
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org

Cybersecurity: We Don’t Have It Right Yet

Von Welch
Director, Trusted CI
Director, IU CACR

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

2018 NSF Cybersecurity Summit

August 22nd, 2018

Cybersecurity Is a New Profession.

Is It Possible We Don’t Have It Right Yet?

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

No, We Don’t Have Cybersecurity Right Yet.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

How Did I Arrive at This Conclusion?

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Dreaded Cybersecurity Demo

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Creating an Interesting Cybersecurity Demonstration Can Be a Major Challenge.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Copper Plumbing Problem: Your House Before Copper Plumbing

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Copper Plumbing Problem: Your House After Copper Plumbing

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Usual Cybersecurity Demo

http://bsdpants.blogspot.com/2010/08/truncated-syslog-messages.html

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

I Found Myself Facing Another Cybersecurity Demo…

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

SWIP

Scientific Workflow Integrity with Pegasus

https://cacr.iu.edu/projects/swip/

TRUSTED CI

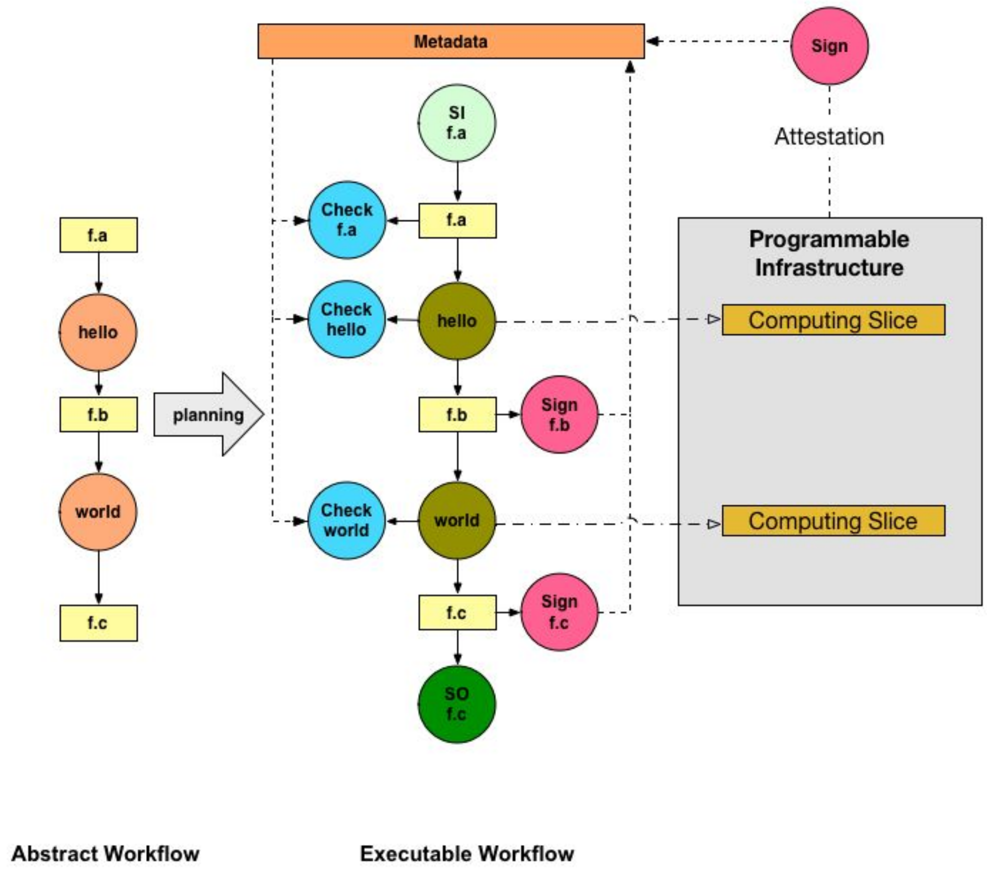
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH

Pegasus

renci

Goal: Add Data Integrity Assurances to Pegasus Workflows



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

My Threat Model: Malicious Actors

- Script kiddies out for glory.
- Nation-states trying to disrupt/embarrass U.S. science.
- Disgruntled insiders.
- Grad students, postdocs, staff going for that publication with (bogus) phenomenal results.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

“Security” Defined by Merriam Webster

https://www.merriam-webster.com/dictionary/security

4: measures taken to guard against espionage or sabotage, crime, attack, or escape

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Non-malicious Risks…

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CERN Study of Disk Errors

Examined Disk, Memory, RAID 5 errors.

“The error rates are at the 10-7 level, but with complicated patterns.” (e.g., 80% of disk errors were 64k regions of corruption.)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Data integrity

Bernd Panzer-Steindel, CERN/IT
Draft 1.3 8. April 2007

https://indico.cern.ch/event/13797/contributions/1362288/attachments/115080/163419/Data_integrity_v3.pdf

Network Corruption

Network router software inadvertently corrupts TCP data and checksum!

XSEDE and Internet2 example from 2013.

Second similar case in 2017 example with FreeSurfer/Fsurf project.

BROCADE

TECHNICAL SUPPORT BULLETIN

June 28, 2013

TSB 2013-162-A

SEVERITY: Critical- Service Impact

PRODUCTS AFFECTED:

Brocade NetIron XMR/MLX 100G module (BR-MLX-100Gx2-X and BR-MLX-100Gx1-X).

CORRECTED IN RELEASE:

The fix will be in patch releases of NI 5.3.00eb, 5.4.00d and 5.5.00c and later releases.
This issue is not applicable to software release NI 5.2.00 and previous releases.

BULLETIN OVERVIEW

When transferring data through 100G modules, a portion of the packet may get corrupted. Corruption is typically seen when transferring jumbo frames.

https://www.xsede.org/news/-/news/item/6390
Brocade TSB 2013-162-A

TCP Checksum Breakdown at Big Data Sizes

"We conclude that the checksum will fail to detect errors for roughly 1 in 16 million to 1 in 10 billion packets."

When The CRC and TCP Checksum Disagree

Jonathan Stone
Stanford Distributed Systems Group
jonathan@dsg.stanford.edu

Craig Partridge
BBN Technologies
craig@bbn.com

ABSTRACT

Traces of Internet packets from the past two years show that between 1 packet in 1,100 and 1 packet in 32,000 fails the TCP checksum, even on links where link-level CRCs should catch all but 1 in 4 billion errors. For certain situations, the rate of checksum failures can be even higher: in one hour-long test we observed a checksum failure of 1 packet in 400. We investigate why so many errors are observed, when link-level CRCs should catch nearly all of them.

We have collected nearly 500,000 packets which failed the TCP or UDP or IP checksum. This dataset shows the Internet has a wide variety of error sources which can not be detected by link-level checks. We describe analysis tools that have identified nearly 100 different error patterns. Categorizing packet errors, we can infer likely causes which explain roughly half the observed errors. The causes span the entire spectrum of a network stack, from memory errors to bugs in TCP.

After an analysis we conclude that the checksum will fail to detect errors for roughly 1 in 16 million to 10 billion packets. From our analysis of the cause of errors, we propose simple changes to several protocols which will decrease the rate of undetected error. Even so, the highly non-random distribution of errors strongly suggests some applications should employ application-level checksums or equivalents.

We found this phenomenon of interest for two reasons. First, the error rate is disturbingly high. A naive calculation suggests that with a typical TCP segment size of a few hundred bytes, a file transfer of a million bytes (e.g., the size of a modest software down-load) might well have an undetected error. (We hasten to emphasize this calculation *is* naive. As we discuss later in the paper, a more realistic calculation requires an understanding of the types of errors.) Understanding why these errors occur could have a major impact on the reliability of Internet data transfers.

Second, there has been a long-running debate in the networking community about just how valuable the TCP (and UDP) checksum is. While practitioners have long argued on anecdotal evidence and personal experience that the checksum plays a vital role in preserving data integrity, few formal studies have been done. Studying these errors seemed a good chance to improve our understanding of the role of the checksum.

In this paper we report the results of two years of analysis, using traffic traces taken at a variety of points in the Internet. While we do not have a complete set of explanations (about half the errors continue to resist classification or identification) we can explain many of the errors and discuss their impact.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Back To That Demonstration...

