

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

Jong Sung (Jason) Kim

PhD Candidate in  $\mu$ arch Security @ Georgia Tech

[nosajmik@gatech.edu](mailto:nosajmik@gatech.edu)  
<https://jas0n.kim/>  
Citizenship: United States

## ABOUT ME

Hello! I am a security researcher interested in hardware security and microarchitectural side-channels. Amid the everlasting pursuit for computing performance, I study the implications of low-level hardware optimizations on protecting information stored in high-level applications, all the way through the layers of abstraction. More specifically, I am curious about how cutting-edge processors affect the security of web browsers, which have become a gold mine for users' credentials and sensitive information.

Through my research, I have developed an understanding of microarchitecture, operating systems, and execution engines in web browsers by observing how they affect each other. This analysis starts with benchmarks for reverse engineering or RTL simulation and dataflow graphs, and ends with memory allocator exploitation and proof-of-concept construction. My work has prompted patches in the process model, rendering engine, and data structure placement in Apple Safari, which is also the sole allowed framework for all iPhone and iPad web browser apps. On Google Chrome, my work has resulted in patches to the extension mechanism, developer tools, and compromised password detection schemes.

Positively impacting the security of billions of users' devices has been my motivation for pursuing a Ph.D., and thus I hope to continue meaningful work of a similar ethos after graduation.

## 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.

## WORK EXPERIENCE

### Research Intern

*Silicon Assurance*

**May 2025 - Aug 2025**

*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

*Hardware Security Lab, Georgia Institute of Technology*

**Aug 2021 - Dec 2025**

*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

*University of Michigan*

**Jul 2020 - May 2021**

*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

*University of Michigan Multidisciplinary Design Program*

**Jan 2020 - Jan 2021**

*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

- **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.

Last updated September 10, 2025.