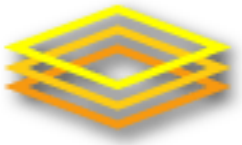


Open Science Grid Security Activities

D. Olson, LBNL
OSG Deputy Security Officer

For the OSG Security Team:
M. Altunay, FNAL, OSG Security Officer, D.O.,
R. Cowles SLAC (past member), J. Basney NCSA (new member),
Ron Cudzwicz FNAL, Rob Quick IU/GOC, Alain Roy U.Wisc./VDT

ISGC2008 Taipei
9-11 April 2008

Open Science Grid

Abstract

The status and directions of the security activities of the Open Science Grid. The high-level goal is to provide a security framework that enables science and promotes autonomous and open science collaboration among VOs, sites, and software providers. Keeping the balance between openness, which is necessary for the science, and the security is at the core of our work. We address these goals by providing: operational security, interoperability with other grids, and education. The operational security processes are modeled on the NIST 800-53 guidelines for security controls for information systems and includes appropriate communications channels for vulnerability awareness and incident response. Interoperability work spans the range from international policy development (JSPG, IGTF) to inter-grid information services to middleware development coordination (MWSG). Using the concept of Integrated Security Management where every person has responsibilities for security, we have started developing awareness materials and providing role-based training on security practices and features to grid participants.

Open Science Grid

Contents

- Goals
- Methodology
- Operations
- Interoperability
- Education
- Development and Directions
- Conclusion

Open Science Grid

Goals

- The **high-level goal** is to provide a security framework that enables science and promotes autonomous and open science collaboration among VOs, sites, and software providers.
- **Availability** - Keeping the balance between openness, which is necessary for the science, and the security is at the core of our work.
- **Integrity** – of resources, VOs, middleware quality
- **Confidentiality** – sufficient to meet the community requirements
- Fine print –
  - data integrity is a data owner issue and VOs own application data
  - Confidentiality between VOs depends on sites' policies and practices and no extraordinary requirements have been expressed

Open Science Grid

Methodology

- NIST 800-53 process
  - used by government laboratories
  - No apparent standards for U.S. universities
- Integrated Security Management
  - Security is part of everyone's responsibilities
- Security processes integrated with Operations

NIST Process

Modeled on NIST IT security process, adapted to meet OSG requirements.

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

National Institute of Standards and Technology

NIST

...working with industry to foster innovation, trade, security and jobs

Slide from Irwin Gaines

Open Science Grid

Security Plan

- Outline of security plan
  - 1 OVERVIEW
  - 2 CONTROLS
    - 2.1 Risk Assessment and Management
    - 2.2 Overview of OSG Security Control Clusters
    - 2.3 Management Controls
      - 2.3.1 Integrated Computer Security Management
      - 2.3.2 Security Processes
      - 2.3.3 Trust relationships
    - 2.4 Operational Controls
      - 2.4.1 Security Training and Awareness
      - 2.4.2 Incident Response
      - 2.4.3 Data Integrity
      - 2.4.4 Configuration Management
      - 2.4.5 Vulnerability Management
      - 2.4.6 Physical Access Control and Site Management for Production Services.
    - 2.5 Technical Controls
      - 2.5.1 Monitoring
      - 2.5.2 Access Control for Core OSG Administrators/Users
      - 2.5.3 Scanning
  - 3 References
- Includes 50 specific controls
- We have started a second pass of NIST800-53 loop
  - First pass included only OSG core
  - Second pass will include OSG participants (resource providers and VOs)

