2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities

Designing Cybersecurity Programs in Support of Science

September 30 - October 2, 2013

Hilton Arlington (near NSF) - Arlington, VA

- AGENDA -

Updated September 25th, 2013

Organizers: James Marsteller, Craig Jackson, Von Welch
jam@psc.edu, scjackso@indiana.edu, vwelch@indiana.edu

The theme for the 2013 NSF Cybersecurity summit is ***Designing Cybersecurity Programs in Support of Science***. This theme suggests a number of challenges to be addressed: How do we build a community for sharing experiences and supporting continuity between projects? What are the goals of a cybersecurity plan for the vast variety of NSF projects; what are the key motivations, assets and threats? How are we similar to and different from other communities addressing cybersecurity (e.g, higher education, government, private sector), and how do we relate to them?

The ideal summit attendee can speak to the needs of the science mission of their project or community has for cybersecurity, as well as the social, human resource, policy and other challenges for creating a cybersecurity program that leaves their community comfortable those needs have been met.

Day 1 (Sep 30): Optional parallel tutorials in the afternoon (1-5pm)

- Open to all attendees; registration required
- Registration Opens: 12pm
- Afternoon Coffee Break: 3:00pm - 3:30pm
- **Building a Cybersecurity Program (CTSC team)**
  - *Location: Da Vinci Room*
  - *Description*: This tutorial will provide principal investigators, project leaders, and project managers planning, building and operating scientific cyberinfrastructure with a method for accessing their security needs, documenting an action plan for addressing those needs, and quantifying resource requirements. Specifically, this tutorial will provide an overview and process for developing a cybersecurity plan for scientific computing projects. Discussion will focus on why security is crucial to an organization and things that senior management can do to establish a proactive stance on cybersecurity. This tutorial will present an overview of security issues that face NSF cyber infrastructure projects. The intent is to give PI's and managers an understanding of these issues and tools to address them.
- **Bro Network Intrusion Detection (Seth Hall, Sam Oehlert, Dr. Adam Slagell)**
  - *Location: Matisse Room*

  - *Description*: Bro is a stateful, protocol aware open source high speed network monitor with applications as a next generation intrusion detection system, real time network discovery tool, historical network analysis tool, real time network intelligence, and dynamic active response. Originally developed by Vern Paxson, he now leads the core team of developers/researchers at both the International Computer Science Institute in Berkeley, CA and the National Center for Supercomputing Applications in Urbana-Champaign, IL. Bro provides a security team with logs of highly structured data about their network, a turing complete scripting language through which they can interact with real time stateful network events, and flexible open interfaces through which Bro can be programmed. Pragmatically able to interface with the entire network stack, Bro includes support for IPv6, tunneled traffic, SSL and more. In this presentation we present multiple case studies and are releasing their corresponding Bro scripts with source.
  - *Please note* that a virtual box VM will be made available prior to this training session. To fully participate, attendees will get this running on their laptops ahead of time.
- **Secure Coding Practices (Prof. Barton Miller & Prof. Elisa Heymann)**
  - *Location: Renoir Suite*
  - *Description*: Security is crucial to the software that we develop and use. With the growth of both Grid and Cloud services, security is becoming even more critical. This tutorial is relevant to anyone wanting to learn about minimizing security flaws in the software they develop. We share our experiences gained from performing vulnerability assessments of critical middleware. You will learn skills critical for software developers and analysts concerned with security. This tutorial presents coding practices subject to vulnerabilities, with examples of how they commonly arise, techniques to prevent them, and exercises to reinforce them. Most examples are in Java, C, C++, Perl and Python, and come from real code belonging to Cloud and Grid systems we have assessed. This tutorial is an outgrowth of our experiences in performing vulnerability assessment of critical middleware, including Google Chrome, Wireshark, Condor, SDSC Storage Resource Broker, NCSA MyProxy, INFN VOMS Admin and Core, and many others.
- **Streamlining Collaboration with InCommon and Identity Federations (Warren G. Anderson and Dr. Jim Basney)**
  - *Location: Picasso Room*
  - *Description*: Because of the success of programs like XSEDE and OSG more and more scientists have access to more computing power than ever and consequently are generating more output than ever before. Efficiently sharing all those generated results with colleagues and collaborators, however, remains a problem--it's too difficult for scientists from different projects and different campuses to quickly and easily find spaces to collaborate. One of the largest barriers to efficient collaboration is creating and managing new electronic

identities for every new tool or web application. Federated identity can help and identity federations like InCommon in the US provide ready to consume identities that help streamline getting scientists into the same applications and spaces so they can collaborate. This tutorial will discuss what are federated identities, why we can trust them, and how to leverage a federation like InCommon and similar federations around the world to support discovery across VOs. We will focus on LIGO’s experiences and lessons learned during their five year effort to build an end-to-end identity management infrastructure that consumes federated identity in support of collaboration with other astronomy and astrophysics projects.

