Open Science Grid

OSG Security Framework

Bob Cowles – SLAC / OSG

Presented at MWSG10

15 November 2006

Based on FIPS and NIST 800 Series

- FIPS 199 – Security categorization
- NIST 800-53A – Security Controls

Tasks

- Roles and relationships
- Threat analysis
- Risk Analysis
- Areas of Concern

Roles and Relationships

- Users
- VOs
- Service providers
- Software providers / packagers
- Resource providers
- Grid Facility
- Identity providers
- Other Grid organizations

Open Science Grid

Threat Analysis

- Flows into Risk analysis
- Covers all perils unique to grids
- Assume some level of due diligence (verify)

Open Science Grid

Risk Analysis

- Based on Confidentiality / Integrity / Availability requirements
- Organizations have three dimensions
  - Users
  - Services/Resources
  - Software
- Levels of risk
  - Affect the whole grid
  - Affect multiple sites or organization
  - Affect single sites / users/ organization
- Objective is to reach LOW risk

Open Science Grid

Areas of Concern

- Technical Controls
  - Over People (administrators / users) - authN, authZ
  - Scanning (logs, intrusion detection, etc.)
  - Physical Security Controls
- Operational Controls
  - Vulnerability Management
  - Configuration Management.
  - Data Integrity
  - Incident Response
  - Security Training and Awareness.
- Management Controls
  - Integrated Security Management (roles & responsibilities)
  - Trust Relationships
  - Security Process Lifecycle

OSG Security Activities

- Security Plan for OSG Facility in Dec 06
- Work needed (multi-year plan)
  - Construction of plan & process for core
  - Construction of plans & policies regarding OSG's relationship with other entities
  - Implementation
  - Operation

Guiding Principles

- Think globally, Act globally
  - Try to be complete in thinking about problems and solutions
  - As we formulate policies, realize they are interim until coordinated with other bodies
- Maximize Interoperability!

Sample Considerations for MWSG

- Maintain contact information
- Vulnerability reporting
- Respond to vulnerability reports
- Logging
- Secure distribution
- Complete AuthN/AuthZ verification