Open Science Grid

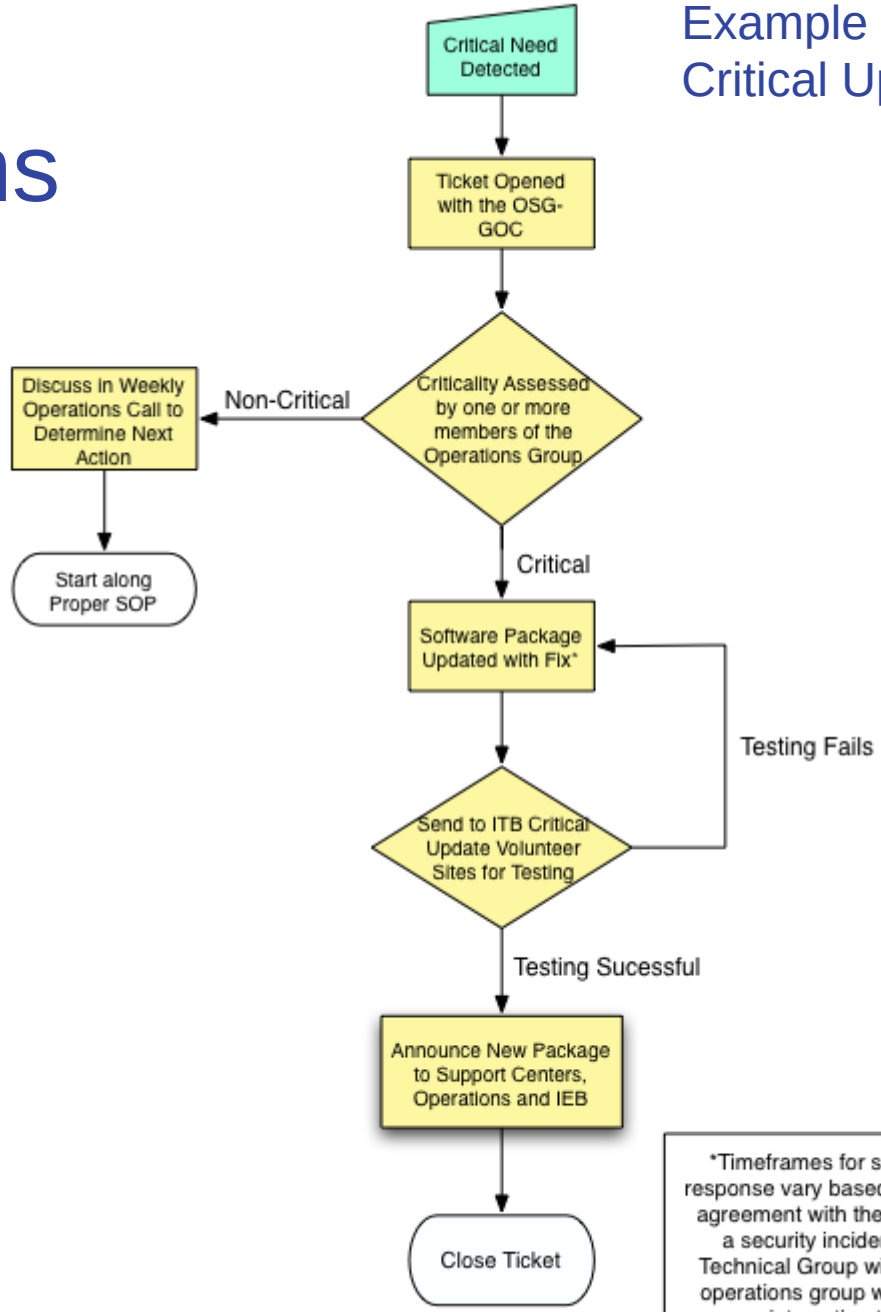
ISM = Owners' Responsible

- **OSG core service - Owner**
  - Software (VDT) – Alain R.
  - Web presence, email lists – Marcia T.
  - GOC services – Rob Q.
    - reg. db, tickets, VOMS, monitoring, …
  - Integration Test Bed – Rob G.
  - Accounting collector (Gratia) – Phillipe C.
  - Engagement – John M.
  - Security processes – Mine A.
  - RA – Doug O.

