OSG VO

D. Petravick

Brookhaven Meeting

Sept 5, 2006

Overview

- Security is a process.
- Decisions Process is Risk Based.
  - A risk is a vulnerability and a threat.
  - Organizations implement controls over their activities to obtain acceptable risk.
  - OSG relies on many organizations feeling secure enough to interoperate.

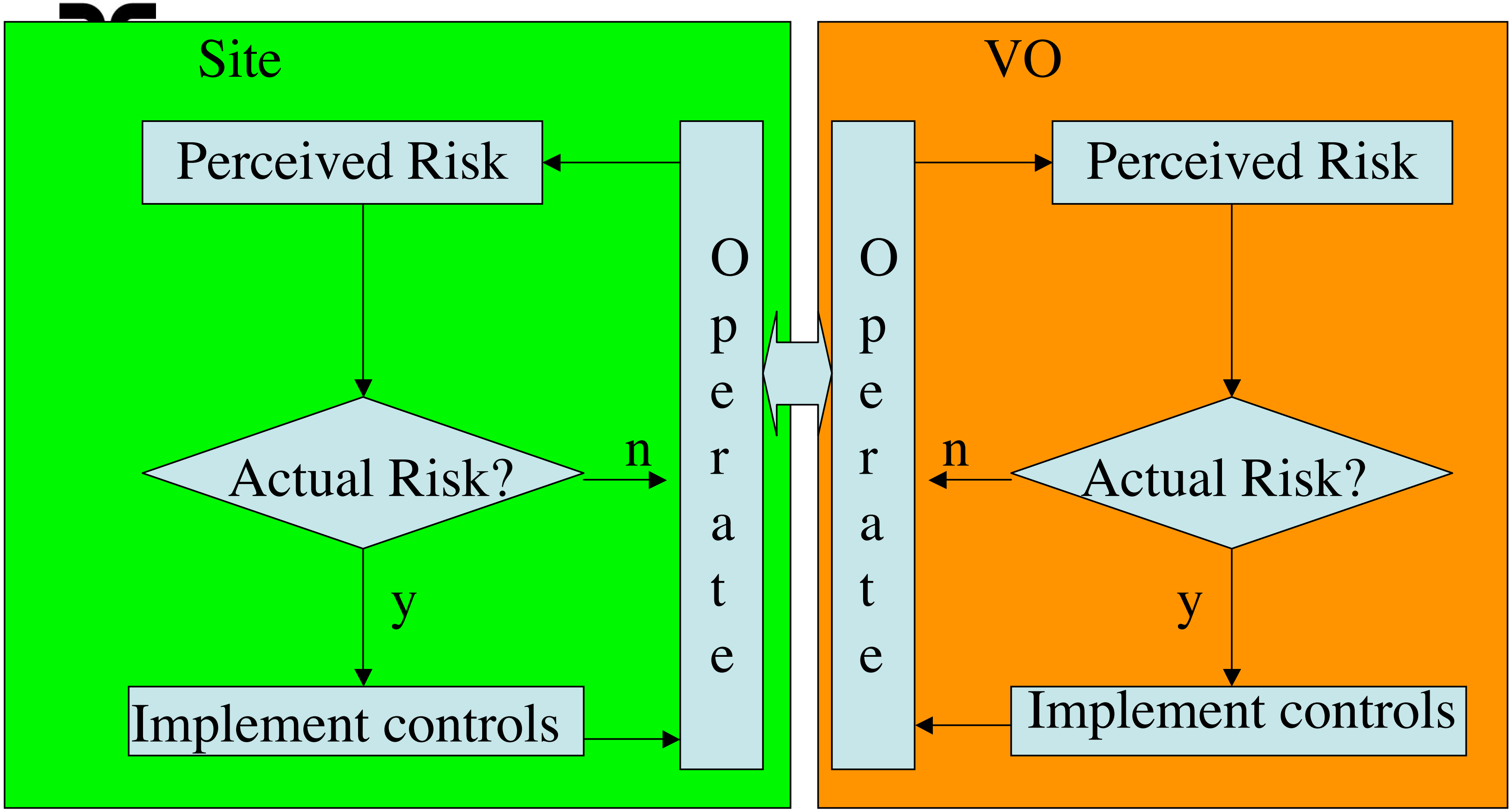
Trust

- Interoperation implies Trust.
- What is Trust?
  - I **rely** that you will
    - do **something specific**,
    - for **some period**.
- Examples:
  - US DOE Lab: Is accountable for the computations run on its computers. --> Needs to know the identity of end user.
  - VO: wants to know its scratch files are private on a site. -- Needs to know there are protections.

Risk based view of the world

- Organizations implement controls over their activities so as to obtain acceptable residual risk. Organizations: Sites, VOs and Grids.
    - Each has a security process lifecycle.
    - Satisfaction jointly and severally.
- Each organization is captain of its own ship.
    - However, constrained to interoperate.
- Standards (e.g. OSG AUP’s) aid interoperation.

Site-VO Interoperation



Scaling :-(

- Every organization has to reduce its risk to acceptable residual risk, and the security has to interoperate.
  - Identified trust.
    - Something specific is relied on
    - Is not checked each time.
  - Apropos Managerial, Operational and Technical Controls, for trust items.
- Scaling is a problem, work needs to be done
  - Common standards -- i.e. OSG AUP.
  - Fewer entities -- Aggregate the small.

