WLCG Group

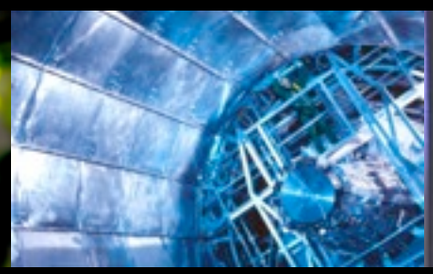
Security update

WLCG Workshop

11-13 July 2011, DESY








WLCG
Worldwide LHC Computing Grid

Identity federation workshop

- Hold at CERN on 9-10 June 2010
  - https://indico.cern.ch/conferenceTimeTable.py?confId=129364
  - Representation from several user communities & infrastructures
  - Scope wider than WLCG

- Covered:
  - User requirements
  - Existing infrastructures/federations
  - Policy aspects
  - Next steps

User requirements

- There are many common needs and hence scope for agreement
  - SSO
  - Easy of use for part-time users
  - Focus is on data access
  - Support homeless users
  - Many tools and technologies deployed
  - Smooth transition from existing systems

Slide from Bob Jones

Existing infrastructures

- Trust is needed, both for tokens and attributes
  - IGTF is the source of trust for many existing projects
  - Identity Provider accreditation a key aspect
- Different Levels of Assurance is important
  - Implementation not trivial
- Traceability across different tokens key is critical
- Aim at global (common?) authentication management system
  - Global scope interoperability is essential
  - Certificate and Security Token services important
  - Significant work ongoing
- A better coordination between ongoing efforts needed

Policy

- Federation policies are well established
  - Delegated down to home institute
  - Trust criteria
  - Plans and processes need effort and preparation
- Identity is only part of the problem
  - Attributes
  - Group membership across boundaries
- Risks increase with single identity
  - Users get casual about giving their primary credentials to service providers

Slide from Tim Bell

Next steps

- Identify/develop concrete use cases
  - Consider the issues and ideas presented during this workshop
  - E.g. biomedical domain:
    - Helsinki 12-13 September 2011
    - http://irisc-workshop.org/irisc2011-helsinki/
  - Get more concrete details of users' true needs

- Nominate architect(s) for each community
  - Someone who understands the security/identity domain and the community

