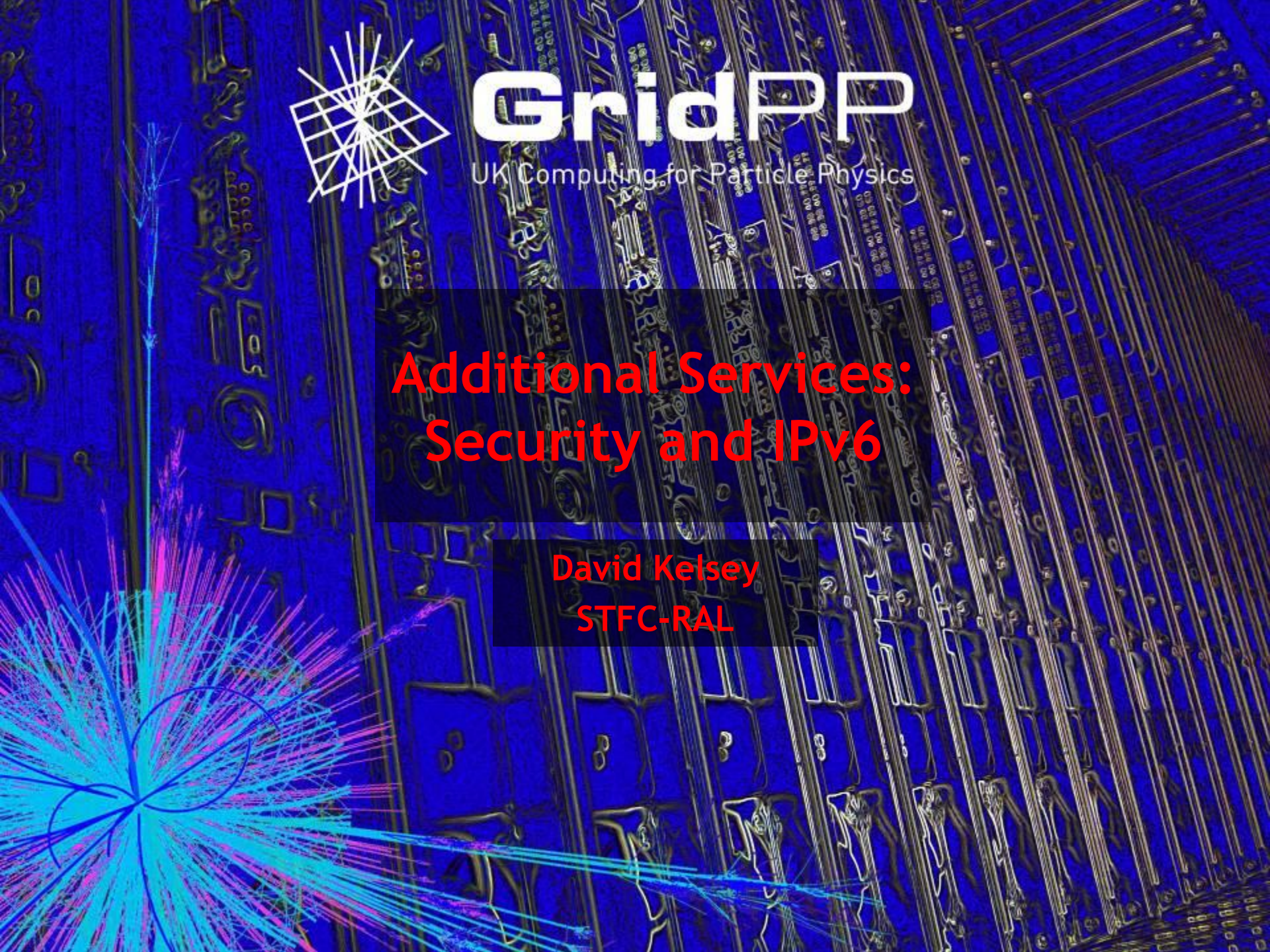

Additional Services: Security and IPv6

David Kelsey
STFC-RAL

Outline

Additional Services

- Security
  - Operations
  - Policy and Trust
  - Identity Management
- WLCG (HEP) and IPv6

Grid Security

- An area with a very long track record of UK leadership
  - Started the CA Coordination Group in December 2000
    - Became EUGridPMA in 2004 – and IGTF in 2005
  - EDG security coordination group 2001
  - WLCG security policy group 2003
  - Joint (WLCG/EGG) security policy group 2004
    - Became EGI Security Policy Group (SPG) 2010
  - WLCG Security Policy Coordinator 2010
  - Proposed EGEE Operational Security Coordination Team (OSCT) 2006
    - With security officer (CERN)
    - Became EGI CSIRT 2010
  - UK Deputy Security Officer in EGEE
  - UK Security Officer in EGI (until 2012)
  - Grid Security Vulnerability Group (GSVG) EGEE 2006
    - Became EGI Software Vulnerability Group 2010
  - Security for Collaborating Infrastructures (SCI) 2011
  - Federated Identity Management
    - Founder member of FIM4R 2011

Why do we do Security?

