Funded by the National Science Foundation, Grant #2127548

Trusted CI Support for Research Infrastructure CI

by Jim Basney & Von Welch

NSF Ecosystem Lightning Talks

March 1, 2022
CI Compass Cyberinfrastructure for NSF Major Facilities Workshop

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

trustedci.org

Trusted CI Support for Research Infrastructure CI

Jim Basney
Trusted CI Deputy Director

Von Welch
Trusted CI Director

NSF Cyberinfrastructure for Major Facilities Workshop

March 1-2

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

BERKELEY LAB

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

PITTSBURGH SUPERCOMPUTING CENTER

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

USA UNIVERSITY OF SOUTH ALABAMA

https://trustedci.org/

CI Compass and Trusted CI

- Two of the premier CoEs funded by NSF/OAC to help the NSF science community.
- Co-founded the Identity Management Working Group
- Share CoE best practices and lessons learned.
- Have standing and open communication and collaboration channels

Not sure which center to approach with a question or challenge?

Approach either and we’ll collaboratively figure out how to best help you.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CI Compass

Our talk…

A quick overview of Trusted CI resources of interest to the broader CI community.

Introduction of Trusted CI Ambassadors for NSF Major Facilities.

We welcome follow-up with more questions.

Annual Challenge: Operational Technology

- Year 3 focuses on investigating the use of Operational Technology(OT) at NSF major scientific research facilities
- OT is the use of hardware and software to monitor and control physical processes, devices, and infrastructure
- Increasingly important in the context of science and research leveraging instruments like telescopes, biological and chemical reactors, sonar, and even vehicles used in scientific discovery
- Annual Challenge team is engaging with IT and OT personnel discussing operations at a variety of NSF Major Research Facilities

Develop a multi-year roadmap of security recommendations to advance the security of scientific operational technology for NSF facilities

https://blog.trustedci.org/2022/01/announcing-2022-trusted-ci-annual.html

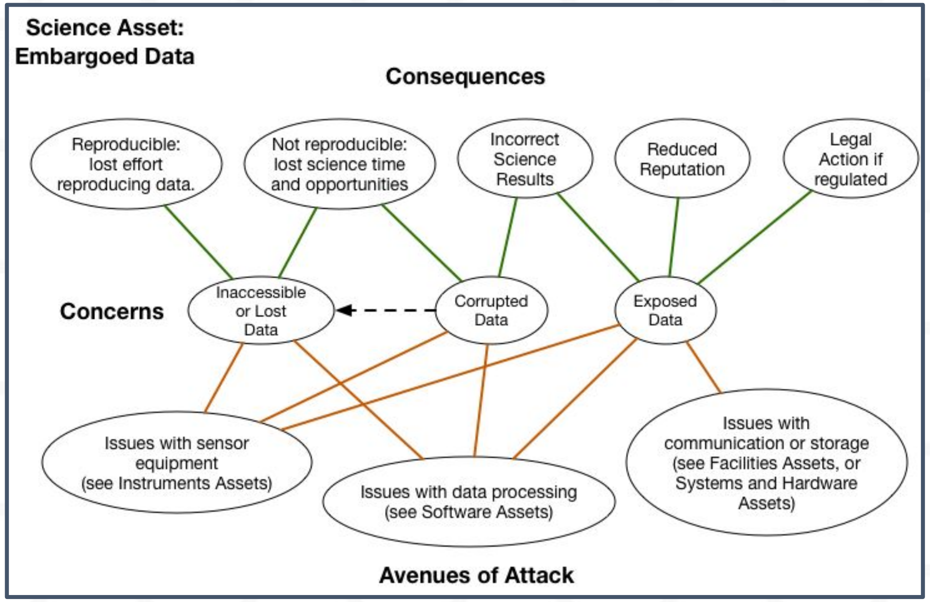
Science DMZ Security

- Partnered with EPOC, University of Arkansas / DART project
  on Science DMZ focused engagement
- Created reusable template security documents related to Science DMZs
- Published Security of Science DMZ whitepaper
  - https://hdl.handle.net/2022/27007
  - Help senior leadership to understand security of Science DMZs
  - Summarize and expand on security recommendations
  - Provide links to more resources

Open Science Cyber Risk Profile (OSCRP)

OSCRP helps science projects understand cybersecurity risks to their science infrastructure and facilitates discussing those risks with their campus security office.

