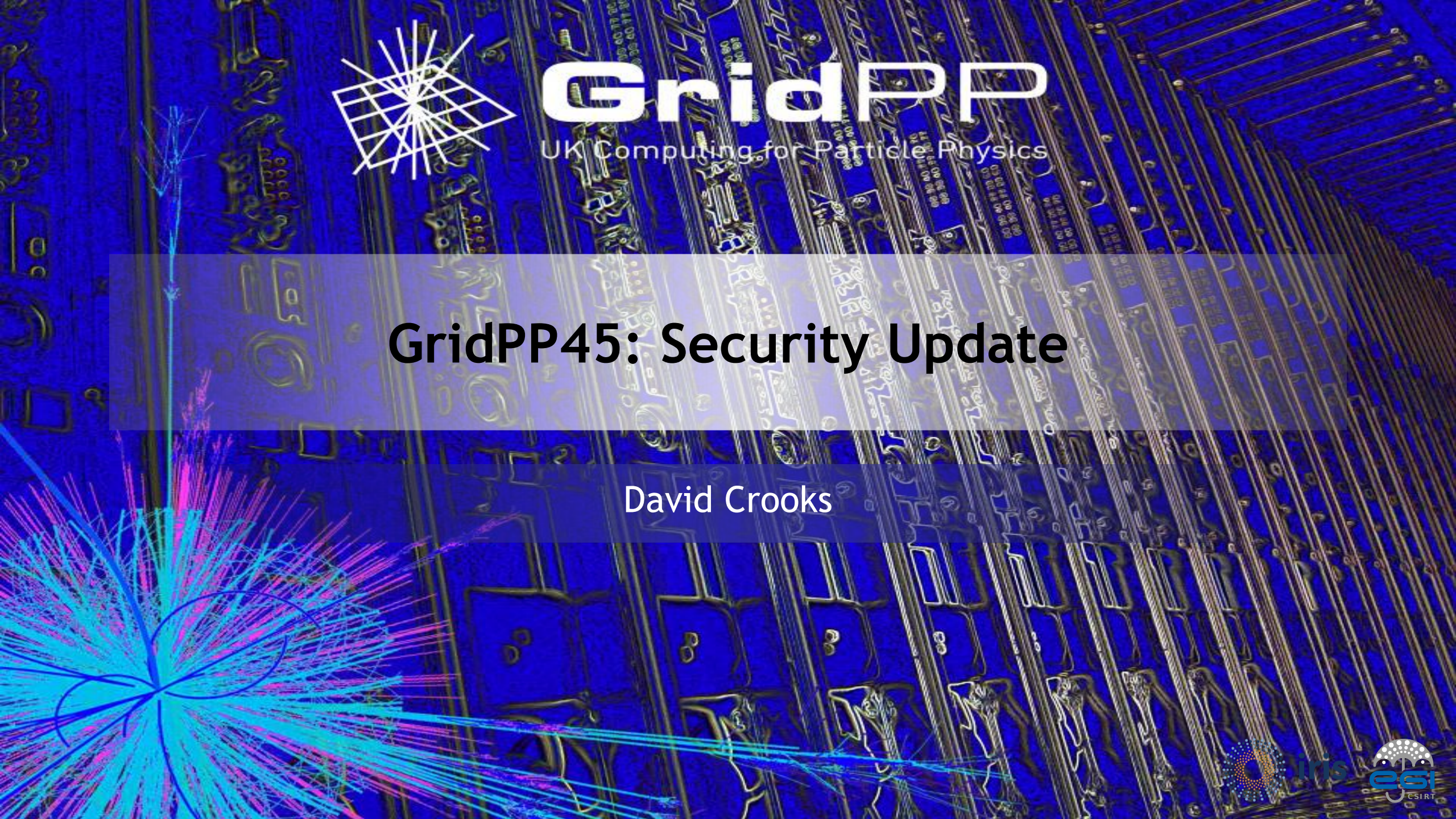

GridPP45: Security Update

David Crooks

GridPP
UK Computing for Particle Physics

Overview

- Summary since last meeting
- IRIS Update
- Landscape
  - Best practices

iris
EGI CSIRT

Summary since last meeting

- GridPP43
  - August 2019
  - Discussed SSC outcomes
- Since then
  - Coordination exercise (EGI/OSG)
  - Storage ACLs
- Incidents near the grid
  - OpenSSH trojan on academic systems
  - May HPC incident

Summary since last meeting

- Vulnerability Advisories (not all relevant to GridPP)
  - 3 CRITICAL
  - 2 HIGH
  - 3 MODERATE
  - 3 LOW
  - 3 without assigned risk

- SVG Deployment Expert Group is getting underway
  - Defined role: https://wiki.egi.eu/wiki/SVG:Deployment_Expert_Group
  - Plan for WISE WG around good vulnerability handling practice

- Communications challenge
  - 3 sites didn't receive the challenge email
  - Lead to investigation of mail infrastructure; issues were then resolved

IRIS Update

- Policy
  - IRIS Infrastructure Security Policy going through approval process with IRIS DB
  - Working AUP and Privacy Notice in place
  - Community and Service Security Policies in development
    - Informing broader policy work for federated infrastructures

- Operational security
  - IRIS Security Team created, augmenting existing GridPP Security Team
    - Representation from IRIS Cloud and HPC resource providers
  - Security communications channels
    - Communications challenge is in planning
  - IRIS Security Workshop [July]
    - Excellent attendance and involvement from different types of sites
    - Some outcomes pending for Security Team
    - Leading to more workshops in the future

Landscape

- We have seen over the last few months examples of academic sites being targeted:
  - Often “next door” to grid sites
  - HPC incident
  - Recent examples of Ransomware attacks

- How do these impact GridPP?
  - How can we prepare?

Preparation

- Grid sites are closely linked with their local infrastructure (of course)
- How do you traverse between network segments?
- Pay particular attention to authentication methods
  - SSH keys
  - Grid Certificates
  - Federated Identity/SSO
  - What is shared with your local institution?

- Token based workflows
  - WLCG Authz WG and others: IRIS-IAM
  - Increasingly part of Grid workflows

- For IRIS, develop an authentication security challenge in due course

Best practice

- Review incident response procedures
  - Know first contact points
- Central logging
  - Central logger should be protected
  - Separate host
- Backup strategy
  - Consider what is appropriate: what data do you store that can't be replaced?
  - Offsite/offline backups give most protection, but have practical issues
  - Backups to devices network close to production hosts may be vulnerable depending on nature of attack

- EGI CSIRT incident response procedure
- EGI CSIRT incident response checklist

- NCSC guidance
  - https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

GridPP
UK Computing for Particle Physics

Threat Intelligence

- Focus for the coming year
  - SOC deployments
  - Working with existing security systems
    - e.g. STFC Information Security
- Working with sites to use intelligence from MISP
  - Continued push to incorporate shared threat intelligence as part of incident response
  - Working with Jisc/Janet CSIRT to share with them
- Ongoing work at several sites

iris
EGI CSIRT

What's next

- Best practices
  - Outcomes from workshop
  - I'd like to set up opportunities to talk to different sites
- Communications/security challenges
- Threat intelligence
- Continue to establish operational security for IRIS alongside policy