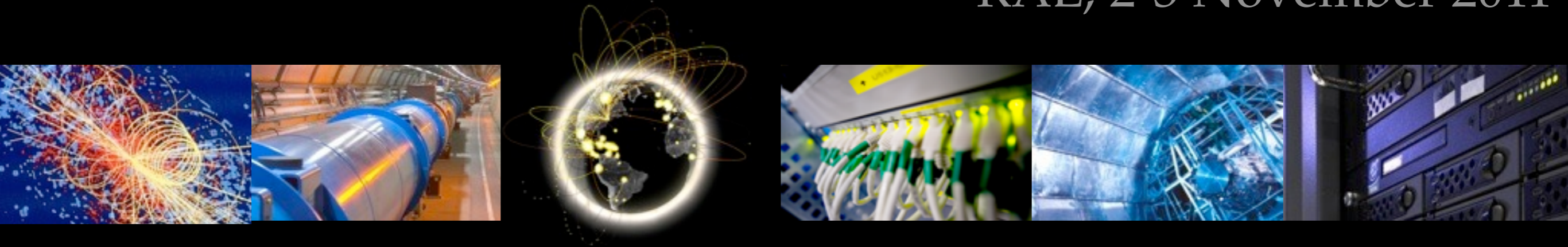


Identity Federation for WLCG/HEP

Romain Wartel

Federated identity system for scientific collaborations workshop

RAL, 2-3 November 2011



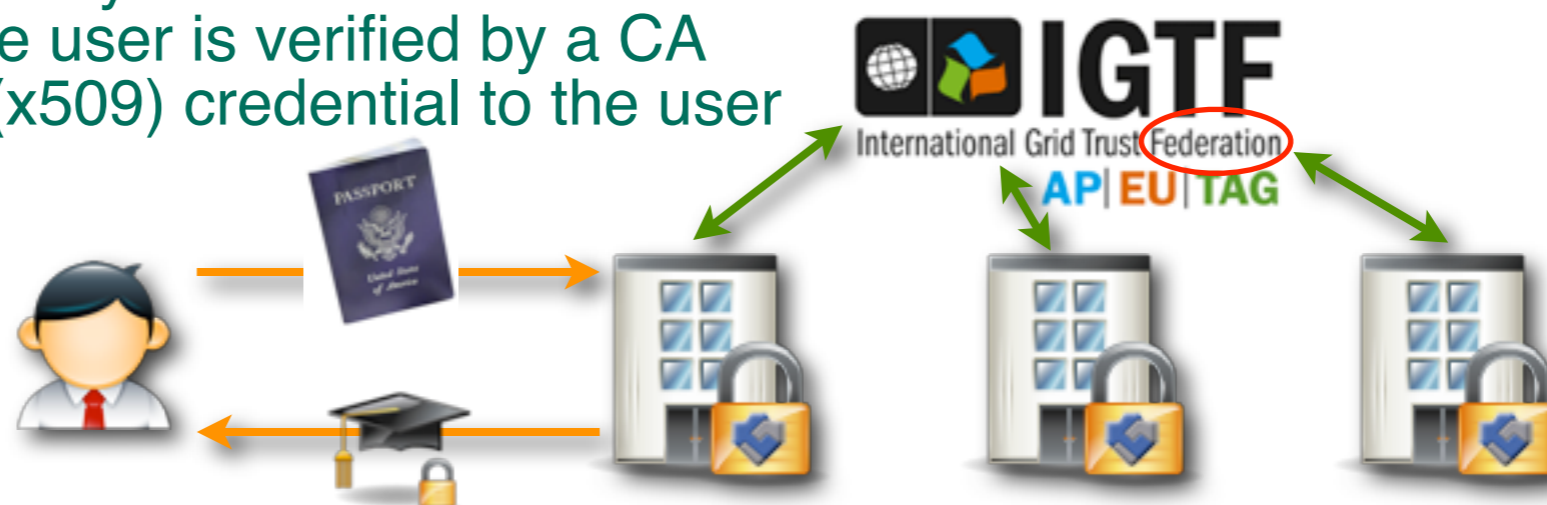


Summary

- ~ 5900 WLCG users distributed all **around the world**
- In WLCG, authentication is done via **X509** credentials
- **IGTF** already provides federated identities for grid services
 - The current system works