Security Operations

- Security notices and incidents:
  - GOC receives notice at security address, filters spam and notifies security officer.
  - Analysis by security team, possible patch preparation by software team, and decision by security officer
    - Software and Operations coordinators are part of security team
  - GOC sends notice to affected participants.
- GOC registration collects security contact info
- Security team plans “fire drills” run by GOC to test aspects of security infrastructure & response
- Inter-grid
  - OSG security officer in direct contact with EGEE and TeraGrid security officers

Example process: Critical Update



Open Science Grid

Additional Activities of the Security Team

- Vulnerability analysis of software stack
- Audit of VOs and sites
  - Starting with accuracy of security contacts
- Starting to monitor accounting data for irregular activities (using splunk)
- Working with CEDPS (Tierney et al.) on log collection for analysis/incident response
- OSG Registration Authority with DOEGrids CA (several thousand valid certificates)
  - Participated in CA audit for EUGridPMA
- Policies (lots of work)

Open Science Grid

Identity vetting in OSG RA

- Most Certificate Authorities use a “simple” identity vetting model, face-to-face presentation of photo ID to a registration agent.
- OSG RA uses a distributed “sponsorship model” where each registration agent develops list of known Sponsors who can vouch for the identity of a subscriber (person requesting a certificate).
  - Communications via signed email or telephone.
  - Enables widely distributed RA network with normally a rapid processing time for requests.
- Discussed this model with EUGridPMA in January with aim to clarify understanding and include in Classic CA accreditation profile.
- Several other CA operators are interested in this model.

