

Nadav Amit

100 N. Whisman Rd., Apt 1614, Mountain View, California 94043, USA
nadav.amit@gmail.com • +1 (650) 272-9111 • <http://nadav.amit.zone/> •
Curriculum Vitae compiled on 2022-10-17

EDUCATION

Technion — Israel Institute of Technology, Haifa, Israel

- Ph.D. in Computer Science Mar 2009 – Jul 2014
 - Thesis: Alleviating Virtualization Bottlenecks
 - Advisers: Prof. Assaf Schuster and Prof. Dan Tsafir
 - Focus: Virtualization, operating systems, performance.
- B.Sc. in Computer Science Oct 2000 – Aug 2004
 - Graduated Cum Laude

EMPLOYMENT HISTORY

VMware Research Group, Palo Alto, CA, USA

- Senior Researcher Jan 2016 –
 - Research Projects: new paravirtualization techniques, efficient memory management, alleviating Spectre and Meltdown overheads.
 - Additional responsibilities: Linux memory ballooning maintainer, tests development, product teams consulting.
 - Focus: virtualization, operating systems, memory management.

Technion—Israel Institute of Technology, Haifa, Israel

- Senior Research Associate Aug 2014 – Dec 2015
 - Projects: hypervisors security and stability, efficient memory management.
 - Focus: hypervisors, memory management.
- Teaching Assistant Mar 2009 – Jul 2014
 - Tutoring "Database Management Systems", "Parallel and Distributed Programming" and "Digital Computer Architecture".

IBM Research Center, Haifa, Israel

- Research Intern Jul 2009 – Oct 2009
 - Projects: Intel IOMMU emulation, direct delivery of interrupts.
 - Focus: hypervisors, I/O.

Intel Cooperation, Haifa, Israel

- Software Engineer Jul 2002 – Dec 2006
 - Building fuzzing tools to test Intel CPUs, debugging of CPU bugs.
 - Focus: virtualization, power management, thermal monitoring and sleep-states.

AWARDS

- Dennis M. Ritchie Doctoral Dissertation Honorable Mention, *ACM SIGOPS* 2015
- Google Security Patch Reward (10,000USD) 2015
- SPEC Distinguished Dissertation Award, *SPEC Research Group* 2014
- IBM PhD fellowship Award, *IBM* 2012

OTHER ACTIVITY

- Program committee member
 - ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2023
 - ACM Virtual Execution Environments (VEE) 2022
 - ACM International Systems and Storage Conference (SYSTOR) 2022
 - Operating Systems: Design and Implementation (OSDI) 2021
 - ACM International Systems and Storage Conference (SYSTOR) 2020
 - ACM Virtual Execution Environments (VEE) 2020
 - ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2019
 - USENIX Annual Technical Conference (ATC) 2019
 - ACM Symposium on Cloud Computing (SoCC) 2018
 - ACM International Systems and Storage Conference (SYSTOR) 2018
 - ACM Workshop on Systems for Multi-core and Heterogeneous Architectures (SFMA) 2018
 - ACM International Systems and Storage Conference (SYSTOR) 2017
 - ACM Virtual Execution Environments (VEE) 2017
 - USENIX Annual Technical Conference (ATC) 2017
 - World Wide Web Conference (WWW) 2017

- External reviewer
 - ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2018
 - IEEE Computer Architecture Letters (CAL) 2013, 2016, 2018
 - EuroSys Conference 2015
 - ACM Virtual Execution Environments (VEE) 2014
 - IEEE Transactions on Computers (TOC) 2014
 - ACM International Conference on Supercomputing (ICS) 2012
 - USENIX Annual Technical Conference (ATC) 2011
- Reported security vulnerabilities
 - CVE-2021-4002: Missing TLB flush on hugetlbfs
 - CVE-2018-15594: Linux vulnerability to Spectre-v2 under KVM & Xen
 - CVE-2015-0239: KVM hypervisor SYSENTER emulation vulnerability
 - CVE-2014-3610: KVM hypervisor WRMSR emulation vulnerability
 - CVE-2014-3647: KVM hypervisor RIP changing emulation vulnerability
 - CVE-2014-7842: KVM hypervisor emulation failure vulnerability
 - CVE-2014-8480: KVM hypervisor NULL dereference vulnerability
 - CVE-2014-8481: KVM hypervisor NULL dereference vulnerability
- Open Source Contributions
 - Linux (KVM, x86, memory management, IOMMU)
 - QEMU emulator
 - LLVM compiler (BPF backend)
 - FreeBSD (IOMMU)
- Academic advising
 - Gil Kupfer (Technion), “IOMMU-resistant DMA attacks,” 2016 – 2018
co-advising with Prof. Dan Tsafir

PUBLICATIONS

JOURNALS

- [J-2] Nadav Amit, Michael Wei and Chun-Chung Tu, “Hypercallbacks,” *ACM Operating System Review (OSR)* 51(1), 2017. Based on [C-9].
- [J-1] Nadav Amit, Abel Gordon, Nadav Har’El, Muli Ben-Yehuda, Alex Landau, Assaf Schuster and Dan Tsafir, “Bare-metal performance for virtual machines with exitless interrupts,” in *Communications of the ACM (CACM)*, Jan 2016. **Invited to the Research Highlights Section.** Based on [C-3].

