Cybersecurity for Science: Why and How

Canada Foundation for Innovation
2021 Major Science Initiatives Workshop
March 18, 2021

Von Welch
Director, Trusted CI, the NSF Cybersecurity Center of Excellence
Cybersecurity and Open Science

A lot of research is regulated.
E.g. HIPAA, FISMA, NIST 800-171

I use “Open Science” loosely for science not guided by compliance
E.g. Astronomy, climate, physics, geology
AKA Fundamental Research

Gemini South on the summit of Cerro Pachón in Chile (left) and Gemini North on the summit of Maunakea in Hawai‘i (right).
Image credit: Gemini/NSF/AURA
My Talk

Why Cybersecurity for Open Science?

How to Implement Appropriate Cybersecurity for Open Science?
Myth:

Cybersecurity is about confidentiality hence, open science does not need cybersecurity.
Reality:

Open Science Needs **Appropriate** Cybersecurity
Appropriate cybersecurity supports organizational mission.
For Open Science, Cybersecurity supports:

- Trustworthiness
- Productivity
- Reproducibility
Trustworthy: Data Integrity

For Open Science, integrity of data is often most important aspect of cybersecurity.

Productivity: Threat of Unavailable Instruments

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

NICOLAS PERPITCH
UPDATED TUE 17 OCT 2017, 6:44 PM AEDT

Cyber attack almost cost team looking at colliding neutron stars.


Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.
Your Data Is Valuable to Criminals!

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
Productivity: Rapid, Collaborative Projects

Research projects tend to be short-lived (3-5 years). They need to progress quickly.

It’s common for research collaborations to span universities and even countries.

Researchers want to define their teams, change those definitions and share access – all unrelated to institutional directories or human resources databases.

Some history of scale...

<table>
<thead>
<tr>
<th>Date</th>
<th>Collaboration sizes</th>
<th>Data volume, archive technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Late 1950's</td>
<td>2-3</td>
<td>Kilobits, notebooks</td>
</tr>
<tr>
<td>1960's</td>
<td>10-15</td>
<td>kB, punchcards</td>
</tr>
<tr>
<td>1970's</td>
<td>~35</td>
<td>MB, tape</td>
</tr>
<tr>
<td>1980's</td>
<td>~100</td>
<td>GB, tape, disk</td>
</tr>
<tr>
<td>1990's</td>
<td>700-800</td>
<td>TB, tape, disk</td>
</tr>
<tr>
<td>2010's</td>
<td>~3000</td>
<td>PB, tape, disk</td>
</tr>
</tbody>
</table>

Credit: Ian Bird
Reproducibility

Can we reproduce what we did on computers we didn’t fully control?

June 9, 2014

The National Science Foundation has banned a researcher for using agency-funded supercomputers to mine bitcoins, a virtual currency that can be converted into traditional currencies through exchange markets. According to a recently surfaced report from the National Science Foundation Office of the Inspector General, the NSF banned the unnamed researcher after receiving reports that NSF systems at two universities had been used for personal gain.

Bitcoin mining refers to how the virtual currency is generated. Miners solve math problems that serve to verify bitcoin transactions. In exchange they are issued a certain number of bitcoins as a reward.

“The researcher misused over $150,000 in NSF-supported computer usage at two universities to generate bitcoins valued between $8,000 and $10,000,” according to the March 2014 Semi Annual Report to Congress. “Both universities determined that this was an unauthorized use of their IT systems. The researcher asserted that he was conducting tests on the computers, but neither university had authorized him to conduct such tests — both university reports noted that the researcher accessed the computer systems remotely and may have taken steps to conceal his activities, including accessing one supercomputer through a mirror site in Europe.”

