OSG Security Overview

D. Petravick

FNAL, OSG Security Officer

CYBO6, Arlington, VA

February 22, 2007

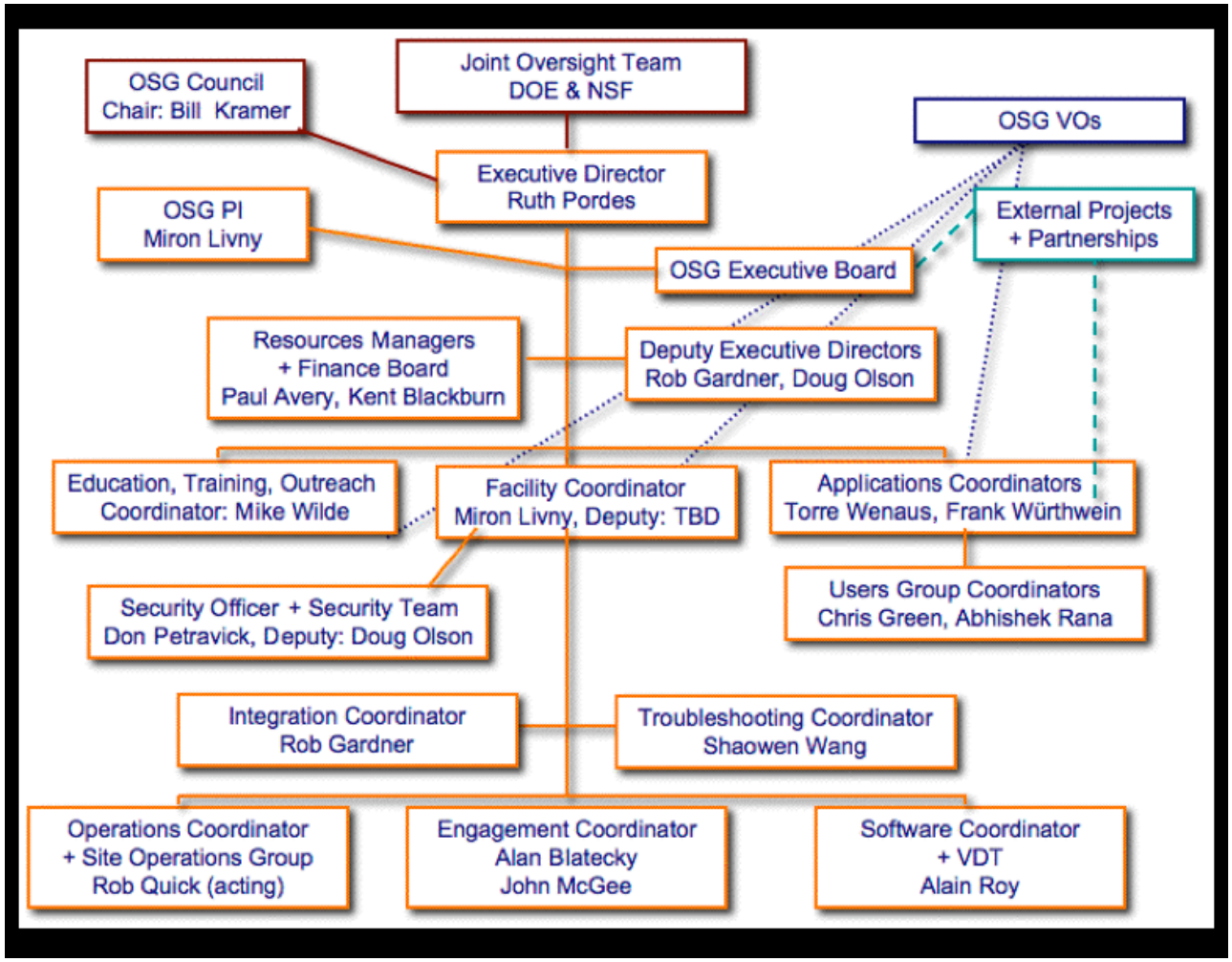
Overview and Vision

- The Open Science Grid is a distributed computing infrastructure for large-scale scientific research, built and operated by a consortium of universities, national laboratories, scientific collaborations and software developers.

