Jae-Won Jang

Falls Church, VA
jw-jang@outlook.com | jwj.fyi | Google Scholar

Active Top Secret Clearance

Education

Virginia Tech — Blacksburg, VA
Ph.D. in Computer Engineering — Aug 2018 – Jul 2024
Dissertation: *Enhancing Software Security through Code Diversification Verification, Control-flow Restriction, and Automatic Compartmentalization*.

University of South Florida — Tampa, FL
Master of Science in Computer Engineering — Jan 2014 – Dec 2015
Thesis: *Security of Non-Volatile Memories – Attack Models, Analyses, and Counter-Measures*.

Bachelor of Science in Computer Engineering — Aug 2009 – Dec 2013

Technical Skills

Languages: Assembly (ARM, x86/64), C, C++, Go, Haskell, Python, Rust, SQL
Security Research: Automated compartmentalization, control-flow integrity, software verification, static and dynamic taint analysis
Analysis & Tooling: angr, Binary Ninja, CMake, Dyninst, GDB, Ghidra, Intel PIN, LLVM/Clang, QEMU, Radare2
Infrastructure & Protocols: AMQP 1.0, Docker, GitLab, Podman, PostgreSQL, Protobuf

Professional Experience

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

- **Architecture & Prototyping:** Co-led the design and end-to-end prototyping of a containerized AMQP 1.0 data ingestion pipeline involving Protobuf, Rust, Go, Docker/Podman, and PostgreSQL.
- **Sponsor Engagement & Technical Trade-space:** Presented architectural prototypes and sponsor-aligned demonstrations directly to primary DoW sponsors; these engagements informed technical trade-space decisions and prototype priorities.
- **AI-Assisted System Analysis:** Led applied research and prototyping of an LLM-based pipeline using MCP, Python, and OpenCode to extract structured, code-traceable architecture knowledge from legacy codebases, supporting software assessment and modernization.
- **Artifact-Based System Modeling:** Prototyped the analysis of binaries, SBOMs, configurations, and delivery artifacts to assess architectural and technical risk without proprietary source code. Proposed extracting these results into textual notation (e.g., SysML v2) for headless, reproducible system modeling to reduce subjectivity for systems engineers.
- **Supply-Chain Security:** Designed and deployed a modular, containerized software supply-chain verification framework. Extended TruffleHog with a custom file detector that extracts import statements from repository files, cross-checks them against SBOMs, and flags missing, unused, and internal-only packages. Combined dependency analysis with embedded-secret and configuration-risk detection.

Research Experience

Virginia Tech — Blacksburg, VA
Research Assistant; Advisor: Dr. Binoy Ravindran — 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 ARM Memory Tagging Extension (MTE) into a compiler toolchain to strengthen runtime memory safety and fault isolation.
- Implemented static and dynamic taint analysis to identify sensitive data paths and compartmentalization targets, with automated assembly rewriting to isolate protected data regions.

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

- Researched hardware security and reverse-engineering countermeasures using transistor-level camouflaging and logic obfuscation.
- Developed a threshold-voltage-based technique to conceal gate interconnects and logic identities.

University of South Florida Tampa, FL
Research Assistant; Advisor: Dr. Swaroop Ghosh Aug 2013 – Jul 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.
- Completed a tape-out of a padframe for prototype fabrication.

Selected Publications

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*.

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, 2019*.

Overview of Circuits, Systems, and Applications of Spintronics
Swaroop Ghosh, Anirudh Iyengar, Seyedhamidreza Motaman, Rekha Govindaraj, **Jae-Won Jang**, et al. *JETCAS, 2018*.

Spintronic PUFs for Security, Trust and Authentication
Anirudh Iyengar, Kenneth Ramclam, Swaroop Ghosh, **Jae-Won Jang**, and Cheng-Wei Lin. *JETC, 2017*.

Security and Privacy Threats to On-Chip Non-Volatile Memories and Countermeasures
Swaroop Ghosh, Nasim Khan, Asmit De, and **Jae-Won Jang**. *ICCAD, 2016*.

Design and Analysis of Novel SRAM PUFs with Embedded Latch for Robustness
Jae-Won Jang and Swaroop Ghosh. *ISQED, 2015*.

Self-Correcting STTRAM under Magnetic Field Attacks
Jae-Won Jang, Jongsun Park, Swaroop Ghosh, and Swarup Bhunia. *DAC, 2015*.

Full publication list: Google Scholar.

Earlier Industry & Teaching Experience

Raytheon State College, PA
Software Engineer Dec 2017 – Jul 2018

- Supported documentation compliance for unclassified deliverables.

Penn State University State College, PA
Teaching Assistant Aug 2017 – Dec 2017

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

Intel Hillsboro, OR
Undergraduate Intern May 2013 – Aug 2013

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