NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST High-Performance Computing Security Working Group

Yang Guo, NIST

For 84th HPC User Forum

April 10th, 2024

Date

Outline

- Introduction to High-performance Computing (HPC) Security Working Group (HPCSec-WG)
- NIST SP 800-223: High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture
- Joint NIST-NSF HPC Security Workshop
- Summary

High-performance Computing Security

- High-performance computing (HPC) serves as a fundamental computing infrastructure
- Cybersecurity plays a pivotal role in HPC by protecting against misuse, ensuring availability, and safeguarding data integrity
- NIST established the HPC Security Working Group (WG) in 2016
- Main tasks:
  - Lead and orchestrate the development of security guidance
  - Listen to the HPC security community's needs, foster synergies, and respond to the feedback from the community at large

Securing HPC Is Difficult

- HPC is shared resources; High availability is important
- **Reluctant to make changes if changes negatively impact system performance**
- **Wide range of vendors with various architectures and scales**
- **Security tool vendors are behind the curve**
- Ongoing authorization requires continuous monitoring and validation

- **RMFs didn't consider HPC's unique requirements**
- **Not-applicable/reasonable controls:**
  - SI-3(1): antivirus in HPC system; scanning not feasible given large storage size
  - CM-7(5): account for all software; impossible
  - CM-11(1): not allow user installed software; monitor every node
- Security guidance has no implementation details
- Interpretation of RMF controls can be very different

- **New hardware, new security requirement**
- Container support
- Compute node sanitization
- Diskless booting
- Sensitive data staying on the system
- **Handle different security requirements of different projects**
- Hardware-based security

HPC security challenges and Issues
(from HPC Security WG minutes)

Sharing Security Best-Practice Is Difficult, Too

- Design and architecture evolve over time
- Applications they run and missions they support are different
- HPC systems, applications run on them, and data used may have own unique security requirements
- Compliance requirement is different
- Institutions often operate in silos
- Some information is deemed to be sensitive and cannot be shared in public
- Complexity and uniqueness impede the sharing of security solutions and knowledge

Build the Foundation for HPC Security

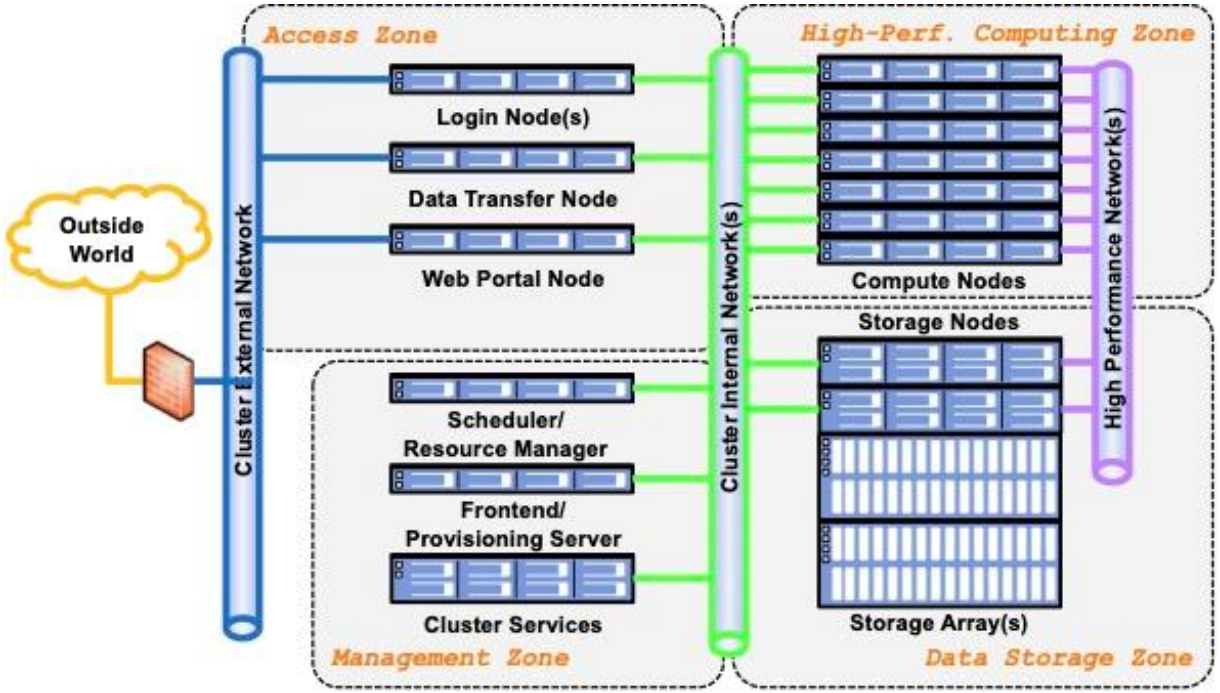
- Introduce an HPC reference architecture that captures common features of HPC systems and serves as a foundation for a system lexicon
- Analyze HPC architecture, conduct threat analysis, and report on the current security posture
- Publish results as a NIST Special Publication and makes best-practice recommendations
- Establish a foundation for High-Performance Computing (HPC) control overlay development

