Update on Identity Management for Research Computing
June 4th, 2014 MAGIC Teleconference

• OSG Connect
  – Rob Gardner, Senior Research Associate, U. Chicago

• Identity and Access Management for LIGO: Update on International Challenges
  – Scott Koranda, Senior Scientist U. of Wisconsin-Milwaukee, LSC

• InCommon Update
  – Klara Jelinkova, Chief Information Technology Officer, U. of Chicago

• Center for Trustworthy Scientific Computing IdM Activities
  – Von Welch, CTSC PI

• eXtreme Scale Identity Management (XSIM) project update
  – Craig Jackson, Senior Policy Analyst, Indiana U.
OSG Connect & Connective Computing to Accelerate Science

Rob Gardner
University of Chicago

MAGIC Meeting, June 4, 2014
OSG Campus Grids

- Deliver distributed high throughput computing capabilities to campuses while enabling campus researchers with DHTC ready computing tasks

- OSG Connect a job service to directly connect users to the >120 sites on the OSG

CI Connect

- Technology to provide connective services to campuses and collaborations: job and data services
OSG’s distributed high throughput infrastructure

Could we provide simple, direct access for small groups and individual researchers?

The OSG fabric of services

- The leading distributed high throughput computing service in the US
  - 104k cores, 75.6 PB, 123 compute endpoints
- Well connected
  - Most sites on OSG have 10 Gbps or greater to 12 or ESnet, many upgrading, plus SciDMZs
  - (at least) 2M transfers/day, 1 PB/day
- Friction free
  - The OSG VO with GlideinWMS offers transparent access to these resources for small groups
The OSG Connect Platform

- “Login to the OSG using your campus identity”

- Launched at OSG Campus Infrastructures Community sponsored Workshop at Duke University
  - August 26-27, 2013
  - About 25 users signed up using Duke credentials
  - Thousands of tutorial jobs executed on OSG
  - Several Duke OSG Projects created
Globus Nexus makes it easy for individuals, teams, and institutions to create web applications for the science community.

It provides a flexible, powerful Platform-as-a-Service to which developers can outsource their identity, group, and profile management needs.

Built an integrated job service for the OSG which leveraged these capabilities.

A “force multiplier” allowing us to rapidly onboard campus users while focusing on job submission services.

1) Identity provisioning
   - Create and manage Globus identities

2) Identity hub
   - Bind other identities to Globus identity; use for authentication to Nexus and to other services

3) Group hub
   - User managed group creation and management, groups available for use in authorization decisions

4) Profile management
   - User managed profile attributes and visibility, can be used in group admission
Components of OSG Connect

- Leverages Globus, HTCondor, CI-Logon, U-Bolt, Bosco technologies

Bundled as instance of a CI Connect service portfolio

*Provided as a Service to reduce Campus IT load*

- Submit host
  - Accounts provisioned automatically upon authorization
  - Flocks to OSG VO front-end, UC3 grid, & Amazon if needed
  - Object storage service (90 TB usable)
    - POSIX, Globus Online, http, Chirp access protocols
  - Accounting (OSG Gratia) and monitoring (Cycle Server) services
Components, cont.

- Inside Science DMZ (NSF CC-NIE) with 80 Gbps uplink

- Direct peering I2 & ESnet at CIC OmniPoP (100 Gbps); PerfSonar monitored

- Co-located with major ATLAS Tier2 center and OSG opportunistic cycle provider

- Full advantage of Globus for identity management, group organization, reliable file transfer, data sharing

- Integrated web portal & group organization

- User-focused knowledge base (ConnectBook)
Login to the OSG

Globus endpoint
user#stash

Sign up
Your campus identity & CILogon

CI Connect to Globus Online, HT Condor submit host, storage server, Chirp server, http, OSG Connect Groups, (OSG Projects) --- automatically

Get started with your own campus NetID
osg connect

Manage identities, keys, certificates
Groups mapped to Projects of the OSG VO

Trust: sites and OSG VO

Full user traceability
Stash: transient data storage for workflows

Share with Globus Online, http, Xrootd, Parrot+Chirp +user or @project data areas

STASH: a data interchange service
osg connect

Globus Online integration built-in

Existing identities & endpoints (users like this; familiar)

