Science Gateway Security Recommendations

Jim Basney
jbasney@illinois.edu
Von Welch
vwelch@indiana.edu

This material is based upon work supported by the National Science Foundation under grant numbers 1127210 and 1234408.

- Our abstract: http://go.illinois.edu/gwsecabstract

- These slides: http://go.illinois.edu/gwsecslides

Science Gateway Security Concerns

- **Confidentiality** of pre-publication research data
- **Integrity** of research results
- **Availability** of services

- Provide **trustworthy** service to researchers
- Maintain **trust** of resource providers
- Use resources in **compliance** with policies

- Each science gateway is **unique**
  - Assess risks to determine appropriate mitigations
  - Risk = Likelihood x Impact

Science Gateway Risk Factors

- small, closely-knit user community
- public data (sky survey data)
- internal resources
- focused functionality

- large, distributed, open user community
- sensitive data (personal health info)
- external resources
- wide range of user capabilities

less risk

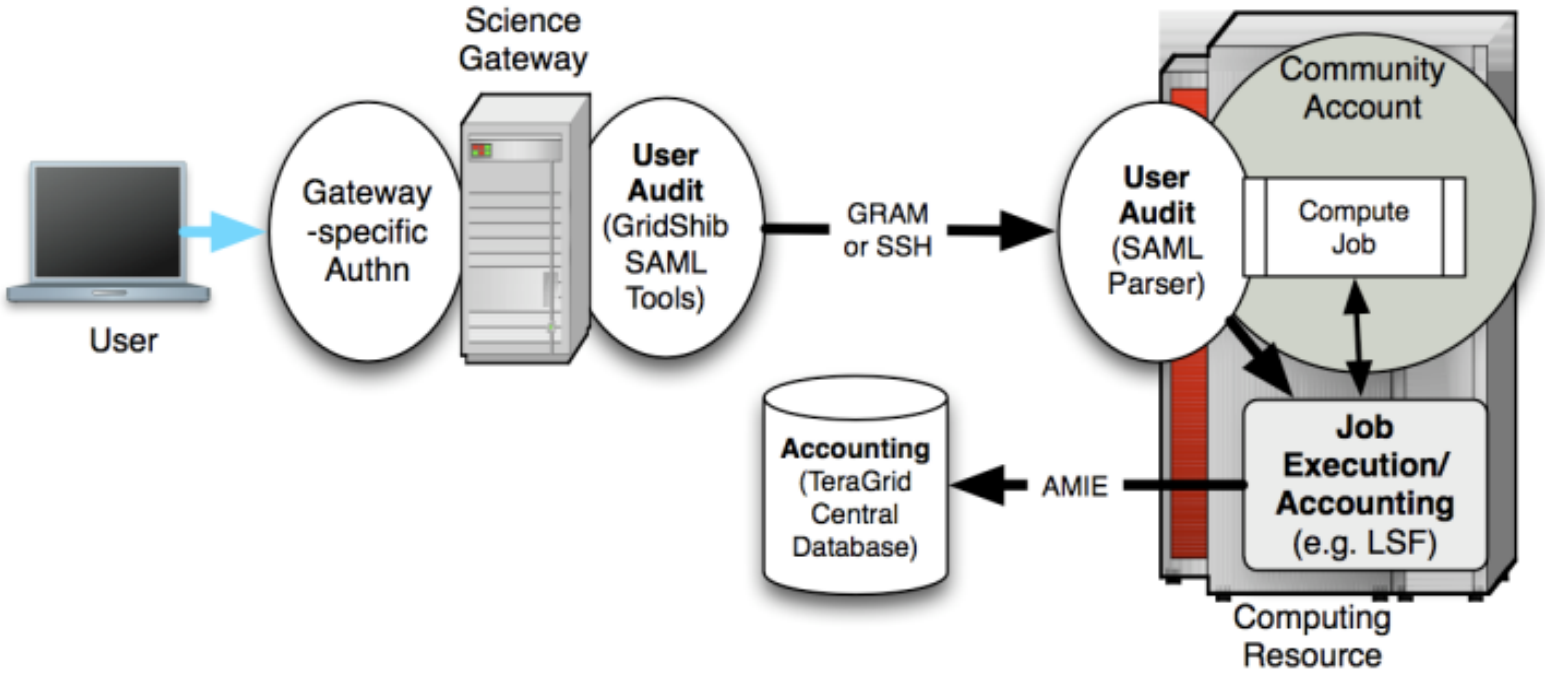
more risk

Science Gateways and Resource Providers

Deployment models include:

- **Dedicated**: Resources managed by science gateway
  - Science Gateway sets its own policies
  - Example: Rosetta Online Server That Includes Everyone (ROSIE)
- **Transparent**: Providing a new interface to existing resources
  - Users have accounts on existing resources
  - Example: TeraGrid Visualization Gateway
- **Tiered**: Science Gateway manages resource allocation
  - Science Gateway manages its own users
    - Using community account / robot certificate at resource provider
    - May send per-user attributes to resource providers
  - Examples: CIPRES, GENIUS

TeraGrid Science Gateway AAAA Model (2005)



http://dx.doi.org/10.1145/1838574.1838576

Existing Security Recommendations

- Virtual Organization Portal Policy (EGI-InSPIRE SPG, 2010)
- Securing Science Gateways (Hazlewood and Woitaszek, 2011)

VO Portal Policy (EGI-InSPIRE SPG, 2010)

Portal Classes			
Portal Class	**Executable**	**Parameters**	**Input**
Simple one-click	provided by portal	provided by portal	provided by portal
Parameter	provided by portal	chosen from enumerable and limited set	chosen from repository vetted by the portal
Data processing	provided by portal	chosen from enumerable and limited set	provided by user
Job management	provided by user	provided by user	provided by user

- General Conditions
  - Limit job submission rate
  - Audit logging
  - Assist in security incident investigations
  - Securely store passwords, private keys, and user data

https://documents.egi.eu/document/80

TeraGrid: Securing Science Gateways (Hazlewood and Woitaszek, 2011)

- Recommendations:
  - Per-user accounting
  - Limiting access at resource providers (restricted shell, grid interfaces)
  - Separating per-user data from shared software and data
  - Individual accounts for science gateway developers
  - Short-lived certificates for remote access

Table 1: TeraGrid Science Gateway Summary

Gateway Name	Gateway Infrastructure	AuthN Credential		Execution	Data Movement
		Community	User		

Table 2: TeraGrid Resource Provider Science Gateway Security Policy Survey

Question	Answers									
	Indiana	LONI	NCAR	NCSA	NICS	ORNL	PSC	Purdue	SDSC	TACC

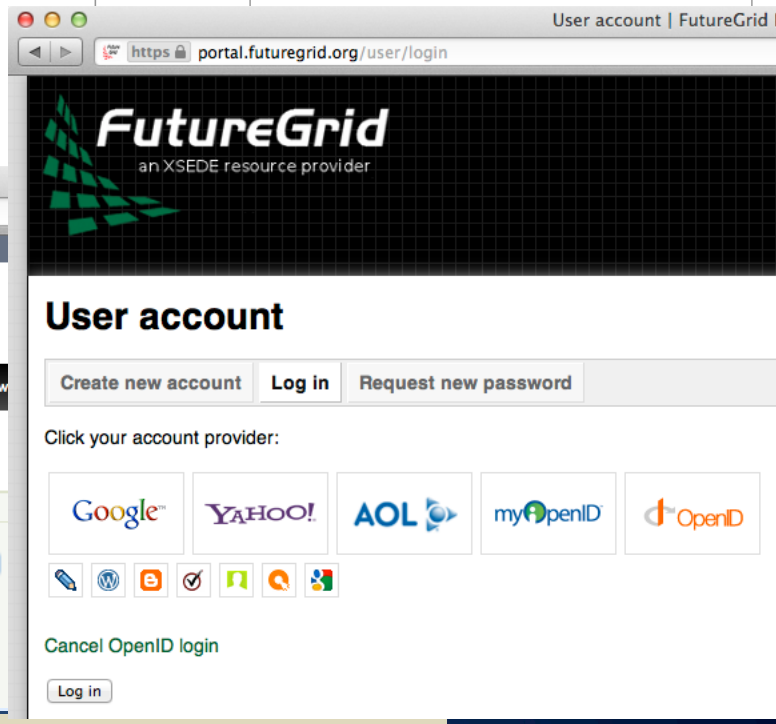
http://doi.acm.org/10.1145/2016741.2016781