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

My Demonstration Fear:
We Add Integrity Assurances.
We Wait For The Integrity Error.
And We Wait...

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

A Little Insurance: Chaos Jungle

Inspired by Netflix Chaos Monkey.

https://github.com/Netflix/chaosmonkey

Virtual infrastructure (ORCA) with intentional integrity errors.

Now we can test - and demo! - how software runs with errors.

https://github.com/Netflix/chaosmonkey/blob/master/docs/logo.png

The Email That Changed My Thinking

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

OSG-KINC

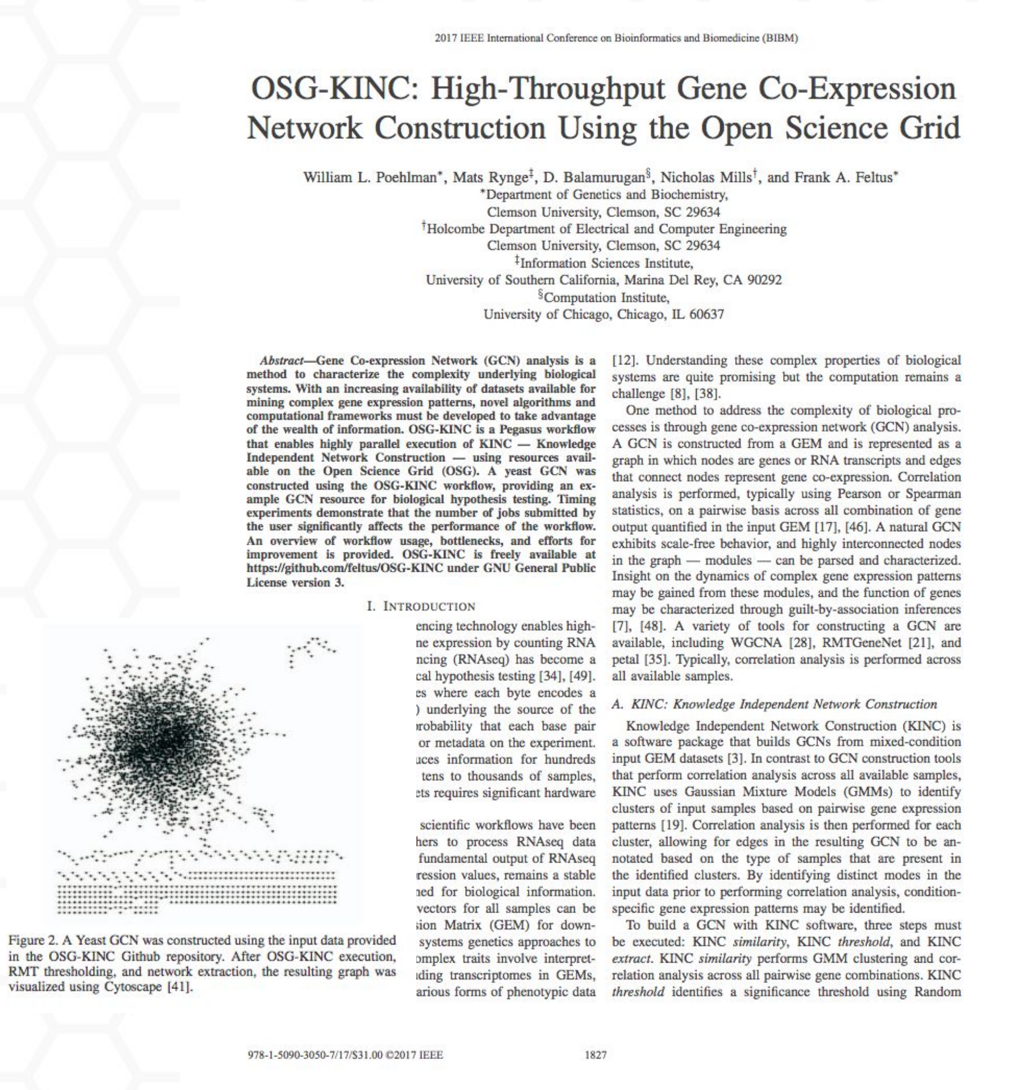
Pegasus workflow from Alexus Feltus and William Poehlman running on the Open Science Grid.

Early user of Pegasus with SWIP integrity checking.

Real-world 50k job workflow.

https://github.com/feltus/OSG-KINC

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



2017 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)

OSG-KINC: High-Throughput Gene Co-Expression Network Construction Using the Open Science Grid

William L. Poehlman*, Mats Rynge‡, D. Balamurugan§, Nicholas Mills†, and Frank A. Feltus*
*Department of Genetics and Biochemistry,
Clemson University, Clemson, SC 29634
†Holcombe Department of Electrical and Computer Engineering
Clemson University, Clemson, SC 29634
‡Information Sciences Institute,
University of Southern California, Marina Del Rey, CA 90292
§Computation Institute,
University of Chicago, Chicago, IL 60637

***Abstract*—Gene Co-expression Network (GCN) analysis is a method to characterize the complexity underlying biological systems. With an increasing availability of datasets available for mining complex gene expression patterns, novel algorithms and computational frameworks must be developed to take advantage of the wealth of information. OSG-KINC is a Pegasus workflow that enables highly parallel execution of KINC — Knowledge Independent Network Construction — using resources available on the Open Science Grid (OSG). A yeast GCN was constructed using the OSG-KINC workflow, providing an example GCN resource for biological hypothesis testing. Timing experiments demonstrate that the number of jobs submitted by the user significantly affects the performance of the workflow. An overview of workflow usage, bottlenecks, and efforts for improvement is provided. OSG-KINC is freely available at https://github.com/feltus/OSG-KINC under GNU General Public License version 3.**

I. Introduction

encing technology enables high-
ne expression by counting RNA
ncing (RNAseq) has become a
cal hypothesis testing [34], [49].
es where each byte encodes a
) underlying the source of the
robability that each base pair
or metadata on the experiment.
uces information for hundreds
tens to thousands of samples,
ets requires significant hardware

scientific workflows have been
hers to process RNAseq data
fundamental output of RNAseq
ression values, remains a stable
ned for biological information.
vectors for all samples can be
sion Matrix (GEM) for down-
systems genetics approaches to
omplex traits involve interpret-
ding transcriptomes in GEMs,
arious forms of phenotypic data

Figure 2. A Yeast GCN was constructed using the input data provided in the OSG-KINC Github repository. After OSG-KINC execution, RMT thresholding, and network extraction, the resulting graph was visualized using Cytoscape [41].

[12]. Understanding these complex properties of biological systems are quite promising but the computation remains a challenge [8], [38].

One method to address the complexity of biological processes is through gene co-expression network (GCN) analysis. A GCN is constructed from a GEM and is represented as a graph in which nodes are genes or RNA transcripts and edges that connect nodes represent gene co-expression. Correlation analysis is performed, typically using Pearson or Spearman statistics, on a pairwise basis across all combination of gene output quantified in the input GEM [17], [46]. A natural GCN exhibits scale-free behavior, and highly interconnected nodes in the graph — modules — can be parsed and characterized. Insight on the dynamics of complex gene expression patterns may be gained from these modules, and the function of genes may be characterized through guilt-by-association inferences [7], [48]. A variety of tools for constructing a GCN are available, including WGCNA [28], RMTGeneNet [21], and petal [35]. Typically, correlation analysis is performed across all available samples.

A. KINC: Knowledge Independent Network Construction

Knowledge Independent Network Construction (KINC) is a software package that builds GCNs from mixed-condition input GEM datasets [3]. In contrast to GCN construction tools that perform correlation analysis across all available samples, KINC uses Gaussian Mixture Models (GMMs) to identify clusters of input samples based on pairwise gene expression patterns [19]. Correlation analysis is then performed for each cluster, allowing for edges in the resulting GCN to be annotated based on the type of samples that are present in the identified clusters. By identifying distinct modes in the input data prior to performing correlation analysis, condition-specific gene expression patterns may be identified.