Overview and Vision

- Researchers from many fields, including astrophysics, bioinformatics, computer science, medical imaging, nanotechnology and physics, use the OSG infrastructure to advance their research….
- …The OSG capabilities are also being driven by the needs of large scientific collaborations : U.S. participants in the ATLAS and CMS particle physics experiments at the Large Hadron Collider, currently being built at CERN in Geneva, Switzerland; the Laser-Interferometer Gravitational-Wave Observatory (LIGO), a facility dedicated to the detection of cosmic gravitational waves. …

OSG Structure



OSG blueprint in a nutshell

- Service based access to resources,
  - Notably compute and storage.
  - Users need no interactive logins.
- Sites get a software stack which they deploy.
- Virtual Organizations get a software stack.
  - There are thin and thick VO's

Core OSG security

- Is **not** the security of the sites, or the Virtual Organizations.
- Is security of….
  - the OSG organization, including data flows like accounting information.
  - the VDT-based software stack and its configuration management methods.
  - good name of Grid Computing.

Core Status

- NIST - style Core security process
  - NIST-800 Secures sites, OSG is a consortium depending on member institutions for tangible things.
- Risk Analysis, Security Plan
  - The Security Plan Specifies Controls which, when implemented, will achieve acceptable risk.
  - Working on implementing the controls in the security plan.

Control Families

- Management Controls
  - How we are be organized
- Operational Controls
  - Things we count on people to do
- Technical Controls
  - Things we count on computers to do.

Management Controls Clusters

- Integrated Computer Security Management
- Security Processes
- Trust Relationships
  - Here is a place we work to innovate.
    - Find a model that provides security, but is apropos to Open Science.
    - "Default" and "Detailed"
  - Detailed controls -- Approval, Documentation, Clear Roles and Responsibilities, Review.

Operational Control Clusters

- Security Training and Awareness
- Incident Response
- Data Integrity
  - bars sensitive info from core
  - Restricted, limited and public data.
- Configuration Management
- Vulnerability Management
- Physical Access control and Site Management

Technical Controls Clusters

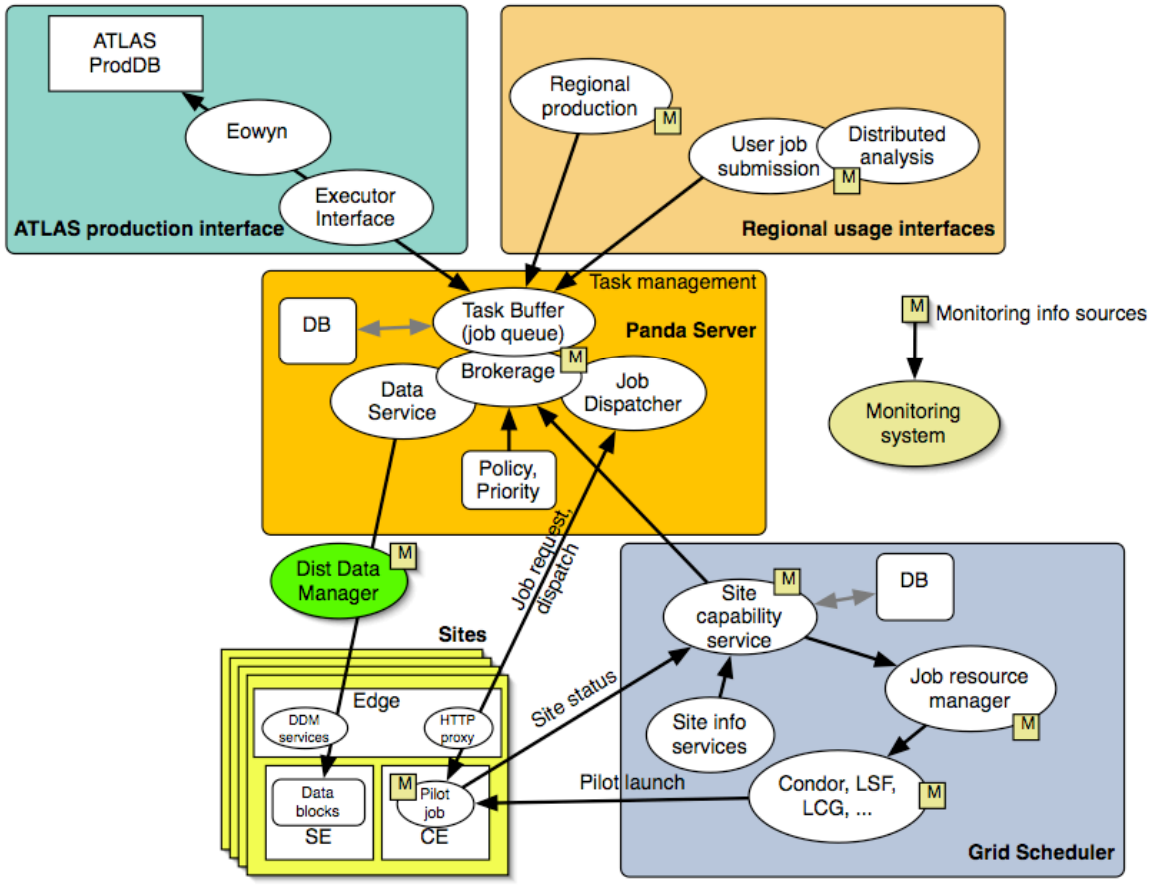
- Monitoring
  - Passive -- looking at OSG data, to infer the securiyt state
  - Includes access to Accounting data for security purposes.
- Access Controls
- Scanning
  - Stimulation of OSG Servinces to infer their security state.

