

# Adrien Ghosn

POST DOC RESEARCHER IN COMPUTER SCIENCE, MICROSOFT RESEARCH CAMBRIDGE

✉ ghosn.adrien@gmail.com | 🏠 aghosn.github.io | 📱 aghosn | 🌐 aghosn

## Education

### Ecole Polytechnique Federale de Lausanne(EPFL)

Lausanne, Switzerland

COMPUTER SCIENCE ENGINEERING

Sep. 2010 - 2021

- 2016 – 2021: PhD in Datacenter System Laboratory, Prof. Edouard Bugnion and Prof. James Larus
- 2013 – 2016: Master Degree, Foundations of Software specialization (avg 5.75/6)
- 2010 – 2013: Bachelor Degree

### Northeastern University(NEU)

Boston, U.S.A.

MASTER THESIS

Sep. 2015 - Mar. 2016

- Supervised by Prof. Jan Vitek in the Programming Languages Laboratory

### Carnegie Mellon University(CMU)

Pittsburgh, U.S.A.

EXCHANGE YEAR, BACHELOR DEGREE IN COMPUTER SCIENCE

Aug. 2012 - Jul. 2013

- Dean's list School of Computer Science for QPA > 3.75/4

## Industry

### Microsoft Azure Research

Cambridge UK

RESEARCHER

November 2023 - present

- Implemented a bare metal Rust monitor for virtualization-based TEEs and sandboxes
- Backward compatible with Linux, enables enclaves, CVMs, and sandboxes
- Exploring side-channel protection, secure device passthrough in CVMs, & DOS mitigation
- Exploring hypervisor-based attested information flow and isolation
- Technologies: Intel VT-x, RISC-V PMP, Linux kernel drivers, Virtualization

### Microsoft Research

Cambridge UK

Post Doc

November 2021 - November 2023

- Trusted Execution Environment on legacy hardware
- Verona: explored WASM and process-based sandboxing of foreign code

### Google Asylo team

Kirkland, USA

SUMMER INTERNSHIP - SUPERVISOR: MATT GINGELL

June - August 2019

- Asylo team: explored designs to support higher-level programming languages in SGX enclaves
- Delivered a prototype to run Java code inside SGX

### ABB Corporate Research

Baden, Switzerland

MASTER INTERNSHIP - SUPERVISOR: DR. MANUEL ORIOL

Feb. 2015 - Aug. 2015

- Aperiodic-Event Support in FASA
- Fixed-priority servers, data-driven events, real-time control applications
- kernel design, dynamic linking/loading & software updates, pi-calculus

## Skills

### Programming

C/C++, Assembly, Rust, Shell scripting, Python, Java, Go

### Systems

OS design, Virtualization, process & VM-based isolation, KVM, Intel VT-x, Intel MPK, Trusted Execution Environments

### PL

Compilers, Language runtimes & virtual machines, software-hardware co-design

Software capabilities, ELF linker/loader, binary instrumentation

## Research & Publications

### Focus Areas

Exploring isolation abstractions and security guarantees for modern cloud workloads involving multiple distrustful parties. Leveraging system design, compiler and language-based techniques, linker/loader instrumentation, and hardware virtualization and security extensions. My work combines confidential computing and compartmentalization while maintaining backward compatibility with existing software. I favor simple, practical, and holistic solutions.

## Tyche: Creating Trust by Abolishing Hierarchies [HotOS 23]

IMPERIAL COLLEGE LONDON: MARIOS KOGIAS, EPFL: PROF. EDOUARD BUGNION, PROF. MATHIAS PAYER

Cambridge, UK

Nov. 2021 - Present

- Isolation monitor, hardware-independent support for compartmentalization & confidential computing.
- Written in Rust, runs on x86 & RISC-V
- Intel VT-x, Intel TXT, RISC-V PMP, Linux Kernel drivers, Virtualization

## Dynamic Linkers Are the Narrow Waist of Operating Systems [PLOS@SOSP 23]

EPFL: CHARLY CASTES

Cambridge, UK

Oct. 2023

- Dynamic linker to port existing software to more secure execution environments.

## Gradient: Gradual Compartmentalization via Object Capabilities Tracked in Types [OOSPLA24]

EPFL: ALEKSANDER BORUCH-GRUSZECKI, MATHIAS PAYER, CLEMENT PIT-CLAUDEL

Cambridge, UK

Oct. 2024

- Gradual compartmentalization with object capabilities & hardware-isolated compiled code.

## PhD Thesis: Trust as a Programming Primitive

EPFL - PROF. EDOUARD BUGNION, PROF. JAMES LARUS

Lausanne, Switzerland

Sep. 2016 - Sep. 2021

- Programming Language extensions for compartmentalization and confidential computing.
- Programming languages, isolation, security, confidentiality, integrity, virtualization, hardware security extensions

## Enclosures: Language-based restriction of untrusted libraries [ASPLOS21]

EPFL - PROF. EDOUARD BUGNION, PROF. MATHIAS PAYER

Lausanne, Switzerland

Sep. 2019 - Oct. 2020

- New fine-grain programming abstraction to restrict public libraries access to program resources
- Frontend extensions to Go and Python PLs, backend hardware isolation enforcement (Intel VT-x & Intel MPK)
- Intra-address-space isolation, Sandboxing, Compiler, Linker, Runtime

## Secured Routines: Language-based construction of TEEs [ATC19]

EPFL - PROF. EDOUARD BUGNION, PROF. JAMES LARUS

Lausanne, Switzerland

Jun. 2018 - May 2019

- Extended Go programming language to support executing goroutines inside Intel SGX.
- Intel SGX, Confidentiality, Integrity, Go, Compilers, Code partitioning, Hardware Extensions

## Light-Weight Contexts in Dune

EPFL - PROF. EDOUARD BUGNION

Lausanne, Switzerland

Sep. 2016 - Jul. 2017

- Process virtualization with Dune
- Intra-address space isolation, protecting secrets, memory snapshots, 5x faster than fork
- Intel VTX, Dune, Virtualization, Kernel module, Virtual Memory Management

## Efficient Runtime Deoptimization for R(Master Thesis)

NORTHEASTERN UNIVERSITY - PROF. JAN VITEK

Boston, U.S.A.

Sep. 2015 - Mar. 2016

- Speculative optimizer for an R JIT compiler
- Removes performance bottlenecks due to the language semantics
- On-stack replacement, speculative optimizations, runtime de-optimization, R, LLVM, JIT compiler

## Scalameta: AST Persistence & Obey: Code Health

EPFL, LAMP - PROF. MARTIN ODESKY & DR. EUGENE BURMAKO

Lausanne, Switzerland

Jan. 2014 - Feb. 2015

- Obey: Scala-linter for user-defined rules enforced at compile-time
- AST Persistence: typed-AST format for Scala for compiler version compatibility & macro expansion

## Operating Systems & Design 15-410

UNDERGRADUATE

CMU

Jan. 2013 - Jul. 2013

- Design & implementation of x86 Unix kernel – thread library, scheduler, virtual memory, drivers, syscalls

## Management & Teaching

### Grants

Swiss Joint Research Grant: Confidential Computing solutions for legacy hardware.

Joint program with Microsoft Research, EPFL, Imperial College London.

### Teaching Assistant

Functional Programming (2020), Introduction to Operating Systems (2019), Introduction to Java (2018)

Systems for Data Science (2017-2020), Introduction to C (2016-2017), Concurrent Programming (2015)

## Personnal

**Languages**    Fluent in French & English