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST SP 800-223: High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture

HPC Reference Architecture

- Four function zones:
  1. Access zone
  2. Management zone
  3. High-Performance computing zone
  4. Data storage zone
- The nodes in a function zone collectively provide services



- Different function zones provide different services, and face different threats
- Different security guidance may apply to individual zones

High-performance Computing Zone

- **Provide key services designed to run parallel jobs at scale**
- A pool of compute nodes connected by high-speed networks
  - number of nodes ranges from a few nodes to thousands of nodes
- High throughput, low latency networking connects compute nodes and parallel file systems – *InfiniBand, Omni-Path, Slingshot, Ethernet*
- Non-high-performance network connects with the management zone
- Often equipped with hardware accelerators to speed up specific applications – *Smart NIC, GPU, TPU*, …
- Installation and configuration of the software stacks are cluster-wide, centrally managed, and controlled by the management zone

High-Performance Computing Zone Threats

- Shared resources
  - exploitation of multi-tenancy environments is a major threat, e.g., side-channel attacks, user data/program leakage, etc.
- Accidental misconfiguration, software bugs introduced by user-developed software, system abuse by running applications not aligned with the HPC mission, …
  - extreme resource consumption, performance degradation, or the outage of the HPC system entirely include
- Container escape, side-channel attacks, and DoS can also be threats if virtualization technologies – such as containers are used
- Accelerators, high-performance interconnects, special protocols, direct memory access between nodes may not be thoroughly tested
  - their speed, novelty, and complexity make monitoring and detecting suspicious activity difficult
  - May bypass the kernel and the protections provided by the kernel

HPC Threat Analysis: Key HPC Security Characteristics and Use Requirements

- Tussles between performance and security
  - HPC security is valuable only to the extent that it does not significantly slow down the HPC system
- Varying security requirements for different HPC applications
  - NIST SP 800-53, CUI (NIST SP 800-171), HIPAA, …
- Limited resources for security tools
- Open-source software and self-developed research software
  - Susceptible to open-source software supply chain threats, low software quality, …
- Data security

Achieving Security While Maintaining HPC Performance

- Security often comes with undesirable performance penalty
- Several effective ways to balance performance and security
  - conduct tests to measure the performance penalty of security tools, and encourage performance-aware tool design
  - incorporate security requirements in the initial HPC design rather than as an afterthought
  - avoid “one size fits all” security: zone based security controls

