

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

## EDUCATION

### Ph.D. in Computer Science

Aug 2021 - May 2026 (expected)

*Georgia Institute of Technology, Atlanta, GA*

GPA 4.0 / 4.0. Advised by Prof. Daniel Genkin in the School of Cybersecurity and Privacy.

### 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

- **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](#))
- **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.  
([PDF](#)) ([Website](#))
- 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](#))
- 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](#))
- 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](#))
- **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](#))
- **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](#))

- 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

- **J. Kim.**  
**SLAP and FLOP: Unveiling the Existence and Real-World Security Implications of Load Predictors in the Wild.**  
Presentation at Intel Product Assurance and Security (IPAS) Tech Sharing, 2025.
- **J. Kim.**  
**iLeakage: An Epilogue.**  
Presentation at Top Picks in Hardware and Embedded Security, 2024.
- **J. Kim.**  
**iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.**  
Presentation at ACM Conference on Computer and Communications Security (CCS), 2023.
- **J. Kim.**  
**iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.**  
Poster Presentation at CSAW Applied Research Competition, 2023.
- **J. Kim.**  
**Checking Passwords on Leaky Computers: A Side Channel Analysis of Chrome’s Password Leak Detection Protocol.**  
Presentation at USENIX Security Symposium, 2023. ([Video](#))
- **J. Kim.**  
**Revisiting Lightweight Compiler Provenance Recovery on ARM Binaries.**  
Presentation at International Conference on Program Comprehension (ICPC), 2023.
- **J. Kim.**  
**Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.**  
Presentation at Georgia Tech SCP Security Seminar, 2022.
- **J. Kim.**  
**Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.**  
Presentation at IEEE Symposium on Security and Privacy (S&P), 2022. ([Video](#))

## PROFESSIONAL EXPERIENCE

**Research Intern**  
*Silicon Assurance*

**May 2025 - Present**  
*Gainesville, FL (Remote)*

- Incoming internship for microarchitectural attack surface detection in SoCs at the RTL and gate levels.

**Graduate Research Assistant**  
*Hardware Security Lab, Georgia Institute of Technology*

**Aug 2021 - Present**  
*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.

## PROFESSIONAL SERVICE

**Program Committee**  
*Financial Cryptography and Data Security (FC '25)*

**2025**  
*Miyakojima, Japan*

## TEACHING

**CS 4235/6035, Introduction to Information Security**  
*Georgia Institute of Technology*

**Jan 2023 - Dec 2023**  
*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**  
*University of Michigan*

**Sep 2019 - May 2021**  
*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, Python, Hardware Reverse Engineering, Microarchitectural Benchmarks, Linux and macOS Kernel Programming, Exploit Development.

## HONORS

- **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 April 8, 2025.