Authentication:

- CAs are accredited by the IGTF
- Real identity of the user is verified by a CA
- The CA issues a (x509) credential to the user



Authorization:

- The user contacts the VO
- The VO confirms membership+role and issues attributes to the user





Use cases

- “HEP” is not really a clearly defined community
 - Many small groups loosely coupled (e.g. astrophysics)
 - Some sites are used by different collections of HEP users
 - Some collections of HEP users use many sites
 - WLCG users heterogenous and very distributed, good use case
- One of the main goals is to **enable HEP users to access resources located at other HEP or academic sites**
 - Working for grid resources
 - But it does not work for non-grid resources (Web portals, etc.)
 - Users need a grid identity + other site-specific identities
 - **Unification** would be beneficial
- Typically VOs retain fine-grained control of authorization



Trust framework

- The trust framework provided by the IGTF is essential
 - Reliable, neutral and stable body - great success
- Need IGTF to provide accreditation of non-x509 IdPs
 - Work is ongoing
- Important to defined different and clear Levels of Assurance
 - Resource providers like elevated LoA (Gov ID check)
 - We run arbitrary user payload - traceability is important
- The goal would be for HEP sites to:
 - Enable their IdP(s) to be fully accredited by the IGTF for both x509 and non-x509 authentication systems
 - Consider IGTF-accredited IdPs as trusted IdPs, providing an elevated LoA
 - Grant a level of trust proportional to the LoA of the credentials presented by the user



Attributes management

- A lot of attributes already owned by existing IdPs
 - But used internally only
 - Need to specify the attributes that can be shared with services
 - User privacy important
- Need to define a consistent attribute namespace
 - Should come from the IGTF authentication profile
 - Some attributes might be optional
 - Problematic attributes: real name, nationality, etc.
- Attributes will continue to be “verified” by the VOs in WLCG



"It's a baby. Federal regulations prohibit our mentioning it's race, age, or gender."



Policies and Procedures

- IdPs will take on **new roles and responsibilities**
- Needs to be incorporated in existing policies & procedures
 - Approval of Identity Providers and LoAs
 - End user registration and identity vetting
 - Roles and responsibility, contact information
 - **Incident response and vulnerability management**
 - Service operations
 - Logging and traceability
 - Attribute release
- **Consistency with other infrastructures is essential**
 - “Security for Collaborating Infrastructures” effort should continue
 - Includes DEISA/PRACE, EGI, OSG, TeraGrid/XSEDE, WLCG



Compatibility and interoperability

- Different standards exist
 - Probably need to support several
- Important to support **industry standards** wherever possible
- Important to ensure WLCG and the HEP community have a **strategy aligned with other communities**
- Credential translation services and certificate services promising
 - Need to understand how to connect them to existing services
 - Need to understand operational and support costs



Security risks

- Identity federation implementations typically **very prone to phishing attacks**
 - Phishing attacks are extremely difficult to prevent and are one of the main causes of compromised accounts at most sites



Leif Nixon's demo

Academic-Initiative.eu x

www.academic-initiative.eu

Other Bookmarks

Academic-Initiative.eu
Building bridges across academic Europe

Home About Contact Links Login

About Academic-Initiative.eu

The European Academic Initiative enables access to information resources for European researchers from all fields of science, from High Energy Physics to Humanities.

The European Academic Initiative project is funded by the European Commission's Seventh Framework Programme.

The Consortium will validate results using 3 business cases: one business case comes from a technological district; one from cross border interoperability and collaboration

Menu

- Common resources
- Article database
- Events
- Internal wiki

WILCOG



Leif Nixon's demo

Identity Provider Se... x

www.academic-initiative.eu/discovery/DS

Other Bookmarks

Select an identity provider

The Service you are trying to reach requires that you authenticate with your home organization, enter the name below.

