OSG Security

D. Petravick
Fermilab
May 2, 2007
Largest Scientific Environments

- May very well be in experimental High Energy Physics.
  - Global collaborations > 2000 scientists
  - Nations make contributions to build the accelerator and experimental equipment.
  - Tremendous amounts of data,
    - need to constantly calibrate, select and analyze.
  - Experiment
    - has pledged computing resources.
    - Has non-pledged resources.
The OSG

• **Proposal:** “We propose to build a cyber-infrastructure that can grow to provide thousands of users effective access to 100,000 CPUs, 10s of PB of storage, located at hundreds of sites and interconnected by multiple 10Gb/s network links.”

• **Technical Basis:**
  - Service-based access to compute and storage services.
  - A software stack used by experiments to manage their users, their jobs, and their jobs.
  - The environment *interoperates* with other similar grid environments.
    - LCG, teragrid, et al.
Example Capabilities

9.6 gbps average rate (binned by hour)

52 TB/day Tape/HSM
## OSG Capacity Targets

<table>
<thead>
<tr>
<th>Org</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATLAS</td>
<td>3</td>
<td>5</td>
<td>14</td>
<td>24</td>
<td>1.1</td>
<td>2.6</td>
<td>7.6</td>
<td>11.8</td>
</tr>
<tr>
<td>CMS</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>22</td>
<td>1.0</td>
<td>2.5</td>
<td>4.5</td>
<td>4.9</td>
</tr>
<tr>
<td>LIGO</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>0.2</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>STAR</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>0.04</td>
<td>0.06</td>
<td>0.1</td>
<td>0.2</td>
</tr>
<tr>
<td>other</td>
<td>10</td>
<td>13</td>
<td>17</td>
<td>22</td>
<td>1.0</td>
<td>1.0</td>
<td>1.4</td>
<td>1.9</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
<td>34</td>
<td>59</td>
<td>86</td>
<td>3.3</td>
<td>6.1</td>
<td>13.6</td>
<td>18.8</td>
</tr>
</tbody>
</table>

In 2008 we estimate: 53 MSI2K = 26,000 CPUs; 74 MSI2K = 37,000 CPUs.
Me, my friends, the grid

VOs: $O(10^1, 10^2)$

Scientists $O(10^4)$

Sites: $O(10^2, 10^3)$

And their $O(10^3)$ security organizations
Illustrative example

I trust it is the user

I trust it is the user's job

I trust the job is for the VO

I trust it is the VO
Grid Security

• The goal of grid security is establish trust that computing organized along these lines will have appropriate integrity, availability, and confidentiality.

• OSG cannot bear the security responsibilities of sites or VO’s.

• Therefore, initially, inter-entity security is conceptually a set of pair-wise agreements.
  - We have more than a few autonomous parties
  - Not a small task.
Operational Grid Security

• Based on NIST model -- Controls based on risk, rooted in policy.
  - Risk == f(vulnerability, threat)
  - Goal: Achieve acceptable risk
    • Recall -- context is open science.
  - Means: Controls
    • Management (what did we decide?)
    • Operational (we count on behaviors)
    • Technical (stuff done in HW/SW)
Some Specifics

- OSG security seeks to **compliment, not replace** site and VO security organizations.
  - Recall Roadmap: $O(10^4)$ parties. Now: $O(10^3)$
  - Make the security discussion scalable by standardizing the many elements of the discussion.
  - Foster a secure software stack for grid services.
  - Foster communications
  - Know what’s going on from the perspective of the whole grid
Scaling:

• Make the discussion standard.
  - Think of the market in mortgages
    • Many standard terms

• Model security policies
  - JSPG: sites, VOs, users.
  - IGTF: Identity providers.
  - TBD:
    • Service providers (likely JSPG),
    • software providers.
Foster secure software stack

• OSG Stack: Primary role is through the OSG software coordinator.
  - Sites use versioned OSG stack w/OSG controls.
  - VO’s -- Less standard, less enumerable

• Absolute dependency on the skills and quality of our system software community.
  - Success depends on sponsors of these groups
  - OSG job is to
    • Demand good qualities
    • Recognize good qualities.
    • Proselytize the scale changes
Foster communications

• Grid operating organization assembles, and maintains list of site security contacts.

• Two levels
  – Incident/urgent matters.
  – Discussion/thinking

• Communication is available for non-grid matters. (e.g sniffed password of a person w/ distributed administration responsibilities).
Current work: Situational Awareness

• Is the configuration of deployed stack at sites as expected?
• Is someone rattling the doorknob systematically at OSG sites?
• Has compromise of a server compromised the grid?
• Are AUP’s abided by?
Summary

• Grid security is federated – O(10^4) entities.
  - The problem is made more tractable
    • By the service oriented access to resources.
    • By standardizing the terms of discussion.
    • Because interoperation is viewed as essential by all parties

• Currently, the security structure of sites is more standard than the structure of VO’s.

• Grid security is complimentary to site and VO security organizations.

• Absolutely dependent on the quality of community written software components.