

Jonah Rosenblum

Computer Science and Engineering
University of Michigan

jonaher@umich.edu
jonahrosenblum.com

Research Interests

I am interested in building zero-trust systems that protect data privacy and integrity. My recent works use trusted hardware technology to protect the sensitive data in genome analytics, prevent Rowhammer attacks between VMs via architecture-aware memory allocation, and provide scalable freshness protections via novel trusted memory design. Our new research focuses on extending trusted hardware to ML accelerators and intelligent “time locked” disks that are immutable for set periods of time to prevent ransomware.

Education

University of Michigan

Ph.D. in Computer Science and Engineering

Advisor: Satish Narayanasamy

GPA: 3.99

Ann Arbor, MI

Sep 2022-Current

University of Michigan

M.S. in Computer Science and Engineering

Ann Arbor, MI

Jan 2021-Dec 2021

University of Michigan

B.S. in Computer Science

GPA: 3.83

Ann Arbor, MI

Sep 2017-Dec 2020

Publications

1. Kevin Loughlin, **Jonah Rosenblum**, Stefan Saroiu, Alec Wolman, Dimitrios Skarlatos, and Baris Kasikci. “*Siloz: Leveraging DRAM Isolation Domains to Prevent Inter-VM Rowhammer.*” In **Symposium on Operating Systems Principles (SOSP)**. 2023.

Under Submission

1. **Jonah Rosenblum**, Juechu Dong, Satish Narayanasamy. “*SECRET-GWAS: Confidential Computing for Population-Scale GWAS.*” Under submission in Nature Methods.
2. Juechu Dong, **Jonah Rosenblum**, Satish Narayanasamy. “*VersionVault: Towards Large Capacity Trusted Memory with HW Protection.*” Under preparation for ISCA 2024.

Employment

Google

Virtual

Software Engineering Intern

May-August 2021

Team: GCloud Infrastructure

Analyzed inversion between network and application priority for high-priority Google traffic across all clusters and identified strategies to align less latency sensitive traffic with appropriate QoS.

Google

Virtual

Software Engineering Intern

May-August 2020

Team: Cloud Trace

Worked on open-source telemetry tool OpenTelemetry, implementing graceful shutdown for processes to ensure all traces and metrics are exported.

Software Artifacts

Siloz

github.com/efeslab/siloz

Extension to the Linux/KVM hypervisor to prevent inter-VM Rowhammer attacks.

SECRET-GWAS

<https://github.com/jonahrosenblum/SECRET-GWAS>

Massively parallel privacy-respecting GWAS system.

Teaching

Parallel Computer Architecture (EECS 570)

Ann Arbor, MI

Graduate Student Instructor for Prof. Ronald Dreslinski.

Jan-May 2023

Advanced Operating Systems (EECS 582)

Ann Arbor, MI

Graduate Student Instructor for Prof. Ryan Huang.

Sep-Dec 2023

(Overall, Jonah Rosenblum was effective Q776) - 4.8/5 (5: Strongly Agree; 1 Strong Disagree)

Parallel Computer Architecture (EECS 570)

Ann Arbor, MI

Graduate Student Instructor for Prof. Satish Narayanasamy.

Jan-May 2021

(Overall, Jonah Rosenblum was effective Q776) - 4.8/5 (5: Strongly Agree; 1 Strong Disagree)

Professional Activities

CSEG Security Reading Group Co-Chair

Ann Arbor, MI

Run weekly security group meetings to discuss current research papers.

Jan 2023-Current

Student Applicant Support Program Volunteer

Ann Arbor, MI

Provide prospective Ph.D. students with advice and feedback on applications.

Oct 2023-Current

Grad Mentor Program Volunteer

Ann Arbor, MI

Research/grad program mentor to Master's and Ph.D. students.

Sep 2023-Current

Technical Skills

Programming Languages: Proficient in C, C++, and Python. Familiar with many other object-oriented languages.

Other skills: Kernel development (QEMU/Linux)