Amir Al Sadi

alsadi.amir@gmail.com | alsadiamir.github.io | linkedin.com/in/amiralsadi | github.com/alsadiamir

Security-focused systems engineer working on the infrastructure underpinning cloud platforms: Linux, virtual machines, workload isolation, networking, and performance. Builds and debugs mechanisms across firmware, KVM/QEMU, and programmable data planes, with recent work on confidential computing for secure multi-VM cloud workloads.

Experience

Postdoctoral Researcher, Systems Infrastructure and Security 2025 - Present
Imperial College London, NetSys Group *London, United Kingdom*

- Design and build low-level infrastructure for isolated multi-VM cloud and AI workloads across Arm CCA firmware, KVM, QEMU, guest VMs, and remote attestation.
- Develop memory-sharing, page-tracking, interrupt-filtering, and protected-communication mechanisms across firmware, hypervisor, and virtual-machine boundaries.
- Build reproducible development and evaluation environments, automate system builds and experiments, and debug changes spanning multiple layers of the virtualization stack.

Doctoral Researcher, Networked Systems 2022 - 2025
University of Bologna / University College London *Bologna, Italy / London, United Kingdom*

- Designed distributed network-monitoring infrastructure for detecting volumetric DDoS, link-flooding, and anomalous traffic close to the data plane.
- Implemented packet-processing and telemetry mechanisms in P4, including in-switch data structures and dynamic pipelines that distributed anomaly-detection computation between the line-rate data plane and the control plane.
- Built automated ns-3 testbeds and evaluated detection accuracy, resource use, and forwarding overhead, including validation on Intel Tofino hardware.

Education

University of Bologna Bologna, Italy

Ph.D. in Computer Science and Engineering 2022 - 2025
M.Sc. in Computer Science and Engineering 2019 - 2021
B.Sc. in Computer Science and Engineering 2016 - 2019

Projects

Mica | *Attestable Multi-VM Infrastructure on Arm CCA* 2025 - Present

- Extended RMM paging, KVM page tracking, and QEMU's ivshmem backend to provide policy-controlled shared memory between confidential VMs; achieved 12x faster inter-VM communication with approximately one second of additional boot latency.
- Added an attested policy DSL for memory and control-flow relationships while limiting the implementation increase to 7% of RMM and less than 1% of the host-kernel TCB.

Line-Rate Distributed Anomaly Detection | *Programmable Network Infrastructure* 2022 - 2025

- Built dynamically reconfigurable P4 pipelines that updated monitoring strategies without switch downtime or disruption to packet forwarding.
- Detected spiked-wave attacks within 400 packets (under 10 ms) and stress-tested distributed detection across more than 750 attack waves in simulation and Intel Tofino hardware evaluation.

Technical Skills and Interests

Infrastructure Systems: Linux, KVM, QEMU, virtual machines, shared memory, workload isolation
Networking: TCP/IP, P4, programmable data planes, network monitoring, Intel Tofino, ns-3
Observability and Performance: systems debugging, telemetry, benchmarking, latency and throughput analysis, reproducible testbeds
Confidential Computing: Arm CCA/RMM, confidential VMs, remote attestation, TCB analysis
Programming: C, C++, Python, Bash; working knowledge of Java and Go
Tooling: Git, Docker, build automation, experiment orchestration, LaTeX