756 W. Peachtree St. NW
Coda Bldg. Floor 9 (East)
Atlanta, GA 30308

Jong Sung (Jason) Kim

Updated May 3, 2024

+1 (224) 200-6674
nosajmik@gatech.edu
https://jas0n.kim/

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

- 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.
  (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.**
  iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices.
  Presentation at ACM Conference on Computer and Communications Security (CCS), 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.**
  Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution.
  Presentation at IEEE Symposium on Security and Privacy (S&P), 2022. (Video)

Experience

Graduate Research Assistant **Aug 2021 - Present**
Georgia Institute of Technology *Atlanta, GA*

- Investigated side-channel attack surfaces and corresponding mitigations on webpages and password leak detection mechanisms for the Google Chrome and Apple Safari web browsers with Prof. Daniel Genkin.
- In conjunction, investigated microarchitectural side-channel primitives for Apple processors.

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

- Developed a shallow-learning 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 the above model for DARPA's Assured Micropatching Program.

Research Assistant Sponsored by Aptiv PLC **Jan 2020 - Jan 2021**
University of Michigan Multidisciplinary Design Program *Ann Arbor, MI*

- Evaluated the adaptability of open-source network intrusion detection systems to Aptiv PLC's requirements for connected vehicle gateways as a seven-person team advised by Prof. Shai Revzen.
- Developed automated testing frameworks and test benches, and presented periodic reports, executive summaries, and design reviews to program directors and Aptiv. Responsible for experiments on Snort.

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

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

Honors

- **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 continue research with the University of Michigan and Aptiv PLC over the Summer of 2020. Built a test bench with a 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.

Trivia

- **Fluent** in C/C++, Python (Flask, PyTorch, scikit-learn, SciPy), JavaScript, English, and Korean.
- **Intermediately Proficient** in x86 and ARM assembly, HTML/CSS, Rust, and Spanish.
- Citizenship: United States.

Projects (on GitHub)

- **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)