Last update: 10/21/25

Seonghun Son

5995 Lincoln Drive, Edina, Minnesota, USA

Tel: +1 (515) 708-1373, Email: seonghun@iastate.edu

Website: https://hunie-son.github.io/

RESEARCH INTERESTS

Hardware security with applications of **Artificial Intelligence (AI)** algorithms**.**
Specialization: **AI-driven side-channel attacks** and **mitigations** in microarchitectures.

EDUCATION

Jan. 2021 – Present (expected May 2026) **Iowa State University**
Ph.D. Candidate (ABD), Electrical and Computer Engineering
- MAIS Lab (Advisor: Dr. Berk Gulmezoglu)
  - Hardware security and mitigations
  - AR/VR security
  - Machine learning security
  - Cryptographic systems

Mar. 2012 – Feb. 2019 **Yeungnam University**
B.S., Information and Communication Engineering
- Data Communication Lab (Advisor: Dr. Jin-Ghoo Choi)
  - B.S. Thesis: Night Collision Avoidance System by Detection of Forward Vehicles.

WORK EXPERIENCE

May. 2025 – Present **Seagate Technology**
- Research Intern, Data Trust Team (Advisor: Dr. Hannah Davis)
  - Cryptography and security research on Fully Homomorphic Encryption (FHE) systems and Trusted Execution Environments (TEEs).

May. 2024 – Jul. 2024 **Purdue University**
- Visiting Scholar, PurSec Lab (Advisor: Dr. Berkay Celik)
  - Explored privacy and security issues on AR/VR devices.

Sep. 2020 – Dec. 2020 **National Information Society Agency (NIA)**
- Project Manager, ICT Infrastructure Strategy and Planning Team
  - Demonstration project to implement 5G network collaboration with major carriers at governmental institutions in South Korea (the Ministry of Science and ICT, Sejong City Hall, and Gyeonggi-do Office).
  - Contributed to security and privacy in 5G networks

Dec. 2018 – Oct. 2019 **SL Corporation, Electronics R&D Center**
- Project Manager, Functional Safety Team
  - Established software functional safety standards based on ISO 26262.

Feb. 2016 – Feb. 2019 **Data Communication Lab, Yeungnam University**
- Undergraduate Researcher (Advisor: Dr. Jin-Ghoo Choi)
  - Built the Advanced Driving Assistance System (ADAS) using OpenCV and a machine learning algorithm.
  - Developed gesture detection for light control.

PEER-REVIEWED PUBLICATIONS

[7] **Seonghun Son**, Hannah Davis. "Orthus: Trusted Execution Environment Assisted Fully Homomorphic Encryption," ***In progress***

[6] **Seonghun Son**, Debopriya Roy Dipta, Kat Christofferson, Leslie Kim, Brad Kline, Berk Gulmezoglu. "The Curious Case of Intrinsic Dimensions in Image Datasets for Adversarial Attack Defenses," ***In progress***

[5] **Seonghun Son**, Daniel Moghimi, Berk Gulmezoglu. "User Privacy Attacks through Self-Modifying Code Conflicts," ***Under review***

[4] **Seonghun Son**, Chandrika Mukherjee, Reham Mohamed, Berk Gulmezoglu, Z. Berkay Celik. "Side-channel Inference of User Activities in AR/VR Using GPU Profiling," *Network and Distributed System Security* ***(NDSS), February 2026 (*****acceptance rate = TBD)**
*** Meta Security Bounty Award ***

[3] **Seonghun Son**, Daniel Moghimi, Berk Gulmezoglu. "SMaCK: Efficient Instruction Cache Attacks via Self-Modifying Code Conflicts," *ACM International Conference on Architectural Support for Programming Languages and Operating Systems* ***(ASPLOS), March 2025*** **(acceptance rate = 17.5%)**
*** AMD Security Bulletin: AMD-SB-7024 ***

[2] **Seonghun Son**, Debopriya Roy Dipta, Berk Gulmezoglu. "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection", *Annual Computer Security Applications Conference* ***(ACSAC), December 2023*** **(acceptance rate = 23.3%)**

[1] Muhammad Shafiq, Jin-Ghoo Choi, **Seonghun Son**, Heejung Yu. "CR-MEGA: Mutually Exclusive Guaranteed Access Control for Cognitive Radio Networks", *Future Technologies Conference (****FTC****), ****November 2017****, Vancouver, Canada*

PRESENTATION/TALKS

[9] **Invited Talk**. "Hardware Security and CyMath: How to effectively shine your presentation" *Iowa State University EE5900 seminar****, October 2025***

[8] **Invited Talk**. "Privacy Preserving Machine Learning at the Intersection of Fully Homomorphic Encryption and Trusted Execution Enclaves" *Seagate AI Summit****, October 2025***