https://trustedci.org/oscrp/

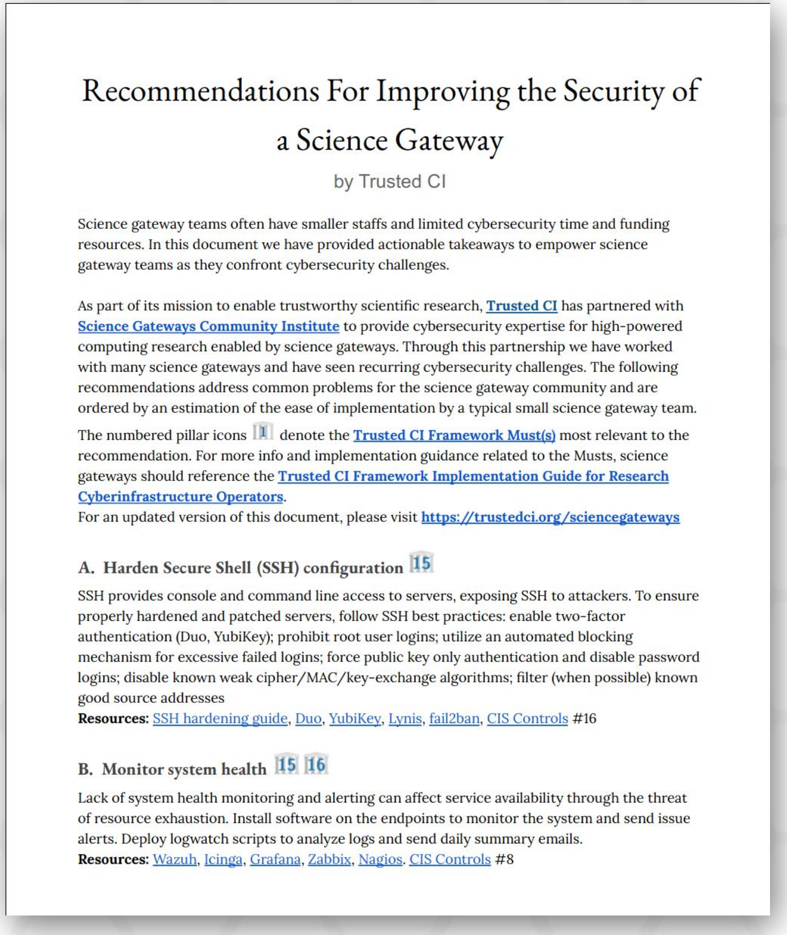

Science Asset:
Embargoed Data
Consequences
Reproducible: lost effort reproducing data.
Not reproducible: lost science time and opportunities
Incorrect Science Results
Reduced Reputation
Legal Action if regulated
Concerns
Inaccessible or Lost Data
Corrupted Data
Exposed Data
Issues with sensor equipment (see Instruments Assets)
Issues with data processing (see Software Assets)
Issues with communication or storage (see Facilities Assets, or Systems and Hardware Assets)
Avenues of Attack

Example mapping from OSCRP of cybersecurity attacks to scientific consequences.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Science Gateway Security Best Practices

- Based on partnership with SGCI over 4+ years
- Published document on recommendations for improving science gateway security
- Based on individual security engagements with gateways
- Short actionable items for small projects
- References to Trusted CI framework for more info as needed



Recommendations For Improving the Security of a Science Gateway

by Trusted CI

Science gateway teams often have smaller staffs and limited cybersecurity time and funding resources. In this document we have provided actionable takeaways to empower science gateway teams as they confront cybersecurity challenges.

As part of its mission to enable trustworthy scientific research, **Trusted CI** has partnered with **Science Gateways Community Institute** to provide cybersecurity expertise for high-powered computing research enabled by science gateways. Through this partnership we have worked with many science gateways and have seen recurring cybersecurity challenges. The following recommendations address common problems for the science gateway community and are ordered by an estimation of the ease of implementation by a typical small science gateway team.

The numbered pillar icons 1 denote the **Trusted CI Framework Must(s)** most relevant to the recommendation. For more info and implementation guidance related to the Musts, science gateways should reference the **Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators**.
For an updated version of this document, please visit **https://trustedci.org/sciencegateways**

A. Harden Secure Shell (SSH) configuration 15

SSH provides console and command line access to servers, exposing SSH to attackers. To ensure properly hardened and patched servers, follow SSH best practices: enable two-factor authentication (Duo, YubiKey); prohibit root user logins; utilize an automated blocking mechanism for excessive failed logins; force public key only authentication and disable password logins; disable known weak cipher/MAC/key-exchange algorithms; filter (when possible) known good source addresses
Resources: SSH hardening guide, Duo, YubiKey, Lynis, fail2ban, CIS Controls #16

B. Monitor system health 15 16

Lack of system health monitoring and alerting can affect service availability through the threat of resource exhaustion. Install software on the endpoints to monitor the system and send issue alerts. Deploy logwatch scripts to analyze logs and send daily summary emails.
Resources: Wazuh, Icinga, Grafana, Zabbix, Nagios. CIS Controls #8

https://hdl.handle.net/2022/26780

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Cyberinfrastructure Vulnerability Alerts

We monitor multiple sources for vulnerability alerts, then determine which ones are of critical interest to the CI community, using the following criteria:

- the affected technology's or software's pervasiveness in the CI community
- the technology's or software's importance to the CI community
- the type and severity of a potential threat, e.g., remote code execution
- the threat's ability to be triggered remotely
- the threat's ability to affect critical core functions
- the availability of mitigations

We also provide guidance on how operators and developers can reduce risks and mitigate threats. We coordinate with XSEDE, Open Science Grid (OSG), the NSF supercomputing centers, and the ResearchSOC on drafting and distributing alerts to minimize duplication of effort and maximize benefit from community expertise.

In 2021 the Cyberinfrastructure Vulnerabilities team discussed 40 vulnerabilities and issued 26 alerts to 183 subscribers.