Project Storage in OSG Connect (stash)
Bringing resources together: Campus, OSG, Cloud
Back to Campuses: typical campus ecosystem
Commodification &
Centralization
Needed: services that offer transparency to users

& natural for HPC providers
And this is repeated at least x100 over in the US
Campus Grids as Service

http://ci-connect.net
built on Globus Platform and HTCondor
Services for the HPC Center for connecting to national ecosystems

Add campus flocking factories for SLURM, LSF, SGE local campus schedulers
Tightly coupled ↔ serial high throughput
Minimize environment, tools & software differences
Virtually extend capacity

Campus Condo Cluster or grid

Value added services for the campus computing center
Connecting communities
e.g. US ATLAS for CERN LHC

Users from 44 US ATLAS institutions

[Diagram showing various campus resources, XSEDE cloud, and miscellaneous nodes like ATLAS T1 (dev) Tier2, TACC Stampede (dev), Cloud (AWS), and others.]

various campus resources

XSEDE cloud
CI Connect Services In Preparation
Summary

- Discovered we could leverage the Globus Platform to connect users to the Open Science Grid
- Suggested a CI Connect model to couple users, data and distributed compute cycles as a service
- Easy path for campuses to “connect” or “bridge” to the national ecosystem
Acknowledgements

- Steve Teucke, Rachana Ananthakrishnan + Globus Team

- Dave Lesny – UIUC (Midwest Tier2 Center), Lincoln Bryant, David Champion – UChicago (Midwest Tier2 Center), Suchandra Thapa (UChicago OSG)

- Open Science Grid User Support, Accounting, GlideinWMS, HTCondor teams

- Jim Basney (CI-Logon), Tom Scavo (Internet2) & InCommon Federation
Identity and Access Management for LIGO: Update on International Challenges

Scott Koranda for LIGO and CTSC

University of Wisconsin-Milwaukee

June 4, 2014
LIGO-XXXXXXXXX-v1
LIGO Continues to Invest in SAML for SSO

- Operate Shibboleth Identity Provider (IdP) 2.4.0
- Soon deploy IdP in high availability configuration
- Three backup IdPs including at sites
- More than 100 Shibboleth Service Providers (SP)
- (Paid) Member of the Shibboleth Consortium
Preparing for SAML Federated Identity

- Early focus on simplest use cases
- LIGO joined InCommon in US
  - Much more effort then expected
  - InCommon requires legal contract
  - InCommon model maps VOs to single university
  - LIGO is not a legal entity
  - Caltech assumed risk for world wide set of LIGO users
- Partnered with CTSC to focus on international interfederation
- Goal was prepare to support world-wide GW astronomy efforts
KAGRA, Japan
Federated access for KAGRA

Date: Fri, 19 Oct 2012 05:15:41 -0500
From: Nelson Christensen <nchriste@carleton.edu>
Subject: access to remote participation wiki

Hi Scott, Warren, Stuart,

I am not sure if you are the right guys for this, but I will start with you.

Is there any way that we can give access to the remote participation wiki to our KAGRA colleague Yoichi Aso who is the new KAGRA member on our remote participation committee.

Thanks,
Nelson
Federated access for KAGRA

Need to share technical drawings and like with about 50 KAGRA scientists
Peer-to-peer federation necessary

InCommon membership enables only US federation
  ▶ Ongoing negotiation with UK Access Federation
  ▶ Early stages with eduGAIN in Europe
  ▶ GakuNin not yet part of eduGAIN

No option early but peer-to-peer negotiation or joining each national identity federation.
LIGO CTSC international federation engagement (6 mo)

Goals

1. Document technical and policy changes for a peer-to-peer
2. LIGO membership in Italian Federation (IDEM)
3. Prototype interoperability with UK via InCommon
4. Research likelihood and timeline for eduGain via InCommon
5. Assist LIGO-India with developing use cases
Peer-to-peer federation with KAGRA

- IdP managed by University of Tokyo
  - Hiroyuki Sato-San
- Metadata exchange was easy
- Negotiation on attributes was easy
  - ePPN, givenName, sn, email
- Access control is largest issue
  - No LIGO/KAGRA working group
  - ACL based on ePPN
  - Only admins know ePPN
  - Grouper can consume federated identity, but no sophisticated onboarding/offboarding or enrollment, notification
Managing Collaboration with COmanage

