Panel: Ethics & Privacy in Advanced Research Computing

Jim Basney
jbasney@ncsa.illinois.edu

ACI-REF Virtual Residency Workshop

June 10, 2021

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

https://trustedci.org/

Ethics Topics / Examples

- Impact on Research Subjects - Institutional Review Board (IRB)
  - Linux Kernel "hypocrite commit" study (2020-2021)
- Abuse of Resources - Acceptable Use Policy (AUP)
  - Bitcoin mining on NSF-funded supercomputers (2014)
- Violation of Data Regulations (ITAR)
  - Export of defense-related materials (2009)

References:

https://cse.umn.edu/cs/statement-computer-science-engineering-confirming-linux-technical-advisory-board-findings-may-9
https://www.nsf.gov/pubs/2014/oig14002/oig14002.pdf
https://www.justice.gov/opa/pr/retired-university-professor-sentenced-four-years-prison-arms-export-violations-involving

Data Privacy - Ransomware

- Ransomware gangs have moved beyond making data inaccessible to publishing sensitive data
- Multiple universities impacted
- Ethics of ransomware payments

> Grades and social security numbers for students at the University of Colorado and University of Miami patient data have been posted online by the Clop ransomware group.
>
> Starting in December, threat actors affiliated with the Clop ransomware operation began targeting Accellion FTA servers and stealing the data stored on them. Companies use these servers to share sensitive files and information with people outside of their organization.
>
> The ransomware gang then contacted the organizations and demanded $10 million in bitcoin or they would publish the stolen data.

References:

https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-colorado-miami-universities/
https://www.bleepingcomputer.com/news/security/list-of-ransomware-that-leaks-victims-stolen-files-if-not-paid/
https://www.bleepingcomputer.com/news/security/university-of-utah-hit-by-ransomware-pays-457k-ransom/
https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

Lessons Learned

- Threat of ransomware to the open science community
- Report coming soon from Michigan State University and Trusted CI

Reference:
https://blog.trustedci.org/2021/04/michigan-state-university-engages-with.html

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Wednesday, April 7, 2021

Michigan State University Engages with Trusted CI to Raise Awareness of Cybersecurity Threats in the Research Community

Cybersecurity exploits are on the rise across university communities, costing valuable resources, and loss of productivity, research data, and personally identifiable information. In a DXC report, it was estimated that an average ransomware attack can take critical systems down for 16 days, and the overall worldwide cost of ransomware in 2020 was predicted to cost $170 billion. Additional reputational impacts of cybersecurity attacks, although hard to measure, regularly weigh in the minds of scientists and researchers.

An event of this nature occurred at Michigan State University (MSU), which experienced a ransomware attack in May 2020. While many organizations attempt to keep the public from finding out about cyberattacks for fear of loss of reputation or follow-up attacks, MSU has decided to make elements of its attack public in the interests of transparency, to encourage disclosure of similar types of attacks, and perhaps more importantly, to educate the open-science community about the threat of ransomware and other destructive types of cyberattacks. The overarching goal is to raise awareness about rising cybersecurity threats to higher education in hopes of driving safe cyberinfrastructure practices across university communities.

To achieve this, the CIO's office at MSU has engaged with Trusted CI, the NSF Cybersecurity Center of Excellence, in a collaborative review and analysis of the ransomware attack suffered by MSU last year. The culmination of the engagement will be a report focusing on lessons learned during the analysis; these 'Lessons Learned' would then be disseminated to the research community. We expect the published report to be a clear guide for researchers and their colleagues who are security professionals to help identify, manage, and mitigate the risk of ransomware and other types of attacks.