This is the latest case of university systems being commandeered to mine for digital currency. Other notable incidents involve a researcher at Harvard and a student at Imperial College London.
Open Science Cybersecurity Resources
From Trusted CI
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.

https://trustedci.org/
### NSF Funds Research and Education across all Fields of Science and Engineering

#### Awards > $1m:
- 644 in FY20
- 4283 active in 3/2021

---

### NSF by the Numbers

<table>
<thead>
<tr>
<th>$8.1 billion</th>
<th>FY 2019 Appropriations (does not include mandatory accounts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,800</td>
<td>Colleges, universities, and other institutions receiving NSF funding in FY 2019</td>
</tr>
<tr>
<td>41,000</td>
<td>Proposals evaluated in FY 2019 through a competitive merit review process</td>
</tr>
<tr>
<td>11,300</td>
<td>Competitive awards funded in FY 2019</td>
</tr>
<tr>
<td>192,000</td>
<td>Proposal reviews conducted in FY 2019</td>
</tr>
<tr>
<td>306,000</td>
<td>Estimated number of people NSF supported directly in FY 2019 (researchers, postdoctoral fellows, trainees, teachers, and students)</td>
</tr>
<tr>
<td>60,000</td>
<td>Students supported by NSF Graduate Research Fellowships since 1952</td>
</tr>
</tbody>
</table>

---

Trusted CI

...is a trusted partner, not an auditor, not selling a product.

...helps projects tackle their cybersecurity challenges.

...builds community and serves.

...leads to advance state of practice.

...is applied research in community engagement.
Trusted CI: Scopes of Impact

National level: Leadership, community building, webinars, annual cybersecurity Summit, situational awareness.

Broad impact: Training, best practice guides, workshops.

Individual project: Consulting and Engagements.
Trusted CI: Impacts

Updated impact as of July 2020:

Trusted CI has positively impacted over 480 NSF projects since inception in 2012.

Members of more than 330 NSF projects have attended our NSF Cybersecurity Summit.

Members of more than 140 NSF projects have attended our monthly webinars.

We have provided more than 300 hours of training to the community.

We’ve had 52 engagements with NSF funded projects, including ten NSF Large Facilities.

https://hdl.handle.net/2022/22148
Best Practices

Security Best Practices for Academic Cloud Service Providers
https://trustedci.org/cloud-service-provider-security-best-practices/

Identity Management Best Practices
https://trustedci.org/iam

Science Gateways
https://trustedci.org/sqci/

Software Assurance
https://trustedci.org/software-assurance/

Software Engineering Guide
https://sweguide.trustedci.org/
The Trusted CI Framework
4 Pillars, 16 Musts

The Trusted CI Framework helps leaders establish and refine cybersecurity programs that work.

Its straightforward structure focuses on foundational decisions about organizational mission alignment, governance, resources, and controls.

This is not yet another long list of technical requirements.
Framework Implementation Guide for Research Cyberinfrastructure Operators

Go to [https://www.trustedci.org/framework](https://www.trustedci.org/framework) and hit the green button. The guide gives research organizations a community-tailored head start on choosing among good paths and avoiding treacherous ones.

Includes:
- roadmaps for establishing mature cybersecurity programs
- tailored advice on overcoming common challenges
- pointers to resources

Built by Trusted CI’s experienced multi-institutional team, and vetted by a Framework Advisory Board representing the diversity of our community.
Getting Started

Check out trustedci.org/framework/core. This briefly explains the 16 Musts. For each, ask yourself, “Have we addressed this? If not, why not? If so, how’s it working out?”

Hit the green button to grab the guide, and share with your teams.
Staying Connected with Trusted CI

**Trusted CI Webinars**
4th Monday of month at 11am ET.
[https://trustedci.org/webinars](https://trustedci.org/webinars)

**Follow Us**
[https://trustedci.org](https://trustedci.org)
[https://blogtrustedci.org](https://blogtrustedci.org)
@TrustedCI

**Monthly Office Hours**
Announced on discuss email list

**Email Lists**
Announce and Discuss
[https://trustedci.org/trustedci-email-lists](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/](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 activities are made possible thanks to the contributions of a multi-institutional team: https://trustedci.org/who-we-are/
Trusted CI License Statement

All materials de novo generated as part of this project that will be distributed will be distributed under the Creative Commons Attribution-NonCommercial 3.0 Unported (CC BYNC 3.0). The full terms of this license are available at http://creativecommons.org/licenses/bync/3.0/.
Thanks!

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