GGF12 Security Workshop, Brussels

Andrew Cormack
A.Cormack@ukerna.ac.uk
Grids are

- Big computers/cpu farms
- Big datasets (some of them sensitive)
- Big traffic flows
- Expensive equipment (earthquake simulators etc.)
- Single (certificate-based) sign on
  - Across multiple sites/countries
  - Private keys often stored on NFS/AFS filesystem 😞
Grids and Security

All the threats we know and love, plus

New Threats

■ Lots of experimental software
■ Complex (firewall-unfriendly) protocols
■ Lots of implicit and explicit trust

Different view of “incident”

■ Identity theft (e.g. key compromise) is a BIG deal
■ But a >1GB flow on ephemeral ports may be normal
Grids and CSIRTs

Need to work together

- They are on our networks
- They need trusted (international) contacts
- Europe/USA experiences differ

Working apart doesn’t work; already:

- CSIRT watches an ongoing Grid incident for 2 weeks
- Unannounced Grid experiment DoSes an NREN