![Image of COmanage interface for KAGRA-LIGO People](image)

| Name               | Status | Email                          
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Masatake Ohashi</td>
<td>Active</td>
<td><a href="mailto:ohashi@nctr.u-tokyo.ac.jp">ohashi@nctr.u-tokyo.ac.jp</a></td>
</tr>
<tr>
<td>Ohkawa Masashi</td>
<td>Active</td>
<td><a href="mailto:ohkawa@eng.nigata-u.ac.jp">ohkawa@eng.nigata-u.ac.jp</a></td>
</tr>
<tr>
<td>Eliechi Hirose</td>
<td>Active</td>
<td><a href="mailto:hirose@nctr.u-tokyo.ac.jp">hirose@nctr.u-tokyo.ac.jp</a></td>
</tr>
<tr>
<td>Ryutaro Takahashi</td>
<td>Active</td>
<td><a href="mailto:ryu.takahashi@nao.ac.jp">ryu.takahashi@nao.ac.jp</a></td>
</tr>
<tr>
<td>Seiji Kawamura</td>
<td>Active</td>
<td><a href="mailto:sel@nctr.u-tokyo.ac.jp">sel@nctr.u-tokyo.ac.jp</a></td>
</tr>
<tr>
<td>Takashi Yokozawa</td>
<td>Active</td>
<td><a href="mailto:yokozawa@yokimura.hep.osaka-u.ac.jp">yokozawa@yokimura.hep.osaka-u.ac.jp</a></td>
</tr>
<tr>
<td>Steve Scott Koranda</td>
<td>Active</td>
<td><a href="mailto:skoranda@gmail.com">skoranda@gmail.com</a></td>
</tr>
<tr>
<td>Nobuhiro Kimura</td>
<td>Active</td>
<td><a href="mailto:nobuhiro.kimura@kak.jp">nobuhiro.kimura@kak.jp</a></td>
</tr>
<tr>
<td>Chihire Tokoku</td>
<td>Active</td>
<td><a href="mailto:tokoku@nctr.u-tokyo.ac.jp">tokoku@nctr.u-tokyo.ac.jp</a></td>
</tr>
<tr>
<td>Atsushi Nishizawa</td>
<td>Active</td>
<td><a href="mailto:nishizawa@nctr.u-tokyo.ac.jp">nishizawa@nctr.u-tokyo.ac.jp</a></td>
</tr>
</tbody>
</table>
COmanage Registry

- NSF SDCI Bedrock Award
- Internet2, LIGO, iPlant, Bamboo
- Enrollment, onboarding, management for federated identity
- Simple group management
- Targeted at research VOs
Prototype Interoperability with UK Access Federation

- Target Cardiff University
- Bi-lateral interfederation
  - Cardiff IdP metadata flow through InCommon
  - LIGO SP metadata flow through UK AF
- Ian Young (UK AF) and Rhys Smith (Cardiff)
- Steve Carmody (InCommon/Brown)
- Custom once-off metadata flows
- Chose main LIGO wiki (Foswiki) as SP/application
  - Problem right away
  - Cardiff IdP only assert opaque ePPN
  - Application not ready for opaque ePPN
  - Application tied too tightly to LDAP
  - Hired Unicon to create Foswiki plugin
COmanage as SAML Attribute Authority (AA)

- COmanage provisions people and groups into LDAP
- Shibboleth IdP configured only as AA reads from LDAP
- SP queries AA using “key identifier” (ePPN usually)
- AA returns other attributes managed via COmanage
  - givenName, sn, uid, employeeNumber, organization, ...
  - employeeNumber is opaque identifier unique to VO
  - employeeNumber does not change
  - allows for identity linking across federated identities
  - integrated experience for users across VO services
- Large VO like LIGO can do this...can all VOs?
- Attribute release significant hurdle for federated identity
Jim Basney spun up InCommon TAC Interfederation WG
Later chaired by Warren Anderson (LIGO), Paul Caskey (UT)

Executive Summary (March 2014)

1. InCommon should sign the eduGAIN Declaration as soon as possible (Done)
2. TAC should work with Ops to operationalize eduGAIN over the next six months
3. TAC should instantiate a new working group with a charter based on the Future Work items
“Interconnecting federations to link services and users worldwide.”

