756 W. Peachtree St. NW
Atlanta, GA 30308
+1 (224) 200-6674

Jong Sung (Jason) Kim

PhD Candidate in μarch Security @ Georgia Tech

nosajmik@gatech.edu
https://jas0n.kim/
Citizenship: United States

Education

Ph.D. in Computer Science **Aug 2021 - Dec 2025 (est.)**
Georgia Institute of Technology, Atlanta, GA

GPA 4.0 / 4.0. Advised by Prof. Daniel Genkin in the School of Cybersecurity and Privacy.
Proposed Thesis: Towards Hardening Web Browsers Against Microarchitectural Side-channel Threats.

B.S.E. in Computer Science **Sep 2017 - May 2021**
University of Michigan, Ann Arbor, MI

GPA 3.944 / 4.0. Summa Cum Laude and Minor in Biology.

Publications

1. **J. Kim**, J. Chuang, D. Genkin, Y. Yarom.
FLOP: Breaking the Apple M3 CPU via False Load Output Predictions.
USENIX Security Symposium, 2025.
(PDF) (Website)

2. **J. Kim**, D. Genkin, Y. Yarom.
SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon.
IEEE Symposium on Security and Privacy (S&P), 2025.
Distinguished Paper Award.
(PDF) (Website)

3. I. Kang, W. Wang, **J. Kim**, S. van Schaik, Y. Tobah, D. Genkin, A. Kwong, Y. Yarom.
SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism.
USENIX Security Symposium, 2024.
(USENIX) (PDF)

4. H. Taneja, **J. Kim**, J. Xu, S. van Schaik, D. Genkin, Y. Yarom.
Hot Pixels: Frequency, Power, and Temperature Attacks on GPUs and ARM SoCs.
USENIX Security Symposium, 2023.
CSAW Applied Research Competition (North America), 2023, Finalist.
(ArXiv) (USENIX) (PDF)

5. A. Kwong, W. Wang, **J. Kim**, J. Berger, D. Genkin, E. Ronen, H. Shacham, R. Wahby, Y. Yarom.
Checking Passwords on Leaky Computers: A Side Channel Analysis of Chrome's Password Leak Detection Protocol.
USENIX Security Symposium, 2023.
(USENIX) (PDF)

6. **J. Kim**, S. van Schaik, D. Genkin, Y. Yarom.
iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.
ACM Conference on Computer and Communications Security (CCS), 2023.
CSAW Applied Research Competition (North America), 2023, Finalist.
Top Picks in Hardware and Embedded Security, 2024.
(PDF) (Website)

7. **J. Kim**, D. Genkin, K. Leach.
Revisiting Lightweight Compiler Provenance Recovery on ARM Binaries.
International Conference on Program Comprehension (ICPC), RENE Track, 2023.
(ArXiv) (PDF)

8. A. Agarwal, S. O'Connell, **J. Kim**, S. Yehezkel, D. Genkin, E. Ronen, Y. Yarom.
Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.
IEEE Symposium on Security and Privacy (S&P), 2022.
(IEEE Xplore) (PDF) (Website)

Presentations

1. **SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon.**
IEEE Symposium on Security and Privacy (S&P), 2025.

2. **SLAP and FLOP: Unveiling the Existence and Real-World Security Implications of Load Predictors in the Wild.**
Intel Product Assurance and Security (IPAS) Tech Sharing, 2025.

3. **Towards Hardening Web Browsers Against Microarchitectural Side-channel Threats.**
Thesis Proposal at Georgia Institute of Technology, 2025.

4. **iLeakage: An Epilogue.**
Top Picks in Hardware and Embedded Security, 2024.

5. **iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.**
ACM Conference on Computer and Communications Security (CCS), 2023.

6. **iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.**
CSAW Applied Research Competition, 2023.

7. **Checking Passwords on Leaky Computers: A Side Channel Analysis of Chrome's Password Leak Detection Protocol.**
USENIX Security Symposium, 2023. (Video)

8. **Revisiting Lightweight Compiler Provenance Recovery on ARM Binaries.**
International Conference on Program Comprehension (ICPC), 2023.

9. **Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.**
Seminar at the School of Cybersecurity and Privacy, Georgia Tech, 2022.

10. **Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.**
IEEE Symposium on Security and Privacy (S&P), 2022. (Video)

Work Experience

Research Intern **May 2025 - Aug 2025**
Silicon Assurance *Gainesville, FL (Remote)*

- Developed automated methods for detecting cross-domain transient execution attack surfaces on RISC-V CPUs at the RTL level. Project supervised by Dr. Raj Dutta and Dr. Travis Meade.
- Discovered security concerns via static analysis and simulation in a hardware root-of-trust and a cryptographic accelerator, then reported them to vendors.
- Learned techniques and tools: RTL data flow and abstract syntax tree analysis, SystemVerilog assertions, Verilator, Cadence Xcelium, Yosys.

Graduate Research Assistant **Aug 2021 - Dec 2025**
Hardware Security Lab, Georgia Institute of Technology *Atlanta, GA*

- Ongoing research in offensive hardware security and microarchitectural side-channel attacks.
- Publications in top computer security venues (USENIX, IEEE S&P, ACM CCS) and conference talks.
- Low-level CPU reverse engineering, web browser engine exploitation, and kernel programming.

