T3 Site Security

Atlas T3 Site Administrators workshop, ANL

June 8-9 2010

Mine Altunay
maltunay@fnal.gov
FNAL

What I will talk about in 15 mins

- 4 security habits that will keep your site out of trouble
- The real risks against your site
- Any questions/issues you have

4 Security actions that take care of many security troubles

1) Designate a security contact, if possible find a back up person. Register their contact info in OSG Information DB (OIM)
2) Pay attention to the security announcements sent from OSG Security team.
   - Any security issues affecting VDT software
   - Severe issues affecting other software, OS, commonly used tools, etc. A **courtesy effort** and only for the **severe cases**

4 Security Actions

3) Make sure you are up-to-date with security patches
   - Severe patches are announced by OSG
   - You can check Pakiti results
   - Check OSG security blog for news http://osgsec.blogspot.com/

4) Make sure you know who is your universities security officer and what the local incident response policy

- What is Pakiti:
  - A security status monitor, checks installed packages against announced vulnerabilities, marks missing updates, shows the severity of the vulnerability

Real Risks against your site

- Grid does NOT add significant risk to your site
  - More secure than many commonly used services such as ssh or Windows services
  - Lots of attacks happen because of random port scans and/or weak passwords
- Residual risks: Insider threat
  - Remote VO users, you do not know face-face.
    - Non-interactive batch access only
    - Apply all OS-patches; no user can escalate to root
    - Apply all OSG-Atlas patches

Real Risks against your site

- Least amount of privilege sufficient for users jobs
- Know how to quickly turn off a VO user's account

- Every software has vulnerabilities. So does grid software
  - Read patch announcements
  - Follow recommendations from the developers
  - e.g. If you have a CE, do not allow fork jobs on the CE; or use glexec with pilot jobs; etc
  - If you cannot follow the recommendation, ask the developers/Atlas/OSG. Usually there is an alternative

Real Risks against your site

- What is the worst-case scenario?
  - Lose the SE, delete all the data
    - Tape backups, archives?
  - Attacker escalates to root, lose the system
    - University security officer must be informed first
    - Inform Atlas and OSG security teams
    - So far only happened during ssh attacks

Q&A on Tier3 issues

- Open discussion on questions, issues, worries, … that Tier 3 site administrators have
- Bring your questions!