One element of the Service AUP

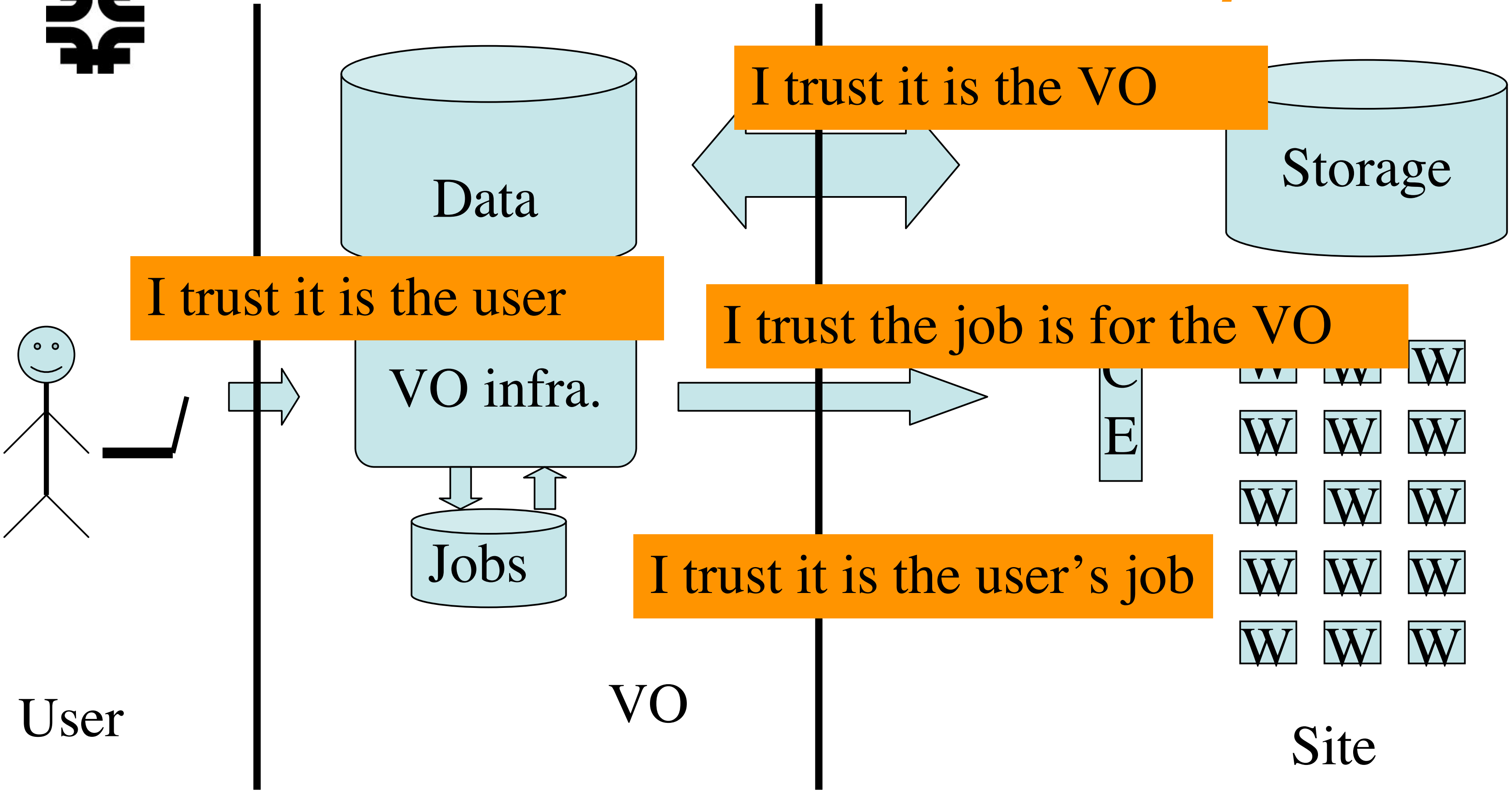
- (4) All services **that hold credentials for another party** are in a position of trust. You agree to broker these **credentials** honestly and not to abuse that trust. You agree to take reasonable precautions to protect the security of those **credentials**, to investigate all reports of compromise of the security of those **credentials**, and to participate in the OSG Incident Response Plan as needed. *You are required to participate in responses to security incidents that involve resources under your control.*
- Comments
  - Credential processing is important but
    - Perhaps there are other aspects to accountablily

Proposed addition to the Service AUP

- (5) You agree to notify OSG of **any(!)** security deficiencies or vulnerabilities of your service that you become aware of and are likely to adversely affect any users or other services beyond your local site. This notification is by **means provided by OSG for maintaining the privacy of these communications**. If warranted, the OSG will provide appropriate information about the issue to OSG VOs and other affected service providers registered with the OSG.

- Comments
  - All extant systems have vulnerabilites.
  - So .. "any" does not precisely convey intent.
  - Intent is "above acceptable residual risk"
  - Evidently, ISM requires distributed Risk Assessment.

Illustrative example



I trust it is the VO

Data

Storage

I trust it is the user

I trust the job is for the VO

VO infra.

CE

W W W
W W W
W W W
W W W
W W W

Jobs

I trust it is the user's job

User

VO

Site

OSG technical controls

- Over its core (moot for computational sites and Experimental VO’s)

FNAL Thinking

- For VO's that have services in their infrastructure….
  - Trust relationship must exist.
  - Transparent technical architecture allows evaluation of trust.
    - Though this is work!
  - Understanding this w.r.t. the OSG Service AUP
  - What is good for the VO is good for FNAL.