Sid **Agrawal**

Systems Software Engineer · Ph.D. Candidate

Vancouver, Canada

sid@sid-agrawal.ca | sid-agrawal.ca | sid-agrawal | sidhartha-agrawal | Google Scholar

Summary

Systems Software engineer with 8 years of industry experience in the kernel, virtualization, security hardware features, filesystem, and orchestration roles. Also, a PhD Candidate with some research experience in the same fields.

Does not require authorization in Canada (citizen) and has an I-140 approved for the US (prior H1B).

Work Experience

Systopia Lab, University of British Columbia

Vancouver, Canada

PhD Candidate | Engineer, Research and Development — *Jan 2021 - present*

- Bootstrapped a research project, and prototype OS to investigate how different isolation mechanisms (Docker, Kata, VM (Xen, KVM) etc..), can be compared from the point of isolation & security. Extend this to aid the discovery of new isolation mechanisms. Publication.
- Developed a new OS on the security-focused **seL4 microkernel** used in Trusted Execution Environments(TEE) on ARM Processors, to demonstrate the research's findings. Led and mentored a team of three engineers for the development effort; 50K SLOC in **C**, and **ARM assembly**. Source Code & Documentation. Source Code &
- Developed hypervisor, device drivers, and new isolation mechanisms in the prototype OS. Documentation
- Developed Python tooling that uses `/proc & /sys` on interfaces **Linux** to enable the comparison of isolation mechanism on **Linux**, digging into Namespaces, Docker, QEMU and Buildroot. Code and Wiki
- Analyze large-scale graphs showcasing the differences in isolation mechanisms Neo4j using CyperQL.
- Research page-prefetching optimizations in **FreeBSD** memory subsystem using CHERI. Publication
- Research userspace & kernel compartmentalization techniques with a focus on ARM Pointer Authentication (PAC), Memory Tagging Extension (MTE), Permission Overlay Extension (POE), Morello/CHERI and Intel Memory Protection Keys (MPK). Publication for the kernel part
- Enrolled in courses related to databases, compilers, and formal-verification. Occasionally conducted classes.

ARM

Remote

Intern, Research - Operating Systems Security — *May 2022 - Aug 2022*

- Ported a microkernel (seL4) to ARM's Morello experimental platform with hardware capability support (CHERI). Blog & Source

Arista Networks

Vancouver, Canada & SF Bay Area

Software Engineer — *Sep. 2016 - Dec. 2020*

- Developed (Golang) and deployed (Kubernetes and Jenkins) micro-services to detect, triage, and fix faulty testbeds. This automation led to savings of 10s of person-hours per month per engineer.
- Developed (Golang) and deployed services to store distributed file systemsb́lob data in a NoSQL (ScyllaDB) store. Code
- Occasional babysitting of the Kubernetes and ScyllaDB clusters, and Linux kernel bug-fixes.

Panzura

SF Bay Area

Software Engineer - File Systems — *Apr. 2015 - Aug. 2016*

- Designed and implemented (C) support to transactionally update file metadata for Panzuras Global Distributed File System, which heavily simplified recovery after crashes.

Oracle

SF Bay Area

Kernel Engineer — *Mar. 2012 - Apr. 2015*

- Enhanced the virtual memory predictor in Solaris by developing an algorithm to determine which segments in the address space can be upgraded to large pages
- Developed C and assembly level kernels to stress test cache interconnects and database co-processor of the SPARC microprocessor

Education

University of British Columbia

Vancouver, Canada

Ph.D. in Computer Science: Operating Systems Architecture and Security (Advisor: Prof. Margo Seltzer) — *Jan. 2021 - Ongoing*

- Develop a formal model to compare and build OS isolation mechanisms.

University of Florida

Florida, USA

MS. in Electrical and Computer Engineering — *Aug. 2010 - Dec. 2011*

BITS(Birla Institute of Technology and Science) Pilani

Goa, India

B.E. in Electrical and Electronics Engineering — *Aug. 2005 - Aug. 2009*

Publications (next page)

OSmosis: No more Déjà vu in OS isolation *ArXiv 2309.09291*

Sidhartha Agrawal, Reto Achermann, and Margo Seltzer

This work lays out the ground for an isolation model for the entire operating system, and it is the groundwork for my thesis.

CHERI-picking: Leveraging capability hardware for prefetching *PLOS 2023, Germany*

Shaurya Patel, **Sidhartha Agrawal**, Alexandra Fedorova, and Margo Seltzer

The work uses a new ISA (CHERI), which was built for security and instead used to build a higher-performance system.

Securing Monolithic Kernels using Compartmentalization *ArXiv 2404.08716*

Soo Yee Lim, **Sidhartha Agrawal**, Xueyuan Han, David Eyers, Dan O'Keeffe, Thomas Pasquier

A survey of intra-kernel compartmentalization techniques