Keeping high-performance computers cybersecure

August 28 2019, by Genoa Blankenship

Credit: Pacific Northwest National Laboratory

Pacific Northwest National Laboratory is leading efforts to address next

generation computing's critical role in protecting the nation from cybersecurity threats.

PNNL's Center for Advanced Technology Evaluation (CENATE) sponsored a roundtable earlier this month to bring the high-performance computing community together and tackle cybersecurity challenges.

"This roundtable enabled researchers from the computer science and cybersecurity domains to come together and map out open fundamental research questions in a critical first step in fulfilling the Department of Energy goal of developing a science of cybersecurity," said CENATE director Kevin Barker.

CENATE, a Department of Energy (DOE) Office of Advanced Scientific Computing Research (ASCR)-funded project, is exploring fundamental research into the science of cybersecurity for emerging and advanced computer architectures. As DOE's mission grows and remains reliant on high-performance computing (HPC), CENATE is in the position to lead exploration of cybersecurity methodologies and challenges. CENATE convened the roundtable as part of that research leadership role.

The roundtable provided an opportunity to exchange information among a diverse cross-section of researchers, developers and practitioners in engineering, hardware security, and computing. Attendees representing DOE, Lawrence Berkeley National Laboratory, PNNL, Washington State University, University of Texas at Arlington, University of California Riverside, University of Illinois, and University of Florida participated in the event.

The roundtable discussions aimed to identify research targeting existiing and future HPC systems and architectures. The goal also was to define gaps in current research ranging from developing cybersecurity

techniques to protecting HPC systems. Discussion topics included the role of modeling and simulation techniques in complex systems and HPC as a platform for performing advanced mathematics for cybersecurity applications.

Machine learning techniques provided a roundtable focus area, particularly, how to identify patterns of misuse of large-scale HPC systems and "rogue" or malicious workloads that may be using HPC resources without authorization. Ang Li, a PNNL researcher in the HPC group, provided a demonstration during the roundtable that examined the use of machine learning to differentiate between authorized and unauthorized workloads that may be running on modern graphics processing unit (GPU)-enabled HPC compute nodes.

HPC systems are an important component of national infrastructure and a fundamental rethinking is needed to protect the country from economic and strategic attacks, Barker said.

David Manz, a PNNL cyber security researcher and team lead, had a more pointed question for the group to unearth: "How much of a snowflake is HPC in cybersecurity?"

Robinson Pino, ASCR Program Manager for CENATE, encouraged the roundtable group to think about research and new technologies that could improve security from a privacy and integrity standpoint.

The CENATE organizers' next step will be to develop a research plan for addressing challenges in cybersecurity research for emerging computing platforms that serve the DOE mission, Barker said. Feedback will be given to the DOE program offices to enable collaborative research.

CENATE offers collaborative access to its technology within the high-performance computing community. The CENATE leadership team

would like to hear from researchers interested in collaborations in cybersecurity research. For more information about potential collaborative opportunities, contact Kevin Barker.

Provided by Pacific Northwest National Laboratory