To build a GCN with KINC software, three steps must be executed: KINC *similarity*, KINC *threshold*, and KINC *extract*. KINC *similarity* performs GMM clustering and correlation analysis across all pairwise gene combinations. KINC *threshold* identifies a significance threshold using Random

978-1-5090-3050-7/17/$31.00 ©2017 IEEE 1827

4 Integrity Errors Caught - One Impacted 56 Jobs!

From: **Mats Rynge** rynge@isi.edu
Subject: [swip-l] First integrity error in the wild
Date: April 5, 2018 at 12:54 AM
To: swip-l@list.iu.edu

One of William's OSG-KINC workflows encountered 60 integrity errors in the wild. The problematic jobs were automatically retried and the workflow finished successfully.

I have not done a full analysis yet, but I will provide a preview as I will be out of the office tomorrow: The workflow had 50606 jobs. 1 error was at UColorado. 59 errors were at UNL. 56 of those 59 was for the same input file, with with the same faulty checksum. I suspect the 56 errors were probably due to something like a corrupted cache - that would explain why multiple jobs got the same broken file.

List of errors:

http://workflow.isi.edu/kinc-1522378583-60-errors/error-list.txt

The first field in the error list points to our/err files inside the run directory, which is available from here (26 GBs):

http://workflow.isi.edu/kinc-1522378583-60-errors/kinc-1522378583.tar.gz

--
Mats Rynge
USC/ISI - Pegasus Team <http://pegasus.isi.edu>

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Broadening My Focus

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

“Security” Defined by Merriam Webster

https://www.merriam-webster.com/dictionary/security

4: measures taken to guard against espionage or sabotage, crime, attack, or escape

"Security" Defined by Merriam Webster

https://www.merriam-webster.com/dictionary/security

1: freedom from danger (safety), freedom from fear or anxiety

4: measures taken to guard against espionage or sabotage, crime, attack, or escape

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity per OMB

"**<u>Prevention of damage</u>** to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

...No mention of malicious intent.

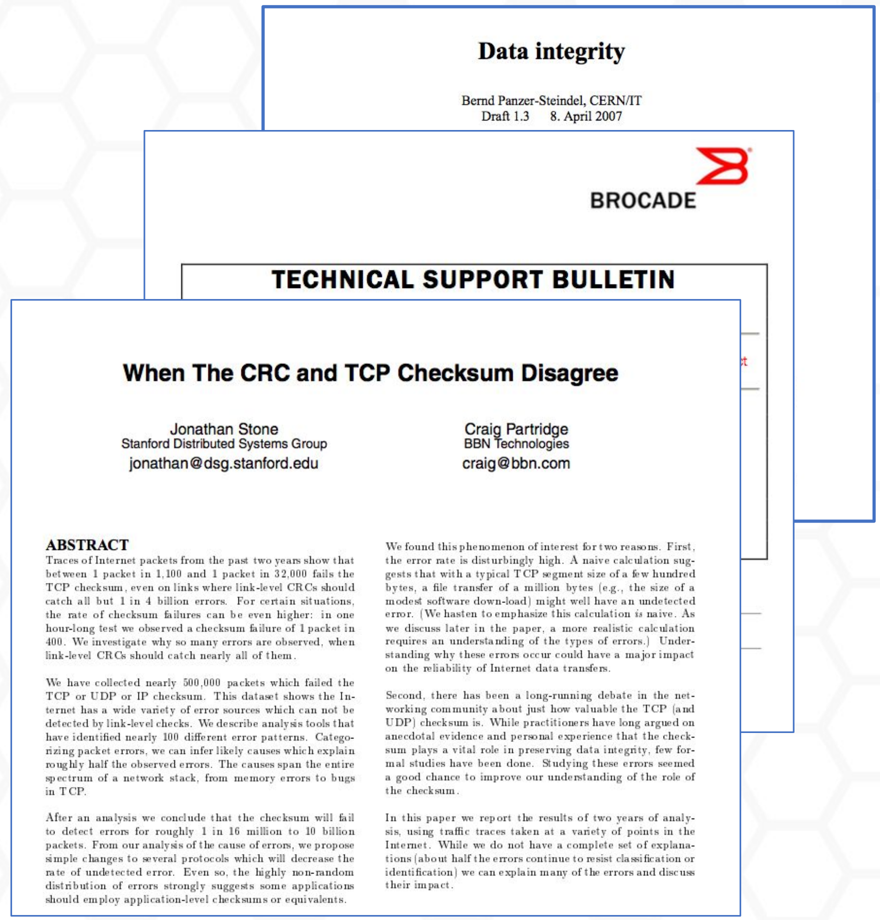
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

What Does Broadening Our Scope to All IT Risks Mean?

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

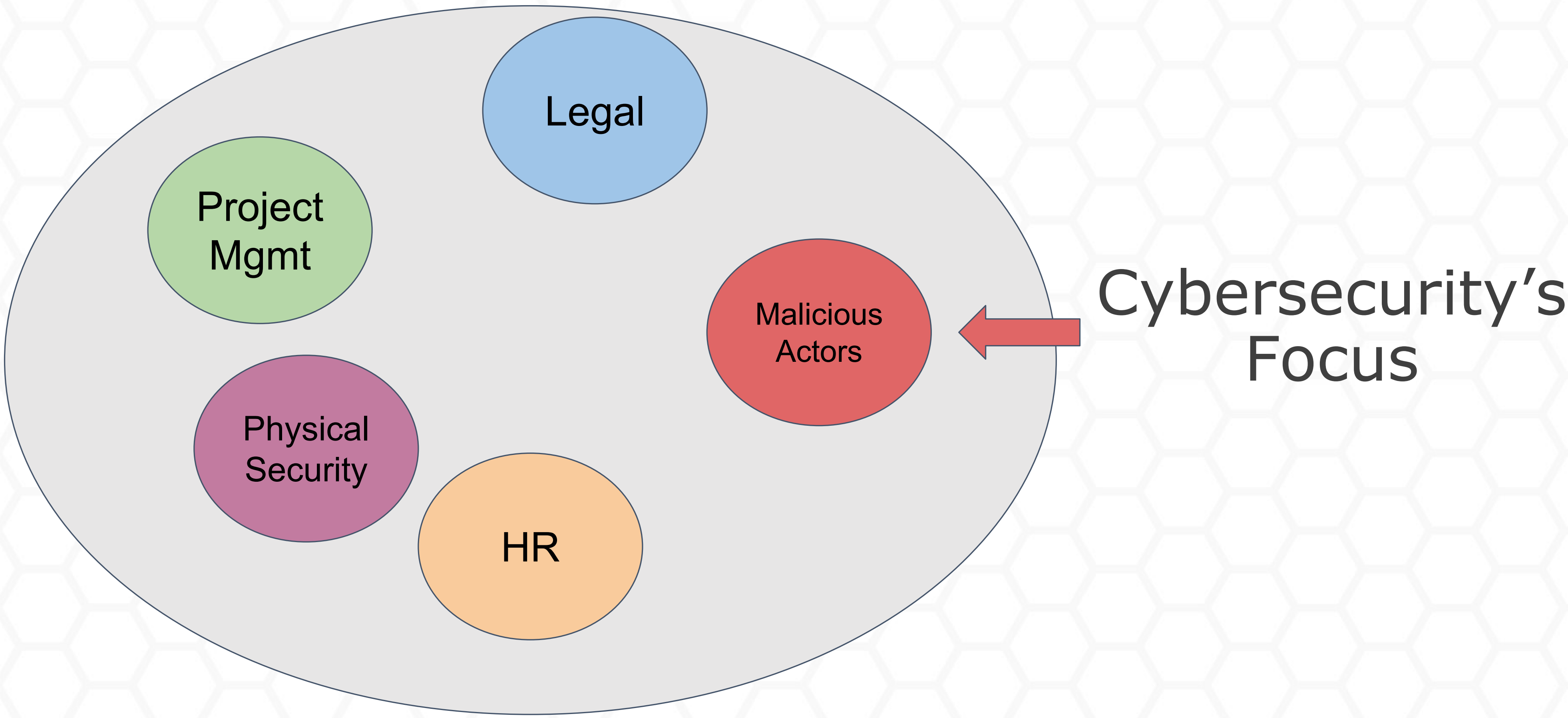
Malicious and Non-malicious Risks

- Script kiddies out for glory.
- Nation-states trying to disrupt/embarrass U.S. science.
- Disgruntled insiders.
- Grad students, postdocs, staff going for that publication with (bogus) phenomenal results.