Recently used organizations:

[Linköping University](#)

Enter institution name:

Or choose from a list:

Federation	organization
SWAMID	Arcada
Kalmar Union	Blekinge Tekniska Högskola (Personal)
All Sites	Blekinge Tekniska Högskola (Studenter)
	Chalmers
	CSC - IT Center for Science Ltd.
	Feide - Norwegian Educational and Research Institutions



Leif Nixon's demo

login.liu.se


https://www.liu.se/cas/login

Other Bookmarks

| Anpassa sidan

Sök på LiU.se **SÖK**

A till Ö | Översikt | Andra sökmöjligheter



Linköpings universitet

[Vill studera](#) [Lediga jobb](#) [LiU-student](#) [Alumni](#) [Näringsliv & Samhälle](#) [Press](#) [Anställd](#)

Välkommen till Linköpings universitets centrala autentiseringstjänst.

Du försöker nå en webbsida som kräver inloggning. Du behöver ditt LiU-ID (typ andan123 eller boek12) och ditt lösenord för att fortsätta. När du är färdig bör du logga ut och avsluta webbläsarprogrammet.

Ange ditt LiU-ID och lösenord.

LIU-ID:

Lösenord:

Varna mig innan jag loggar på en annan webbtjänst. Den här tjänsten kan automatiskt logga in dig i vissa av universitetets webbtjänster, vill du få en varning om när så sker så bockar du i den här rutan.

LOGGA IN

Senast uppdaterad: 2011-01-05

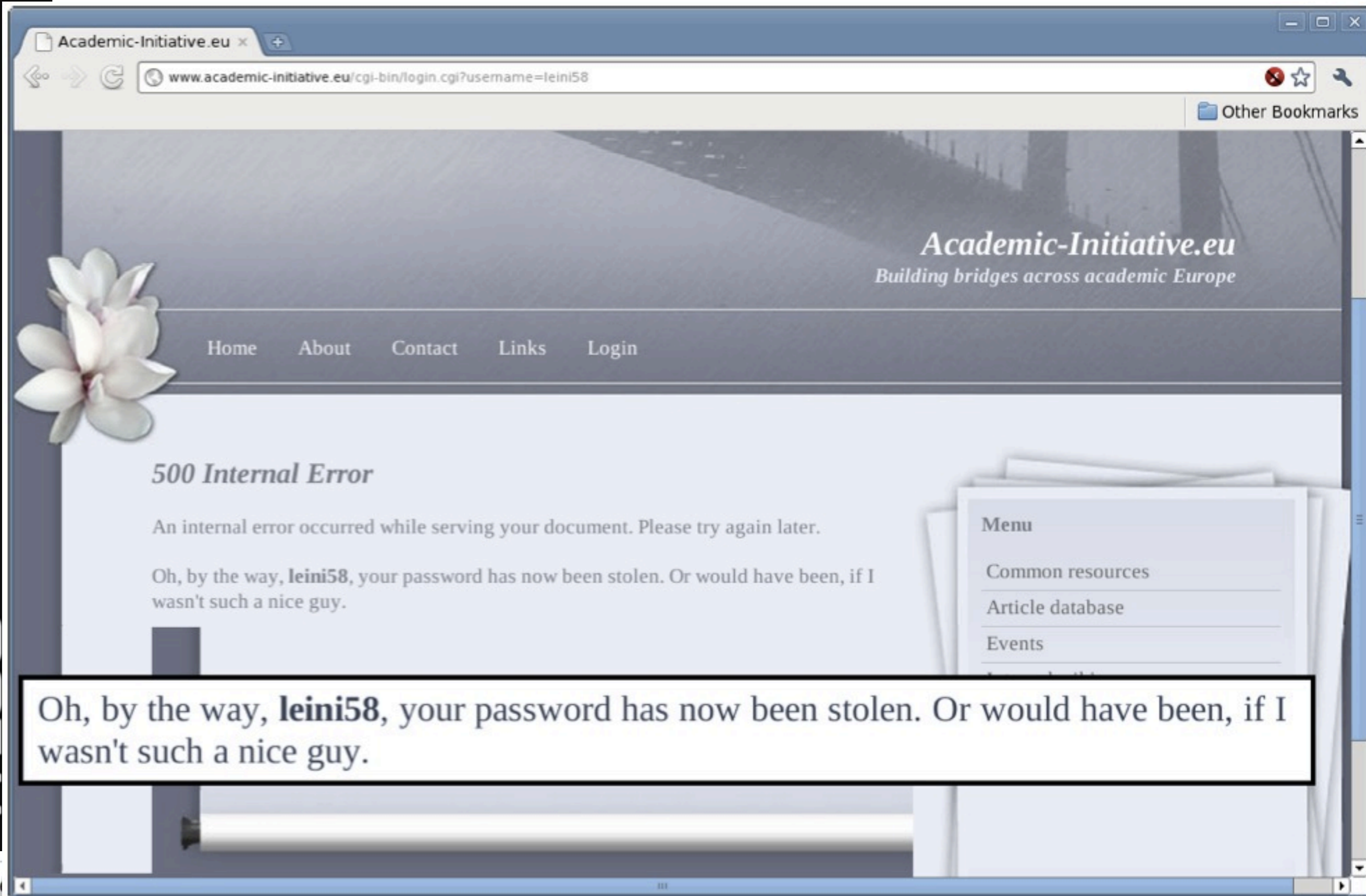
Linköpings universitet
581 83 LINKÖPING
[Kontakta oss](#) | [Kartor](#)

