

Amir Rahmati, Ph.D., CISSP

🌐 amir.rahmati.com | ✉ amir@rahmati.com | 🔗 linkedin.com/in/ameerr | 🎓 Google Scholar | 📞 413-331-9438 | 📍 New York, NY

Cybersecurity and privacy leader with 15+ years of experience spanning security architecture, product security, generative AI/ML security, privacy engineering, threat and fraud defense, and applied security R&D across industry and academia. Combines deep technical expertise with experience building and directing security programs, advising executives and engineering organizations, and translating advanced research into deployable technologies adopted in commercial platforms.

- **Security Architecture & Product Leadership:** Led architecture and security reviews for Samsung Knox, Samsung Pay, and St. Jude Medical connected-device platforms, spanning IAM, trusted computing, secure enclaves, platform hardening, and privacy-by-design.
- **AI & Agentic System Security:** Led research and development across generative AI/LLM security, adversarial ML, model robustness, and AI system attack surface. Experience threat-modeling AI systems across training pipelines, model boundaries, and deployed inference, covering prompt injection, data leakage, excessive agency, and supply chain risk, and defining security controls across the AI/ML lifecycle.
- **Technology Transfer & Industry Adoption:** Developed security and privacy architectures adopted by Apple, Google, and Samsung, translating research in access control, system integrity, and platform security into commercial technologies.
- **Executive Advisory & Risk Leadership:** Advised fintech, AI, and critical-infrastructure organizations on security architecture, zero-trust design, threat modeling, technical due diligence, and regulatory alignment, translating technical risk into prioritized mitigation roadmaps and architecture decisions. Served on the *SUNY AI Task Force* on Data Privacy & Security.
- **Program, Team & Talent Leadership:** Built and led a \$14M+ externally funded security and privacy portfolio and developed a sustained talent pipeline of 50+ graduate and undergraduate researchers, with alumni advancing to teams at Apple, Meta, IBM Research, Microsoft, Amazon, Bloomberg, and other leading organizations.

EXPERIENCE

- **Assistant Professor, Computer Science Department, Stony Brook University** 2018 – Present
 - Built and directed an applied security and privacy R&D lab, defining research roadmaps across IoT and AR/VR platforms, AI/ML systems, and threat and fraud detection.
 - Translated fundamental systems security research into deployable commercial technologies, resulting in access-control and privacy architectures adopted in *Apple Vision Pro*, *Google Android OpenXR*, and *Samsung Knox*.
 - Secured and managed \$14M+ in research funding as PI/co-PI from federal agencies (*AFOSR*, *ONR*) and industry leaders (*Meta*, *RevBits*, *NVIDIA*), defining multi-year research roadmaps.
 - Mentored and directed 50+ graduate and undergraduate researchers, building a talent pipeline that placed alumni into top industrial research labs and engineering teams at *Apple*, *Meta*, *IBM Research*, *Microsoft*, *Amazon*, and *Bloomberg*.
 - Contributed to open-source projects including IBM's *Adversarial Robustness Toolbox (ART)* and led the institutional initiative securing the NSA Center of Academic Excellence in Cybersecurity Research (CAE-R) designation.
- **Consulting and Advisory Engagements** 2018 – Present
 - Led end-to-end security architecture reviews and advised fintech, AI, and critical infrastructure organizations on cloud zero-trust architectures, threat modeling, and regulatory alignment (NIST CSF, ISO/IEC 27001, SOC 2, MITRE ATT&CK).
 - Delivered technical due diligence and threat assessments for C-suite and engineering executives, translating vulnerability findings into prioritized mitigation roadmaps and hardened system designs.
- **System Architect, KNOX Security, Samsung Research America** 2017 – 2018
 - Architected security features and conducted design reviews for Samsung Knox Enterprise, shaping trusted platform capabilities, defense-in-depth controls, and system-level protections.
 - Led security and tokenization architecture reviews for Samsung Pay, validating secure enclave integration and compliance with EMVCo/PCI-DSS payment standards.
 - Engineered privacy-preserving data aggregation models for location-based services, applying differential privacy and data minimization to protect user telemetry while preserving analytics utility.
- **Senior System Engineer, St. Jude Medical (acquired by Abbott)** 2016 – 2017
 - Rearchitected authentication, trust, ID management, and access control for embedded and cloud-connected medical devices.
 - Defined the product security roadmap across embedded and cloud-connected platforms, ensuring compliance with industry best practices and FDA pre-market cybersecurity guidelines.
- **Research Assistant, University of Michigan** 2011 – 2017
 - Developed system security mechanisms across hardware, embedded, mobile, IoT, and cloud environments, focusing on access control, information-flow enforcement, end-to-end integrity protection, and privacy-preserving data collection.
 - Identified fundamental security flaws in medical-device, smart-home, trigger-action, and approximate-computing systems.