Posted by Andrew K. Adams at 10:12 AM

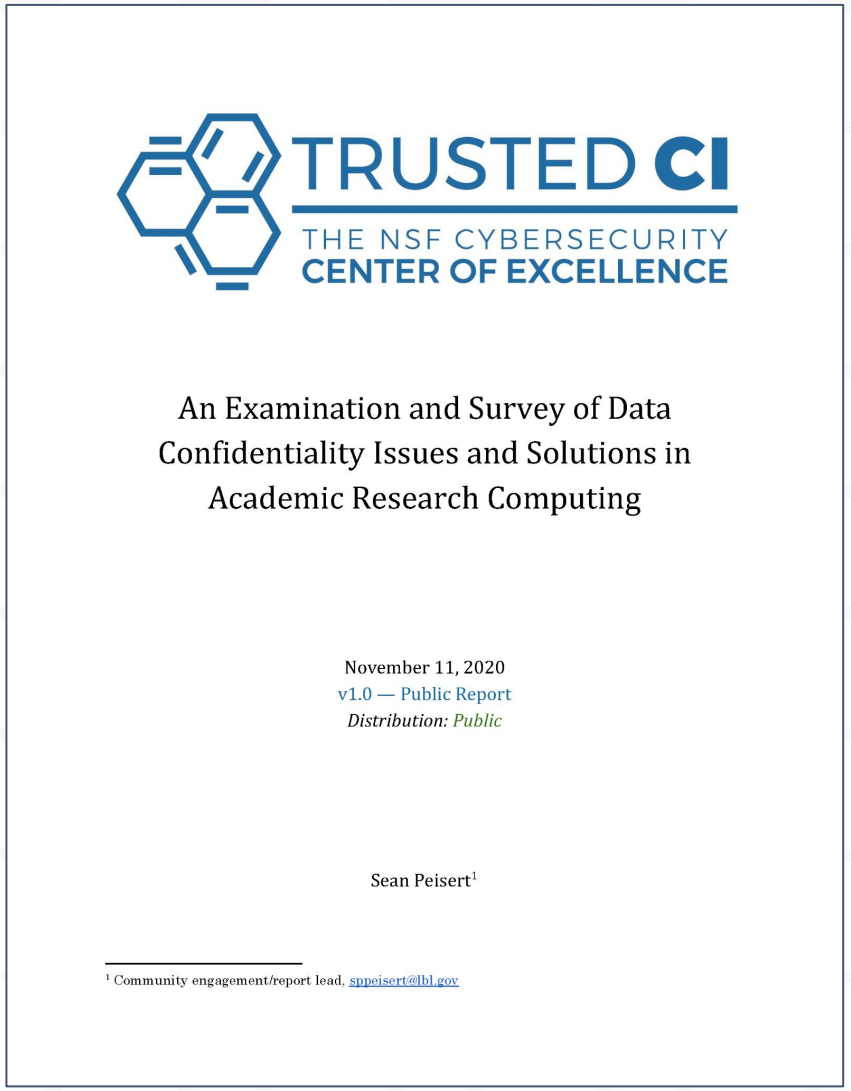
Labels: engagements, incident response, ransomware

2020 Data Confidentiality Survey

- Recommendations to campuses supporting research on sensitive data while ensuring security & privacy
- Sensitive Data Examples
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Controlled Unclassified Information (CUI)
- Documentation
  - Data Management Plan (DMP) with sponsor
  - Data Use Agreement (DUA) with data provider

Sean Peisert, "An Examination and Survey of Data Confidentiality Issues and Solutions in Academic Research Computing," Trusted CI Report, November 2020. https://escholarship.org/uc/item/7cz7m1ws

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

An Examination and Survey of Data Confidentiality Issues and Solutions in Academic Research Computing

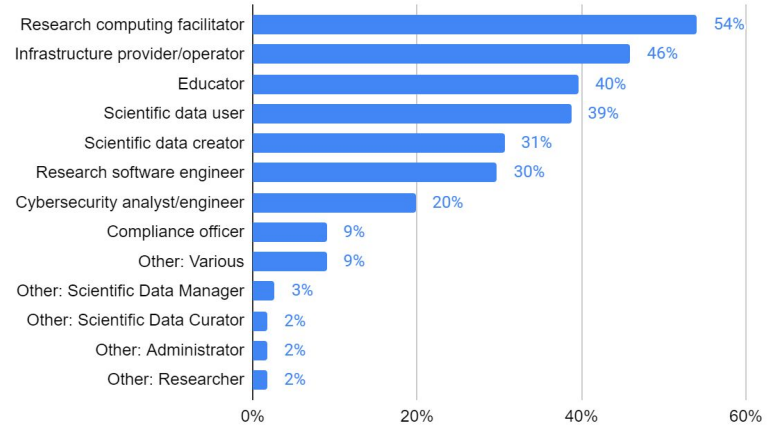
November 11, 2020
v1.0 — Public Report
Distribution: Public