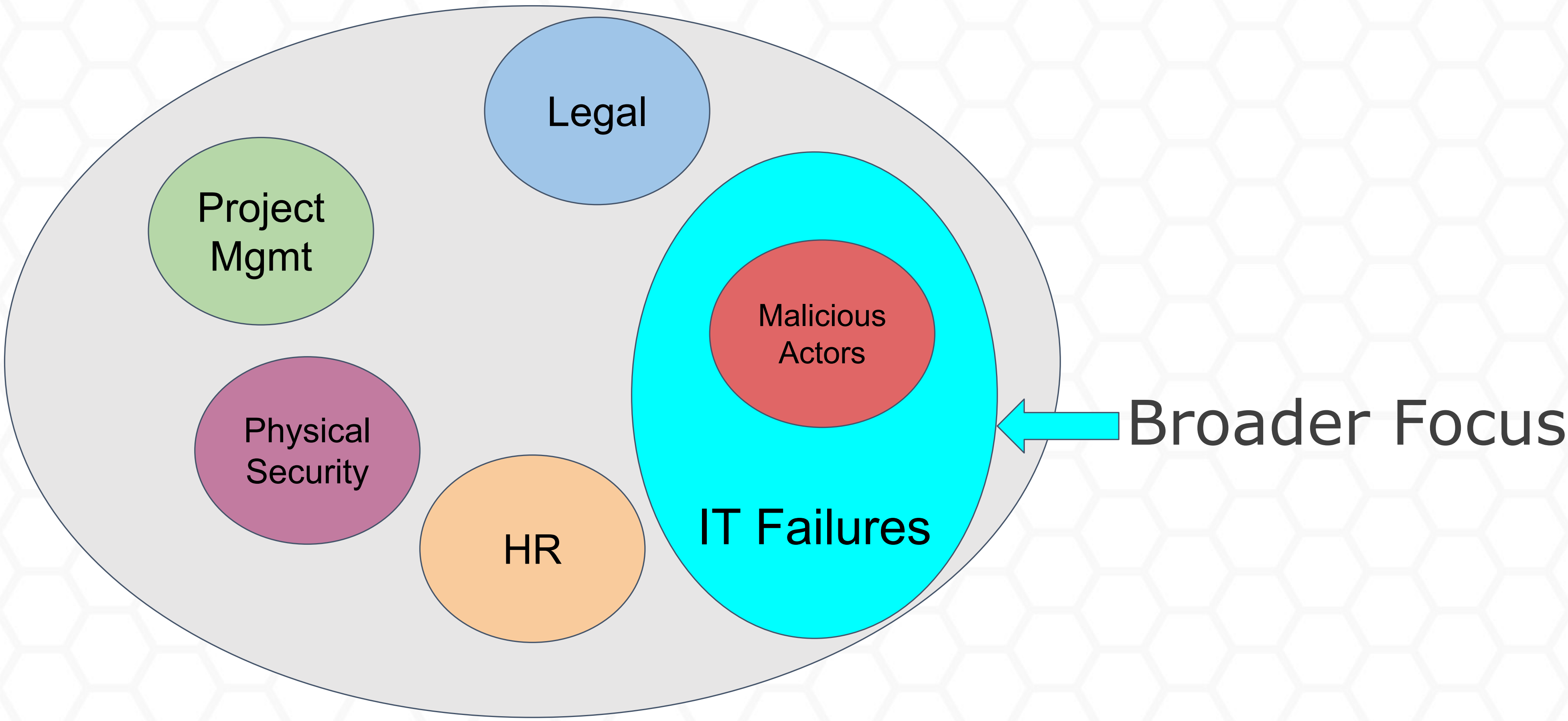


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Risk Pool:
What Keeps A Project Leader Awake



The Risk Pool:
What Keeps A Project Leader Awake



Cybersecurity Triad

Confidentiality

Integrity

Availability

Cybersecurity for Science Triad?

TRUSTED CI

THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Efficient

Availability

Collaborative

Fast

http://www.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816

Some history of scale…

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

Credit: Ian Bird

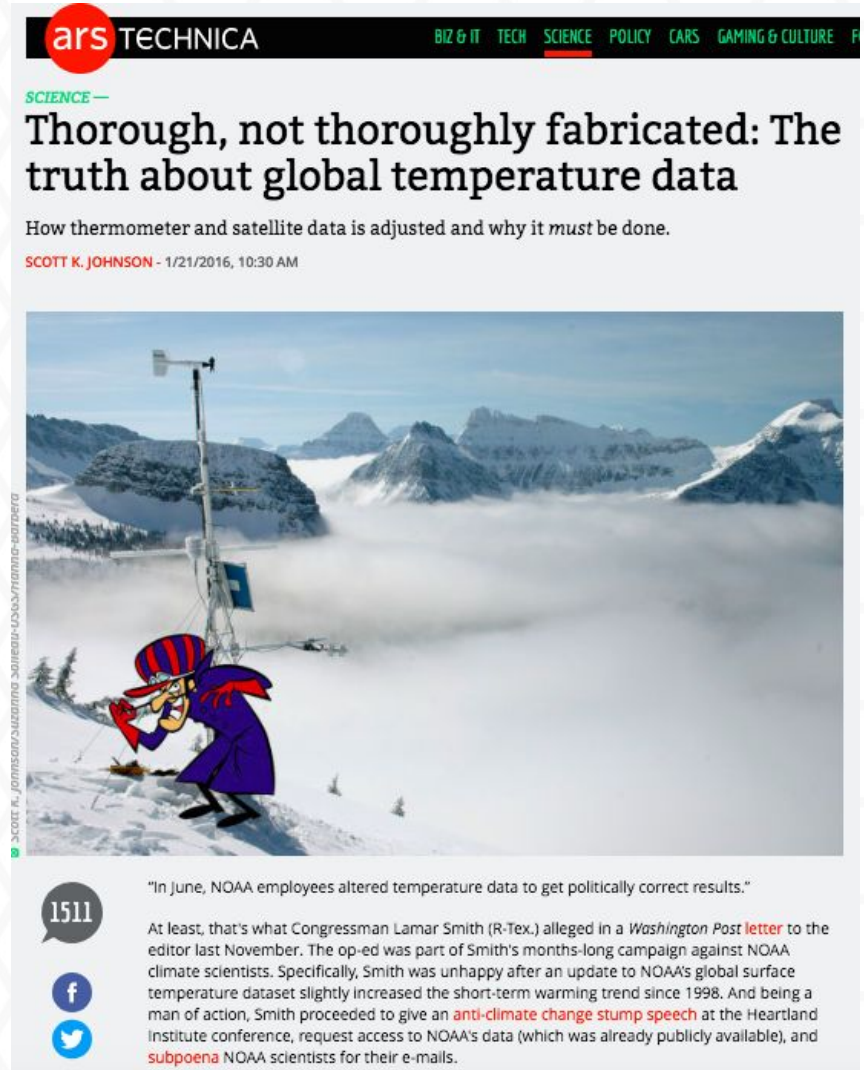
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted

Integrity

Quality Assured

Defensible


ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

SCIENCE —

Thorough, not thoroughly fabricated: The truth about global temperature data

How thermometer and satellite data is adjusted and why it *must* be done.

SCOTT K. JOHNSON - 1/21/2016, 10:30 AM

1511

"In June, NOAA employees altered temperature data to get politically correct results."

