# Security and Access Control Management Services

MINE ALTUNAY, PHD
OSG SECURITY OFFICER
SCIENTIFIC COMPUTING INFORMATION SECURITY
FERMILAB

# Agenda



- We will cover 2 main topics
  - Most common security problems we observe and tips to prevent them
  - FIFE needs and requirements.

# Identity Management and Certificate Service



- Currently, Fermi Kerberos Certificate Authority provides the certificate services to the FIFE Community
- Each user gets a personal certificate to submit jobs through his/her Kerberos ticket.
- Currently, FIFE can only use Fermi KCA certificates because JobSub has been working with this CA for a while, although this may change in future.

# Common Security Problems & Tips



- Permission on output directories unset.
  - Usually user tries to copy the output files on the submit node where she/he has no permission.
  - Do not try to write output files in $APP.
- Users forget to set the execute permission on the cron job.
- Deploy experiment code in a read-only area, most experiments write into /grid/fermiapp. When a scientist copies it into their own directory, they can include faulty code and cause issues on the grid .

# Common Security Problems & Tips



- Serious memory leaks or buffer overflow problems observed. Check your code over and over again
- Delete or remove the users who left the experiment
- Experiments using shared accounts
  - It is only OK for Production jobs, otherwise FNAL security policy does not allow account sharing.
  - Allow 3-5 people into a shared account. As the number increases, the does the likelihood of issues.
  - Security team does not allow more than 5-8 people in a shared account at most.
  - Annually control the user list, rmeove people who left the experiment or no longer need to access.
- Do not put group account credentials in shared unprotected areas.
- Crontabs are unprotected, anyone can change your code.
  - We already observed mistakes that led to waste of resources

# Common Security Problems & Tips



- Jobs often run as production, but in the past since the SAM project was started as the user id, often data transfer failed. But this seemed to fix now.
- Minerva runs production files in shared accounts because they have problems accessing the output data
  - Like to learn more about this problem
- Also, we want to hear if there are more problems with output data transfer. We noted a few instances of this problem.
  - Is this a bigger problem that we should focus on?

# FIFE Requirements and Needs



- What are the biggest security problems
  - Did we capture them all in the previous slides?
  - Is there something fundamentally wrong in our model?
- Currently, all FIFE users must have Fermi Kerberos accounts.
  - Is this acceptable to your experiments?
  - Do you wish that we did not have to have this requirement?
  - Is this a big burden on the users?

# FIFE-Connect?



- FIFE-Connect
  - What do you think about a FIFE-Connect service, similar to OSG-Connect where users do NOT have to have certificates?
  - OSG and Fermilab already accepts jobs without end user certificates, granted VO performs the appropriate security controls