Tel: 013-28 10 00
Fax: 013-14 94 03

[Om webbplatsen](#)



Leif Nixon's demo



Academic-Initiative.eu x

www.academic-initiative.eu/cgi-bin/login.cgi?username=leini58

Other Bookmarks

Academic-Initiative.eu
Building bridges across academic Europe

Home About Contact Links Login

500 Internal Error

An internal error occurred while serving your document. Please try again later.

Oh, by the way, **leini58**, your password has now been stolen. Or would have been, if I wasn't such a nice guy.

Menu

- Common resources
- Article database
- Events

Oh, by the way, **leini58**, your password has now been stolen. Or would have been, if I wasn't such a nice guy.

WILCOG



Real incidents

New “highly sophisticated” cyber attacks on U.S. government labs

July 7, 2011 | [Regina Sinsky](#)

[View Comments](#)

Today two government-funded research laboratories and a government contractor in the United States are still recovering from a “highly sophisticated” cyber attack that took place during the July 4 holiday weekend.

The attacks are under investigation, and not many details have been released by investigators.

The first attack happened at the Energy Department's Jefferson Lab, located in Newport News, VA. The lab's website is currently live at www.jlab.org and it appears to be fully restored. We have put in a request for an update with the public affairs manager, but have not heard back yet.

The Pacific Northwest National Laboratory in Richland, Washington (PNNL) was the second laboratory attacked. PNNL's website is still down as of today, but [according to Government Computing News \(GNC.com\)](#), it has restored internal communications and external e-mail. The Department of Homeland Security's [Daily Open Source Infrastructure Report](#) cites a Pacific Northwest spokesman saying the lab's external computer network averages 4 million unauthorized access attempts each day.

Battelle, a government contractor that manages PNNL, was the third attack over weekend.

