# Security for Open Science Project

Lead PI - Deb Agarwal, Lawrence Berkeley National Laboratory
-
Lawrence Berkeley National Laboratory - Brian Tierney, Mary Thompson
Argonne National Laboratory - Frank Siebenlist, Ian Foster
Pacific Northwest National Laboratory - Jeff Mauth, Deb Frincke
University of Illinois, NCSA - Von Welch, Jim Basney
University of Virginia - Marty Humphrey
University of Wisconsin - Miron Livny, Bart Miller
National Energy Research Scientific Computing Center - Howard Walter
Energy Science Network - Michael Helm
University of Delaware – Martin Swany

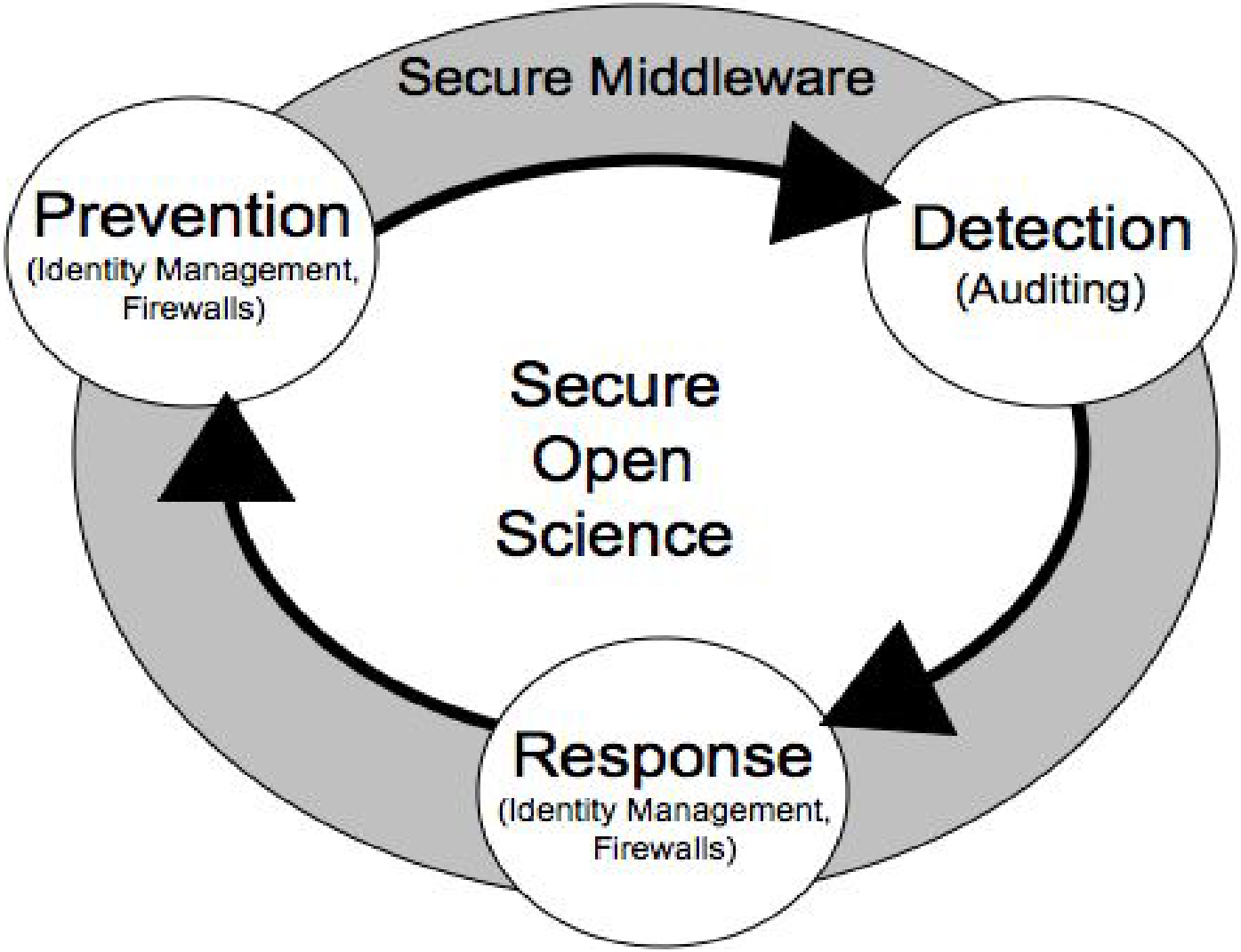
# Guiding Principles

- Focus on capabilities that are priorities for and are NEEDED by DOE applications and facilities
- Work closely with a few committed applications and facilities to develop capabilities
- Provide development and deployment of security solutions with and in support of DOE applications and facilities
- Deliverables
  - 18 months - Concrete near term goals for deployment activities
  - year 3 and year 5 - Longer term deliverables for deployment and possible research activities
- Will provide extensive deployment support

# Distributed Science Security Problem

- Applications and Middleware poorly integrated with site security
- Difficult to track users and usage across sites
- Virtual organizations and sites do not have all the tools needed to manage security
- Forensics in distributed environments is tedious and information is scarce
- Grid middleware poses a potentially inviting hacker target in the future as we deploy these large grids
- Credential revocation is very difficult currently
- Firewalls often limit the application connectivity options

# Strategy - Prevent, Detect, and Respond



# Interrelated Topic Areas

- Auditing and forensics
  - Services to enable sites, communities, and application scientists to determine precisely *who* did *what, where* and *when*.
- Dynamic ports in firewalls
  - Services to open and close ports dynamically for applications while enforcing site policy.
- Identity management
  - Services to seamlessly manage identity and access control across sites and collaborations, and to allow for rapid response to security incidents.
- Secure middleware
  - Services to proactively find and fix software vulnerabilities and guarantee deployed security software is current and correctly configured.

