OSG Security

Bob Cowles (SLAC/OSG) for
EGEE'07/MWSG in Budapest

02-Oct-2007

NIST Process

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

Grid Connection

- Grids are virtual sites in a sense, and will be examined and audited using same criteria
- And all the US labs that have resources used by grids must live by NIST guidelines, so it is necessary to use on the NIST framework for documenting grid computing security requirements
- OSG is starting with the core services

NIST Process Details

- Each system needs:
  - Functional description
  - Hardware and software description (especially description of boundaries)
  - Risk assessment
  - Security plan (showing controls to mitigate the greater impact or likelihood risks)
  - System Sensitivity Categorization (low/moderate/high sensitivity)
  - Contingency plan
  - Security control testing and evaluation

Security Plan

- Fully describe each control mentioned in your risk assessment
- Controls organized into management, operational and technical controls
- Show how each control will be assessed (Interview, Examination, Test)

NIST Control families

OSG Relevance

- Management
  - Management Risk Assessment RA
  - Management Planning PL
  - Management System and Services Acquisition SA
  - Management Certification, Accreditation, and Security Assessments CA
- Operational
  - Operational Personnel Security PS
  - Operational Physical and Environmental Protection PE
  - Operational Contingency Planning CP
  - Operational Configuration Management CM
  - Operational Maintenance MA
  - Operational System and Information Integrity SI
  - Operational Media Protection MP
  - Operational Incident Response IR
  - Operational Awareness and Training AT
- Technical (Access Control, Usage Accounting, Scanning)
  - Technical Identification and Authentication IA
  - Technical Access Control AC
  - Technical Audit and Accountability AU
  - Technical System and Communications Protection SC

Work Plan (Sep-Dec)

- Test Incident Response
  - Revoked certificate
  - Suspended (by VO) user
- Define Categories of Data Sensitivity
  - No personal or financial data
  - OSG need-to-know (e. g. unpatched vulns)
  - OSG and friends
  - Public

Work Plan (cont-1)

- Monitoring
  - Version control
  - Review proposed changes
- Vulnerability Management
  - Awareness
  - Reporting
  - Mitigation

Work Plan (cont-2)

- Access Controls for core services
  - Ensure controls are consistent with categories of data stored or processed by the various core services
- Usage data
  - Available appropriately to VOs, sites, users
- Web Services
  - Vulnerability scanning
  - Intrusion Detection

Work Scope

- Some controls are manual for now
- Automate in later stages
- Aggressive plan but a good start
- Demonstrate responsible care to funding agencies

- Questions?