Frank Lynam
410-501-7378 – lynamf@gmail.com – frank.lynam.website – github.com/frank-lynam

Safety, Security and Software Engineering. Over a decade of experience in analyzing, improving, developing and delivering innovative, complex and large-scale solutions that extend the boundaries of “the art of the possible” even in restrictive, highly-regulated environments. Leader of mutli-disciplinary teams that delivered nuclear safety and cyber-security solutions, as well as sensitive AI/ML integrations.

Skills

Cyber Operations Specialist

- Attack graph automation and reverse engineering for decomposition and monitoring integration
- Working experience with NIST SP 800-53 access controls, as well as ATT&CK and D3FEND
- Analysis experience with authentication, special-purpose encryption systems and insider threat
- Security clearance, TS/SCI with polygraph

Software Development Expertise

- Python (including TensorFlow, Torch, Numba, Cython, FastAPI, Flask)
  - Experienced developing distributed monitoring, AI/ML and numerical methods tools
- Javascript (vanilla, React, SvelteJS, NodeJS, Electron)
- C, C++, Java, Bash, Terraform, CloudFormation, Jenkins, DevSecOps, CI/CD, Agile
- Delivered user-facing tools and capabilities worldwide in Windows, Linux, LXD, AWS and Docker

Front-Line Leadership

- Led small teams (3-5 developers) for several multi-customer research and development efforts
- Project management, staffing, budgeting and customer interface (requirements elicitation)
- Active mentorship of cyber and software junior staff who have grown into technical lead roles

Roles

Expert Software Developer, ReindeerTek 2023 – Present
Supporting federal government projects and development efforts

- *Enhanced Reliability.* Technical lead for stabilizing and securing a critical, high security legacy system (>10k daily users), going from weekly outages to 100% uptime by identifying failing interfaces and developing custom analysis tools and monitoring capabilities used by multiple teams.

- *Modernized Architecture.* Led development of architecture changes for a high-throughput, multi-source intelligence analysis capability to secure and modernize deployment and integrate CI/CD tooling, increasing reliability and resilience, and eliminating maintenance outages.

- *Integrated Legacy Systems.* Reverse engineered legacy technologies and unsupported COTS software to enable secure enterprise service integrations across a high-security network, to include accessibility improvement and x509 certificate support.

Systems Security Engineering Researcher, MITRE Corporation 2016 – 2023
Defined and led systems security research priorities across the company

- *Led Security Research Initiatives.* Led multiple internal and customer-focused research and analysis efforts, including applied cyber and supply chain attack path analysis and other special-purpose needs. Led MITRE TRACE distributed Monte Carlo attack path analysis research project (github.com/mitre/trace), collaborating with NSA D3FEND and ATT&CK teams.

- *Cyber Defense Strategy.* Led small analysis team and crafted a multi-year, high-impact cyber defense strategy for national defense nuclear weapons control systems, focusing on detailed risks from the highest capability nation state threat actors. Addressed globe-spanning systems analysis for network-based, cyber-physical and RF-based intrusions as well as personnel, insider and supply chain threats across operations and the defense industrial base.

- *AI/ML Safety and Security Tools.* Lead developer for rapid-deployment deepfake and AI-generated-content detection and analysis tooling for a critical intelligence customer.

Nuclear Engineer, US Navy 2011 – 2016
Government project manager for multiple surface and subsurface warship nuclear systems

- *Lead Engineer, OHIO Replacement (COLUMBIA Class).* Project manager for power electronics and stealth research and development programs, reactivity control equipment and cybersecurity. Coordinated among multiple laboratories, shipyards and industry partners, overseeing a fully custom operating system, software, firmware and hardware system delivering novel operational capabilities meeting both demanding reactor criticality safety needs and emerging cyber risks.

- *Cybersecurity "Tiger Team" Member.* Part of the initial core team focused on transitioning reactor systems to NIST standards, and developing internal practices for cyber risk and incident response.

- *Enterprise Business Process Software.* Developed internal electronic workflow tool (SQL, ASP.NET, Word integration) transitioning off existing paper-based engineering review across multiple departments at Naval Reactors headquarters (~500 staff, to include senior military staff).

- *Nuclear Engineer, Operating Aircraft Carriers*. Lead for reactor and propulsion control systems technology and operation. Real time support for fleet reactor issues across all Atlantic / Mediterranean theater aircraft carriers.

Education

BS Electrical Engineering, SUNY Maritime College 2008 – 2011
STA-21 Program, 4.00/4.00, Valedictorian, APPA DEED research grant, 5-year degree in 3 years

Qualified Navy Nuclear Operator, S8G AFR Prototype 2006 – 2008
First to qualify (of ~30 cohort), Ranked 1/~260 Nuclear Power School, 1/~30 Nuclear 'A' School