Undergraduate Research Assistant **Jul 2020 - May 2021**
University of Michigan *Ann Arbor, MI*

- Developed a lightweight model to recover the compiler provenance of stripped binaries with Prof. Kevin Leach, with accuracy on par with state of the art and runtime three orders of magnitude faster.
- Presented demos and reports of this model for DARPA's Assured Micropatching Program.

Research Assistant c/o Aptiv PLC **Jan 2020 - Jan 2021**
University of Michigan Multidisciplinary Design Program *Ann Arbor, MI*

- Developed an automated testing framework for evaluating open-source network intrusion detection systems on Aptiv PLC's requirements for low-power/embedded connected vehicle gateways.
- Presented periodic reports on project planning and results, executive summaries, and design reviews under the supervision of mentors at Aptiv PLC and Prof. Shai Revzen.

Professional Service

Program Committee **2026**
USENIX Security Symposium *Baltimore, MD*

Program Committee **2026**
Financial Cryptography and Data Security (FC '26) *St. Kitts*

Program Committee **2025**
Financial Cryptography and Data Security (FC '25) *Miyakojima, Japan*

Teaching

CS 4235/6035, Introduction to Information Security **Jan 2023 - Dec 2023**
Georgia Institute of Technology *Atlanta, GA*

- Graduate Teaching Assistant supervised by Profs. Daniel Genkin and Paul Pearce (Jan 2023 - May 2023).
- Responsibilities as Head TA: agenda writing, exam drafting and testing, project development and testing, course communications, student accommodations, and scheduling reservations.

EECS 388, Introduction to Computer Security **Sep 2019 - May 2021**
University of Michigan *Ann Arbor, MI*

- Undergraduate Instructional Aide supervised by Profs. Peter Honeyman and J. Alex Halderman (Sep 2019 - Apr 2020), Daniel Genkin (Sep 2019 - May 2021), and Z. Morley Mao (May 2020 - Dec 2020).
- Responsibilities (Winter 2020 Evaluations) (Fall 2019 Evaluations)
  - Regular: weekly discussion, office hours, grading, answering student questions over email and Piazza.
  - Seasonal: cheat checking, revising course projects, autograders, and infrastructure.

Graduate Coursework

Network Security and Measurement, Applied Cryptography, Algorithms, Advanced Computer Architecture, Computer Vision, Machine Learning, Advanced Operating Systems, Secure Computer Systems, Web Systems.

Languages and Skills

English (Fluent), Korean (Fluent), C, C++, Rust, WebAssembly, JavaScript, x86-64 Assembly, aarch64 Assembly, Verilog, SystemVerilog, Python, Hardware Reverse Engineering, Microarchitectural Benchmarks, Linux and macOS Kernel Programming, Exploit Development.

Honors

- **Distinguished Paper Award, IEEE Symposium on Security and Privacy (S&P), 2025**
  SLAP was one of 13 distinguished papers, representing less than 1% of all submissions.
- **Top Picks in Hardware and Embedded Security, 2024**
  Top Picks in HES is a workshop co-located with ICCAD 2024, recognizing impactful hardware security papers from the last six years. iLeakage was crowned as Top Picks.
- **CSAW Applied Research Competition (North America), Finalist, 2023**
  iLeakage and Hot Pixels were 2 of 10 selected papers out of 161 submissions. CSAW ARC is a poster competition for the real and potential impact of top-tier security papers.
- **CVE-2023-38599** (NIST NVD)
  CVE assigned by Apple as part of Hot Pixels, where SVG filters on anchor elements could disclose whether a target has visited a link or not previously.
- **Google Chrome Vulnerability Reward Program, 2021**
  Received a bug bounty of 3,000 USD as part of our disclosure for Spook.js, for a bug where HttpOnly cookies would be copied into the rendering process upon opening Chrome's developer tools.
- **EECS Scholar; James B. Angell Scholar; University Honors and Dean's List, 2017-2021**
  Collection of undergraduate awards at the University of Michigan for distinguished academic records.
- **Multidisciplinary Design Program, Summer Research Fellowship, 2020**
  Received a grant of 5,000 USD to develop a test bench for network intrusion detection systems consisting of a local network of Raspberry Pi devices.
- **William J. Branstrom Freshman Prize, 2018**
  Awarded to the top five percent of the freshman class at the University of Michigan.

Projects

- **JasonDrive**: Replica of Google Drive to use as a home file server. (Link)

- **Rosalind**: Platform for competitive bioinformatics programming maintained by the University of California, San Diego. Ranked in top 1% of approx. 74,000 users in Aug 2019. (Link)
- **ZeroSteg**: JavaScript web app to create steganographic text using zero-width Unicode characters. (Link)
- **BitmapParser/EasyLSB**: Lightweight C++ library to read and edit bitmap images, and a program that embeds messages in them using least significant bit steganography. (Link 1) (Link 2)

Last updated September 10, 2025.