High-Performance Computing Security Workshop

NIST

Gaithersburg, Maryland

Building 101, Green Auditorium

March 27-28, 2018

AGENDA

	Tuesday, March 27, 2018 9:00 a.m. – 5:00 p.m.	
9:00 – 9:10	Chuck Romine (NIST)	**Welcome to NIST and the Information Technology Laboratory**
9:10 – 9:20	Ketan Mehta (NIST)	**Workshop Goals**
9:20 – 9:40	Matt Barrett (NIST)	**Presentation:** NIST Cybersecurity Framework
9:40 – 10:10	Victoria Pillitteri (NIST)	**Presentation:** NIST Risk Management Framework (SP 800-37 Rev. 2) and NIST Security Controls (SP 800-53 Rev 5)
10:10 – 10:20	Krisa Rowland (NSA)	**Presentation:** Conclusions from HPC Insider Threat Workshop
10:20 – 11:10	Moderator: Lee Beausoleil (NSA)	**Panel:** Expert Panel on Implementation of Security on HPC System. - Adam Slagell (National Center for Supercomputing Applications) - Scott Campbell (Lawrence Berkeley National Lab) - Alexander Perry (GreenRose, LLC) - Cyrus Proctor (Texas Advanced Computing Center)
11:10 – 11:30	**Networking Break**	
11:30 – 12:45	**Breakout Session 1:** *"HPC Use Cases / Workflow"*	
12:45 – 1:45	**Lunch Break**	
1:45 – 2:45	**Breakout Session 2:** *"HPC Architectures: Define HPC System, Identify Baseline(s)"*	
2:45 – 3:00	**Networking Break**	
3:00 – 4:15	**Breakout Session 3:** *"Threats to HPC Systems"*	
4:15 – 5:00	**Report Out:** Regroup and Discuss the Outcome of Day 1 Breakout Sessions	

	Wednesday, March 28, 2018 9:00 a.m. – 5:00 p.m.	
9:00 – 9:30	Sean Peisert (Lawrence Berkley National Laboratory)	**Keynote.** Importance of Planning for Security in HPC Systems.
9:30 – 10:45	**Breakout Session 4:** *"HPC Security Implementations: Impediments and Solutions"*	
10:45 – 11:05	**Networking Break**	
11:05 – 12:20	**Breakout Session 5:** *"Application of NIST Cybersecurity and Risk Management Framework"*	
12:20 – 1:20	**Break for Lunch**	
1:20 – 2:30	**Breakout Session 6:** *"Implications of Added Security: Performance, Compliance, Usability, Cost"*	
2:30 – 2:50	**Networking Break**	
2:50 – 3:50	Dr. Mouli (NIST)	**Presentation:** HPC in Virtualized Platforms: Current Status
	Dr. Michaela Iorga (NIST)	**Presentation:** NIST Work on Cloud Security
	Erik Deumens (University of Florida)	**Presentation:** Case Study: Applying NIST Risk Management Framework to Controlled Unclassified Information on HPC
3:50 – 4:45	**Report Out:** Discuss the Outcome of Breakout Sessions	
4:45 – 5:00	**Wrap up**	

DESCRIPTION OF EACH BREAKOUT SESSION:

Breakout Session 1: HPC Use Cases / Workflows

Summary The goal of this session is to identify important HPC use cases and develop high level workflows. Workshop participants explore use cases that identify HPC user communities in diverse sectors including academic, commercial, public infrastructure, and national security. HPC includes all use cases requested by users who need more capacity, capability, availability, accessibility, and/or performance than they can get from their laptop or desktop/office devices. This includes storing, accessing, sharing data sets with collaborators and using them while "on the road". It also includes processing and visualizing these data sets with high-performance graphics capabilities, GPU accelerated as needed, without the need to transfer large data sets to or have powerful graphics capabilities on the end stations.

Objectives Provide a list of single-sentence use cases that identify HPC workflows relevant to HPC users.

Breakout Session 2: HPC Architecture: Define HPC System, Identify Baselines(s)

Summary For the use cases and workflows identified in Session 1, the workshop participants will develop one or more notional HPC architecture that fits the use cases. Although we know that HPC architectures are horizontal: One powerful platform with advanced capability and performance to handle a wide variety of projects and activities, the workshop participants will identify all storage, network, and computational components and its inter-networking. Also, identify any security components used in the existing architectures or perhaps the workshop participants may recommend appropriate security components to be inserted in the architecture.

Objectives List architectural elements that are special to HPC and those that are shared with all computing infrastructure. Identify those elements that define a core HPC system as a baseline.

Breakout Session 3: Threats to HPC Systems

Summary Traditional threat detection and analysis methods, such as scanning files for malware, are ineffective within HPC infrastructures due to their complexity and variability across systems. Additionally, intentionally-based threats (e.g. social engineering) are particularly harmful because the overall goals of the user of interest also need to be considered. Given the scenario of use cases posed in the "HPC Use Cases / Workflows Session", this session will aim to qualify the level of threat to each particular use case via answering the following three questions: 1.) "What threats should we try to manage?", 2.) "How are they different from or similar to threats to general purpose workstations", 3.) "What short and long terms impacts does this threat impose?".

Objectives Provide a prioritized list of threats that we care about in HPC. The results of this session will help to provide a framework for properly itemizing threats and their associated impacts for various HPC applications within academia, industry, and government.

Breakout Session 4: HPC Security Implementations: Impediments and Solutions

Summary This session will explore the HPC security solutions that are relevant and have been implemented and security solutions that are desired and / or required but are not feasible to implement perhaps due to performance issues, may cost too much, or lack of availability of products that meet standards / requirements. The participants will be asked to share their domain expertise, come up with principal pragmatic security strategies that are invariant across scale and determine structure for further discussion and consensus building process.

Objectives Provide a list of criteria to judge solutions to meet certain security goals versus risk, performance, and usability.

Breakout Session 5: Application of NIST Cybersecurity and Risk Management Framework

Summary The NIST Cybersecurity Framework, Risk Management Framework, and SP 800-53 Security and Privacy Controls provide control outcomes. To implement and maintain a system, or series of systems, with rapidly changing capabilities and capacities as in HPC, it is important to identify a set of control instruments (policies, business processes, architectural principles, and technical controls) that are used by the system owner, designer, and operator to meet the control outcomes. The workshop participants will engage in a discussion of what controls are appropriate for HPC use cases from Session 1 or the HPC architectures from Session 3. Threats identified for the use cases in Session 2 may also be used to selectively choose NIST control instruments.

Objectives Provide a list of control instruments relevant to HPC systems, architectures, and workflows.

Breakout Session 6: Implications of Added Security: Performance, Compliance, Usability, Cost

Summary We are looking for a cost effective balance adapted to the needs and workflows of the HPC community to manage risk and balance security, compliance, auditability, usability, and performance nimbleness. Once it has been decided what NIST security controls are applicable to HPC systems (based on previous sessions), it is important to know if these controls will impede the progress of HPC systems. This session will explore in what ways the NIST security controls brings complexity to the HPC systems. The session discussion will be focused on the impact of new security controls on performance, compliance, usability, and cost of updating (retrofitting existing) HPC system. How difficult or easy it would be to implement these security controls. Can we add more hardware storage or processing capability to counter the performance hit with new security controls? Will there be additional testing and compliance needed to meet the security requirements? Will it require complete overhaul of an HPC system? How can we determine the worthiness of applying additional security controls?

Objectives Build a decision table for HPC system operators listing the issues relevant to deciding where the balance lies.