At least, that's what Congressman Lamar Smith (R-Tex.) alleged in a *Washington Post* letter to the editor last November. The op-ed was part of Smith's months-long campaign against NOAA climate scientists. Specifically, Smith was unhappy after an update to NOAA's global surface temperature dataset slightly increased the short-term warming trend since 1998. And being a man of action, Smith proceeded to give an anti-climate change stump speech at the Heartland Institute conference, request access to NOAA's data (which was already publicly available), and subpoena NOAA scientists for their e-mails.

http://science.sciencemag.org/content/354/6317/1240

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Based on these definitions, the *Association for Computing Machinery* has adopted the following definitions (Association for Computing Machinery, 2016)

Repeatability *(Same team, same experimental setup): The measurement can be obtained with stated precision by the same team using the same measurement procedure, the same measuring system, under the same operating conditions, in the same location on multiple trials. For computational experiments, this means that a researcher can reliably repeat her own computation.*

Replicability *(Different team, same experimental setup): The measurement can be obtained with stated precision by a different team using the same measurement procedure, the same measuring system, under the same operating conditions, in the same or a different location on multiple trials. For computational experiments, this means that an independent group can obtain the same result using the author's own artifacts.*

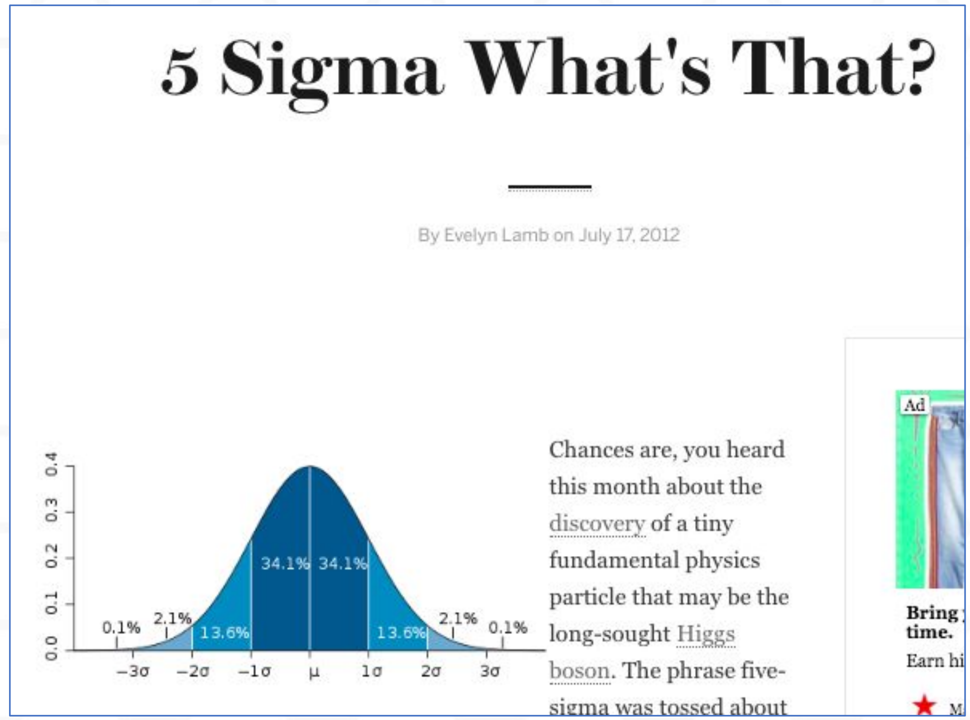
Reproducibility *(Different team, different experimental setup): The measurement can be obtained with stated precision by a different team, a different measuring system, in a different location on multiple trials. For computational experiments, this means that an independent group can obtain the same result using artifacts which they develop completely independently.*

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5778115/
https://www.acm.org/publications/policies/artifact-review-badging

This Won’t Be Easy

We need to really understand the needs of science

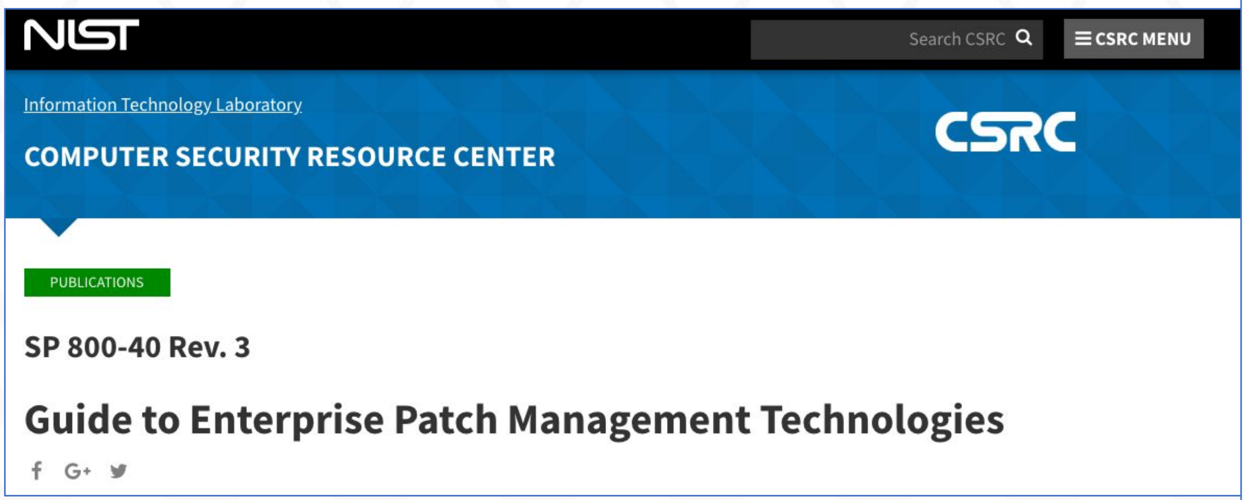
Are all bits equal?

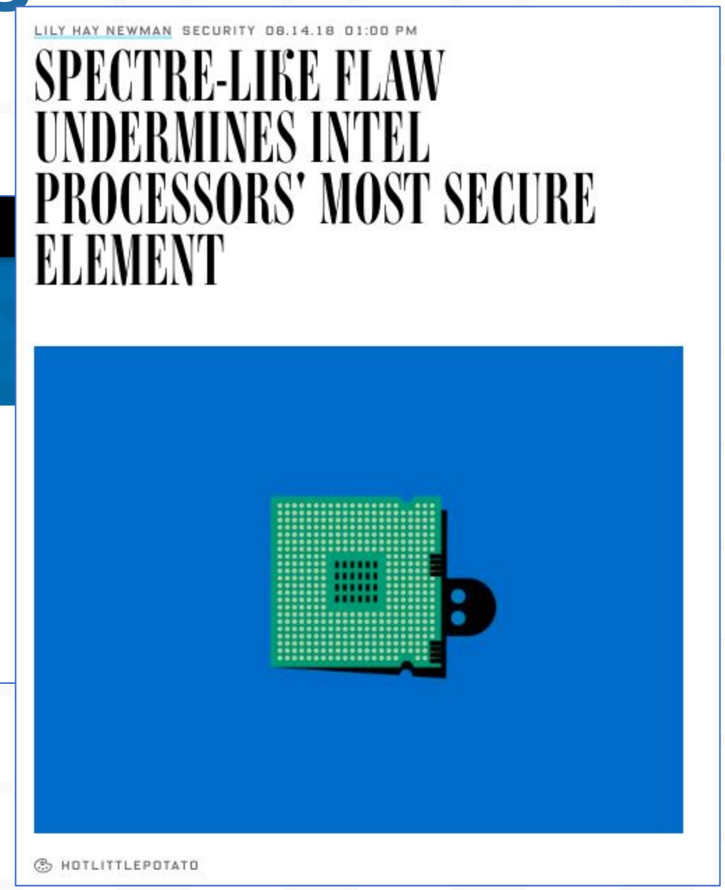


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://blogs.scientificamerican.com/observations/five-sigmawhats-that/

Reproducibility and Patching: A Grand Challenge?





TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
https://www.wired.com/story/foreshadow-intel-secure-enclave-vulnerability/

We Need to Work With Our CI Developers and Operators On These Risks

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

- Software must be well engineered to be secured.
- Computers must be well administered to be secured.
- Networks must be well administered to be secured.
- Systems must be understood to be secured.

What’s the Payoff?

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

We Have to Deal with IT Risks Anyways…

Any IT failures create noise cybersecurity has to deal with.

Better Relationship To Science Community

Address More Of The Risk Pool

==

Better Value To Scientists.