- “Federation of SAML Identity Federations”
- Effort led by GEANT
- Latest revised eduGAIN policy effective date 30 Sep 2013
- Policy framework:
  - eduGAIN Declaration
  - eduGAIN Constitution
  - eduGAIN Metadata Profile
  - eduGAIN Attribute Profile
31 Production Federations (Purple)

17 Pilot Federations (Red)

Courtesy Brook Schofield (TERENA)
LIGO Engagement

Fall 2012 - Spring 2013

> Laser Interferometer Gravitational-Wave Observatory (LIGO)

The LIGO Scientific Collaboration (LSC) is over 800 people strong with member groups from around the world, but with especially strong links to groups in the United Kingdom, Germany, Australia, and Canada. The LSC enjoys a data sharing agreement with the Virgo Collaboration centered in France and Italy and we expect over time to develop a closer collaboration with peers from the KAGRA project in Japan. CTSC, LIGO and the Open Science Grid are collaborating on establishing an international identity federation spanning Europe, Australia, Canada, and Japan to ease barriers to and facilitate more efficient collaboration in support of LIGO's scientific mission.

View deliverables from this engagement:

- Final Report for LIGO Engagement
- A Study of Three Approaches to International Identity Federation for the LIGO Project
- InCommon Membership in eduGAIN: the LIGO Perspective
- Presentation: INFED
- Presentation: Identity & Access Management for Scientific Organizations
We tried to prepare...

Then the real use case arrived.
Electromagnetic (EM) Followup on Gravitational Wave (GW) Triggers

- Around April 2014 LIGO signed 60+ MOUs for EM followup
- Science drives two types of federated identity use cases
  1. Access to Gravitational Wave Candidate Event Database (GraceDB)
  2. Access to collaboration supporting infrastructure like wikis, email lists
To facilitate collaboration in support of gravitational wave astronomy please register. After your registration is approved you will gain access to services including a wiki, list server, and other LIGO services as they become available.

Click to Register

If you have any questions please email the Help Desk.
Which Federated Identities?

- Surveyed the 60+ “contact” persons for the MOUs
- Asked from which university(ies), institution(s), or organization(s) users might come to LIGO services
- Quick and gracious response from contact persons
- So far...
  - 26 countries including Australia, Canada, Chile, China, Germany, UK, Ireland, India, Mexico, Poland, United States
  - 161 unique institutions
  - 72 of 161 are US institutions
  - Many MOUs signed by international VOs
Federated Identity in US

- 72 US institutions
- Major R1 universities to small liberal arts colleges
  - Size not good indicator of federated identity success
- 64 are InCommon members
- 61 have registered IdPs
- Primary concern is attribute release—will the IdP release **any** attributes to our SPs?
- **At the very least need ePPN**
- *InCommon participant IdPs under no obligation to interoperate with SPs or release any attributes*
- Experience is that most will interoperate but minority will release attributes
InCommon Research & Scholarship Entity Category

- SPs may petition InCommon to be tagged as R&S
- IdPs may agree to release simple set of attributes to R&S SPs
  - personal identifiers: email address, “name”, ePPN
  - pseudonymous identifier: eduPersonTargetedID
  - affiliation: eduPersonScopedAffiliation
- gw-astronomy.org is InCommon R&S
- Petition is straightforward and quick for LIGO

28 of the 72 US institutions operate InCommon R&S IdPs

What to do?
InCommon Research & Scholarship Entity Category

- R&S participation is passive activity for InCommon
- Send Tom Scavo list he will help solicit
- LIGO has done that, emails going out soon
- Would like to see InCommon CIOs make R&S priority
- Need sustained push with full weight of InCommon
Until all IdPs support R&S...

