U.S. Department of Energy

Office of Science

Advanced Scientific Computing Research Program

DOE Cybersecurity R&D Challenges for Open Science Workshop

Marriott Bethesda North Conference Center
24-26 January 2007
http://www.dsd.lbl.gov/Workshops/CyberWorkshop/

Gary M. Johnson

Gary.Johnson@science.doe.gov

Workshop Charge

- Identify the research needs and opportunities associated with cybersecurity for open science.
- Focus on those needs particularly associated with DOE supercomputing, user facilities, high-speed networks, laboratories, and other open collaborative science stakeholders.
- Include a discussion of how open science cybersecurity differs from general cybersecurity and explore the implications this may have for cybersecurity research activities.
- Prepare a preliminary letter report within one week of workshop completion and follow with a full report within 60 days of workshop completion.

Organizing Committee

Deb Agarwal	Lawrence Berkeley National Laboratory
Walter Dykas	Oak Ridge National Laboratory
Mike Robertson	Office of Science Information Officer

Participation

- 55 registered for this invitation-only workshop
- Participants from:
  - 14 DOE Laboratories
  - 8 Non-DOE Organizations
  - DOE Headquarters

Workshop Structure

- Welcoming remarks by workshop organizers and DOE representatives
- Workshop consisted primarily of breakout sessions and had very few plenary talks
- Details at http://www.dsd.lbl.gov/Workshops/CyberWorkshop/

Disclaimer

This is a preview of *potential* coming attractions…

The workshop final report has not yet been submitted. Thus, all findings reported here should be viewed as preliminary and subject to change.

Proposed Research Directions

1. Multi-Site Situational Awareness and Response
2. Managing Authentication and Attribute-Based Authorization
3. Software, Data, and Systems Assurance
4. Cybersecurity Policy Specifications

Conclusions

- The diversity, heterogeneity, and scope of the open science environment bring unique cybersecurity challenges.
- The software that supports modern open science and provides high-speed data transfers, specialized computations, distributed computational capabilities, virtual organization support, and experiment control is not available from commercial sources.
- The high performance environment, global user population, and diversity of custom applications and software in the open science environment make protecting the facilities and detecting malicious attacks uniquely challenging.
- The expertise and tools developed in a cybersecurity research program for open science would have a broad impact and would establish the Office of Science as a leader in cybersecurity - not only within the open science community, but in the wider cybersecurity community as well.
- While the benefits of a cybersecurity research program for open science are fairly clear, additional effort is required to adequately define its priority research directions.

Postscript

The Office of Science (SC), in collaboration with DOE's Office of Electricity Delivery and Energy Reliability (OE), is planning the following workshop:

Cybersecurity Research Needs for Open Science

Further details are pending