Jang, Jae-Won

Falls Church, VA • Top-Secret Clearance (Active) • Email • Google Scholar • Website

Education

Virginia Tech — **Blacksburg, VA**
Ph.D. in Computer Engineering (GPA: 3.74/4.00) — *Aug 2018 - July 2024*

- *Thesis Title: "Enhancing Software Security through Code Diversification Verification, Control-flow Restriction, and Automatic Compartmentalization"*
- *Research Focus:* Software verification, control-flow integrity, and automated compartmentalization.

University of South Florida — **Tampa, FL**
Master of Science in Computer Engineering (GPA: 3.76/4.00) — *Jan 2014 - Dec 2015*

- *Thesis Title: "Security of Non-Volatile Memories – Attack Models, Analyses, and Counter-Measures"*
- *Research Focus:* Spintronics-based memory security.

University of South Florida — **Tampa, FL**
Bachelor of Science in Computer Engineering (GPA: 3.69/4.00) — *Aug 2009 - Dec 2013*

Work Experience

MITRE Corporation — **McLean, VA**
Senior Cyber Engineer — *Jan 2025 - Present*

- Developed a modular, containerized framework for automated software supply-chain verification, extending TruffleHog to improve secret-scanning and dependency-analysis coverage across source repositories.
- Authored technical documentation and conducted architectural analyses of processor (RISC/CISC) and system design trade-offs to support modernization and performance optimization decisions.
- Led the design and deployment of an automated, non-source-artifact assessment pipeline that enables stakeholders to assess contractor proficiency without requiring proprietary source code.
- Co-led the architectural design and rapid prototyping of containerized Multi-Level Security (MLS) environments. Developed MVPs to validate robust data protection, labeling challenges, and cross-classification data sharing, directly informing trade-space evaluations for critical federated systems.
- Directed automated Infrastructure-as-Code (IaC) analysis workflows and engineered headless system modeling templates (e.g., Cameo), enabling the programmatic extraction of architectural insights from high-level artifacts to conduct predictive risk assessments.

Raytheon — **State College, PA**
Software Engineer — *Dec 2017 - July 2018*

- Supported documentation compliance for unclassified deliverables pending clearance activation.

Intel — **Hillsboro, OR**
Undergraduate Intern — *May 2013 - Aug 2013*

- Development of analytics modules for the AIM Suite project to measure customer engagement with digital displays in the store.
- Evaluated MongoDB integration for production deployment, assessing scalability, data modeling, and system compatibility.

Academia Experience

Research Assistant **Virginia Tech**
Research Assistant, Advisor: Dr. Binoy Ravindran, Blacksburg, VA *Aug 2018 - Dec 2024*

- Designed and deployed compiler- and binary-level security mechanisms to enforce control-flow integrity and automated data compartmentalization across untrusted code modules.
- Integrated the ARM Memory Tagging Extension (MTE) into a compiler toolchain, strengthening runtime memory safety and fault isolation.
- Implemented static and dynamic taint analysis to identify sensitive data paths and compartmentalization targets, automatically rewriting assembly code to isolate protected data regions.

Penn State University **State College, PA**
Teaching Assistant *Aug 2017 - Dec 2017*

- Taught the course CMPSC 122: Intermediate Programming and led discussion sessions.

Penn State University **State College, PA**
Research Assistant, Advisor: Dr. Swaroop Ghosh, State College, PA *Aug 2016 - Aug 2017*

- Researched hardware security and reverse-engineering countermeasures using transistor-level camouflaging and logic obfuscation.

University of South Florida **Tampa, FL**
Research Assistant, Advisor: Dr. Swaroop Ghosh, Tampa, FL *Aug 2013 - July 2016*

- Researched hardware security primitives leveraging CMOS and spintronic memory technologies, exploring MTJ-based techniques to improve PUF stability and STT-MRAM robustness against magnetic/thermal attacks.

Publication

- **sMVX: Multi-Variant Execution on Selected Code Paths.**
  Sengming Yeoh, Xiaoguang Wang, Jae-Won Jang, and Binoy Ravindran. ***MIDDLEWARE***, 2024.
- **Verification of Functional Correctness of Code Diversification Techniques.**
  Jae-Won Jang, Freek Verbeek, and Binoy Ravindran. ***NFM***, 2021.
- **Threshold-Defined Logic and Interconnect for Protection against Reverse Engineering.**
  Jae-Won Jang, et al. ***TCAD***, Impact Factor: 2.9, 2020.
- **MTJ-based State Retentive Flip-Flop with Enhanced-Scan Capability to Sustain Sudden Power Failure.**
  Anirudh Iyengar, Swaroop Ghosh, and Jae-Won Jang. ***TCAS-I***, Impact Factor: 5.1, 2019.
- **Overview of Circuits, Systems, and Applications of Spintronics.**
  Swaroop Ghosh, Anirudh Iyengar, Seyedhamidreza Motaman, Rekha Govindaraj, Jae-Won Jang, et al. ***JETCAS***, Impact Factor: 1.6, 2018.
- **Spintronic PUFs for Security, Trust and Authentication.**
  Anirudh Iyengar, Kenneth Ramclam, Swaroop Ghosh, Jae-Won Jang, and Cheng-Wei Lin. ***JETC***, Impact Factor: 0.83, 2017.
- **Threshold Defined Camouflaged Gates in 65nm Technology for Reverse Engineering Protection.**
  Anirudh Iyengar, Deepak Vontela, Ithihasa Reddy, Swaroop Ghosh, Syedhamidreza Motaman, and Jae-Won Jang. ***ISLPED***, 2018.

- **Investigation of Magnetic Field-Based Attacks on Magnetoresistive Random Access Memory.**
  Alexander Holst, Jae-Won Jang, and Swaroop Ghosh. ***ISQED***, 2017.
- **Performance Impact of Magnetic and Thermal Attack on STTRAM and Low-Overhead Mitigation Techniques.**
  Jae-Won Jang and Swaroop Ghosh. ***ISLPED***, 2016.
- **Security and Privacy Threats to On-Chip Non-Volatile Memories and Countermeasures.**
  Swaroop Ghosh, Nasim Khan, Asmit De, and Jae-Won Jang. ***ICCAD***, 2016.
- **Self-Correcting STTRAM under Magnetic Field Attacks.**
  Jae-Won Jang, Jongsun Park, Swaroop Ghosh, and Swarup Bhunia. ***DAC***, 2015.
- **Design and Analysis of Novel SRAM PUFs with Embedded Latch for Robustness.**
  Jae-Won Jang and Swaroop Ghosh. ***ISQED***, 2015.

Skills

Languages: Assembly (ARM, x86/64), C, C++, Haskell, Python, Rust, TypeScript, SQL

AI & LLMs: Prompt Engineering, AI-Assisted Development (Claude), Groq API, LLaMA 3, Whisper, Structured Output Parsing (Zod)

Web & Cloud: Next.js (App Router), React, Tailwind CSS, PostgreSQL, Prisma ORM, Vercel, Clerk

Systems & Security: angr, Binary Ninja, CMake, Docker, dyninst, GDB, Ghidra, Intel PIN, LLVM/Clang, QEMU, Radare2