- Deployed “LIGO Guest” IdP of last resort
  - Completely separate IdP and IdMS
  - Once-off code, FTE expensive
  - InCommon chatter about IdP of last resort as service offering but does not exist today

- Negotiating with “well known vendor” for Social-to-SAML gateway service
  - Expect to sign contract July 2014
  - Allow Google authentication
  - Hosted service
  - Gateway asserts ePPN and other attributes
  - Leverage COmanage identity linking if later use other federated identity
  - InCommon chatter about Social-to-SAML gateway service but does not exist today
Federated Identity Outside US

- Goal is to leverage eduGAIN
  - First step is to publish LIGO SPs into eduGAIN metadata
  - Unfortunately InCommon not ready to move forward with publication, unclear timeline
  - Swedish federation (SWAMID) has agreed to publish SPs in its federation and then also push into eduGAIN (Done)
  - Thanks to Leif Johansson!

- SP appearing in eduGAIN is only first step
  - A federation’s declaration to participate in eduGAIN makes no statement about the availability of its member IdPs in the eduGAIN metadata, nor the willingness of the IdPs to consume eduGAIN SP metadata and release attributes to SPs
  - eduGAIN practice still very much in flux
  - Right now mostly opt-in
Leverage help from REFEDs

REFEDS mission is to be the voice that articulates the mutual needs of research and education identity federations worldwide. It aims to represent the requirements of research and education in the ever-growing space of access and identity management, working with and influencing the direction of organizations such as Kantara, OIX and Identity Commons on behalf of our participants.

The work of REFEDS will be prioritised by its participants based on the most important requirements of the identity federations.
Leverage help from REFEDs

- Nicole Harris (TERENA) has agreed to assist LIGO
- Work with IdPs through federation operators
- Pursue both interoperability and attribute release
- What legal issues await?
- Not all organizations and countries represented
- Rely on LIGO Guest and Social-to-SAML gateway for rest
Leveraging Federated Identity as a Science VO?

Today it requires:
- Flexible, domesticated applications
- Collaboration management platform (ala COmanage)
- VO SAML Attribute Authority
- IdP of last resort
- Social-to-SAML gateway
- Close relationship with InCommon staff (R&S)
- Friends in Sweden
- Friends in REFEDs
Leveraging Federated Identity as a Science VO?

- Barrier is still quite high
- LIGO can do this because it has at least two people professionally invested in “the vision”
- Higher Ed SAML identity federations need to continue to invest in supporting research and quicken the pace or events will overtake them
- VOs need to engage more directly and show up at InCommon, TNC, and REFEDs meetings and help make the investment
InCommon Update

MAGIC Meeting
June 4, 2014

Klara Jelinkova, Chief Information Technology Officer, University of Chicago
IdM Services for Research

- InCommon Background
- InCommon: Focus on research and what that means
- Status of R&S
- eduGain agreement
- Challenges and benefits of supporting research via federated IdM from a campus perspective
InCommon

- InCommon is trust framework for U.S. education and research
  - Best practices/policies
    - Federation support, metadata, and attribute exchange
    - Assurance (Shared practices: Bronze and beyond)
  - Mature consumable services
    - Certificates (Comodo)
    - MFA (Duo, SafeNet)
  - Community of participants
- InCommon shared architecture integrates and supports other Internet2 development efforts
  - Grouper, Shibboleth, MACE, Comanage, etc.
  - Catalyzed by NSF through NMI and SDCI grants
InCommon Overarching Goals

- Making it easier to federate IdPs and SPs
- Increasing value of InCommon participation
- Interfederation
- Innovation influence and leadership where it matters
- Putting trust and privacy into identity
- Research support
InCommon Priorities 2014-2015

- Develop more mature, scalable, and resilient operations
  - Deploy SHA2 metadata aggregates
- Expand the portfolio of in-house services
  - Establish a managed IdP, complete with self-service account management, audit, and reporting capabilities
  - Implement an IdP of Last Resort (Google Gateway?)
  - Pilot a Social2SAML Gateway service
  - Establish executive dashboards, reports, and analytics
InCommon Priorities 2014-2015

- Expand the portfolio of third-party services
  - Launch eduroam service
  - Launch DocuSign service
  - Develop a tagging and certification program for Sponsored Partners
- Create more tools to aid with deployment and management of federating technology
  - Develop new GUI-based configuration application
  - Deploy new IdP discovery interface
- Enhance the certificate service offering
  - Complete deployment of InCommon IGTF Server CA for XSEDE
Federation Context