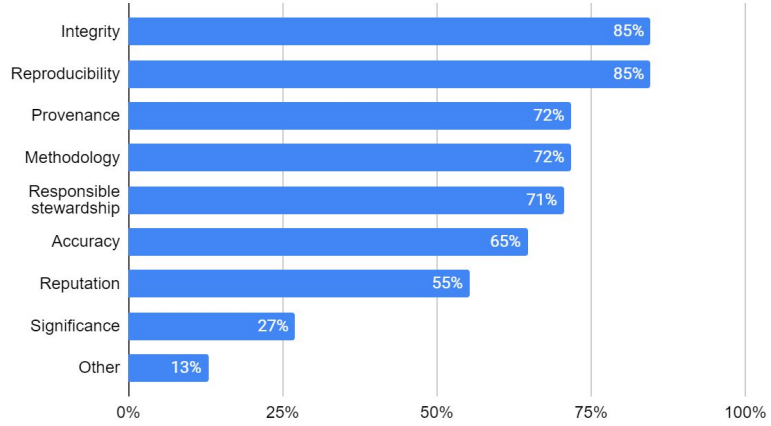
Sean Peisert[1]

[1] Community engagement/report lead, sppeisert@lbl.gov

2020 Trustworthy Data Survey

- 111 survey responses from April/May 2020
- Common definition of trustworthiness was elusive
- Most (90%) agreed that trustworthiness of scientific data is important
- Only 69% believed that trustworthiness fell within their job duties
- Top concerns were: impact on scientific results, reputational risks, & integrity of the scientific process
- Community as a whole welcomes guidance
- Full Report: https://doi.org/10.5281/zenodo.3906865





TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/trustworthy-data

Guidance from the Trustworthy Data Working Group

- Stakeholders: Data User, Data Provider, Infrastructure Provider, Research Facilitator, & Compliance Professional
- Barriers to Trustworthiness: conflicts between security and reproducibility (e.g., software patching), accidents, lack of funding/incentives, data quality
- Tools exist for Availability, Authorization, & Integrity
- Authenticity, Confidentiality, and Reproducibility need stronger support
- Communicate trustworthiness via metadata and repository certifications/policies
- Full Report: https://doi.org/10.5281/zenodo.4056241

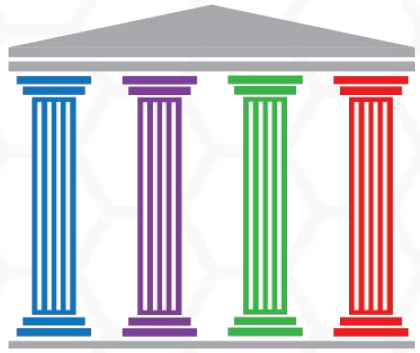
Tool / Attribute	Availability	Integrity	Authenticity	Accepted Techniques	Authorization	Confidentiality	Credible Source	Reproducibility
3rd party data repo	O	O	O				O	O
Policy for network/cloud storage	N	O			N		N	
Archival storage	N	O					O	O
Workflow integrity checking		S	N	N				N
Access controls	N	N			S	N		
Physical security protections	N	N			N	N		
Network controls	N	N			N			
Logging	O	O			O			
Multifactor Authentication	O	O			O			
Intrusion detection/protection	O	O			O			
File/host integrity check	O	N			O			
RAID file system	N	N						
External backups	N	O						

Symbol	Meaning
S	Sufficient: This tool/technology alone can establish an assertion of the desired attribute, however weak it may be.
N	Necessary: This tool/technology is required to provide a stronger, credible assertion of the desired attribute.
O	Optional: This tool/technology can help strengthen the assertion of the desired attribute, however that is not its design intent.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/trustworthy-data

The Trusted CI Framework



Mission Alignment

- Information classification, asset inventory, external requirements

Governance

- Roles and responsibilities, policies, risk acceptance, program evaluation

Resources

- People, budgets, services and tools

Controls

- Procedural, technical, administrative safeguards and countermeasures

https://trustedci.org/framework

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

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/