EDUCATION

- **Ph.D. in Computer Science and Engineering**, University of Michigan 2017
- **M.S.E. in Computer Science and Engineering**, University of Michigan 2014
- **B.Sc. in Computer Engineering**, Sharif University of Technology 2011

HONORS & AWARDS

- **Certified Information Systems Security Professional (CISSP)** 2026
- **Young Academic Inventor Award**, National Academy of Inventors (NAI) 2026
- **National Academy of Inventors (NAI) & IEEE Senior Member** 2025, 2024
- **CSAW Applied Research Competition Finalist** 2024
- **Leadership Award**, Department of Computer Science, Stony Brook University 2024
- **Research & Presentation Awards** NDSS'24, ICCPS'24, HealthSec'24, IEEE S&P'21, SecDev'18
- **Industry Research Awards** RevBits'26, Meta'22, Facebook'20, NVIDIA'18

SELECTED PATENTS

- An Advanced Privacy Filter for System Logs on Computing Devices 2026
- System and Method for Flow-based Architecture 2020

SELECTED PUBLICATIONS (8.5K+ CITATIONS)

- Subscribe for Free: Security Analysis of the iOS In-App Subscriptions Under Review
 - ★ Discovered two vulnerabilities in Apple in-app purchase framework
- Anansi: Scalable Characterization of Message-Based Job Scams Under Review
 - ★ Adopted by defDone in RTidx
- AppScopes: Fine-grained Access Control for App Collaboration on Android IEEE TPS-ISA 2026
 - ★ Adopted by Samsung in Knox SDK
- Obfusc8: LLM-Augmented PowerShell Obfuscations SecDev 2025
- The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams WWW 2025
- Biosignal Authentication Considered Harmful Today USENIX Security 2024
 - ★ Revealed inherent weakness of PPG/ECG/SCG/BCG-based authentication methods to spoofing attacks
- Zero-One Attack: Degrading Closed-Loop Neural Network Control Systems using State-Time Perturbations ICCPS 2024
- Erebus: Access Control for Augmented Reality Systems USENIX Security 2023
 - ★ Adopted by Apple in Vision Pro and Google in Android OpenXR in 2024
- Accelerating Certified Robustness Training via Knowledge Transfer NeurIPS 2022
- Valve: Securing Function Workflows on Serverless Computing Platforms WWW 2020
- Robust Physical-World Attacks on Deep Learning Visual Classification CVPR 2018
 - ★ First physical-world adversarial attack on ML models
- Decentralized Action Integrity for Trigger-Action IoT Platforms NDSS 2017
 - ★ Adopted by Samsung in Knox Configure for Wearables

EXPERTISE

- **Security & Privacy Strategy:** Security architecture, privacy engineering, privacy by design, threat modeling, risk assessment, security and privacy reviews; NIST CSF 2.0, NIST Privacy Framework, ISO/IEC 27001/27701, SOC 2, STRIDE, LINDDUN, DPIA/PIA
- **Product, Application, & Cloud Security:** Product security, secure design, cloud and distributed systems security, API security, DevSecOps, vulnerability management, platform hardening; OWASP ASVS/SAMM, zero trust
- **Identity, Access, & Data Protection:** IAM, authentication and authorization, RBAC/ABAC, PAM, federated identity, PKI, key management, secrets management, data governance, data minimization; GDPR, HIPAA, CCPA/CPRA
- **Detection, Response, & Cyber Defense:** Incident response, detection engineering, logging and monitoring, threat intelligence, abuse/scam detection, SIEM/SOAR; MITRE ATT&CK/ATLAS
- **Generative AI/ML Security & Applied Automation:** Adversarial ML, LLM-assisted security automation, intelligent triage models, automated remediation logic, privacy-preserving machine learning, secure generative AI/ML system architectures
- **Technical Domains & Tooling:** Mobile security, IoT security, cloud and distributed systems, AR/VR privacy, cyber-physical systems, AI/ML security, adversarial machine learning; proficient in Python and C/C++; prior experience in Java, SQL, MATLAB, and Verilog