Relationship to VO's

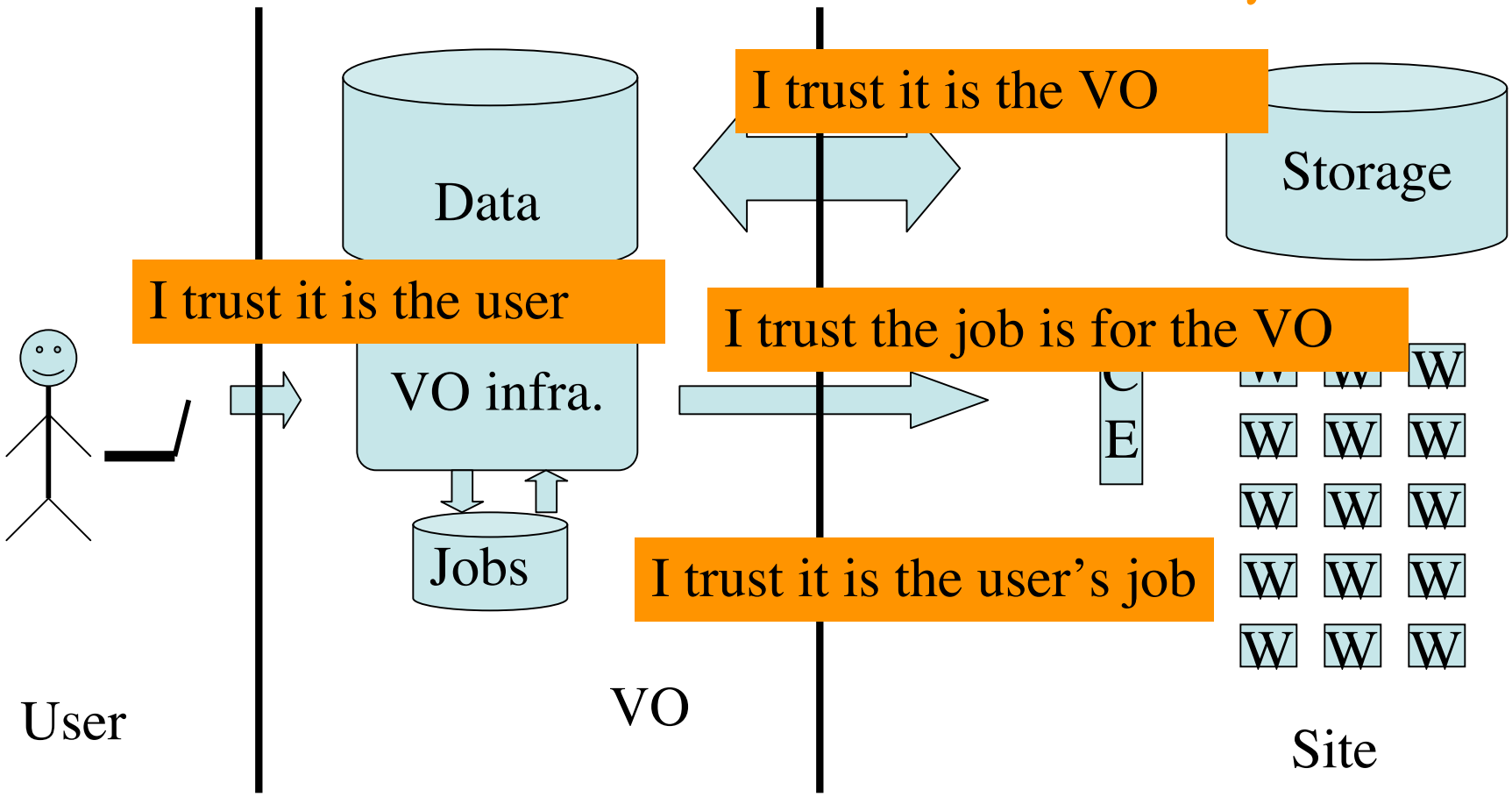
- OSG VO's assemble their own software stacks using VDT Components and other software.
  - Grid computing for data intensive science is open, evolving.
- In general OSG VO's run services, and/or supervise the services others run for them.
  - -- an example is VOMS (people,roles)
  - -- more informative -- PANDA (ATLAS)