- Compatibility with U.S. Government: FICAM TFPAP
  - Federal Identity Credential and Access Management
  - Trust Framework Provider Adoption Process
    - Based on OMB M-04-04 and NIST SP 800-63
    - InCommon is a certified TFP at Levels 1 and 2
      - InCommon Assurance Profiles: Bronze (L1) and Silver (L2)
  - Aligning trust policy and practices via REFEDs
    - Research and Education Federations
      - refeds.org
  - EduGAIN metadata aggregation export/import
    - edugain.org
R&S Status

- InCommon has 356 IdPs
- 80 IdPs are subscribed to R&S
- We need at least all R1 institutions subscribed
- We are working on a direct outreach to CIOs and Registrars
  - This means the Steering Committee Chair e-mailing them and explaining repercussions
- Assessment in Fall (at Educause meeting)
- User managed attribute release software (LARPP)
eduGAIN Agreement

- Agreement to collaborate signed
- Expectation to operationalize
- Discussions with InCommon management (Internet2) on timeframes and deliverables
- Internet2 committed to making progress
Campus Perspective

- University of Chicago all in (Grouper, Shibboleth, InCommon R&S, working on Bronze and Silver)
- Ability to use campus infrastructure to support researchers and research computing needs
  - Reduces startup costs and service provisioning
  - Manages liability at campus level
- This can be a good service that enables research on a campus committed to supporting it
- VOs and federations
  - More complex
- User-enabled access (user permitted / discretionary attribute release)
- Scalable access control
Campus Perspective: Where do we need to get to?

Adjusted Design Point for all Trust and Identity Activities from “Enterprise” to “Virtual Organization”

Empower “Individual Opt In” and Require Standards plus “Commitment of Participation” for Release of key Institutional Attributes
TIER

TRUST & IDENTITY IN EDUCATION AND RESEARCH

InCommon

Ping Identity

Kuali

CIFER

Groupalia

Duo

CAS

REFEDS

InCommon Certificates

ORACLE Identity Management

eduGAIN
Trust and Identity in Education and Research (TIER)

TIER

- Standards and development efforts
  - InCommon Federation, InCommon Metadata, MACE
- Mature consumable subscription services
  - Shibboleth, Grouper, etc.
- InCommon
TIER Plan

- Provide context for disjointed efforts
- Provide context for InCommon and place within which federation can operate more efficiently
- Charter being drafted by leaders from InCommon and Kuali/Rice
- Plan for a charter by Fall of 2014 and operationalize in 2015
Questions and Comments

Klara Jelinkova
klaraj@uchicago.edu

University of Chicago
InCommon Steering
Internet2 Board
CTSC Identity Management Activities

MAGIC

Von Welch, CTSC PI
June 4th, 2014

trustedci.org
CTSC Vision

CTSC will provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and the resources to achieve and maintain an appropriate cybersecurity program.
Leadership

Training for CI Professionals

One-on-One Engagements
Engagements
(with IdM Focus)

Globus - Review of new sharing system (ongoing).

Pegasus WMS - Delegation with SSH pubkeys.

DataONE - Federated IdM review.

LIGO - International federated IdM.

http://trustedci.org/engagements/
LIGO Collaboration Impact

International identity federation efforts between LIGO, CTSC and InCommon came to fruition with InCommon signing eduGAIN declaration.

- First step in connecting InCommon with 30 other National federations.

http://www.isgtw.org/spotlight/federated-trust-expands-internationally-edugain-declaration
Training:
Streamlining Collaboration with InCommon and Identity Federations

In collaboration with LIGO

Presented at 2013 NSF Cybersecurity Summit

Slides freely available:
http://trustedci.org/trainingmaterials/

CTSC
Presentation to MAGIC, June 4th 2014
Identity Management Best Practices

- Provide identity management guidance that is broadly applicable to NSF CI
- Document IdM lessons learned and real examples from NSF CI
- “Put a stake in the ground” on IDM questions. Give opinions and guidance
- Identify growing trends (multi-factor, etc.)
- E.g. [http://blog.trustedci.org/2014/04/idm.html](http://blog.trustedci.org/2014/04/idm.html)
- More in the pipeline on ORCID, Password Reset, and other topics.
HeartBleed

OpenSSL vulnerability that impacted 1/3 of the WWW

CTSC provided guidance to community and central source of information.