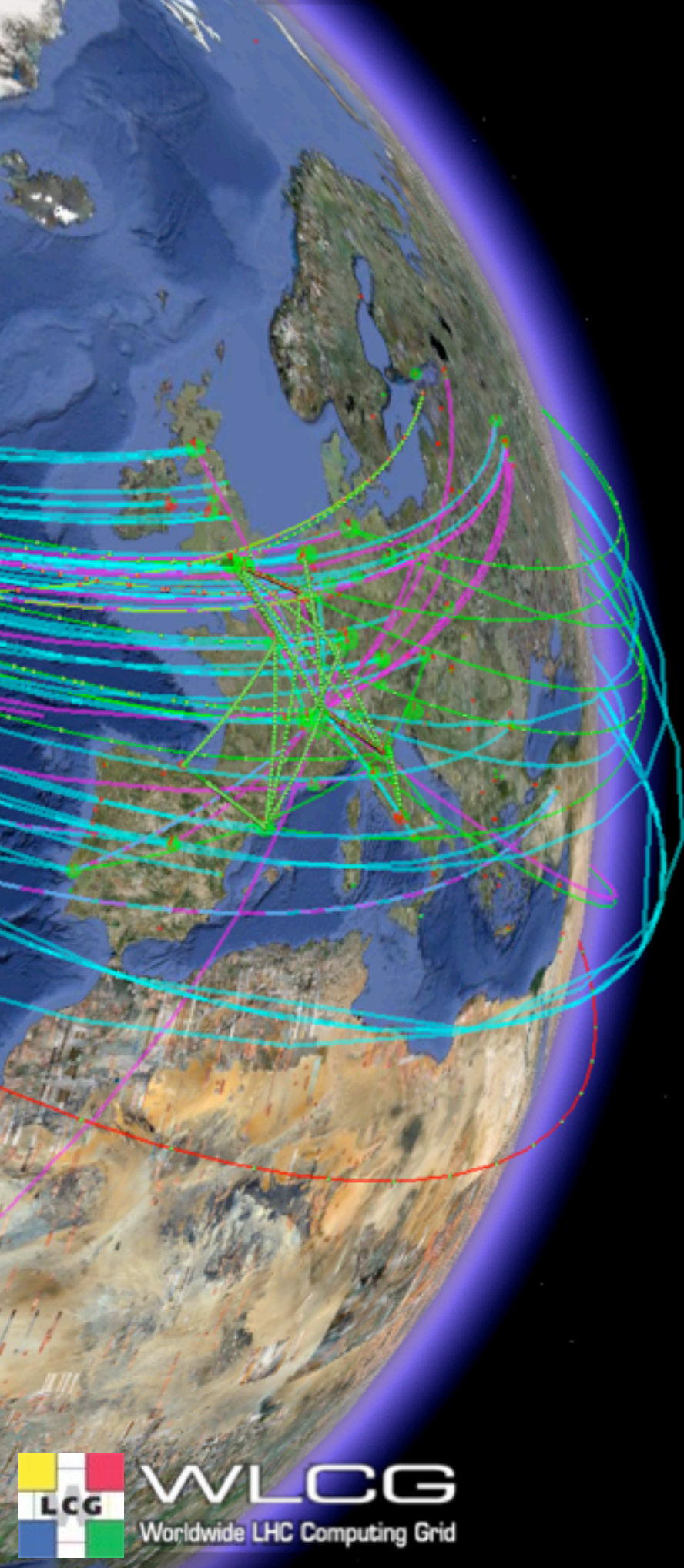
“The good news is no classified information has been compromised or is in danger from this attack,” said PNNL spokesman Greg Koller [in an interview with Reuters](#). “At this time, we have not found any indication of ‘exfiltration’ of information from our unclassified networks as well.”

There has been a string of attacks on U.S. government organizations in recent months. Network access was shut down in May after a cyber attack at Lockheed Martin and the Oak Ridge National Laboratory, which is also managed by Battelle. [Oak Ridge was attacked via spear-phishing: More than 50 employees clicked on a malicious link in a false e-mail from the human resources department.](#)



Security risks

- Identity federation implementations typically **very prone to phishing attacks**
 - Phishing attacks are extremely difficult to prevent and are the main cause of compromised accounts at most sites
 - Ethical phishing tests conducted
 - 45-50% response rate against Facebook (<http://cern.ch/go/W6dp>)
 - 5-15% against academic/HEP users, despite training
 - HEP accounts are being sold on the black market
 - Attackers will continue to capture credentials - easy and profitable
- **IdP databases both exposed and essential to protect**
- The infrastructure needs to sustain
 - Malicious IdPs
 - Malicious Service Providers



Questions / Discussion