Panda

Panda Architecture



Illustrative example



One site's basis for VO trust.

AUP's (conceptual)

- Grid Roles -- User, Site, VO
- Service AUP
  - Ought to automatically apply to anyone provisioning services.
    - Analogous to "merchant" and UCC
    - Require apropos levels of diligence
- Software AUP
  - Ought to apply automatically to anyone supplying software.
  - Require apropos level of diligence.

Scaling security

- There can be a complex relationship between site and VO.
  - Security responsibilities are best born by the party best able to execute them.
  - In the system just shown it is best if the VO takes on substantial responsibilities.
    - Why not? The ATLAS collaboration built a physics detector the size of an apartment block, and a large body of middleware.

The OSG's role

- Cannot bear security responsibility for site or VO.
- Helps facilitate the discussion by trying to standardize the discussion.
- Standardizing the discussion (as well as the technical environment) enables the creation of security service providers for VO's
  - A VO can find someone to do much of the work.
  - Examples
    - OSG provides VOMS services for various VO's
    - OSG DOEgrid Registration Agents.

AUP work --

- The Value of the AUP is
  - An agreed on schema for at least part of the security problem.
    - Makes it possible to talk about the domain.
  - The standardization of pair-wise security discussions.
    - Which sites and VO's are free to have.
    - If the discussion is not held something exists.

Common pattern seen elsewhere

www.incommon.org

Benefits of joining InCommon include:

…..

Economies of scale for contractual agreements: Some or all of the policy and legal requirements for bilateral agreements between institutions for sharing of resources may be consolidated by or leveraged from the Federation policies, agreements and requirements documents. This could minimize the need or scope of multiple relying party agreements.

AUP work.

- The OSG prefers to conduct AUP discussions in broad fora.
- Grid interoperation is an OSG value, and required by some stakeholders.
- JSPG, IGTF, etc. Much travel.
- Much to do.

Summary

- Reduce risks from attacks on site and VO's via grid services to acceptable levels,
  - Desiderata include:
    - hardened services for its stack.
      Good suppliers, additional VDT support.
    - Good processes. Config mgt; Resp, lifecycle.
    - Assessing deployed grid via monitoring and scanning.
- Facilitation of security discussions between sites and VO's by making them uniform.
- Build a security system consitent w/ consortium values.