Gavin Black, PhD

AI/ML Security Researcher | Active Clearance

Home Page | GitHub | LinkedIn | [redacted] | [redacted]

Experience

LEIDOS | Principal Research Scientist | Solutions Architect

2020 – Current | Remote

- ➔ Cyber Automation PI: Oversee multiple AI-focused security research projects.
  - Direct >10 research scientists and engineers across projects.
  - Regular communication and demonstrations to senior leadership.
  - Planning, engagement tracking, and budgeting for project management.
  - Deliver prototypes, contract proposals, and publications.
  - Agentic security direction, focused on increased AI threat landscape.
  - General AI/ML weakness research for tool-enabled LLMs.
  - Automation of offensive and defensive cyber operations through agents.
  - Retrieval augmented generation (RAG) security and limitations.
  - Cross-team collaboration with corporate IT and business sectors.
  - Agile/Scrum lead experience using Jira and Confluence.
- ➔ CyberAI Security Researcher: Lead for specific project efforts
  - Multiple first-author publications and conference talks.
  - Proof of concept implementations in AWS and Air Force environments.
  - Developing reinforcement learning based network attack models.
  - Firmware library fuzzing and resource usage feedback signals.
  - Reviewing research papers and positioning new efforts.
  - Applying SoTA techniques and models (hugging-face, llama.cpp, etc.)

MITRE | Lead Cyber Systems Engineer

2008 - 2020 | Bedford, MA

- ➔ Cyber Security SME: Task lead for next generation Air Force (AF) platforms.
  - Working closely with AF counterparts to modernize multiple platforms.
  - Evaluating contractor proposals, progress, and development processes.
  - Adding security auditing and analysis tools to PlatformOne DevOps pipeline.
  - Technical lead responsible for modernizing CVE backend.
  - Development lead for statistical Crown Jewel Analysis (CJA) tooling.
- ➔ Engagement Lead: Department tech direction, hiring, placement
  - Responsible for team of seven full-time engineers
  - Bedford campus intern manager, supporting 20+ interns per year
  - Securing work opportunities and business development for staff.
  - Performance reviews and career direction for staff and interns.
- ➔ iOS Application Security: PI for iMAS OSS security research
  - Created open source library with 700+ GitHub stars, 200+ forks.
  - Assembly-level reverse engineering of protection mechanisms.
- ➔ GPS Ground Control Systems: Prototype SV control/ecosystem

LOCKHEED MARTIN | GPS Software Engineer

2006 – 2008 | Gaithersburg, MD

- ➔ Communications security: Encryption drivers for satellite payloads in-transit.
- ➔ Ephemerides Updates: Kalman filter development for broadcast updates.
- ➔ Software developer: New features and bug fixes for GPS ground stations.

PURDUE UNIVERSITY | Teaching Assistant

2003 – 2006 | Lafayette, IN

- ➔ Laboratory Instructor: Administered computer science lab courses.
- ➔ Computer Science Undergraduate Onboarding Coordinator

Education

DAKOTA STATE UNIVERSITY

PhD in Cyber Defense (2024)

Dissertation: Resource Fuzzing w/ ML

UNIV. OF MASSACHUSETTS

MS in Mathematics (2014)

Focus: Applied and Computational

PURDUE UNIVERSITY

B.S. in Computer Science (2006)

Dual Major in Mathematics

Skills

SECURITY

LLM Code Security • Agentic Vulns • Model Hardening • Red-Teaming • AI/ML-driven Security Testing • Kali • Fuzzing • Reverse Engineering •IDA

SOFTWARE

Python • C/C++ • Linux/Shell • Docker • Jupyter • OpenAI/Anthropic APIs • LaTeX • PyTorch • TensorFlow • Hugging Face • Ray • Scikit • Agno

MACHINE LEARNING

LLMs • Transformers • Reinforcement Learning • Prompt Engineering • VAE

FRAMEWORKS

NIST (AI, 800) • FedRAMP • CWE • CVE • MITRE ATT&CK

Publications

LLM Code Weakness
IEEE Transactions
Code Generation Security

LLM Assisted Fuzzing
IEEE Access
Coverage Improvements

Security Invariance Measures
IEEE ICNC 2024
Augmentation w/ SW Signals

Fuzzing Distributions
IEEE Access
LLM Sample Uniqueness

Firewall Obfuscation Dataset
IEEE Data Descriptions
Semi-Synthetic Network Attacks