Interfacing Operational Grid Security to Site Security

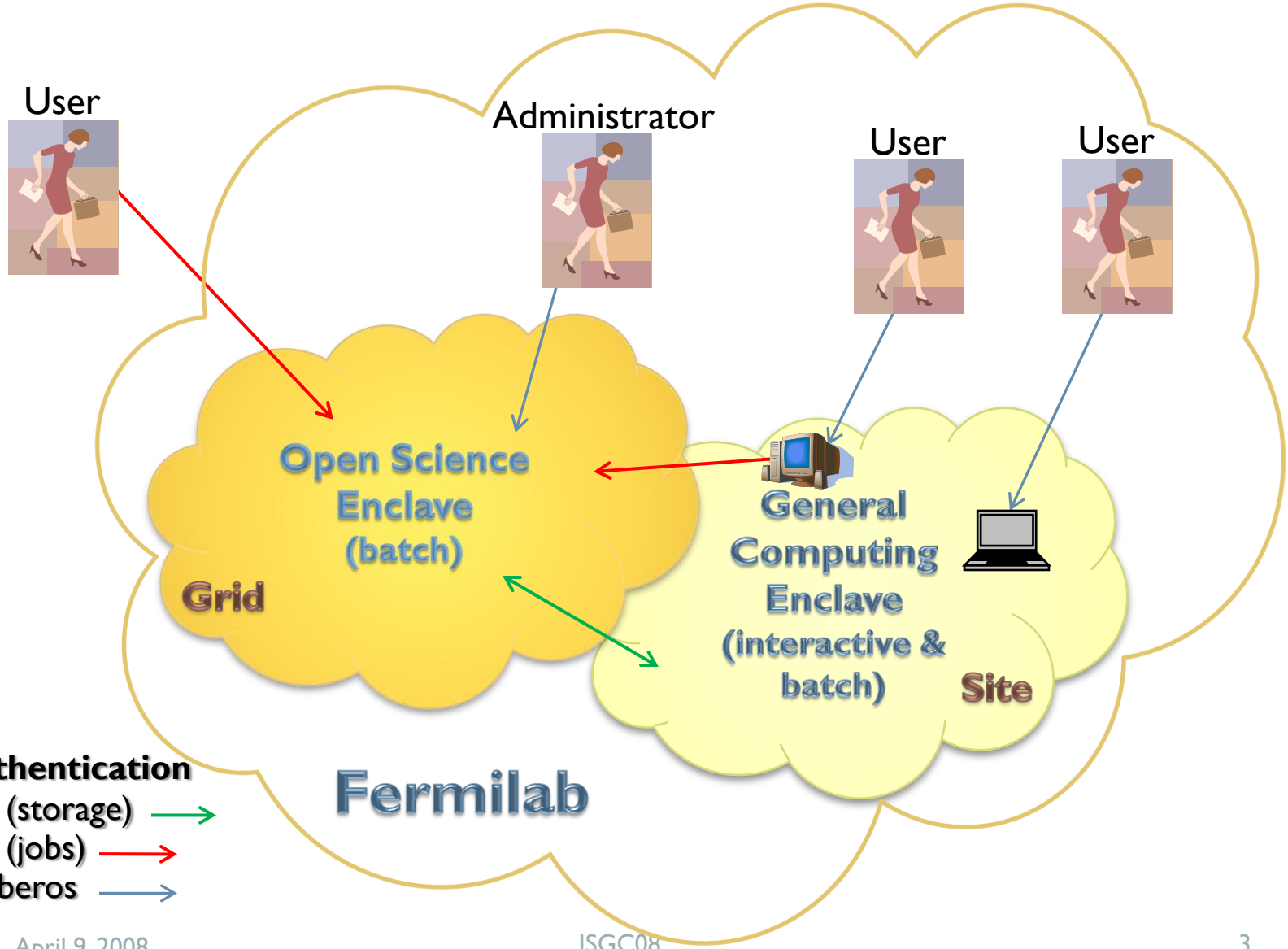
Eileen Berman

Fermi National Accelerator Laboratory

Introduction

- Computing systems at Fermilab belong to one of two large enclaves –
  - The General Computing Enclave (GCE) supports the general scientific, engineering and administrative communities.
    - Site security policies apply here
    - Well defined policies, procedures, processes
  - The Open Science Enclave (OSE) supports scientific collaboration with other institutions whose users are not under the direct management control of Fermilab.
    - Grid security policies apply here

