GRISL: Protecting and Hardening Scientific Use Of Software Libraries With GRISL

PI: Justin Cappos (New York University) Co-PIs: Yuchen Zhang (New York University)

Project Overview

- Harden unsafe scientific libraries (C/C++) without changing scientists' code.
- Use lightweight userspace isolation to prevent crashes and data corruption.
- Deliver pre-hardened libraries with ~1% performance overhead.
- Improve reliability of HPC, AI/ML, and scientific workflows nationwide.

Cybersecurity Innovation

- High performance, backwards-compatible, legacy library isolation for HPC.
- Instead of: failures in one library can crash entire workflows or corrupt results.

Approach For Transitioning the Innovation

- Strong community relationships: build on 15+ years of secure software deployments (TUF, Uptane, in-toto, etc.)
- Open-source release with strong community engagement and maintenance plan.

Benefits to Scientific Cyberinfrastructure

- Society needs science to be accurate. Libraries (e.g., ML/AI) often are performance optimized and have flaws.
- Significant reduction in crashes and silent data corruption in scientific workflows.
- Improved reproducibility and reliability of computational research results.

Risks Versus Potential For Advances

- **Risks:** Integrating isolation into complex, performance-critical libraries may expose unforeseen compatibility / performance issues. Adoption requires sufficient POC / momentum.
- **Payoff:** Increased reliability, safety, and reproducibility for HPC, AI/ML, and scientific computing. This framework can be applied to AI, etc. use across domains.

Evaluating and Demonstrating Transition

- Metrics for success:
  - Substantial improvements to ~10 widely used libraries.
  - Minimal performance overhead (~1% target).
  - Reduction in crashes, data corruption, and debugging time reported by users.
- Integration into major HPC and cloud research platforms (JupyterHub, Open OnDemand, CloudLab, Chameleon). **Open-source implementation and community**. Prebuilt packages available via Conda, pip, and Spack for easy installation.

Programmatic Details

- **3-year project** starting **January 2026.**
- Led by **New York University (NYU).**
- Working with Intel, EngageLively, w/ plans to engage others moving forward.

This material is based upon work supported by the National Science Foundation under Grant No. 2531027