Welcome and Introductions

Prof. Mohammad Husain (CPP) and Dr. Jim Basney (CTSC)
OVERVIEW

• First ever technical workshop exclusively for cybercorps scholarship for service students
• Based on an engagement program between NSF Center for Trustworthy Scientific Cyberinfrastructure (CTSC) and Cal Poly Pomona (CPP)
Cal Poly Pomona Team

Tingting Chen
Ron Pike
Dan Manson
Mohammad Husain
NCSA-CTSC Team at CPP

Jeannette Dopheide
Jim Basney
John Zage
Kay Avila
Logistics

● Ms. Annie montes (amontes@cpp.edu)
● Please make sure to
  ○ return paperwork to her on time
  ○ respond to the post-workshop survey
● WiFi SSID is GUEST
Goals of the workshop

- Introduction to cyberinfrastructure (CI)
- Gain Knowledge on how to protect CIs from cyber attacks
- Complement the knowledge with hands-on exercise
- Grow an interest about careers in this domain
Agenda-Saturday

- Intro to CI
- Real world projects in CI
- Crypto overview and its usage in securing CI
- Security policies for CI
- Looking at logs for policy violations
- Network security issues in CI
- Career development panel
Agenda-Sunday

- Federated identity management in CI
- Automation in datacenter
- Incident response in CI
- Security incident and event management
About NCSA

- Established in 1986 as one of the original sites of the NSF's Supercomputer Centers Program
- A department of the University of Illinois at Urbana-Champaign
- Supported by the state of Illinois, the University of Illinois, the National Science Foundation, and grants from other federal agencies
- Home of NSF's Blue Waters supercomputer
About CTSC

- CTSC began with a 3-year NSF grant in 2012.
- NSF 2015 Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation called for an NSF CCoE.
- CTSC submitted a proposal to continue its funding as a CCoE and was awarded this honor for 2016-2018.

3. Cybersecurity Center of Excellence

NSF-funded cyberinfrastructure presents unique challenges for operational security personnel. The research environment is purposefully built as an "open" one, in which data is freely accessed among collaborators. As such, sites, centers, campuses and institutions that host cyberinfrastructure must find the right balance of security, privacy and usability while maintaining an environment in which data are openly shared. Many research organizations lack expertise in technical and policy security and could benefit from an independent, shared security resource pool.

A Cybersecurity Center of Excellence must:

- Provide leadership to the NSF research community in the continuous building and distribution of a body of knowledge on the topic of trustworthy cyberinfrastructure;
- Conduct security audits and security architecture design reviews for projects at multiple scales, from large Major Research Equipment and Facilities Construction (MREFC) projects to small CI development;
- Ensure adoption of security best practices in the NSF research community;
- Provide situational awareness of the current cyber threats to the research and education environment, including those that impact scientific instruments;
- Develop a threat model (or multiple threat models if appropriate), identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure and recommending countermeasures to protect the systems; and
- Host an annual workshop in addition to meetings, seminars, training and other events in order to interact with members of the NSF community, industry, government and academia who wish to collaborate on projects and other initiatives.
What is cyberinfrastructure (CI)?

"United States federal research funders use the term cyberinfrastructure to describe **research environments** that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other **computing and information processing services distributed over the Internet** beyond the scope of a single institution. In scientific usage, cyberinfrastructure is a technological and sociological solution to the problem of **efficiently connecting laboratories, data, computers, and people** with the goal of **enabling derivation of novel scientific theories and knowledge**."

- More info
  - https://www.nsf.gov/cise/oac/about.jsp
Example Large CI Projects

Laser Interferometer Gravitational-Wave Observatory (LIGO)

Extreme Science and Engineering Development Environment (XSEDE)
Campus CI

- High performance compute cluster(s)
- High speed research networks
  - Supporting IPv6, Software Defined Networking (SDN)
- High capacity/performance data storage
- "Friction-free access" via the ScienceDMZ
- Specialized scientific instruments and software
- Expert staff: research facilitators, consultants, operators
Security for CI

- CI projects need security professionals
  - Developing and implementing security programs
  - Leading incident response teams
  - Designing and deploying identity and access management solutions
  - Securing unique software platforms
  - Deploying intrusion detection/prevention systems on high speed networks

- CI staff work at universities and gov't labs
  - Many CI projects are eligible to hire SFS graduates!

- CI is an ecosystem of heterogeneous, evolving systems
  - Campus cyberinfrastructure
  - Large facilities (e.g., https://www.nsf.gov/bfa/lfo/)
  - Distributed systems (e.g., https://www.opensciencegrid.org/)
Questions? Comments?