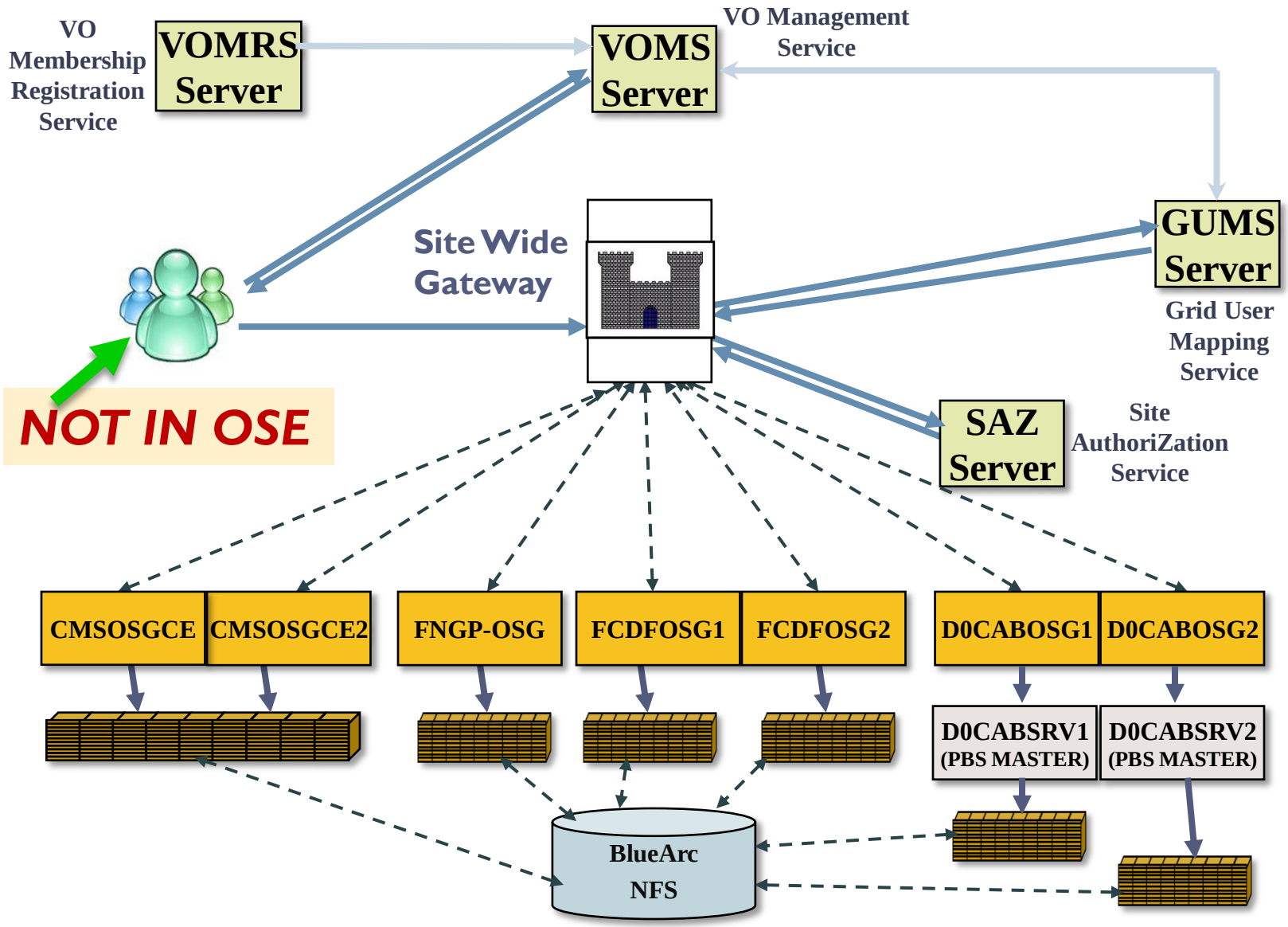
GCE and OSE


User
Administrator
User
User
Open Science Enclave (batch)
Grid
General Computing Enclave (interactive & batch)
Site
Fermilab
Authentication
GSI (storage)
GSI (jobs)
Kerberos

Open Science Enclave

- A computing resource is part of the OSE if it is managed by Fermilab and allows grid users to install and/or run software using credentials which are not issued and revocable by Fermilab.
- Other explicitly identified computing resources supporting the operation of the OSE may be designated part of the OSE by Fermilab.

OSE Resources



Motivation for OSE

- The lack of operational control that exists over badged employees and experimenters determines a need to provide compensatory controls to cover for this to
  - Minimize the exposure of computing resources in the OSE to known vulnerabilities
  - Reduce the risk of compromise of computing resources in the General Computing Enclave.
- Need to define and implement
  - Security Plan, Risk Assessment, Contingency Plan
  - Baseline Document
  - Policies, Procedures, Processes governing the OSE

OSE Security Controls

- Security of computing systems is achieved and maintained by a combination of
  - Management controls
    - over the users and administrators
  - Operational controls
  - Technical controls
- Follow National Institute of Standards and Technology (NIST) guidelines

