# Security in the Russian region

Eygene Ryabinkin

March 18th 2008

OSCT-5

# General situation

- Conceptually, Russia is one big distributed Tier-2 site.
- Two types of sites:
  - Big ones: IHEP, ITEP, JINR, PNPI, RRC-KI and SINP.
  - Smaller sites: MEPHI, Phys-SpbSU, SpbSU, INR, KIAM, FIAN, PSN, GCRAS.

# Big sites

- They compose the core of the ROC and provide major resources.
- The Grid teams are working since the EDG times, so they are skilled both in Grid-related work and in the general system administration.
- Teams are providing > 2 full-time employers to support Grid operations.
- Monitoring and best practices are typically in-place and just should be adopted for the specifics of the Grid. Some sites even have CSIRT teams or good relations to foreign/higher-level CERTs.

# Big sites: typical problems

- The biggest security problem are new administrators who just came to the site and received their trainings, but a bit overwhelmed with the complexity and trying to omit some steps in order to ease the diving into the topic.
- The solution is to carefully prepare the tasks for the new administrators, supervise them and make them first train on the disconnected testbeds and only then – on the real resources.

# Small sites

- Typical situation: ≈ 0.5-1 full-time administrators, small cluster, only site services.
- Two reasons to join (or the combination of the reasons):
  - Try the Grid and understand if they are interested;
  - Tier-3-like site: local physicists need to do perform analysis.
- No previous experience in the Grid-related activities; a rush to join the community and get things working ‘immediately’.

# Small sites: typical problems

- The biggest one is to persuade the sites to report the security incidents.  I had myself used to think that it is a shame to be hacked ;)), so I partly understand them.
- Lack of the manpower to perform the full-scaled monitoring and to continuously improve the security.
- The solution is simple: work with these sites, provide consulting, explain the common and specific things about Grid and security, provide recipes and explanations of these recipes.

# Instruments

- Mailing lists and personal meetings
- RDIG monitoring: http://rocmon.jinr.ru/
- RDIG user/administrators support: http://ussup.itep.ru/
- Russian ROC Wiki: http://grid.sinp.msu.ru/grid/roc/main
- OSCT RSS feed
- Best practices from the FIRST, NIST, various How-To documents, etc.

# The last slide

The presented material clearly shows that there are many issues that are still to be solved and brought to the security coordination in our region.

So, I will be indebted to all people who will provide their suggestions and criticism.

Thanks for your time!