Open Science Grid

Data Security

Jim Basney
OSG Security Team
security@opensciencegrid.org

OSG All Hands Meeting
Data Management Foundations Workshop
March 2009

Data Security

- Confidentiality
  - Preventing unauthorized disclosure
- Integrity
  - Preventing unauthorized modification
  - Maintaining trust in your data
- Availability
  - Preventing data loss
  - Providing reliable access to data

Confidentiality

- Encryption
  - Data in transit (SSL, SSH, WS-Security, IPsec, VPN)
  - Data at rest (S/MIME, PGP, XML-Enc)
  - Depends on proper key management
- Access Control
  - File system permissions
  - Data service authorization
  - Depends on operating system and data service security

Integrity

- Access control (again)
- Checksumming
- Digital signatures
- Audit logging
- Provenance

Availability

- Physical data replication
- Data service redundancy
- Data backup and archiving
- Data consistency and coherence

GridFTP

- Data Channel Authentication (DCAU)
  - Enabled by default; disable with caution!
- Data Channel Safe (DCSAFE)
  - Integrity protected / checksummed
  - Disabled by default due to performance
- Data Channel Private (DCPRIV)
  - Encrypted and checksummed
  - Disabled by default due to performance

Data Security In OSG

- Many sites map VO members to shared accounts
  - Implication: data is shared among VO members
- SRM/GridFTP services typically do not encrypt data in transit
- Data typically stored unencrypted
- If you have stronger data security requirements, let us know!

Discussion

- What questions do you have about data security in OSG?
- What are your CIA requirements?
- What data management systems will you use?
- Any other questions/comments?

Thanks!