Better Understanding is Better

Better Understanding of Science

==

Better Cybersecurity, No Matter the Scope.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI’s Role

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Celebrating five years of Trusted CI and the NSF Cybersecurity Center of Excellence

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CENTER FOR APPLIED
CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

PITTSBURGH
SUPERCOMPUTING
CENTER

THE UNIVERSITY of WISCONSIN
MADISON

NSF

I would add an image of Kevin Thompson if I could find a good one.

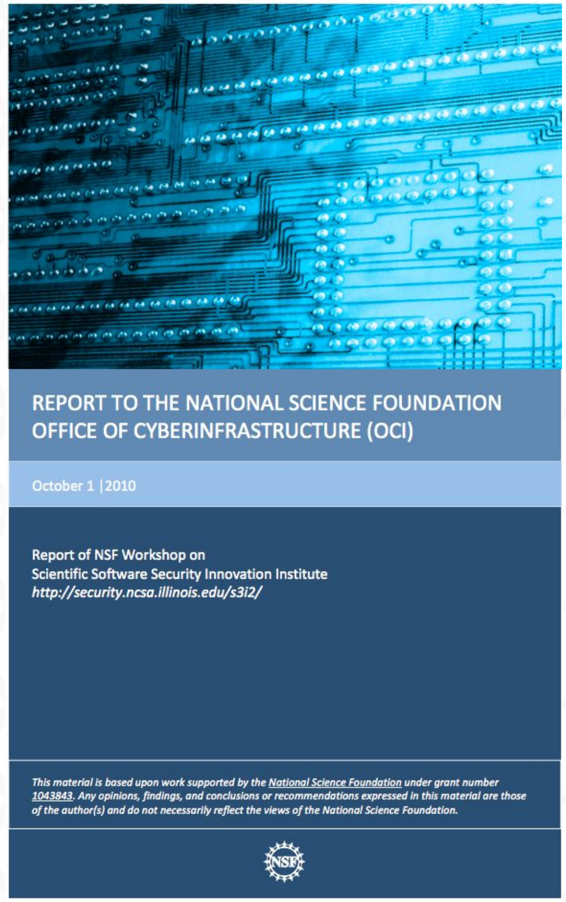
We don’t make the technology.
We help you make sense of it.

Trusted CI:

Provides cybersecurity leadership and guidance.

Helps community tackle problems and form consensus.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



http://security.ncsa.illinois.edu/s3i2/

The Trusted CI Broader Impacts Project Report

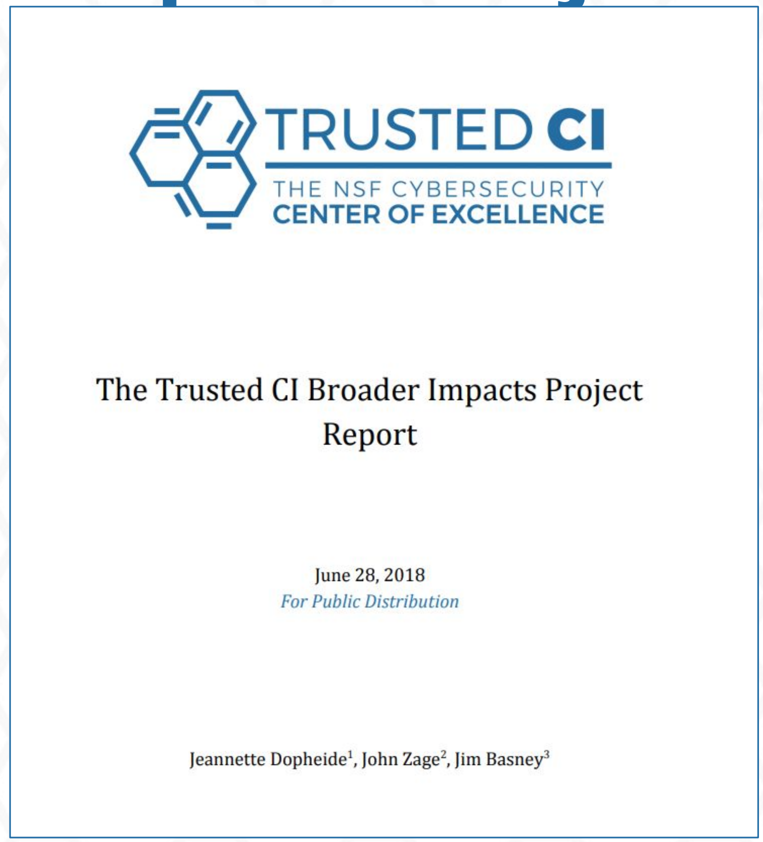
Trusted CI has impacted over 190 NSF projects.

More than 150 members of NSF projects attended our NSF Cybersecurity Summit.

Seventy NSF projects attended our webinars.

More than 250 hours of training.

Thirty-five engagements (nine LFs).


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Broader Impacts Project Report

June 28, 2018
For Public Distribution

Jeannette Dopheide[1], John Zage[2], Jim Basney[3]

http://hdl.handle.net/2022/22148

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

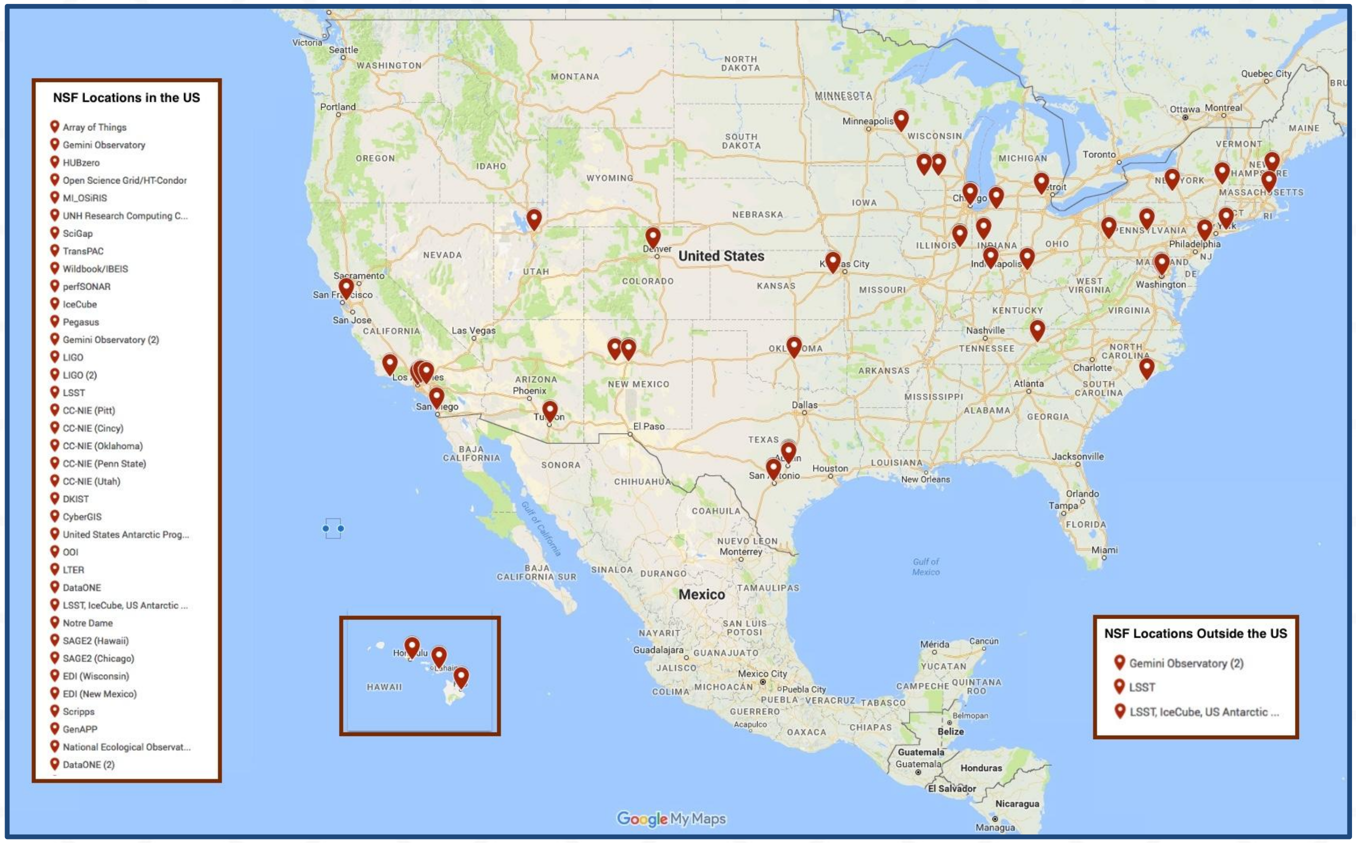
Engagements:
One-on-one Collaborations

Take applications every six months.