[7] **Conference & Poster Presentation**. "SMaCK: Efficient Instruction Cache Attacks via Self-Modifying Code Conflicts," *ACM International Conference on Architectural Support for Programming Languages and Operating Systems* ***(ASPLOS), Rotterdam, Netherlands, April 2025***

[6] **Poster Presentation,** "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection," *9th Midwest Security Workshop* ***(MSW 9), West Lafayette, Indiana, November 2024.***
*** Best Poster Award ***

[5] **Poster Presentation,** "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection," *Center of Academic Excellence in Research* (*CAE-R), National Cybersecurity Education Colloquium* ***(NCEC), St.Louis, Missouri, October 2024***

[4] **Invited Talk,** "Application of Microarchitectural and Machine Learning Security for Reliable Autonomous Driving Systems," *Kyungpook National University****, August 2024***

[3] **Poster Presentation**, "Exploring Intrinsic Dimension Estimation for Enhanced Machine Learning Security," *INSuRE program****,*** *Center of Academic Excellence (CAE) in Cybersecurity Community Symposium****, Louisville, Kentucky, April 2024***

[2] **Conference Presentation**. "DefWeb: Defending User Privacy against Cache-based Website Fingerprinting Attacks with Intelligent Noise Injection", *Annual Computer Security Applications Conference* ***(ACSAC), Austin, Texas, December 2023***

[1] **Workshop Presentation**, "Vehicle crash avoidance systems based on rear lamp detection," *International Workshop on Emerging ICT****, October 2016****.*
*** University President's Award ***

PROPOSALS WRITTEN

Mar. 2025 **BlackHat USA 2025**

Aug. 2024 **Defense Advanced Research Projects Agency (DARPA)**
- Participated in group meetings and experiments.

TEACHING

Feb. 2025 **Guest Lecturer,** Iowa State University
- **EE 2850**, *Problem-Solving Methods and Tools for Electrical Engineering* (Prof. Shakil Ahmed)
  - Served as a guest lecturer for the class of approximately 100 students.
  - Teaching C programming.

Aug. 2024 – Dec. 2024 **Teaching Assistant,** Iowa State University
- **CprE 381**, *Computer Organization and Assembly Level Programming* (Prof. Berk Gulmezoglu)
  - Served as a teaching assistant for the entire semester class with approximately 120 students.
  - Created new homework assignments covering basic microarchitecture concepts and assembly programming questions, graded work, and conducted office hours to explain the fundamentals.

Aug. 2023 – Dec. 2023 **Teaching Assistant,** Iowa State University
- **CprE 381**, *Computer Organization and Assembly Level Programming* (Prof. Berk Gulmezoglu)
  - Served as a teaching assistant for the entire semester class with approximately 120 students.
  - Graded homework associated with basic microarchitecture knowledge with assembly programming questions.
  - Held office hours to explain core concepts.
  - Served as a guest lecturer for one class.

Jan. 2022 – May. 2022 **Teaching Assistant,** Iowa State University
- **CprE 419**, *Software Tools for Large-Scale Data Analysis* (Prof. Goce Trajcevski)
  - Created slides for effectively explaining lab materials.
  - Conducted two lab sessions among four lab sessions and graded homework and lab assignments, serving as head TA.

Aug. 2021 – Dec. 2021 **Teaching Assistant,** Iowa State University
- **SE 421**, *Software Analysis and Verification for Safety and Security* (Prof. Suraj Kothari)
  - Graded homework and explained basic concepts during office hours.

Jan. 2021 – May. 2021 **Teaching Assistant,** Iowa State University
- **CprE 419**, *Software Tools for Large-Scale Data Analysis* (Prof. Goce Trajcevski)
  - Created slides for lab materials.
  - Conducted three lab sessions out of four lab sessions and graded homework and lab assignments.

Mar. 2017 – Dec. 2018 **Teaching Assistant,** Yeungnam University
- **Embedded System** (Prof. Gyu-Sang Choi)
  - Created lab materials and led entire lab sessions with approximately 50 students.
  - Embedded software design
- **Electronic Circuit** (Prof. Jin-Ghoo Choi)
  - Created lab materials and led lab sessions.
  - An electronic circuit design course to support student learning.
- **Logical Circuit** (Prof. Jin-Ghoo Choi)
  - Led lab sessions.
  - Simulated and implemented circuit design using Simulink and implementation.

Jul. 2017 – Aug. 2017 **Instructor,** Can Tho University of Technology, Vietnam
- Programming Languages C/C++
- Korean Language and Culture
  - Served as a team leader in a class with approximately 50 students.
  - Teaching programming languages, the Korean language, and culture.

STUDENTS MENTORING

Feb. 2025 – Present Leslie Kim (Undergraduate student) - Yale University
- Topic: Adversarial attacks on image datasets and their mitigation.

Aug. 2024. – Feb. 2025 Kat Christofferson (Undergraduate student) - Iowa State University
- Topic: Machine learning security and mitigation.