Slide from Bob Jones

When and where

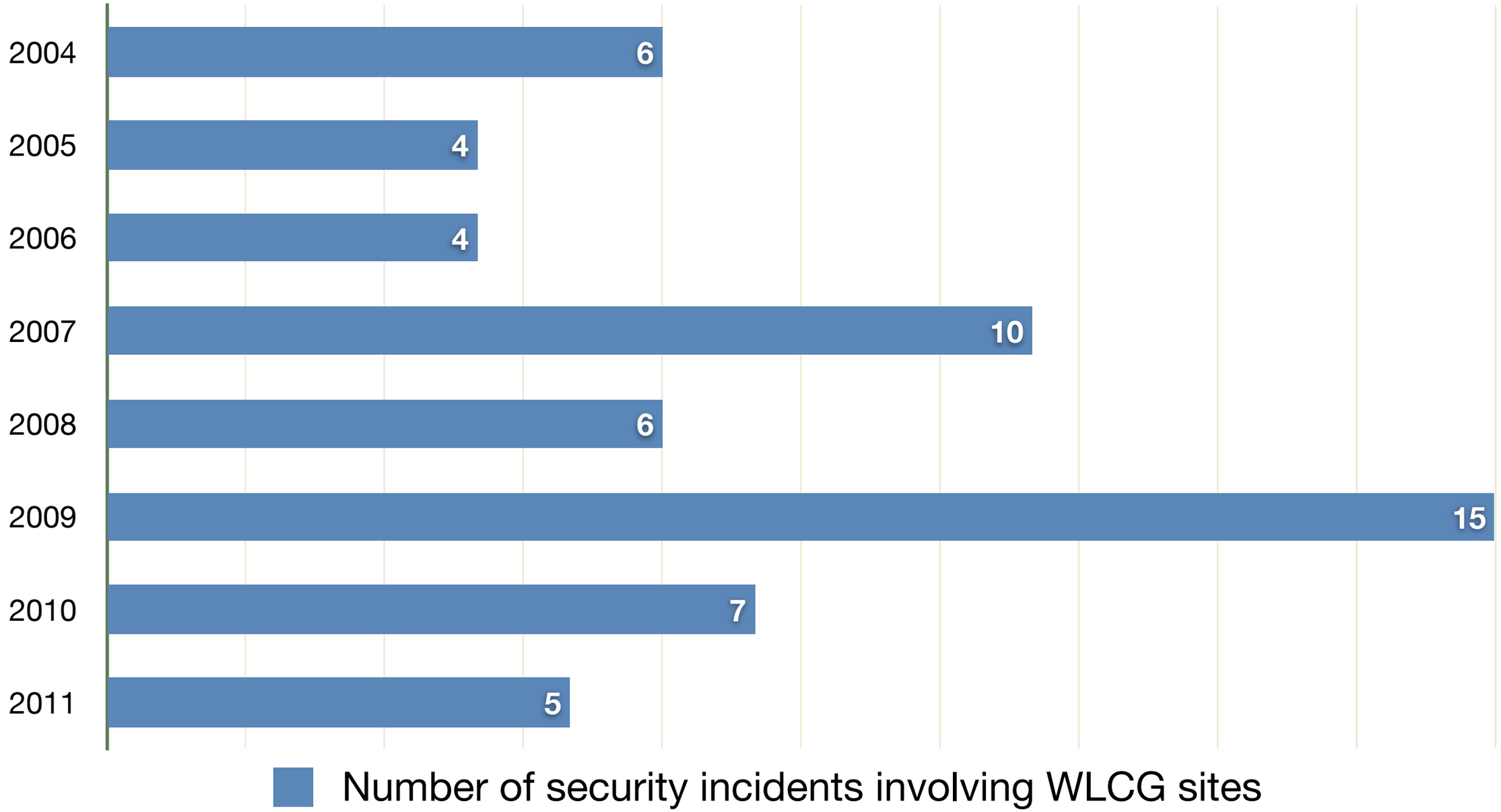
- Consider repeating this style of workshop
  - Rotate it between the user communities
    - Autumn 2011
    - Spring 2012
    - Summer 2012
    - With the goal of developing a roadmap we can all agree to

  - Need to work on the points shown on previous slides in between the workshops – we can't just talk!

  - We will keep alive the email list – please let us know if you want to add other names

Slide from Bob Jones

Security incidents in WLCG



- Most common causes
  - Compromised SSH accounts (9 out of the last 10 incidents)
    - Multifactor authentication seen as the main (only?) solution
  - Unpatched systems, Web applications vulnerabilities

SSC5

- Security Service Challenge 5 now complete
  - Focused on collaboration between team
    - Security teams had to collaborate to resolve the challenge
  - Results will be published in the coming weeks
    - Overall good response, although 30% sites still fail to ban bad users
      - Highlights again the need for central banning
  - Collaboration with ATLAS very fruitful
  - http://www.nikhef.nl/grid/ndpf/files/Global-Security-Exercises/FIRST2011/
  - Details at the next GDB?

Virtualisation

- HEPiX “Virtualisation” security policy
  - Now being expanded into a more general security policy in EGI
  - Close collaboration with the HEPiX WG
  - Aim at writing a single document addressing the different use cases

- Draft EGI Virtualisation policy:
  - “Policy on the Endorsement and Operations of Virtual Machine Images”
  - https://wiki.egi.eu/wiki/SPG:Drafts:Virtualisation_Policy

- Most security discussions focus on
  - Definitions
  - Roles and responsibility

Virtualisation

- Virtualisation brings no major changes to the security model

Virtualisation

- May be affected by security incidents in the (private) clouds
  - A small loss for Amazon may be a disaster for some customers
  - Private cloud providers are not bound by our security policies
  - Some VOs started sending jobs (proxies) to EC2

Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data

Henry Blodget | Apr. 28, 2011, 7:10 AM | 52,330 | 53

Tweet Email AAA

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's huge EC2 cloud services crash permanently destroyed some data.

The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is.

(And a small loss on a percentage basis for Amazon, obviously, could be catastrophic for some companies).

Um...

Questions / discussions