Now have email lists for notifying community of issues and advice:

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

---

**Heartbleed: Should I change my password? (And when?)**

Yesterday, news of the Heartbleed OpenSSL bug swept the Internet, and lots of web site administrators worked to update software and replace potentially compromised cryptographic keys. Estimates are this vulnerability affected over half a million websites and major sites such as Yahoo Mail were vulnerable.

Today people are starting to wonder what this bug means to them, specifically should they change their passwords? It's possible as the news spread yesterday, websites could have been re-compromised.

---

**Which cyberinfrastructure components are impacted by Heartbleed?**

This table captures Heartbleed vulnerability information about CI components that we are aware of. If you have information to add, please send email to info@trustedci.org

<table>
<thead>
<tr>
<th>CI Impacted by Heartbleed: Sheet1</th>
<th>Component</th>
<th>Impacted?</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CILogon</td>
<td>No</td>
<td><a href="http://www.cilogon.org/news/cilogonandtheopensslheartbeat">More information</a></td>
<td></td>
</tr>
<tr>
<td>FutureGrid</td>
<td>No, but requiring password change.</td>
<td><a href="https://support.globus.org/entries/50667608">More information</a></td>
<td></td>
</tr>
<tr>
<td>Globus (including GridFTP and GRAM)</td>
<td>Yes</td>
<td><a href="http://lists.globus.org/pipermail/globus-announce/2014-April/000016.html">More information</a></td>
<td></td>
</tr>
</tbody>
</table>
| GSI-OpenSSH                     | Yes       | [More information](https://lists.cs.wisc.edu/archives/condor-users/2014-)

---

**CTSC**

May 2014 Advisory Committee Meeting
Thank You

trustedci.org
@TrustedCI

We thank the National Science Foundation (grant 1234408) 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.
A Model for Identity Management in Future Scientific Collaboratories

Von Welch (PI), Bob Cowles, Craig Jackson
XSIM’s Work on VO IdM

Our Mission
Develop a VO-IdM model that (a) expresses observed variations in collaboratory identity architectures and (b) can be leveraged into guidance for selection.

Semi-structured interviews with 20+ VO-RP relationships.


Some core findings....

1. The VO can and often does play a role in collaboratory IdM implementation.
2. This VO role alters the traditional direct trust relationship between users and RPs.
3. We’ve seen a variety of different approaches at this RP-to-VO *delegation* of IdM tasks.
4. Trends are toward *mediated trust*, utilizing the VO’s capacity to represent its members, particularly *transitive trust*. 
VO IdM Trust Model Extremes
... via 800-39

**Classically** RPs produced and consumed all IdM data.

*Brokered trust relationships* entail VOs & TTPs generating user data, to be consumed by RPs.

*Transitive trust relationships* forego all user data consumption by RP.
VO IdM Model: *Data-centric*

**Production & Consumption**

Identity data is *produced* to provide functionality to other workflows when needed.

Identity data is *consumed* to perform these functions. Three *basic types* of identity data, produced and consumed by different parties: (1) User “identity”; (2) User contact info; (3) VO membership/role

**Functionality**
- authentication
- authorization
- allocation/scheduling
- accounting
- auditing
- user support
- incident response
Identity Data Flow in the “Classic Model”

RP produces and consumes all IdM information.
Identity Data Flow in Multi-user Pilot Jobs
Continuing Work

1. Evolve findings and modeling into guidance and real-world testing;... engaging with NERSC, DESC, OSG.

2. Map influential factors to specific data flows.
Factors Impacting Delegation

Barriers
Low risk tolerance and historical inertia
Compliance and assurance requirements
Technology limitations

Motivations
Scaling and Dynamicity of VO
Complex VO roles and policies

Enablers
Available VO IT/IdM effort and expertise
VO-run collaboration services
Related Work

- Work by I2, Klingenstein, et al.
- NSTIC IDESG Functional Model Group.
- NIST 800-39 (Trust Models).
- Lin, Vullings, and Dalziel. “Trust-based Access Control Model for Virtual Organizations.”
Thank you

http://cacr.iu.edu/collab-idm

We thank the Department of Energy Next-Generation Networks for Science (NGNS) program (Grant No. DE-FG02-12ER26111) for funding this effort.

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 sponsors or any organization.