NIST Process

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

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

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

OSE Security Controls - Trust

- In the OSE, the trust relationship is established and maintained between Fermilab and each Virtual Organization (VO)
  - Often brokered through the Grid (e.g. OSG)
- Controls are partially delegated to the VOs
  - Management Controls
  - Technical controls
- This generally results in more compensatory controls on the resources

OSE Additional Security Controls

- Management Controls
  - System administrators of resources within the OSE will be highly professional well trained Fermilab administrators.
  - Each VO requesting access to OSE resources shall execute an agreement with Fermilab governing the use of the resources.
    - User training
    - Credential access
    - Support level
    - May be brokered by Grid (e.g. OSG)

OSE Additional Security Controls

- Operational Controls
  - Use OSE Baseline Configuration
  - Handle grid security incidents to ensure coordination and communication among different grid computing service providers and users.
  - Grid Users are trained in OSE use by their VOs.

OSE Additional Security Controls

- Technical Controls
  - All VO members are to be either
    - Entered in CNAS (Fermilab personnel db), or
    - Each VO will keep documentation of their procedures for granting credentials and a list of currently authorized individuals
  - All resources in the OSE must have prior management authorization
  - Resources may not offer network services that do not demand either Kerberos or GSI credentials
    - Except for web servers
  - Wireless and modem access to OSE resources is not permitted. Temporary network connections of unregistered resources is not permitted

OSE Security Baseline

- The **Fermilab OSE Security Baseline** configuration settings represent industry best practices for securing Grid computing resources, based on recommendations from several sources including
  - The Virtual Data Toolkit
  - The Open Science Grid Collaboration
  - The Fermilab OSE Working Group
- It details both the minimum (mandatory) and recommended (best practice) levels of security settings.

OSE Security Baseline - Common

- In common with the General Computing Enclave (site) there are rules that govern
  - Physical Security
  - Secure Installation
  - Account Security – passwords (root accounts for administration)
  - Unnecessary Services

OSE Security Baseline

- Minimize interactive user accounts
- Grid job accounts configured to use /sbin/nologin
- Use Grid User Mapping Service (GUMS)
  - Grid credential mapping to site identity
  - For jobs, pilot glideins, glExec, and storage
- Use Site AuthoriZation Service (SAZ)
  - For jobs, glideins, glExec, and storage
- Pilot Workload Management Systems (WMS) must use glExec
- Special authorization needed for a VO to run a Pilot WMS
- All Compute resources must use the Gratia Accounting System

OSE Security Baseline - Network

- No offering of bridging or routing services (except hypervisor)
- Firewall - restrict connections to necessary services only (iptables)
- Database write or update access subject to additional constraints
- IPMI services must use a private network
- X11 service cannot accept network connections
- Cannot be configured as a boot server

OSE Security Baseline – Network

- Cannot offer
  - network file services (AFS, NFS, …)
  - LDAP services
  - email services on the network
  - SNMP write operations on the network
  - TFTP services across the public network backbone
  - DHCP services (except for virtual machines – internal only)
  - DNS services
  - XDMCP services
  - modem or wireless access services

OSE Security Baseline - Services

- Only OSG or EGEE repository base grid middleware to be used
  - job authentication, authorization, execution and file transfer
- Only approved Certificate Authorities
- Required permissions on host certs (644) and keys (600)
- Should disable web server indexing

OSE Security Baseline - Services

- Only approved instances of
  - VO Member Registration Service (VOMRS)
  - VOMS, GUMS, SAZ
  - MyProxy services with X.509 certificate authentication
  - VOBox or Edge services

OSE Security Baseline – Files

- NFS file permissions
  - User home areas of GCE computer accounts are not to be made accessible in the OSE
  - All shared file systems writable in the OSE must have the "noexec" option set wherever they are mounted in the GCE
- Umask for non-root users must disallow write by others and perhaps group
- Umask for root must disallow write by group and other and perhaps all access
- Home ares and '.' files must not be writeable by other
- All world writeable directories should have the sticky bit set

OSE Security Baseline – Logging

- Sytems and grid middleware should be configured to provide logging
- Logs will be forwarded to a central location
- System logs should be maintained for one year
- Grid middleware logs should be maintained for one year
- Log files should have 644 protection or stronger

OSE Policies & Procedures

- Extensive communication between Site security and OSE working group aids development of policies and procedures
- An inventory service has been developed to allow job dispatching headnodes to report about the worker nodes to which they dispatch jobs
- Current discussions include
  - End-to-End security for user jobs
  - VO responsibilities
    - Provide an Operational organization to respond in a reasonable time to requests
    - Provide a Security incident response plan
    - Describe and operate its technical infrastructure in a transparent manner which permits verification of its functioning
    - Not permit use of unlicensed software
    - Have an Acceptable Use Policy (AUP)

Conclusion

Security policies for grid resources must generally be different from those of general computing. Good policies and implementation serve to protect the site's resources, reduce security incidents and the effort of responding to them, preserve the site's reputation, and reassure site security officers.