To subscribe, visit: https://trustedci.org/vulnerabilities/

Software Assurance

https://www.trustedci.org/software-assurance

2021 Annual Challenge

Interviewed six large CI project who develop scientific software to understand their practices surrounded software security. Produced a “Findings” document report on the state of the art.

To provide direction in developing secure software, we produced the initial version of the “Guide to Securing Scientific Software”. This is a living document with ongoing development this year.

Software Secure Training

Free and open online resources (cc’d in English & Spanish), including extensive hands-on exercises and instructor materials:

`https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/`

Teach tutorials at conferences, workshops, labs, and government agencies.

In-depth vulnerability assessment

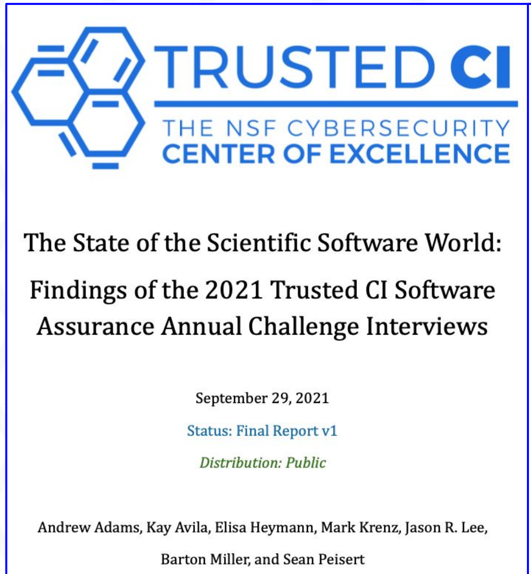
Have done multiple project engagements.

Development new techniques to automate such assessments.

Ransomware

Developing comprehensive threat model of ransomware attacks.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The State of the Scientific Software World:

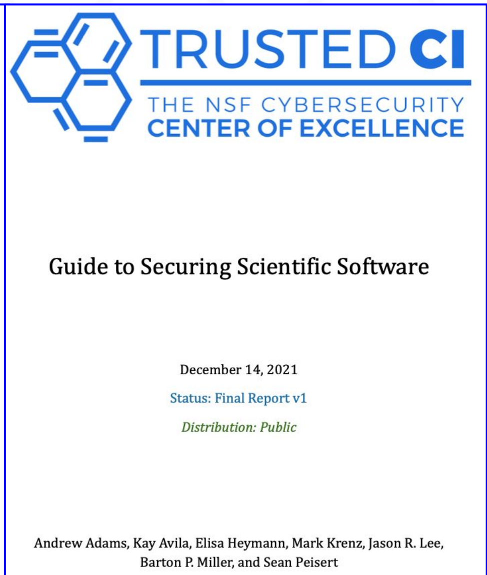
Findings of the 2021 Trusted CI Software Assurance Annual Challenge Interviews

September 29, 2021

Status: Final Report v1

Distribution: Public

Andrew Adams, Kay Avila, Elisa Heymann, Mark Krenz, Jason R. Lee, Barton Miller, and Sean Peisert



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Guide to Securing Scientific Software

December 14, 2021

Status: Final Report v1

Distribution: Public

Andrew Adams, Kay Avila, Elisa Heymann, Mark Krenz, Jason R. Lee, Barton P. Miller, and Sean Peisert

Trusted CI Fellows

- In 2019, Trusted CI established the Open Science Cybersecurity Fellows program, now in its fourth cohort.
- This program establishes and supports a network of Fellows with diversity in both geography and scientific discipline.
- These Fellows have access to training and other resources to foster their professional development in cybersecurity.
- The Fellows champion cybersecurity for science in their scientific and geographic communities and communicate challenges and successful practices to Trusted CI.

https://trustedci.org/fellows

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Ambassadors to Major Facilities

New in 2022

To better support the cybersecurity needs of the NSF Major Facilities, Trusted CI now assigns a staff member as an "ambassador" to each facility. This helps Trusted CI maintain connections with all the facilities, including an up-to-date understanding of cybersecurity needs.

Current Ambassadors:

Andrew Adams: NCAR, OOI

Kay Avila: NEON

Adrian Crenshaw: US-ATLAS, US-CMS

Terry Fleury: LIGO

Josh Drake: GAGE, SAGE

Ryan Kiser: ARF

Mark Krenz: USAP, IceCube

Ranson Ricks: NOIRLab

Mike Simpson: Arecibo, NRAO, NSO

John Zage: IODP, LCCF, NHMFL, NSCL

https://www.trustedci.org/ambassadors

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Staying Connected with Trusted CI

Trusted CI Webinars

4th Monday of month at 11am ET.

https://trustedci.org/webinars

Follow Us

https://trustedci.org

https://blog.trustedci.org

@TrustedCI

Slack

Email ask@trustedci.org for an invitation.

Email Lists

Announce and Discuss

https://trustedci.org/trustedci-email-lists

Ask Us Anything

No question too big or too small.

info@trustedci.org

Cyberinfrastructure Vulnerabilities

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

Trusted CI License Statement

Thanks!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.