# Identity Management

- Problem:
  - Revocation mechanisms are slow and cumbersome
  - Level of integration amongst various solutions incomplete
  - Nagging issues of credential renewal, configuration management, etc.
- Near Term Approach:
  - Build on existing solutions:
    - VOMS, CAS, GUMS, MyProxy, GSI, OCSP
  - Integrate and deploy, e.g.
    - Deploy OCSP service; client support in GT, MyProxy, etc.
    - VOMS support in GridFTP, MyProxy
    - GUMS callout into GT, MyProxy

# SOS CET MyProxy Deliverables

Von Welch and Jim Basney
NCSA

# MyProxy News

- MyProxy Certificate Authority is 1 year old
  - Issues short-lived certificates based on PAM, Kerberos, X.509, and/or Pubcookie authentication
  - Many improvements over past year:
    - LDAP and custom call-outs
    - Support for credential renewal
  - See http://myproxy.ncsa.uiuc.edu/ca
- MyProxy VOMS authorization support
  - Developed by / Presented by Daniel Kouril
  - See http://myproxy.ncsa.uiuc.edu/voms
- MyProxy Java improvements
  - Support for credential renewal in Java CoG
  - MyProxy JAAS module (http://myproxy.ncsa.uiuc.edu/jaas)

# Plans in Bugzilla

- Many plans are described in MyProxy bugzilla
- Numbers in presentation correspond to bugzilla entry number
  - e.g. “(#101)” refers to bug 101
- Visit bugzilla to see more details and provide feedback
- Add yourself to cc list for bugzilla item to stay up-to-date on development
- Bugzilla can be found by visiting URL below and clicking on “Bugs” link on left:
  - http://myproxy.ncsa.uiuc.edu

# FY 07 MyProxy Deliverables

- Audit logging (#343)
  - Integration with general SOS audit framework
  - Logging of events to allow for intrusion detection, forensics, usage analysis, etc.
- Brute Force attack protection (#325)
  - Resistance to password-guessing attacks on MyProxy server
- Continued…

# FY 07 MyProxy Deliverables (cont)

- Code audit
  - In collaboration with UW-Madison
- VOMS support
  - MyProxy issuing credentials with VOMS assertions (#298)
  - Item #1 from http://grid.ncsa.uiuc.edu/myproxy/voms/
  - Daniel Kouril just did item #2: MyProxy server support authorization based on VOMS

# FY08 MyProxy Deliverables

- Renewal capabilities (#296)
  - Generalization of EGEE renewal service concept to work with other Grid Infrastructure
  - Collaborate to also support Glite delegation service interface also a possibility
- Replication capabilities
  - Server replication for high-availability (#275)
  - Fail-over support in clients (#306)
- Continued…

# FY08 MyProxy Deliverables (cont)

- Cryptographic assessment
  - In collaboration w/LBNL
- Integration with OCSP (#281)
  - Determination of invalid credential prior to issuance
  - Allows RPs to increase trust in MyProxy-issued credentials, decrease need for RP to check
  - Decreases trouble-shooting aspects by detecting bad credentials early

# FY09-FY11 MyProxy Deliverables

- PKCS11 Support
  - Obtain Grid credentials via existing HW tokens
    - E.g. FIPS 201, Smart Cards
  - Provide MyProxy credentials to PKCS11-aware applications (#291)
    - E.g. Web browsers
- Name-mapper service callout (#344)
  - Allow MyProxy to callout to determine mapping from authenticated client identity to DN
  - Support for existing Grid services - e.g. GUMS
- Continued…

# FY09-FY11 MyProxy Deliverables (cont)

- Site credential translation hooks
  - Enhancement of GT with hooks to callout to MyProxy in order to automatically translate between local credentials and Grid credentials
    - E.g. Kerberos->X509
  - Also hooks to translate between Grid credentials and local credentials (e.g. pkinit)

# Identity Management

- Longer term:
  - XKMS support to ease configuration management
  - Integrate data access control policy with work on semantic workflows
  - PKCS 11 support
  - Ubiquitous hooks in middleware for site security integration
    - E.g. Kerberos, auditing,

# Secure Middleware

- Problem
  - Grid middleware has become an essential part of the science infrastructure security of this infrastructure is an essential consideration
- Approach - steps
  - *Architectural analysis* to understand the system level view of a middleware component and its external interactions
  - *Identify trust boundaries/threat model* to understand the dependencies and areas of concern
  - *Component and system analysis* of the particular software to understand vulnerabilities
  - *Disclosure of results* process is handled carefully to allow time for mitigation efforts
  - *Mitigation mechanisms* to provide means of patching or mitigating the potential security vulnerability

# SOS Current Plan for Start

- Start will be some time after October 2006
- Five year development and implementation plan
- Aggressive schedule and tight funding
- Expect to be able to work closely with and leverage extensively other efforts already underway internationally