Welcome to the Workshop on Trustworthy Scientific Cyberinfrastructure @ PEARC 17

Organizers:
Jim Basney, James A. Marsteller, Von Welch

July 13th 2017

trustedci.org
Our Agenda

9am  Welcome / NSF CCoE Overview
     Von Welch
10am  Cybersecurity for Small CI Projects
      Jim Basney, James Marsteller, Von Welch
10:30am  Break
11am  Security for Science Gateways
      Nancy Wilkins-Diehr, Von Welch
11:30am  Community Lightning Talks & Grill the Experts
12:30pm  Conclude
Want to give a lightning talk @ 11am?

We have a couple slots left.

Please see Jim Basney to sign up and/or send slides to jbasney@uiuc.edu.
We want your feedback

This event is organized by the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). We want your feedback:

https://trustedci.org/feedback
The NSF Cybersecurity Center of Excellence

Jim Basney, James A. Marsteller, Von Welch

Workshop on Trustworthy Scientific Cyberinfrastructure
PEARC17
July 13th 2017

trustedci.org
NSF Cybersecurity Center of Excellence (CCoE)

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.

What Really Matters?
Trusted and Reproducible Science

A biotechnology firm is releasing data on three failed efforts to confirm findings in high-profile scientific journals — details that the industry usually keeps secret.

Ampen, headquartered in Thousand Oaks, California, says that it hopes the move will encourage others in industry and academia to describe their own replication attempts, and thus help the scientific community to get to the bottom of work that other labs are having trouble verifying.

The data are posted online at a newly launched channel dedicated to quickly publishing efforts to confirm scientific findings. The ‘Preclinical Reproducibility and Robustness’ channel is hosted by PLoS (Public Library of Science). A link to the channel is provided on Ampen’s website.

The data suggest that many of the findings that have been replicated in the past are not always reproducible in the lab. Some of the findings are of questionable value, and the field is at a turning point in which it is possible to move the field forward and avoid repeating mistakes of the past.

Scientists who are concerned about the irreproducibility of preclinical research say that they welcome the initiative — but are not sure whether it will catch traction.
Mission

CTSC’s mission is to provide the NSF community a coherent understanding of cybersecurity’s role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.
Vision for the NSF Science Community

1. For the NSF science community to understand fully the role of cybersecurity in producing trustworthy science.

2. For all NSF projects and facilities to have the information and resources they need to build and maintain effective cybersecurity programs appropriate for their science missions, and responsive to evolving risks and requirements.

3. For all NSF Large Facilities to have highly effective cybersecurity programs.
CCoE Thrusts

Building Community
NSF Cybersecurity Summit, Monthly Webinars, Blog, Email Lists, Partnerships, Benchmarking Survey

Sharing Knowledge
Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Identity Management Best Practices, Situational Awareness, Training, OSCTP

Collaboration to Tackle Challenges: Engagements

More information at trustedci.org
Collaboration to Tackle Challenges: Engagements
Engagements

Focused collaborations with one (or small group) of NSF projects to tackle a project’s cybersecurity or identity and access management challenge.

CCoE’s time is covered by our NSF grant. You are expected to contribute comparable effort.

Examples:
- Developing a cybersecurity program
- Assessing an existing program
- Software assurance/evaluation
- Custom training
- IAM design

*Your challenge here...*
Any challenge is in scope!

More examples...
Drafting a Privacy Policy (AoT)
Security Officer search (LIGO)
Identity and Access Management:
http://trustedci.org/iam/
Software Assurance:
http://trustedci.org/software-assurance/

Science Gateways w/SGCI SI2 Institute:
http://sciencegateways.org/news/collaboration-ctsc/
Online application process: http://trustedci.org/application

Demand outpacing supply. Will soon begin accepting applications for consideration for execution in the first half of CY 2018. Please subscribe to our announce list to be informed: https://trustedci.org/ctsc-email-lists/
Sharing Knowledge
Guides, Best Practices, Situational Awareness, Training
Situational Awareness

Advise NSF CI community about relevant software vulnerabilities and provide guidance on mitigation. Leverage NIST, US-CERT, XSEDE, REN-ISAC, and other sources of vulnerability information. Please subscribe to the email list(s) to receive situational awareness notifications of relevance to you.

http://trustedci.org/situational-awareness/
Cybersecurity Guides and Tools

Addressing concerns unique to science

Policy templates:
  Acceptable Use, Access Control, Asset Management, Disaster Recovery, Incident Response, Inventory, Awareness, Physical Security, ...

