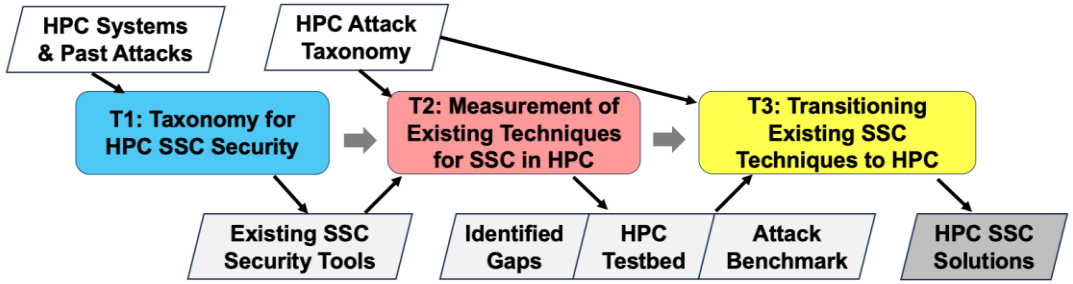
# HPCSafeChain: Software Supply Chain Security in High-Performance Computing: Understanding, Evaluation and Transition

PI: Mu Zhang (University of Utah) Co-PIs: Heng Yin (UC Riverside), Xunchao Hu (DeepBits)




- Scientific computing relies on open-source software vulnerable to software supply chain (**SSC**) **attacks** and **vulnerabilities**
- The **applicability** of SSC security research to HPC is **underexplored**, given HPC's limited C/C++ package management, rapid AI package evolution, and weaker installation controls.

## Cybersecurity Innovation

- Novel Attack Taxonomy for HPC SSC
- First HPC testbed/benchmark for evaluating SSC security solutions
- Validating and transitioning SSC security techniques in HPC

## Approach For Transitioning the Innovation

- Collaboration with real-world HPC centers: CHPC, HPCC, INL
- A student co-advised by the HPCC team and given cluster admin rights
- Use collaborators' feedback to verify the fidelity of our taxonomy, testbed, attacks and solutions

## Benefits to Scientific Cyberinfrastructure

- HPC admins: identifying outdated, vulnerable packages
- HPC users: detecting compromised, malicious artifacts
- HPC (security) researchers: developing a realistic HPC security testbed integrated with a comprehensive attack suite benchmark.

## Risks Versus Potential For Advances

- Risk 1: Completeness of attack surface exploration
- Risk 2: Challenges for admins/users in adopting SSC security techniques
- Mitigation: Prioritize high-profile attacks; focus on automation
- Payoff: A practical solution to counter existing threats, which severely compromise the integrity and confidentiality of scientific computing tasks and data.

## Evaluating and Demonstrating Transiton

- Expert/community's feedback on our taxonomy, testbed and attack benchmark
- Evaluating applicability of SSC security solutions using our HPC SSC security testbed and attack suite

## Programmatic Details

- 3-year project started on January 2026
- Led by University of Utah and with UC Riverside and DeepBits
- Unfunded collaborations with CHPC at UofU, HPCC at UC Riverside and Idaho National Laboratory

Award No. 2530911