CONFERENCES

- [C-21] David Hildenbrand, Martin Schulz and Nadav Amit, “Copy-on-Pin: The Missing Piece for Correct Copy-on-Write,” in *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2023 [To Appear].
- [C-20] Alex Markuze, Shay Vargaftik, Gil Kupfer, Boris Pismenny, Nadav Amit, Adam Morrison and Dan Tsafir, “Understanding DMA Attacks in the Presence of an IOMMU,” in *European Conference on Computer Systems (EuroSys)*, 2021
- [C-19] Nadav Amit, Amy Tai and Michael Wei, “Don’t shoot down TLB shootdowns!,” in *European Conference on Computer Systems (EuroSys)*, 2020. **Received Best Paper Award.**
- [C-18] Eitan Rosenfeld, Aviad Zuck, Nadav Amit, Michael Factor and Dan Tsafir, “RAIDP: ReplicAtion with Intra-Disk Parity for Cost-Effective Storage of Warm Data,” in *European Conference on Computer Systems (EuroSys)*, 2020.
- [C-17] Nadav Amit and Michael Wei, “JumpSwitches: Restoring the performance of indirect branches in the era of Spectre,” in *USENIX Annual Technical Conference (ATC)*, 2019.
- [C-16] Elazar Gershuni, Nadav Amit, Arie Gurfinkel, Nina Narodytska, Jorge A Navas, Noam Rinetzky, Leonid Ryzhyk and Mooly Sagiv, “Simple and precise static analysis of untrusted Linux kernel extensions,” in *ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, 2019.
- [C-15] Lluís Vilanova, Nadav Amit and Yoav Etsion, “Using SMT to Accelerate Nested Virtualization,” in *ACM International Symposium on Computer Architecture (ISCA)*, 2019.
- [C-14] Nadav Amit and Michael Wei, “The Design and Implementation of Hyperupcalls,” in *USENIX Annual Technical Conference (ATC)*, 2018. **Received Best Paper Award.**
- [C-13] Marcos K. Aguilera, Nadav Amit, Irina Calciu, Xavier Deguillard, Jayneel Gandhi, Stanko Novakovic, Arun Ramanathan, Pratap Subrahmanyam, Lalith Suresh, Kiran Tati, Rajesh Venkatasubramanian and Michael Wei, “Remote regions: a simple abstraction for remote memory,” in *USENIX Annual Technical Conference (ATC)*, 2018.
- [C-12] Nadav Amit, Michael Wei. “Hypercallbacks: a new mechanism for trusted, secure introspection”, in *Workshop on System Software for Trusted Execution (SysTEX)*, 2017.
- [C-11] Marcos K. Aguilera, Nadav Amit, Irina Calciu, Xavier Deguillard, Jayneel Gandhi, Pratap Subrahmanyam, Lalith Suresh, Kiran Tati, Rajesh Venkatasubramanian and Michael Wei. “Remote memory in the age of fast networks,” in *ACM Symposium on Cloud Computing (SOCC)*, 2017.
- [C-10] Nadav Amit, “Optimizing the TLB shutdown algorithm with page access tracking,” in *USENIX Annual Technical Conference (ATC)*, 2017.
- [C-9] Nadav Amit, Michael Wei and Chun-Chung Tu, “Hypercallbacks: decoupling policy decisions and execution,” in *ACM Workshop on Hot Topics in Operating Systems (HotOS)*, 2017.
- [C-8] Nadav Amit, Dan Tsafir, Assaf Schuster, Ahmad Ayoub and Eran Shlomo, “Validating Virtual CPUs,” in *ACM Symposium on Operating Systems Principles (SOSP)*, 2015.
- [C-7] Moshe Malka, Nadav Amit, Muli Ben-Yehuda and Dan Tsafir, “rIOMMU: efficient IOMMU for I/O devices that employ ring buffers,” in *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2015.
- [C-6] Moshe Malka, Nadav Amit and Dan Tsafir. “Efficient intra-operating system protection against harmful DMAs,” in *USENIX Conference on File and Storage Technologies (FAST)*, 2015.
- [C-5] Nadav Amit, Dan Tsafir and Assaf Schuster, “VSWAPPER: a memory swapper for virtualized environments” in *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2014. **Received HiPEAC Award.**

- [C-4] Eitan Rosenfeld, Nadav Amit and Dan Tsafir, “Using disk add-ons to withstand simultaneous disk failures with fewer replicas,” in *Workshop on the Interaction amongst Virtualization, Operating Systems and Computer Architecture (WIVOSCA)*, 2013
- [C-3] Abel Gordon, Nadav Amit*, Nadav Har’El, Muli Ben-Yehuda, Alex Landau, Assaf Schuster and Dan Tsafir, “ELI: Bare-Metal Performance for I/O Virtualization,” in *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2012. **Received the Pat Goldberg Memorial Best Paper Award and HiPEAC Award.**
- [C-2] Nadav Amit, Muli Ben-Yehuda, Dan Tsafir, and Assaf Schuster, “vIOMMU: Efficient IOMMU Emulation,” in *USENIX Annual Technical Conference (ATC)*, 2011.
- [C-1] Nadav Amit, Muli Ben-Yehuda and Ben-Ami Yassour, “IOMMU: Strategies for Mitigating the IOTLB Bottleneck,” in *Workshop on Interaction between Operating System and Computer Architecture (WIOSCA)*, 2010.

PATENTS

- [P-2] Assaf Schuster, Nadav Amit, Dan Tsafir. “Memory swapper for virtualized environments”, US9811268B2 (granted), product of [C-5]. 2017
- [P-1] Nadav Amit, Shmuel Ben-Yehuda, Abel Gordon, Nadav Har’el, Alex Landau. “Enhancing interrupt handling in a virtual environment”, US8892802B2 (granted), product of [C-3]. 2014

[Curriculum Vitae compiled on 2022-10-17]

*Both authors contributed equally