Risk assessment table

Securing commodity IT

Self-assessment Tool

Identity Management Best Practices

http://trustedci.org/guide
http://trustedci.org/iam
Training materials

2016 Spring Practical Cybersecurity for Open Science Projects

2015 NSF Cybersecurity Summit Training Materials (August 17, 2015)

- Bro Platform Training Workshop - Johanna Armann (ICSI), Justin Azoff (NCSA) & Adam Slagell (NCSA)
- Developing Cybersecurity Programs for NSF Projects - Bob Cowles, Craig Jackson, Jim Marsteller & Susan Sons (CTSC)
- Vulnerabilities, Threats, and Secure Coding Practices - Barton P. Miller & Elisa Heymann
- Industrial Control Systems, Networking, and Cybersecurity - Phil Salkie (Jimarrah Industrial Automation)
- Aligning your Research Cyberinfrastructure with HIPAA and FISMA - Anurag Shankar (Indiana University)
- Incident Response Training - Randy Butler (NCSA)

2014 NSF Cybersecurity Summit Training Materials (August 26, 2014)

- Developing Cybersecurity Programs for NSF Projects (PDF) - Jim Marsteller, Susan Sons, Craig Jackson, Jared Allar (CTSC)
  - Also available as a series of online videos
- Vulnerabilities, Threats, and Secure Coding Practices (PDF) - Barton P. Miller, James A. Kupsch, Elisa Heymann (University of Wisconsin)
- HPC, HIPAA, and FISMA: Meeting the Regulatory Challenge through Effective Risk Management (PowerPoint) - Bill Barnett & Anurag Shankar (Indiana University)
- Incident Response Training (Powerpoint part 1, Powerpoint part 2) - Randy Butler, Warren Raquel, Patrick Duda (NCSA)

NSF Cybersecurity Summit, XSEDE, SuperComputing, other locations by request.
Topics: Cybersecurity Program Development, Incident Response, Secure Coding, Software Engineering...

http://trustedci.org/trainingmaterials/
The Open Science Cyberthreat Profile: Understanding the Cybersecurity of Science

Scientists and cybersecurity professionals need to communicate to understand the risks related to science assets to the science mission.

OSCTP working group is developing a profile of open science assets and their common risks to aid risk management for open science.

Presentations from ATLAS, IBEIS, LSST, and OOI (& DataONE in Sep.)

Published in late 2016.

https://trustedci.org/oscrp/

Members: Altintas (SDSC), Bevier (Caltech), Cuff (Harvard), LeDuc (Northwestern), Meunier (Purdue/HUBzero), Moore (iRods), Schwab (ISI), Stocks (UCSD)

Organizers: Adams (CTSC), Dopheide (ESnet), Peisert (ESnet), Welch (CTSC).
Building Community

NSF Cybersecurity Summit, Webinars, Blog, Email Lists, Partnerships
NSF Cybersecurity Summit

- Inaugural summit in 2004 in response to cyber attack affecting many NSF funded projects
- CTSC Relaunched Summit in 2013 after 4 year hiatus
- **Growing!** 90 registrants in 2015, **100** in 2016.
- Opportunity for LFs, CI projects, MREFCs to collaborate: build **connections**, identify and solve **common challenges**, develop **best practices**, share **experiences**, receive **training**.
- **Address** the changing threat landscape for NSF CI.

More info at http://trustedci.org/summit/
CTSC Webinar Series
trustedci.org/webinars

Upcoming Webinars:

- July 24th: Internet2 Cyberinfrastructure by Paul Howell (Registration coming soon)
- August 28th: Improving the Security and Usability of Two-Factor Authentication for Cyberinfrastructure with Nitesh Saxena & Stanislaw Jarecki
- September 25th: Threat Intelligence Sharing with Romain Wartel

Contact info@trustedci.org if have a suggestion for a presentation or would like to present.

Suggestion: CICI projects and RCNs, CC*, etc.
Partnerships

Interoperability with and best practices from our global collaborators.

ESnet: Open Science Cyberthreat Profile
AARC: Identity Management with the EU
SGCI SI2 Institute: Science Gateway cybersecurity
Bro CoE: Training, network security
REN-ISAC: Situational Awareness

http://trustedci.org/partners/
2016 NSF Community Benchmarking Survey

https://hdl.handle.net/2022/21355

Collected and analyzed information about the NSF science community’s cybersecurity programs, practices, challenges, and concerns from 27 projects (including 9 responses from the ~25 NSF Large Facilities).
Staying in contact with the CCoE

Join our email lists for discussions and updates: trustedci.org/ctsc-email-lists/

Webinars: trustedci.org/webinars

Blog: blog.trustedci.org

Twitter: @TrustedCI

Questions: ask@trustedci.org
Thank You

trustedci.org

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.