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 operating security, hardware security features, virtualization, filesystem, and orchestration roles. PhD Candidate with research experience in OS security.

Canadian citizen with US I-140 (prior H1B)

Experience

Systopia Lab, University of British Columbia — *Vancouver, Canada*

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

- Bootstrapped a research project, and developed a 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.
- Developed hypervisor, device drivers, and new isolation mechanisms in the new OS. Source Code & 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
- Analyzed large-scale graphs stored in Neo4j showcasing the differences in isolation mechanisms using CypherQL. Examples
- Researched page-prefetching optimizations in **FreeBSD** memory subsystem using CHERI. Publication
- Researched userspace & kernel compartmentalization techniques with a focus on **ARM Pointer Authentication (PAC), Memory Tagging Extension (MTE), Permission Overlay Extension (POE), Morello/CHERI, Intel Memory Protection Keys (MPK), Intel VT-X, and Extended Page Tables (EPT)** Publication for the kernel part
- Enrolled in courses related to databases, compilers, and formal verification. Occasionally conducted classes on OS security.

ARM — *Remote, Canada*

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

- Ported the seL4 microkernel to **ARM's Morello** experimental platform with hardware capability support (i**CHERI**), digging into kernel capability system, bootloader, context switching, and process bootstrapping code paths. Blog & Source

Arista Networks — *Vancouver, Canada & SF Bay Area*

Software Engineer - Internal Tools and Microservices — *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. Scaled it from a solo project to a 3 member team.
- Developed (Golang) and deployed services to store distributed file system's block data in a NoSQL (ScyllaDB) store. Code
- Participated in DevOps responsibilities, for the Kubernetes and ScyllaDB clusters.
- Fixed Linux kernel bug as the 10% project.

Panzura — *SF Bay Area*

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

- Designed and implemented (C) support to transactionally update file metadata for Panzura Global Distributed File System (ZFS on FreeBSD). This simplified recovery after crashes, thus preventing an entire class of support tickets.

Oracle — *SF Bay Area*

Software Engineer - Solaris Kernel — *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

Skills

Languages	C, Golang, ARM, x86 Assembly, CypherQL
Operating Systems & Tooling	seL4 microkernel, Solaris, Linux, Buildroot, gdb, kdb, DTrace
Orchestration & CI	Docker, Kubernetes, Jenkins
Security and Virtualization	QEMU; Intel:MPK, VT-X; ARM: MTE, PAC, CHERI, POE

Education

University of British Columbia *Vancouver, Canada*

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

University of Florida *Florida, USA*

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

BITS(Birla Institute of Technology and Science) Pilani - Goa Campus *Goa, India*

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

Publications

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

Sidhartha Agrawal, Reto Achermann, and Margo Seltzer

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

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

Securing Monolithic Kernels using Compartmentalization *ArXiv 2404.08716*

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