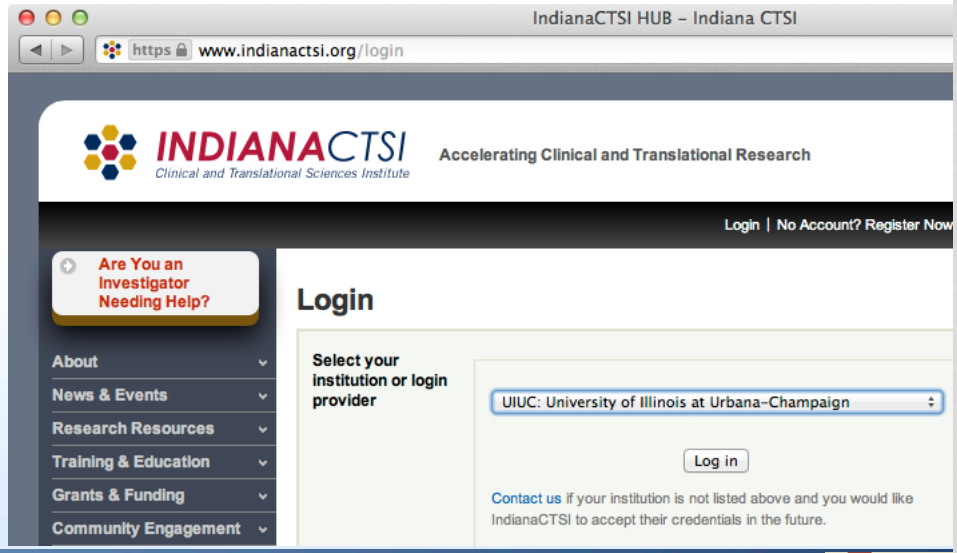
Science Gateway User Authentication

- Why authenticate users?
  - Access to external resources
  - Personalization
  - Maintaining state across sessions
  - Accounting / tracking usage
- How to authenticate users?
  - Outsourced: federated identities, identity as a service
  - Internal: password DB managed by science gateway

Federated User Authentication

- Avoid managing user passwords!
- SAML: campus identities
- OpenID/OAuth: public identities
- Enables two-factor authentication





Passwords

If your science gateway needs to handle user passwords:

- Protect passwords from online attack
  - Use HTTPS
  - Block brute-force attacks (e.g., Fail2Ban)
- Protect passwords from offline attack
  - Store password hashes
  - Use a strong hashing algorithm, with per-password salt
  - Use existing password hashing implementation
    - e.g., PHP password_hash()
  - http://security.blogoverflow.com/2013/09/about-secure-password-hashing/

Science Gateway Operational Security

- **Prevent** (eliminate) threats (when possible)
- **Detect** security incidents
- **Respond** effectively to security issues

- **Goal**: manage risks

- **First Step**: Early communication with local security staff
  - Provide security services (monitoring, scanning, logging, etc.)
  - Identify security policies and best practice recommendations tailored to your local environment
  - Establish relationships now in case of security incident later

Basic Operational Security Checklist

Prevent

- Software patching
- Control admin access
- Vulnerability scanning
- Firewalls
- Physical security

Detect

- File integrity checking
- Intrusion detection
- Log monitoring

Respond/Recover

- Centralized logging
- Secure backups

Continuous Software Assurance

The Software Assurance Market Place (SWAMP) is a DHS S&T sponsored open facility to become operational in January 2014. It is driven by the goal to expand the adoption of software assurance (SwA) by software developers.

The SWAMP will enable you to:

- **Identify** new (possible) defects in **your** software every time **you** commit a change
- **Identify** new (possible) defects in a software/library/module **you** are using every time a new version is released
- **Track** the SwA practices of your project

While protecting your privacy and the confidentiality of your data.

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

http://continuousassurance.org

Science Gateway Security: Community Resources

http://trustedci.org/help

http://sciencegatewaysecurity.org/discussion

http://xsede.org/gateways