Aug. 2023. – Dec. 2023 Tiffanie Fix (Undergraduate student) - Iowa State University
- Topic: Microarchitectural attacks.

VOLUNTEERS

Oct. 2024 **Youth Cyber Summit,** Iowa Cyber Hub
- Showcasing cybersecurity knowledge led by Dr. Doug Jacobson.

June. 2024 **4H Outreach,** Purdue University
- Computer science outreach program (K-12) led by Jessica Brewer and Dr. Berkay Celik.

May. 2021– May. 2024 **CyMath,** Iowa State University
- Mathematics outreach program (K-12) led by Dr. Namrata Vaswani.
- Sep. 2023-May 2024: CyMath 3.0
  - Sawyer Elementary School, Ames, Iowa (In-person).
- Sep. 2022-May 2023: CyMath 2.0
  - Des Moines Public School (Virtual).
- May 2021-May 2022: CyMath 1.0
  - Moulton Elementary School, Des Moines, Iowa (Hybrid).

Jul. 2017 – Aug. 2017 **World Friend ICT Volunteer,** Can Tho University of Technology, Vietnam (**Team Leader**)
- Taught Programming Languages (C/C++) and Korean Culture.
- National Information Society Agency & Korea International Cooperation Agency.

Jan. 2017 – Jan. 2017 **Educational Service,** Myeongdeok Elementary School **(Team Leader)**
- Taught Science and Math classes.
- Korean Student Aid Foundation.

Jul. 2016 – Jul. 2016 **Educational Service,** Chenogdo Area
- Psychological counseling program for students (K-12) in the Cheongdo Area, South Korea.
- http://www.ksmnews.co.kr/default/index_view_page.php?idx=146832&part_idx=299#09HT

Jan. 2016 – Jan. 2016 **Educational Service**, Hamchang Middle School
- Educational service in rural areas of South Korea.
- Taught Science and IT classes.
- Korean Foundation for the Advancement of Science & Creativity.

Feb. 2012 – Jun. 2012 **Korean Student Ambassador**
- Korean American Friendship Circle, Team 19
- https://www.facebook.com/Korean-American-Friendship-Circle-130490893669558/

SERVICE EXPERIENCES

May. 2024. **Subreviewer**, 29th European Symposium on Research in Computer Security **(ESORICS)**

May. 2023., Aug. 2023. **Subreviewer**, 28th European Symposium on Research in Computer Security **(ESORICS)**

May. 2013 – May. 2015 **Military Service,** Republic of Korea Air Force **(ROKAF)**
- Electric power operations at an Air Force Tower.

CERTIFICATES

Sep. 2025 – Nov. 2025 **Preparing Future Faculty Workshop, Auburn University**
- Selected participant in a competitive virtual workshop series for STEM scholars covering interview strategies, elevator-pitch practice, preparation of cover letters, research, and teaching statements, including hiring perspectives from department chairs.

Aug. 2024 – May. 2025 **Preparing Future Faculty (PFF), Iowa State University**
- Selective program providing an overview of faculty and student life, including differences in expectations, hiring, promotion, and tenure processes across institutions. Moreover, it covered teaching styles and syllabus writing.

Dec. 2024. **Center for the Integration of Research, Teaching, and Learning (CIRTL) Associate Certificate**
- Awarded by the Center for the Integration of Research, Teaching, and Learning (CIRTL), this certificate emphasizes evidence-based teaching strategies, preparing future STEM faculty to enhance student learning through teaching-as-research principles within diverse academic environments.

Oct. 2019. **Electrical Component System Function, Safety Design, and Analysis Training**
- Completed a three-day course on functional safety standards for electronics and semiconductors. The training provided an overview of ISO 26262 concepts and their practical applications in system design and analysis.

Dec. 2016. **Dale Carnegie Leadership Training**
- Completed a program focused on developing effective communication, leadership, and interpersonal skills. The training aimed to enhance both personal and professional success.

GRANTS & AWARDS

Mar. 2025 **Meta Security Bounty Award,** for reporting side-channel vulnerabilities in the Meta Quest series. **($500)**

Feb. 2025 **2025 ASPLOS Student Travel Grant,** ACM International Conference on Architectural Support for Programming Languages and Operating Systems. **($1,000)**

Nov. 2024 **Best Poster Award,** 9th Midwest Security Workshop. (MSW)

Sep. 2024 **Charles B. and Carolyn S. Sidebottom Scholarship in Electrical Engineering ($5,000),** Iowa State University
- Students who are pursuing a career in higher education, specifically in science and technology, as determined by the administering authority.

Jan. 2018 **Department Designated Scholarship ($1,000),** Yeungnam University, South Korea

Mar. 2018, Sep. 2017 **Scholarship for Academic Excellence ($1,200),** Yeungnam University, South Korea