Collaborators

- **A collaborative, cross-agency effort:** *14 authors from 11 institutions*

- NIST: **Yang Guo, Ramaswamy Chandramouli (Mouli)**
- AWS: **Lowell Wofford**
- DoD/HCPMP: **Rickey Gregg, Gary Key**
- Laboratory for Physical Sciences: **Antwan Clark**
- Los Alamos National Laboratory: **Catherine Hinton**
- MIT Lincoln Laboratory: **Andrew Prout, Albert Reuther**
- Oak Ridge National Laboratory: **Ryan Adamson**
- Sandia National Laboratories: **Aron Warren**
- University of Alabama: **Purushotham Bangalore**
- University of Florida: **Erik Deumens**
- University of South Carolina: **Csilla Farkas**

Joint NIST-NSF HPC Security Workshop

- Joint effort with the National Science Foundation (NSF)
  - Bring in SC centers for open science research communities
- In-person, with over 100 attendees
- > 10 Super Computer Centers (SC) present their security practice
- Continue to collaborate with NSF on future workshops
  - 4th HPC Security Workshop is scheduled for May 2024 at Wichita State University

3rd High-Performance Computing Security Workshop

Executive Order 13702 established the National Strategic Computing Initiative (NSCI) to maximize the benefits of high-performance computing (HPC) for economic competitiveness and scientific discovery. Security is an essential component of HPC. NIST HPC Security Working Group (WG) has been leading the effort to create a comprehensive and reliable security guidance for HPC systems. As part of the Working Group mission and to reach greater HPC scientific community, NIST, in collaboration with National Science Foundation (NSF), will host the 3rd High-Performance Computing Security Workshop on March 15-16, 2023. The workshop aims to listen to community's needs and feedbacks, report and reflect on the ongoing activities at HPC Security WG, and define and discuss future directions with stakeholders from industry, academia, and government.

Agenda –

WORKSHOP

March 15 - 16, 2023

In-Person Event EST
National Cybersecurity Center of Excellence
9700 Great Seneca Highway
Rockville, Maryland

Registration is now closed.

Coronavirus (COVID-19) Guidelines for NIST Conferences and Meetings

TECHNICAL CONTACTS

Dr. Yang Guo, yang.guo@nist.gov

Dr. Robert Beverly, rbeverly@nsf.gov

4th High-Performance Computing Security Workshop

Introduction:

Executive Order 13702 established the National Strategic Computing Initiative (NSCI) to maximize the benefits of high-performance computing (HPC) for economic competitiveness and scientific discovery. Security is an essential component of HPC. NIST HPC Security Working Group (WG) has been leading the effort to create a comprehensive and reliable security guidance for HPC systems. The workshop aims to listen to community's needs and feedbacks, report and reflect on the ongoing activities at HPC Security WG, and define and discuss future directions with stakeholders from industry, academia, and government.

Summary

- Securing HPC systems is difficult
  - Due to size, performance requirements, diverse and complex hardware, software, and applications, varying security requirements, and the nature of shared resources
- NIST SP 800-223 standardizes and facilitates the information and knowledge-sharing of HPC security
- The collaborative effort and consensus among major players, including agencies/national labs/industries, have expanded the impact of the initiative
- The development of the HPC security control overlay is ongoing
- **Welcome to join the HPC Security WG**

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

THE END

HPC Security Compliance Requirement Difference

- HPC systems belonging to US government are required to conform to NIST RMF (Risk Management Framework)
  - ❑ Apply NIST SP 800-53 security overlay
  - ❑ Authorization and audit are required

- HPC systems funded by NSF has no formal compliance requirement
  - ❑ NSF primary focus is on supporting NSF's science and discovery mission
    - ➢ proponent of open science, and recognizes the unique environments, instruments, users, and experiments within our research community
  - ❑ Incentivize cybersecurity rather than mandate / regulate / audit
  - ❑ Promote cybersecurity best-practice

Joint NIST-NSF HPC Security Workshop

- Two-day, March 15th to 16th, 2023, in-person workshop hosted at NCCoE
- Num of Attendees: ~100
  - Government: 41%
  - Universities: 33%
  - Industries: 21%
  - Others: 5%
- CISO/Security Engineer/SCA/Architect/System Engineer: ~50%
  - Good representation of HPC security community