Hossam ElAtali

E-mail: hossam.elatali@gmail.com LinkedIn: hossam-elatali-05545b20 Website: elatalhm.github.io

Education

PhD Computer Science – System Security	*University of Waterloo*	*2021 - present*

Topics: HW-assisted security, confidential computing, memory safety, side channels
Supervisor: Prof. N. Asokan

Experience

- ***Computer architecture development***
  Extensive experience with computer architecture. Heavily modified RISC-V CPU pipelines and cache hierarchies for multiple projects (BliMe [5], CacheSquash [2], BLACKOUT [1]) in RTL (Verilog/Chisel/Bluespec) and simulation (gem5). Also implemented encryption co-processor in Chisel for BliMe [5].
- ***ML HW acceleration***
  Modified open-source Gemmini accelerator to implement taint tracking and enforce a security policy for Dolma [4].
- ***Compiler extensions (LLVM)***
  Created LLVM passes for taint flow analysis and control-flow and data-flow linearization. Also added new assembly instructions to LLVM RISC-V backend for BliMe [5].

M.Sc. Computer HW & SW Engineering	*University of Stuttgart*	*2012 - 2015*
B.Sc. Electronics	*German University in Cairo*	*2007 - 2012*

Professional Experience

PhD Intern – Helsinki System Security Lab	*Huawei*	*2025*

- Developed novel Aarch64 hardware primitive for memory safety. Implemented design on QEMU. Modified Linux kernel to add feature support. Created demos for management. Modified shadow stack support in LLVM Aarch64 backend for performance evaluation. Integrated support in V8 Javascript engine to improve sandbox performance.
  → ***Patent submitted. Paper in-progress.***
- Implemented modifications to secure boot and EL0 isolation in UEFI firmware for Aarch64 (C and assembly).

Technical Lead	*Mentor Graphics*	*2020 - 2021*
Senior SW Development Engineer	*Mentor Graphics*	*2018 - 2020*
SW Development Engineer	*Mentor Graphics*	*2015 - 2018*

- Led team developing HDMI/DisplayPort protocol verification solutions for emulation hardware.
  - Added new spec-compliant features. Overhauled application interface using Qt. Created Verilog modules to interface with emulation hardware. Met directly with customers abroad to demo features and get feedback.
- Put in charge of a brand-new product for verifying Optical Transport Network designs-under-test (DUTs).
  - Created and implemented initial design. Met with customers to understand requirements.

Publications

1. **H. ElAtali,** et al., "*BLACKOUT: Data-Oblivious Computation with Blinded Capabilities*", arXiv:2504.14654 (2025). [link]
2. **H. ElAtali** and N. Asokan, "*CacheSquash: Making caches speculation-aware*", arXiv:2406.12110 (2025). [link]
3. **H. ElAtali**, et al., "*BliMe Linter*", IEEE SecDev Conference (2024). [link]
4. **H. ElAtali**, et al., "*Data-Oblivious ML Accelerators using Hardware Security Extensions*", HOST (2024). [link]
5. **H. ElAtali**, et al., "*BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking*", NDSS (2024). [link]
6. **H. ElAtali**, "*Configurable Shared Cache and Memory Model for Parallel NoC Simulation*", Master's thesis (2015).
7. **H. ElAtali**, "*Simulation of Realistic Defects for Validating Test-and Diagnosis-Algorithms*", Bachelor's thesis (2012).

Awards

- Distinguished Artifact Reviewer (2024) – USENIX Association
- Best Poster Award (2022) – Cybersecurity and Privacy Institute, University of Waterloo
- Entrance Scholarship (2021) – University of Waterloo
- DAAD Full Scholarship (2012-2015) – German Academic Exchange Service