifter CPU scanning with perf counters & ring0 execution
  - **Confidential Computing**: Participated in a continuous fuzzing effort to secure the Linux Guest Kernel (Confidential Computing, TDX) (ccc-linux-guest-hardening project)
- **ANSSI - French National Cybersecurity Agency** — Paris, FR
  Project Engineer in Intrusion Detection — *Jan 2019 - Jan 2022 (3y)*
  - **Research**: Leveraged virtual machine introspection to enhance the agency's intrusion detection capabilities
  - **Open-Source**: Contributed to multiple open-source VMI related projects (LibVMI, KVM-VMI, and Drakvuf)
  - **Production Management**: Maintained production deployment, ensuring detection system's availability

Education

- **EPITA - School of Engineering and Computer Science** — Paris, FR
  Master's Degree - Major: SRS (Systems, Networks and Security) — *2012 – 2015*
  - **Teaching Assistant**: Programming teacher (C, C++, Java, Unix) in a team of 30 for 400 students
  - **Co-System Administrator**: Led infrastructure management for department-wide student services

Conferences

- **FOSDEM**: Rustifying the VMI ecosystem (2020)
- **Hack.lu**: Leveraging KVM as a Debugging Platform (2019)
- **Insomni'Hack**: Building a Flexible Hypervisor-Level Debugger (2019)

Projects

- **libmicrovmi (Rust)**: Cross-platform unified low-level VMI API. Co-mentored student for GSoC 2020
- **LibVMI (C)**: Complete rewrite of the KVM driver to integrate the new KVM introspection subsystem by Bitdefender
- **KVM-VMI**: Online community dedicated to bring VMI capabilities into QEMU/KVM
- **pyvmidbg (Python)**: Hypervisor-level debuggeer based on LibVMI with GDB stub interface
- **checksec.py (Python)**: checksec-like tool with parallel processing and enhanced output. Based on LIEF
- **awesome-virtualization**: Collected, organized and references awesome resources on virtualization related topics

Skills

- **Languages**: Python, C, Rust
- **DevOps**: HashiCorp (Packer, Vagrant, Terraform), Ansible, Github Actions
- **Awards**: HashiCorp Core-Contributor 2024
- **Technologies**: VueJS, Neo4j, GraphQL

Trainings

- **Windows Internals**: (A. Ionescu - 2021)
- **FOR500**: Windows Forensics Analysis Class (O. Caroll 2021)
- **Linux/UNIX System Programming**: (M. Kerrisk - 2019)