Aarno Labs, LLC — Capability Statement

AI-Enabled Cybersecurity R&D | Software Assurance | Compiler and Performance Engineering

Company Overview

Aarno Labs is a Boston-based small business founded by MIT researchers, specializing in software assurance, AI-enabled cybersecurity R&D, and compiler engineering with $35M+ in combined funding. We blend program analysis, formal verification, compilers, and AI/LLM workflows to protect, modernize, and optimize software. As both a prime and subcontractor, we deliver impactful results through advanced research, custom tools, and integrated workflows.

Core Capabilities and Services

Software and supply-chain assurance: Automatically analyze source code, binaries, firmware, and third-party components for vulnerabilities and suspicious behavior. Enrich software bills of materials (SBOMs), assess reachability, investigate root causes, and generate reproducing tests.

Vulnerability remediation and patch assurance: Rapid and high-assurance workflows for creating source or binary patches, manually or AI-generated. Create and verify targeted binary patches without source code or build environments. Assess vendor updates and verify fixes against specified behavior.

AI-enabled security automation: Build custom static and dynamic analyses, instrumentation, test-generation systems, and evaluation infrastructure. Combine program analysis, testing, verification, and AI-assisted techniques into automated vulnerability-investigation workflows.

Performance-oriented compilation and LLVM engineering: Extend LLVM toolchains for automatic parallelization, performance analysis and optimization, GPU compilation, and backend development. Support AI-guided optimization with rigorous analysis and validation.

Memory-safe modernization: Automated memory safety instrumentation and C-to-Rust translation and validation tools to support migration to memory-safe software. Apply program analysis, compiler transformations, optimizations, and testing to assess behavior preservation during modernization.

Applied R&D and workflow integration: Build customer-specific prototypes and workflows integrating Aarno-developed technology, third-party open-source tools, and AI/LLM services. Provide documentation, training, technical handoff, and scoped maintenance.

Differentiators

High-assurance automation

Apply program analysis and formal verification to automate tasks requiring costly specialist effort, including work on legacy and embedded systems.

Research depth with hands-on delivery

PhD researchers from MIT, Stanford, Columbia, and Penn who translate advanced methods into implemented, evaluated, and integrated software.

AI + Formal Assurance

Combine LLMs with program analysis and formal verification to generate, check, and refine software solutions against requirements.

Open-source foundations and transferability

Maintain and extend open-source platforms to support sustainable technical review, reuse, and handoff without lock-in to proprietary software.

Contact Michael Gordon, PhD — Cofounder | info@aarno-labs.com | www.aarno-labs.com

Small business | UEI: E24AMLJUN625 | CAGE: 71TF0

Selected Past Performance



Best-in-class, independently evaluated performance on large DARPA & ARPA-H research grants. Multiple commercialization and productization transitions.

Selected completed results and ongoing funded research:

High-Assurance Binary Patching (DARPA Assured Micropatching): Built a high-assurance patching workflow; independent evaluators produced a correct binary patch in 20 minutes—the fastest result in the program's Phase II evaluation. Productized with ARPA-H funding as a commercial Binary Ninja plugin.

Runtime Application Security (DARPA OPS-5G): Developed runtime protections against compromised third-party libraries; secured In-Q-Tel Emerge commercialization funding and formed spin-off company to develop the software supply-chain security product.

Application Vetting (DARPA APAC): Developed Android security analysis incorporated into Raytheon BBN's Artemis SAST product and delivered to the FBI through that system.

Medical Device Security (ARPA-H DIGIHEALS & UPGRADE): Under a DIGIHEALS subcontract to STR, developed a verified patient-monitor vulnerability fix without source code and assessed the vendor's firmware update. Under UPGRADE, developing automated patches, network filters, and assurance reports.

Vulnerability Remediation and Triage (DARPA E-BOSS): Developed an open-source memory-safety instrumentation tool for legacy C/C++ applications incorporated into AI-driven automated remediation pipeline. Remediated more vulnerabilities than all other performers for E-BOSS final evaluation.

Automated Exploitation (DARPA HACCS): Developed automated proof-of-vulnerability (PoV) generation system. Delivered the most automatically-generated PoV inputs across all performers for DARPA HACCS.

C-to-Rust Translation (DARPA TRACTOR): Developing translation and validation tools to enable low-cost and high-assurance migration of C software to safe Rust.

Sponsors and Partners

Government research sponsors: DARPA, ARPA-H, NSF.

Research and industry partners: MIT CSAIL, STR, Brown University, University of Utah, University of Illinois Urbana-Champaign, Raytheon BBN.

Company and Contracting Information

Aarno Labs, LLC | Small business | 11 employees | Formed in Delaware in 2013
Headquarters: 330 Washington Street, 4th Floor, Boston, MA 02109
UEI: E24AMLJUN625 | **CAGE:** 71TF0 | **NAICS:** 541715 | **DCAA Approved** Accounting System & Rates
Engagements: Prime contracts and specialized research and engineering subcontracts.
Security: No current facility clearance.
Contact: Michael Gordon, PhD — Cofounder | info@aarno-labs.com | www.aarno-labs.com