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 2023-07-07

PERSONAL DETAILS

ORCID iD: 0000-0002-6643-6232
Phone number: +1 (650) 272-9111, +972 (54) 808-5555
E-mail address: namit@technion.ac.il

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 Tsafrir
  - 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 –
  - Improved Linux kernel TLB flushing: speeding up TLB shootdown, identifying and fixing multiple security vulnerabilities and correctness issues.
  - Developed and implemented novel paravirtualization mechanism in which the host executes verifiable guest code (eBPF) to provide advanced services and for better resource utilization.
  - Adapted kvm-unit-tests to test VMware hypervisor and bare metal systems. Found dozen of VMware bugs, Intel SDM mistake and upstreamed 40+ patches for kvm-unit-tests.
  - Other research projects: userspace memory manager; alleviating Spectre and Meltdown overheads; syscall failure analyzer.
  - 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
  - Operating Systems: Design and Implementation (OSDI) — 2024
  - ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) — 2024
  - 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 Transactions on Computer Systems (TOCS) 2023
  - IEEE Transactions on Cloud Computing (TCC) 2023
  - 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
  - KVM-unit-tests support for bare-metal and VMware (∼60 patches) 2017–2023
  - VMware balloon driver for Linux (∼30 patches) 2017–2023
  - Linux TLB flushing performance improvements (∼20 patches) 2020–2022
  - Linux userfaultfd enhancements (∼10 patches) 2022
  - Linux self-modifying code security enhancements (∼10 patches) 2019
  - KVM virtualization correctness issues (∼140 patches) 2014
  - QEMU emulator
  - LLVM compiler (BPF backend)
  - FreeBSD (IOMMU)
- Academic advising
  - Gil Kupfer (Technion), “IOMMU-resistant DMA attacks,” 2016 – 2018
    co-advising with Prof. Dan Tsafrir

PUBLICATIONS

UNDER SUBMISSION

[U-1] Nadav Amit and Michael Wei, "DeepErr: Automatic Root-Cause Analysis of Syscall Failures," under submission.

JOURNALS

[J-3] Marcos K. Aguilera, Emmanuel Amaro, Nadav Amit, Erika Hunhoff, Anil Yelam, Gerd Zellweger, "Memory Disaggregation: Why Now and What Are the Challenges," in *SIGOPS Operating Systems Review (OSR) 57(1)*, 2023.

[J-2] Nadav Amit, Michael Wei and Chun-Chung Tu, "Hypercallbacks," in *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 Tsafrir, "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-23] Mathé Hertogh, Manuel Wiesinger, Sebastian Österlund, Marius Muench, Nadav Amit, Herbert Bos, Cristiano Giuffrida, "Quarantine: Mitigating Transient Execution Attacks with Physical Domain Isolation," in *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, 2023.

[C-22] 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. **Received Distinguished Artifact Award.**

[C-21] Nadav Amit, Michael Wei and Dan Tsafrir, "Dealing with (Some of) the Fallout from Meltdown," in *ACM International Systems and Storage Conference (SYSTOR)*, 2021.

[C-20] Alex Markuze, Shay Vargaftik, Gil Kupfer, Boris Pismenny, Nadav Amit, Adam Morrison and Dan Tsafrir, "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 Tsafrir, "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 Shootdown 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 Tsafrir, 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 Tsafrir, "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 Tasfrir. "Efficient Intra-Operating System Protection Against Harmful DMAs," in *USENIX Conference on File and Storage Technologies (FAST)*, 2015.

[C-5] Nadav Amit, Dan Tsafrir 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 Tsafrir, "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 Tsafrir, "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 Tsafrir, 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-12] Irina Calciu, Muhammad Talha Imran, Nadav Amit. "User-Space Remote Memory Paging", US2022398199A1. 2022

[P-11] Michael Wei, Nadav Amit. "Enforcing Code Integrity Using a Trusted Computing Base", US11500787B2 (granted). 2022

[P-10] Michael Wei, Nadav Amit, Amy Tai. "Early Acknowledgement of Translation Lookaside Buffer Shootdowns", US11321242B2 (granted). 2022

[P-9] Michael Wei, Nadav Amit, Amy Tai. "Consolidating Shared State for Translation Lookaside Buffer Shootdowns", US11341051B2 (granted). 2022

[P-8] Amy Tai, Igor Smolyar, Dan Tsafrir, Michael Wei, Nadav Amit. "Software-Controlled Interrupts for I/O Devices", US11068422B1 (granted). 2021

[P-7] Michael Wei, Dan Tsafrir, Nadav Amit. "Separate Cores to Secure Processes from Speculative Rogue Cache Loads", US10713353B2 (granted). 2020

[P-6] Nadav Amit, Frederick Joseph Jacobs, Michael Wei. "Target Injection Safe Method for Inlining Registration Calls", US10871974B1 (granted). 2020

[P-5] Michael Wei, Marcos Aguilera, Irina Calciu, Stanko Novakovic, Lalith Suresh, Jayneel Gandhi, Nadav Amit, Pratap Subrahmanyam, Xavier Deguillard, Kiran Tati, Rajesh Venkatasubramanian. "File System Interface for Remote Direct Memory Access", US2019179794A1. 2019

[P-4] Nadav Amit, Michael Wei, Cheng Chun Tu. "Safe Execution of Virtual Machine Callbacks in a Hypervisor", US2018321963A1. 2018

[P-3] Nadav Amit. "Trapless Shadow Page Tables", US10114759B2 (granted). 2018

[P-2] Assaf Schuster, Nadav Amit, Dan Tsafrir. "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 2023-07-07*]

[*] Both authors contributed equally