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

Foreword

Hello! I am a security researcher interested in hardware security and microarchitectural side-channels. I study the implications of low-level optimizations in cutting-edge CPUs on high-level application security, mainly web browsers due to the sheer amount of secrets they hold and their popularity.

I bring an understanding of microarchitecture, operating systems, and browser execution engines by studying their effects on each other. My works have culminated in patches being introduced to Google Chrome and Apple Safari (the sole allowed browser engine on iPhones/iPads). I am humbled to positively impact the security of billions of users, and hope to continue meaningful work of a similar ethos.

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.

Selected 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.

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.*

3. 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.

4. 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.

5. **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.

6. 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.

Selected 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 Teaching Assistant **Jan 2023 - Dec 2023**
Georgia Institute of Technology *Atlanta, GA*

- CS 4235/6035, Introduction to Information Security. Supervised by Profs. Daniel Genkin and Paul Pearce.
- Responsibilities as Head TA: agenda writing, exam drafting and testing, project development and testing, course communications, student accommodations, and scheduling reservations.
- Organized and updated a digital forensics Capture-the-Flag for the course's final project.

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.

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.

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.

Selected 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.
- **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.

End of Curriculum Vitae, brief version (industry). Last updated September 18, 2025.