- Operational security and international trust
  - Essential for availability and integrity of services and data
  - Allows interoperation and security teams to work together
  - We do it because it is needed by GridPP *and* WLCG (a UK contribution)
- The problems are very general
  - Benefits in working together with others (PRACE, XSEDE, EUDAT, …)

Quote: Ian Bird's plenary keynote at TERENA Networking Conference 2011

- "The reason we have a Grid is because we need to collaborate and we need to share resources. So no matter what we do and no matter what technology we deploy underneath we will always have a Grid. Our network of trust and all of the security infrastructure that goes with that is of enormous value to us and I don't think we want to lose that. I think it is also of enormous value to eScience in general because I think this is one of the things that allows people to collaborate across these infrastructures and I think that probably should sit on top of the pile as one of the major achievements of this 10 years of work on Grids."

Security operations

EGI/WLCG/GridPP

- SCG – overall coordination, risk analysis, requirements
- CSIRT
  - Incident response team – and handling (Sweden & NL)
  - EGI CSIRT now accredited member of the TERENA TI club
- SSC
  - Security service challenges (NL)
- SVG
  - Handling risk assessment and fixes of vulnerabilities (GridPP)
- Monitoring (CZ)
- Training/Dissemination (all)
  - Very useful and popular
- Work was all reported at last week's EGI Technical Forum
- Future plans
  - Much more to do in all areas
  - work closer with other infrastructures
  - Much to do understanding risks in Clouds and changes required to security operations

GridPP security team

- Security Officer (vacancy)
- Linda Cornwall, Alessandra Forti, Rob Harper, Ewan McMahon
- Ian Collier, Jeremy Coles, Dave Kelsey

- GridPP funds 1.5 FTE plus effort from the Ops team
- EGI currently funds 50% of ~ 1.3 FTE

- Future – wherever it makes sense work together with other activities

- Future work
  - Clouds and virtualisation
    - Modify top-level policy document
  - Starting to work with HelixNebula
  - Need to engage more with EGI Federated Clouds Team

SCI

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Developed initially out of EGEE and WLCG
- We are developing a *Trust framework*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies
- V1 of the SCI document was submitted to ISGC 2013 proceedings
  - under review
- SCI has met since then
  - new version (V1.3?) under way

EGI Software Vulnerability Group (SVG)

- Aim: eliminate existing vulnerabilities and avoid incidents
- Issue handling starts with the Risk Assessment Team (RAT)
- Issue placed in one of 4 risk categories
  - Critical, High, Moderate or Low
- Target Date for resolution set according to the Risk
  - Critical - 3 days, High - 6 weeks, Moderate – 4 months, Low - 1 year
- New procedures following end of EMI and IGE
- 36 Vulnerabilities reported
  - 24 in last 6 months
- Risk categories – 2 ‘critical’, 7 ‘high’, 8 ‘moderate’, 6 ‘low’
  - Some not assessed (not relevant/out of scope, invalid, duplicate, problems with single instances quickly fixed, no action needed)
- Majority (26) concern Grid Middleware
- SVG also coordinates work on Code assessment (EMI and Univ Barcelona)

Identity Management and trust

- IGTF
  - UK CA - see Jens' slides
  - New IOTA profile potentially very interesting
    - Less identity vetting by CA, when VO/sites already do it
  - Ease of use for Certificate requesting and handling
  - Trusted credential stores
- FIM4R, TERENA, REFEDS, Geant, EduGAIN, …
  - Working with the identity federations, IdPs and other communities
  - Common vision on use of federated identities
- WLCG Federated IdM working group
- CERN protoype public cloud using EduGAIN
- UK – Janet(UK) new working group on AAI

IPv6

- See Duncan's slides from yesterday
  - Will not repeat details today
- Getting better engagement with the experiments and some sites
- Working on use cases for the CERN Wigner Tier0 (IPv6-only WN)
- Why does it matter?
  - WLCG does not know when we will need to support IPv6-only WNs
  - CERN says it could be as early as next year
  - CERN and now DESY are pushing ahead on site roll-out of IPv6
  - But when we need to do it there will be little time
- Testing and planning takes lots of time!
- We also need to move operations & security
  - And train loads of people
- UK has a leading role in this activity
- A contribution to WLCG (and HEP in general)
- I think this should continue (will take whole of GridPP5 :=))

Discussion