



Science & Technology
Facilities Council

NGS Security

Mingchao Ma

STFC – RAL

25 Mar 2008



Overview

- Security Policy
- Incident handling procedure
- Security backup
- A dedicated security area on NGS website



Security Policy

- Joint Security Policy Group Policies
 - [http://www.jspg.org/wiki/JSPG Docs](http://www.jspg.org/wiki/JSPG_Docs)
 - Policies, currently being worked on
 - Recently approved policies
 - Links to the policies can also be found at:
 - <http://osct.web.cern.ch/osct/policies.html>
- or
- <http://www.gridpp.ac.uk/security/policies/index.html>



Grid Security Policies

- Grid Security Policy
 - Grid Acceptable Use Policy
 - Grid Site Operations Policy
 - Site Registration Policy
 - Audit Requirements Policy
 - Grid Security Incident Response Policy
 - VO Security Policy
 - VO Operations Policy
 - User Registration Policy
 - Approval of Certification Authorities



Incident Handling

- Incident handling procedure
 - [http://www.ngs.ac.uk//NGS Security v2.pdf](http://www.ngs.ac.uk//NGS%20Security%20v2.pdf)
- Communication channel
 - Report: NGS-SECURITY@JISCMail.AC.UK
 - Discussion: NGS-OPERATIONS@JISCMail.AC.UK
- At <http://www.ngs.ac.uk/security.html>
 - Email to security@grid-support.ac.uk
- Confusion on how to report incident



Incident Handling (cont.)

- Current communication channels
 - NGS-OPERATIONS@JISCMAIL.AC.UK used for incident notification
 - security@grid-support.ac.uk for incident reporting???



Incident Handling (cont.)

- Site CSIRT email, telephone and contact must be added into GOCDB
- An email address/**CLOSED** mailing list for incident reporting/notification
 - Incident, alert and warning etc.
- An **CLOSED** mailing list for security-related discussion
- A ticket system (as a repository) to record all above information
- Prevent information from leaking!



Incident Handling (cont.)

- Procedure
 - Define clear communication channels for incident report and discussion
 - A set of requirements/steps/actions must be taken
 - An agreed timeframe associated with each step



Six Steps to Handle Security Incident

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lesson Learnt



Backup

- Need at least one, better two backups
 - On holiday/business trip etc.
 - Nick Hill and Andy Richards??



NGS Security pages

- Security page
 - <http://www.ngs.ac.uk/security.html>
- Wiki page for security
 - ???
- Who maintains it?