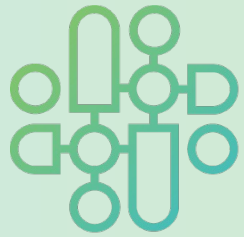


SC23
Denver, CO | i am hpc.

Second International Workshop Security in High Performance Computing (S-HPC 2023)

Andrés Márquez on Behalf of the S-HPC Committee

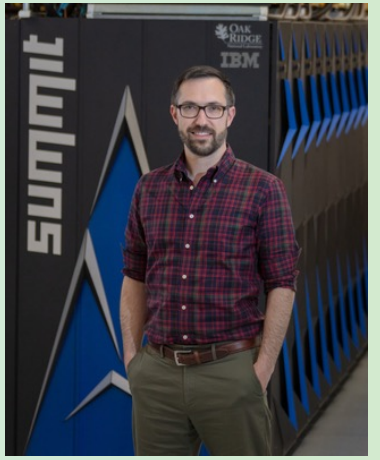
Motivation

- Security in HPC
  - Performance is everything: Still true?
    - HPC is a critical resource driving innovation: What about securing that innovation?
    - Considering a tilt towards data analytics/ML: What about privacy, confidentiality?
- Is this just an operational challenge exercise or is there more to it?
  - Isn’t HPC pushing the HW and SW envelopes? Doesn’t that merit special consideration?

Program

Time	Event	Presenter
02:00 – 02:02 PM	Welcome	
02:02 – 03:00 PM	Distinguished Speaker: The ‘S’ in HPC stands for Security	Ryan Adamson (ORNL)
03:00 – 03:30 PM	Break	
03:30 – 03:55 PM	Invited Talk: Thoughts on security for CXL-3.x-GFAM clusters with embedded computing	Craig Warner (Micron)
03:55 – 04:20 PM	Invited Talk: Information Security Controls Prioritization – SABSA for HPC	Nicolas Erdody (Open Parallel LTD)
04:20 – 04:40 PM	Research Paper: Analyzing the Performance Impact of HPC Workloads with Gramine+SGX on 3rd Generation Xeon Scalable Processors	Shinobu Miwa (University of Electro-Communications)
04:40 – 05:28 PM	Panel: RMF for HPC and RDT&E	Rickey Gregg (DoD HPCMP)
05:28 – 05:30 PM	Closing Remarks	

Distinguished Speaker: Ryan Adamson (ORNL)



Title: The 'S' in HPC Stands for Security

Abstract: HPC systems are designed to meet peak performance and scalability goals, but today's security guidance and tools are designed for enterprise infosec. This means that it is quite difficult to secure HPC resources without impacting performance goals. In this talk, we will examine the key security differences between enterprise systems and the common features of HPC environments. We will also discuss a new HPC Security NIST publication (currently draft) and touch on how secure 'open science' research really needs to be. From there, we will explore emerging trends to keep track of such as scientific workflows that span multiple security domains and whether trusted computing and zero trust models can be adapted to HPC. Finally, we will demonstrate one example of a zero-day vulnerability found on a previous #1 top 500 system (disclosed and patched in 2018) to help motivate broader action to put an 'S' in HPC.

Bio: Ryan leads the HPC Security and Information Engineering Group at the Oak Ridge Leadership Computing Facility (OLCF). His group is responsible for delivering highly-scalable and reliable security services and telemetry platforms to the high-performance computing resources and staff at the OLCF. He holds a MS in Computer Science from the University of Tennessee. He has taught several computer architecture, hardware, and systems administration courses at Tennessee Tech and Pellissippi State Community College and has held the GIAC Exploit Researcher and Advanced Penetration Tester certification (GXPN). Ryan is currently pursuing a PhD in Engineering from Tennessee Tech University and is focusing on the challenges overlapping both HPC and Security disciplines.

Thanks to …

- Center for Advanced Technology Evaluation **(CENATE)** from Pacific Northwest National Laboratory for their support in this effort.
- Funded through the Department of Energy's Advance Advanced Scientific Computing Research
- Dedicated to better understand the applicability of novel architecture concepts to scientific discovery
- Provides a proving ground that is advancing scientific computing, artificial intelligence, machine learning, and cybersecurity through assessment and evaluation of advanced technologies and concepts
- Established in launched in 2015 with collaborations with University of Florida, University of California Riverside, Worchester Polytechnic Institute, North Carolina State University, among others.

- Memory has always been a second-class citizens
  - Concepts in memory research and tools (PIM / dataflow designs, memory profilers, memory centric runtimes, etc) have been "in the works" for decades
- Novel architectures has exposed the need orchestrate memory more carefully due to the challenges of heterogeneity: i.e., the limitations of current memory hierarchies
- A novel view is being taken across several research domain, especially exemplify in the PNNL's **AMAIS** project
  - It aims to provide end to end solution to memory challenges using a comprehensive approach to software, codesign hardware, and accelerators
- Currently collaborators with major industry partners with full support of the DOE ASCR office of science

Thanks also to the NIST **working group in High Performance Computing Security** for all their help and support in organizing this event: https://csrc.nist.gov/projects/high-performance-computing-security

Thanks, and Hope to see you next year!!!

- ***Steering Committee***:
  - Andres Marquez, Pacific Northwest National Laboratory
  - Yang Guo, NIST
  - Kevin J. Baker, Pacific Northwest National Laboratory
  - Sean Peisert, Lawrence Berkeley National Laboratory
  - Nael B Abu-Ghazaleh, University of California Riverside

- ***Organizational Chairs:***
  - **Program Chairs:** Purushotham Bangalore (University of Alabama); and Amro Awad (North Carolina State University)
  - **Diversity Chair:** Cimone Wright-Hamor (Pacific Northwest National Laboratory)
  - **Publication Chair:** Yuede Ji (University of North Texas)
  - **Web Chair:** Joseph Manzano (Pacific Northwest National Laboratory)
  - **Publicity Chair:** Sankha Dutta (Pacific Northwest National Laboratory)
  - **Regional Chairs:** Shuaiwen (Leon) Song (university of Sydney, Microsoft); and Haipeng Cai (Washington State University)