Open Science Grid

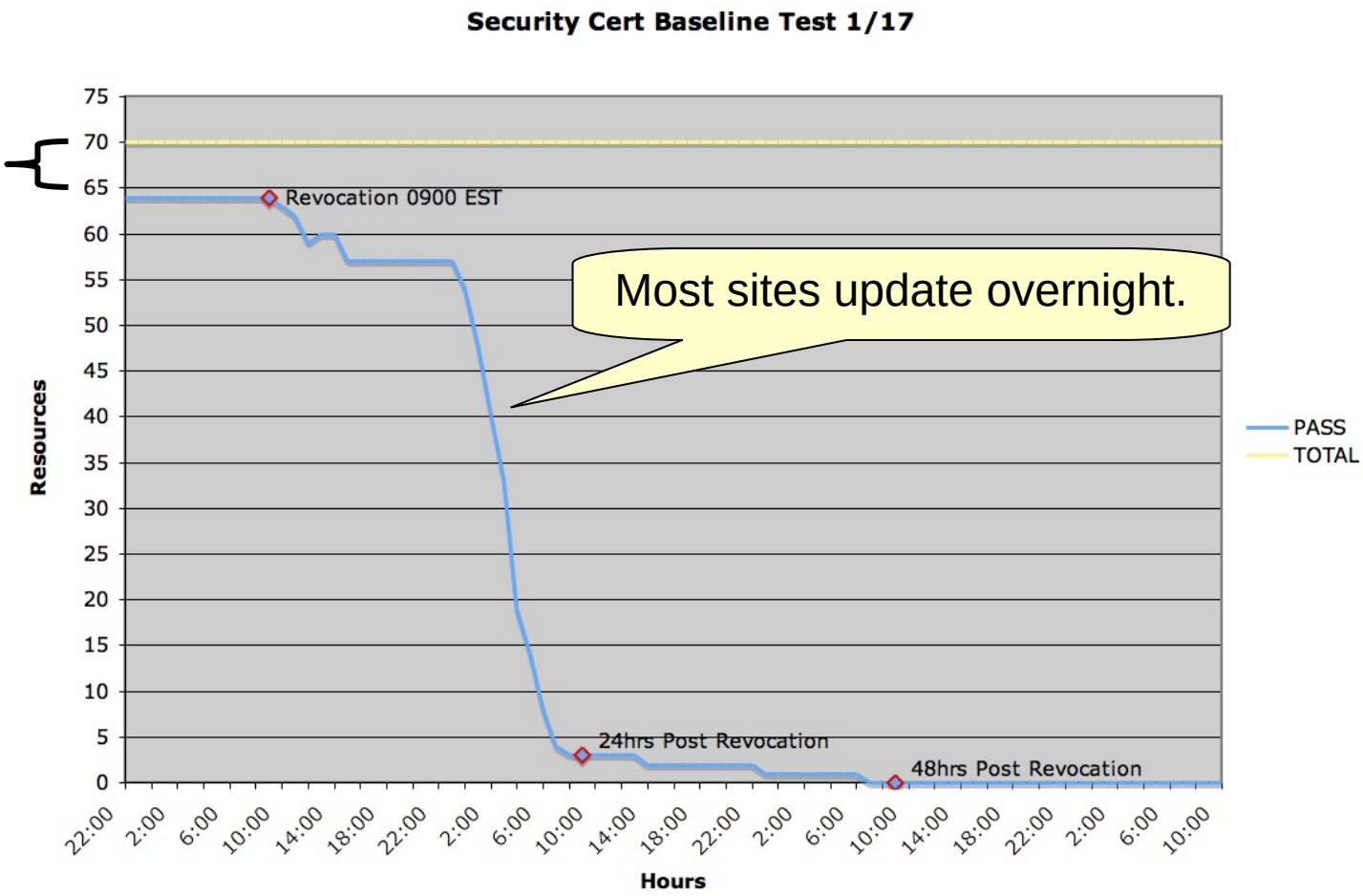
Metrics

- Timeliness of software patches
  - Goal is 95% of vulnerabilities have patch released within 1 week
  - Performance in past year
    - 12 vulnerabilities
    - 4.5 days average patch release time
    - Longest – 13 days
    - 3 vulnerabilities > 1 week

Example “fire drill” response

Measure time to authentication failure following certificate revocation.
Shows sites’ CRL update performance.

Few sites fail authN initially.



Open Science Grid

Controls Assessment

- Controls are assessed by one or more of
  - Interview
  - Examination
  - Test
- In fall of 2007 we performed assessment primarily by interview of service owners.
  - Was a lot of work.
- Lessons learned feed into update of security plan in 2008.

Open Science Grid

Interoperability

- Inter-grid
  - Communications between grid security officers
  - Incident response procedures
  - Shared PKI trust fabric and authN/authZ credential “standards”
- Policies
  - Participant in Joint Security Policy Group
  - Participant in IGTF/TAGPMA
- Infrastructure
  - Co-chair of Middleware Security Group (MWSG)
  - Identify and participate in specific projects
    - VOMS/GUMS
    - authZ architecture, FQAN standards
    - glexec
  - Reliance on and coordination with external projects
    - VO Services, VOMS, Condor, Globus, …

Open Science Grid

Education

- Awareness training is a key part of the NIST process.
  - Knowledgeable people are less risky than ignorant people.
- NIST control recommendations are:
  - Security Awareness and Training Policies and Procedures
  - Security Awareness
  - Security Training
  - Security Training Records
- OSG Controls
  - Awareness for Managers
    - Briefing of the Executive Board
  - Role-based training (for Users, VO managers, Site Administrators, Management)
    - Security briefings and discussions at All Hands Meetings
    - Included in Grid School materials
    - Included in Site Administrators meetings
    - Included in Users Meetings
  - Weekly meetings of security team
  - Security addresses and mail lists

Open Science Grid

Developments and Directions

- Proxy cleanup – don't leave old proxy credentials laying around
- CRL handling – ensure that sites use CRLs since GSI is "fail open" when CRL is missing
- Timely CA certificate updates by sites
- Ability to enforce or check limited proxy lifetimes
- Site user authZ suspension (bar banned DN)
- More secure communications for incident handling and analysis

Open Science Grid

Developments and Directions (2)

- Uniform FQANs across sites, grids – privileges are not uniformly interpreted or enforced
- Encourage federated Id management – would like grid credentials based on home institution or user facility authN
- Better (easier) management of 1000's of host credentials – work in progress
- Simpler site security configuration management
- Better monitoring to identify & limit security incidents
- Advancing policies – still many incomplete and not yet existing policies
- Continue "fire drills" and develop more realistic "incidents"

Open Science Grid

Conclusion

- NIST model provides helpful guidance
- Iterative process is useful and we can look forward to several more iterations
- Interoperation/interoperability is challenging for security as in other aspects of grid
  - Incident response, information sharing, responsiveness of sites – all challenging
- The partnerships with EGEE and TeraGrid are very fruitful
- Bottom-line goal is to help the science and not hinder it.