Accepting applications:

trustedci.org/application/

Deadline: Oct 1



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Addressing Science's Cybersecurity Concerns

New: Security Best Practices for Academic Cloud Service Providers

https://trustedci.org/cloud-service-provider-security-best-practices/

Coming Soon: Software Engineering Guide

Securing Software Supporting Science

Operational Security

http://trustedci.org/guide

Identity Management Best Practices

http://trustedci.org/iam

Open Science Cyber Risk Profile

https://trustedci.org/oscrp/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Building Community
Leading a Conversation

HPC wire

Since 1987 · Covering the Fastest Computers in the World and the People Who Run Them

- Home
- Technologies
- Sectors
- AI/ML/DL
- Exascale
- Specials
- Resource Library
- Events
- Job Bank
- About
- Solution Channels

Hacking Academia at PEARC18

By Ken Chiacchia

July 31, 2018

Despite decades of funding for cybersecurity efforts, the problem has fundamentally not been addressed, Anita Nikolich of the Illinois Institute of Technology said in a plenary talk at the PEARC18 conference in Pittsburgh, Pa., on July 26. Moving the needle on cybersecurity will require engagement of academic researchers with the hacking community, she argued.

"I've seen both sides of this," said the former Program Director for Cybersecurity at the NSF. "You have these two worlds of professional, academic researchers and

SCIENCE NODE

Home Archive Contribute Sponsor About Give Now

Securing the scientific workflow

The 21st century scientific workflow has unique security challenges, with data and instrumentation among the targets criminals find attractive. The NSF is sponsoring innovation to secure tomorrow's discoveries.

Speed read

- Anita Nikolich outlines the state of security in the modern scientific workflow.
- Sensitive data sets and expensive instruments are vulnerable cybertargets.
- The US National Science Foundation (NSF) is investing in smart shields for these vital international interests.

Science in the 21st century is increasingly reliant on high-performance computation, boutique instrumentation, and low latency, high bandwidth research network connectivity. To shield scientific targets from cyber attacks, the US National Science Foundation (NSF) is fostering research to ensure the discoveries of tomorrow aren't stolen today. The Science Node spoke with Anita Nikolich, director of the NSF's Cybersecurity Innovation for Cyberinfrastructure (CICI) program, about the state of cybersecurity in the modern scientific workflow and how the NSF is sponsoring innovations to secure this space for future discovery.

Posted on 09 MAR, 2016

Lance Farrell
Managing Editor

Share this story

Republish

Tags

National Science Foundation (NSF)

Vision for the Next Five Years

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI 5-year Vision and Strategic Plan

"A NSF cybersecurity ecosystem, formed of people, practical knowledge, processes, and cyberinfrastructure, that enables the NSF community to both manage cybersecurity risks and produce trustworthy science in support of NSF's vision of a nation that is the global leader in research and innovation."

Basis for Trusted CI going forward.

I want your feedback!

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Trusted CI Vision for an NSF Cybersecurity Ecosystem

And Five-year Strategic Plan

2019-2023

Version 1

June 20th, 2018

http://hdl.handle.net/2022/22178

Example Challenges and Initiatives from the Vision

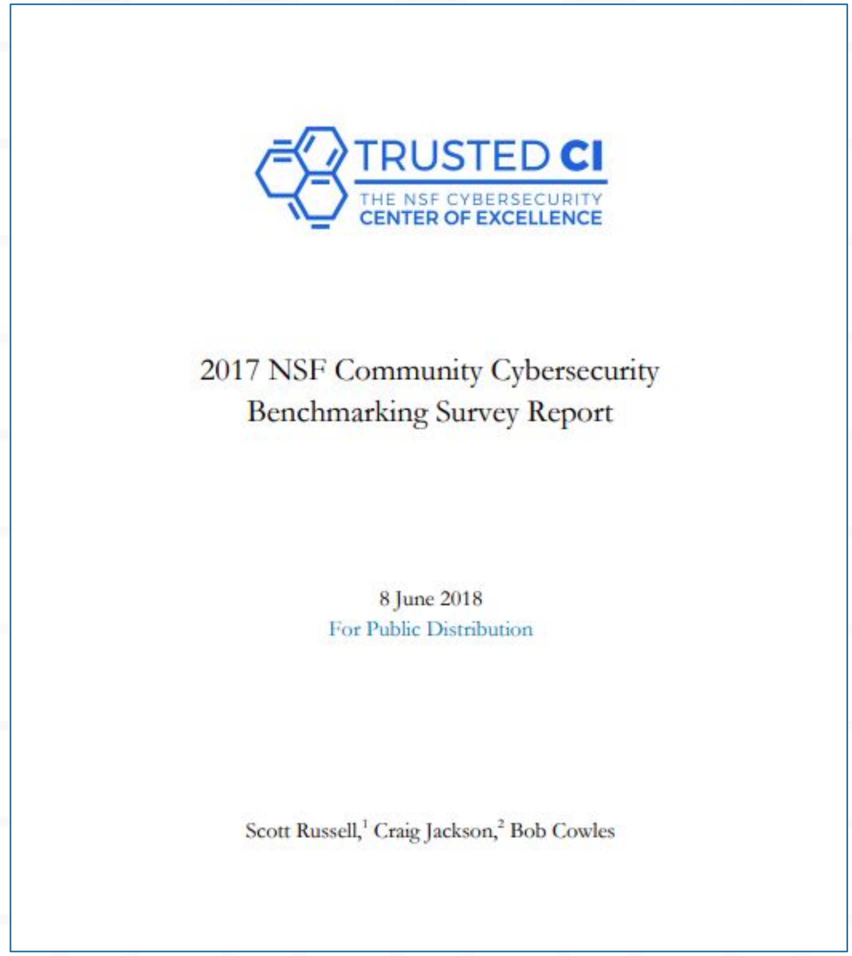
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Room To Grow

Some select results:

- Respondents' cybersecurity budgets vary widely.
- Respondents inconsistently establish cybersecurity officers.
- Residual risk acceptance is inconsistently practiced.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE



TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

2017 NSF Community Cybersecurity Benchmarking Survey Report

8 June 2018
For Public Distribution

Scott Russell,[1] Craig Jackson,[2] Bob Cowles

http://hdl.handle.net/2022/22171

Building Trust Is Hard

We have made great progress in building community and sharing knowledge.

Still a long way to go: We need to be sharing more, especially regarding breaches, incidents, and lessons learned.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Strategic Objective 1.3: Build the Community needed for the NSF Cybersecurity Ecosystem

"...continue to mature and grow the community"

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Under Pressure

The Higher Ed community is seeing increasing pressure to adopt cybersecurity.

This is good.

But…

https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108175

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Is It Appropriate for Science?

Abstract

[The errata update includes minor editorial changes to selected CUI security requiremer
additional references and definitions, and a new appendix that contains an expanded di
about each CUI requirement.] The protection of Controlled Unclassified Information (CL
resident in nonfederal systems and organizations is of paramount importance to federal
and can directly impact the ability of the federal government to successfully conduct its
missions and business operations. This publication provides federal agencies with a set
recommended security requirements for protecting the confidentiality of CUI when such
information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

"This publication provides federal agencies with a set of recommended security requirements for **protecting the confidentiality** of CUI when such information is resident in nonfederal systems and organizations;..."

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

Strategic Objective 1.1: Develop and Support the Adoption of the Open Science Cybersecurity Framework

We need our own Open Science Cybersecurity Framework that **meets our needs** and **is broadly accepted.**

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Research Right Next Door

NSF cybersecurity R&D programs:
CICI, SaTC.

How do we (the NSF CI community and the nation) take full advantage of these programs?