Day 2 (Oct 1): Main plenary for all attendees in Gallery II/III (8am-5pm)

- 7:00 am: Registration and continental breakfast.
- 8:00 am: Welcome and Goals (Jim Marsteller)
- 8:20 am: Intro by NSF (Cliff Jacobs)
- 8:45 am: Opening Keynote - Vern Paxson
    - Focused on community building for cybersecurity
- 9:45 am: Coffee Break
- 10:00 am: Panel and discussion on community building - real world experiences from communities for cybersecurity and otherwise
    - Confirmed Panelists: Joel Cutcher-Gershenfeld, Jim Marsteller, Leif Nixon, Rodney Petersen
    - Moderator: Peter Arzberger
- 11:00 am: Panel and discussion on the goals of a cybersecurity program
    - Confirmed Panelists: Brian Bockelman, Cliff Jacobs, John Towns
    - Moderator: Ardoth Hassler
- 12:00 pm: Lunch (in Masters Ballroom)
- 1:00 pm: NSF remarks (Dr. Farnam Jahanian, CISE/NSF)
- 1:15 pm: A view from the field of NSF cybersecurity challenges, goals, and opportunities (Von Welch, CTSC PI)
- 1:45 pm: Panel and discussion on differences, similarities and relationships between NSF projects and other organizations (e.g., higher education, government, private sector)
    - Confirmed Panelists: Michael Bailey, Michael Corn, Vic Thomas
    - Moderator: Greg Bell
- 3:00 pm: Coffee Break
- 3:30 pm: Evolution of Network Security Threats and Capabilities for Science Communities (Adam Slagell)
- 4:00 pm: Open discussion - Recap progress towards goals. Refine topics to address in working groups on Day 3. (Jim Marsteller and Von Welch)
- 4:45 pm: Closing remarks. (Jim Marsteller, Cliff Jacobs)

        - Present path forward on collaboration until next summit.
    - 5:00 pm: Adjourn (dinner on own)

Day 3 (Oct 2): Break out into working groups for morning (8am-Noon)

- A long-term goal for the summit and CTSC is to build and support community that spans from year to year. Participants are invited to join one of the following four working groups. The primary goal for each group is to define a problem statement or charter around the working group topic to serve as a basis for collaboration after the 2013 summit, and feeding into the anticipated 2014 summit. Participants will have the opportunity to join dedicated groups in the Trusted CI Forum (trustedci.groupsite.com) to continue working together. In support of this goal, Day 3 objectives for each group may include (a) identifying the most critical and vexing questions for making progress in the topic area, (b) identifying resources and expertise that can be leveraged to address these challenges, and (c) identifying ways to usefully build community and communication around the topic area. Topics for the groups are:
    a. Cybersecurity Planning & Programs Group (Jim Marsteller, moderator)
    b. Identity & Access Management Group (Jim Basney, moderator)
    c. Network Security & Monitoring Group (Adam Slagell, moderator)
    d. Unconference Group: *Focus TBD!* (Von Welch, moderator)

    - 7:00 am: Continental breakfast provided.
    - 8:00 am: Kick-off working groups (moderators)
    - 10:00 am: Coffee Break
    - 10:30 am: Reconvene working groups
    - 11:30 am: Recap discussion, post-summit steps (moderators)
    - Noon: Adjourn (lunch on own)

Reference Materials

Past Summit Reports

- 2009: http://net.educause.edu/ir/library/pdf/PUB1001.pdf
- 2008: http://net.educause.edu/ir/library/pdf/PUB9002.pdf
- 2007: http://www-cdn.educause.edu/ir/library/pdf/CYB0701.pdf
  - NSF Response: http://net.educause.edu/ir/library/pdf/CYB08006B.pdf
- 2005: http://net.educause.edu/ir/library/pdf/CYB0525.pdf
  - NSF Response: http://net.educause.edu/ir/library/pdf/CYB0525c.pdf
- 2004: http://net.educause.edu/ir/library/pdf/CSD4296.pdf

Scientific Software Security Innovation Institute Workshops: http://security.ncsa.illinois.edu/s3i2/

"Cybersecurity 2011... and beyond. What Makes a Good Security Plan?" Ardoth Hassler, Senior IT Advisor, National Science Foundation. Associate VP University Information Services, Georgetown University: http://trustedci.org/s/Cybersecurity-for-Managers-LF-Group-0106-2011.pptx

NSF Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions for Managers of Large Facilities. Effective February 1, 2012. Information Security Requirements (p. 6, item 56).