© 2013 IEEE. Appears in IEEE Security & Privacy Magazine, Vol. 11, No. 2, March-April 2013, pp. 14-23.
(https://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6493323)

Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice

Douglas Maughan
Department of Homeland Security, Science and Technology Directorate

David Balenson, Ulf Lindqvist, Zachary Tudor
SRI International

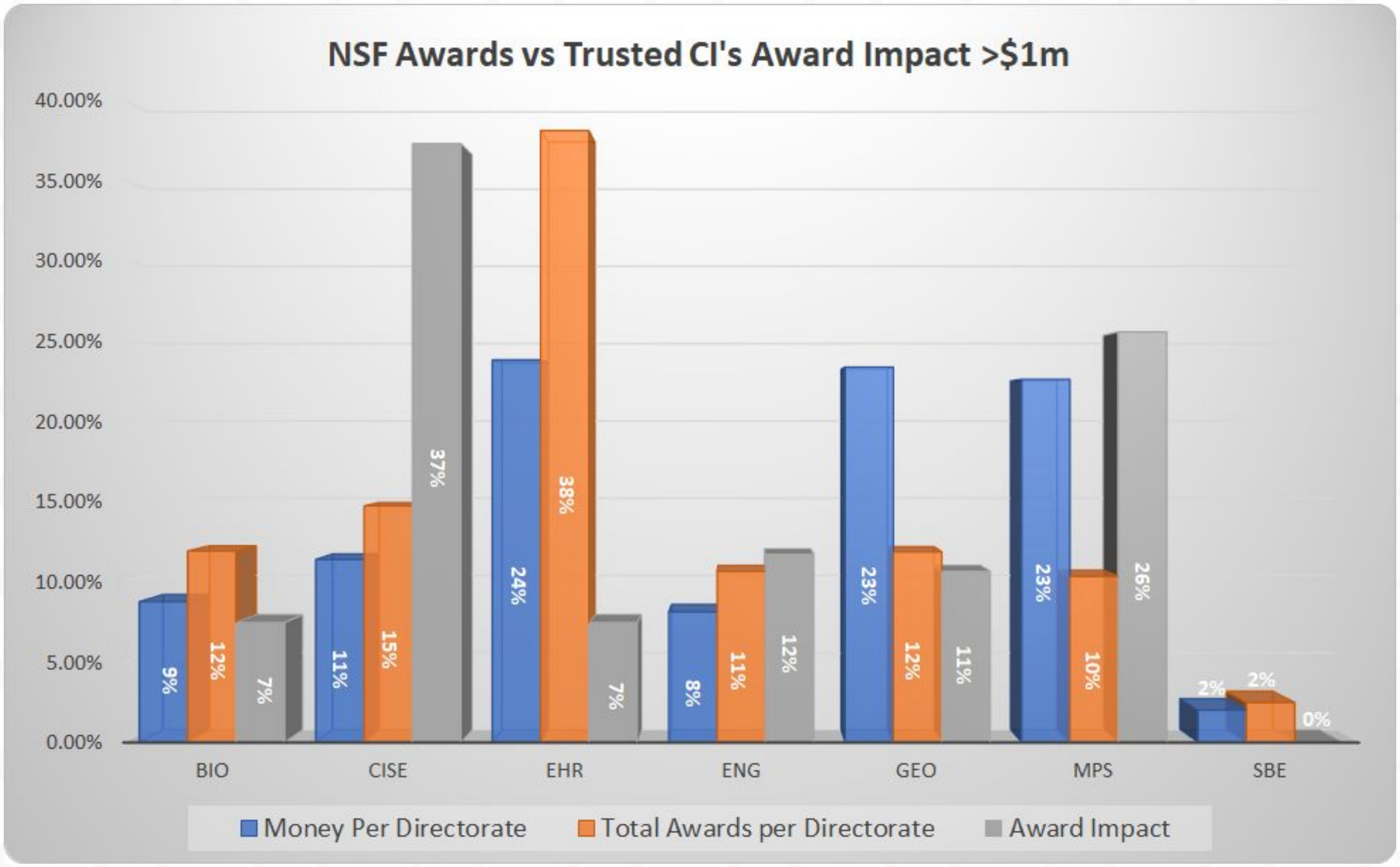
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Strategic Objective 4.5: Cybersecurity Transition to Practice

Florence Hudson recently joined Trusted CI to lead our Transition to Practice (TTP) efforts.

If you have unmet needs or research to transition, contact: TTP@trustedci.org

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

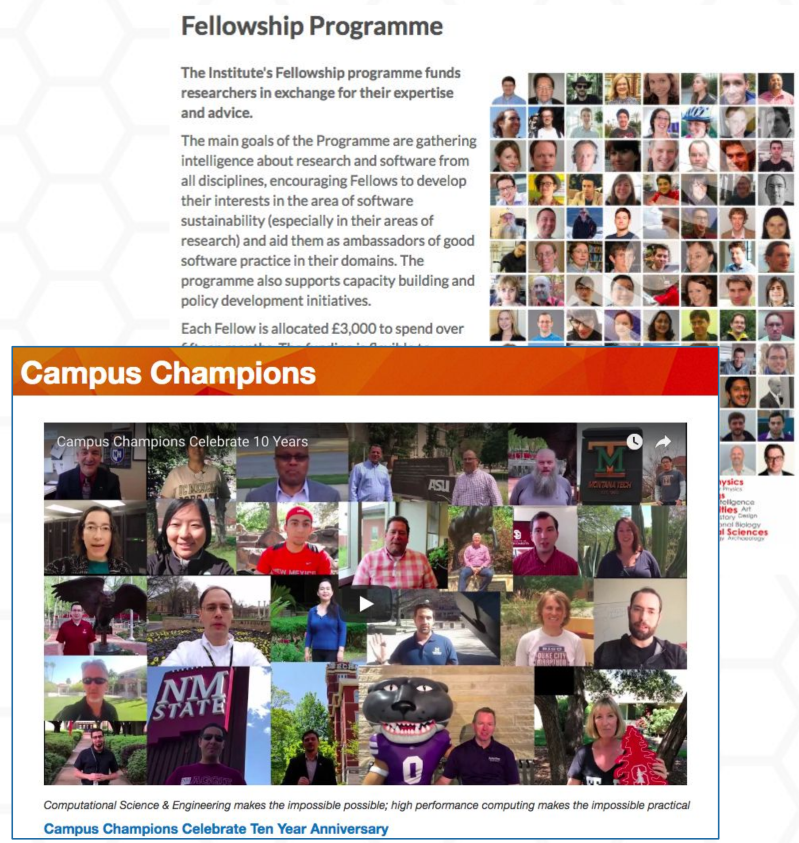
http://hdl.handle.net/2022/22148

Strategic Objective 4.4: Build a Network of Cybersecurity Fellows

A network of fellows who liaise between Trusted CI and their communities.

Fellows receive training, travel support, and prioritized support.

Examples: UK Software Sustainability Institute, ACI-REFs, Campus Champions.



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Strategic Objective 3.2: Coordinate with the NSF CSRC

The 2018 CICI (NSF 18-547) solicitation calls for an NSF Collaborative Security Response Center (CSRC).

CSRC will bolster the NSF Cybersecurity Ecosystem by building community incident response capabilities.

Trusted CI will coordinate and collaborate with the new CSRC to foster the success of both centers and the ecosystem.

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

In Summary…

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Cybersecurity must keep a broad focus on all IT risks to science. Do not stop with the malicious.

Broaden thinking to:
Efficient, Trusted, Reproducible

Provide feedback on Trusted CI’s Five-year Vision

Look for Fellows Program, TTP, Open Science Cybersecurity Framework.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Acknowledgments

The SWIP Project is supported by the National Science Foundation under Grants 1642070, 1642053, and 1642090. 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, is supported by the National Science Foundation under Grant ACI-1547272. 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

Contact Trusted CI

Contact us to request help, from small questions to month-long engagements:

https://trustedci.org/help/

vwelch@iu.edu

See also:

https://trustedci.org/situational-awareness/

https://trustedci.org/webinars/

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

http://blog.trustedci.org/

@TrustedCI

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

NSF