WLCG Security:
A Trust Framework for Security Collaboration among Infrastructures

David Kelsey (STFC-RAL, UK)

CHEP2013, Amsterdam

17 Oct 2013

And many thanks to SCI members

- K. Chadwick (FNAL)
- R. Cowles (Univ of Indiana)
- I. Gaines (FNAL)
- D. Groep (Nikhef)
- U. Kaila (CSC)
- C. Kanellopoulos (GRNET)
- J. Marsteller (PSC)
- R. Niederberger (FZ-Juelich)
- V. Ribaillier (IDRIS)
- R. Wartel (CERN)
- W. Weisz (University of Vienna)
- J. Wolfrat (SURFsara)

Outline

- What is Trust and why do we need it?
- Early days of cooperation in security policy
- Building a new Trust Framework
  - *Security for Collaborating Infrastructures (SCI)*
- The SCI document
- Assessment versus SCI requirements
- Future plans

Trust?

SCI at CHEP2013

A better definition of *Trust*

- eXtreme Scale Identity Management for Scientific Collaborations XSIM (Bob Cowles)

  - "Trust is a disposition willingly **to accept the risk of reliance** on a person, entity, or system to act in ways that benefit, protect, or respect one's interests in a given domain."

Based on Nickel & Vaesen, Sabine Roeser, Rafaela Hillerbrand, Martin Peterson & Per Sandin (eds.), *Handbook of Risk Theory*. Springer (2012)

Risk Management & Trust

- Management of IT security
  - Management of risk
  - balanced with availability of services
- Risk analysis
- Security Plan
  - to mitigate and manage the risks
- Security Plan includes various "Controls"
  - Technical
  - Operational
  - Management
- **Security Policy is part of Management Controls**
- Agreed policy framework – part of building **trust**

Early days of Grid Security Policy

- Joint (WLCG/EGEE) Security Policy Group
- We (EGEE, OSG, WLCG) agreed a common version of the *Grid Acceptable Use Policy*
- EGI and WLCG in general continue to use the same Security Policies
- BUT often not easy to agree on identical policy words
- We need a better way of agreeing policy

And now to SCI …

Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Developed out of EGEE – started end of 2011
- 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

SCI Document

- V1 of the SCI document was submitted to ISGC 2013 proceedings
  - Will (hopefully) be published soon
- Latest public draft always at
  http://www.eugridpma.org/sci/

SCI: areas addressed

- Operational Security
- Incident Response
- Traceability
- Participant Responsibilities
  - Individual users
  - Collections of users
  - Resource providers, service operators
- Legal issues and Management procedures
- Protection and processing of Personal Data/Personally Identifiable Information

SCI example text:
Incident Response

Imperative that an infrastructure has an organised approach to addressing and managing events that threaten the security of resources, data and overall project integrity.

Each infrastructure must have:

[IR1] Security contact information for all service providers, resource providers and communities together with expected response times for critical situations.

[IR2] A formal Incident Response procedure, which must address roles and responsibilities, identification and assessment of … *(text continues)*

And continues …

SCI Assessment of maturity

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: … and comprehensively documented
  - Level 3: … and reviewed by independent external body

A fictitious assessment
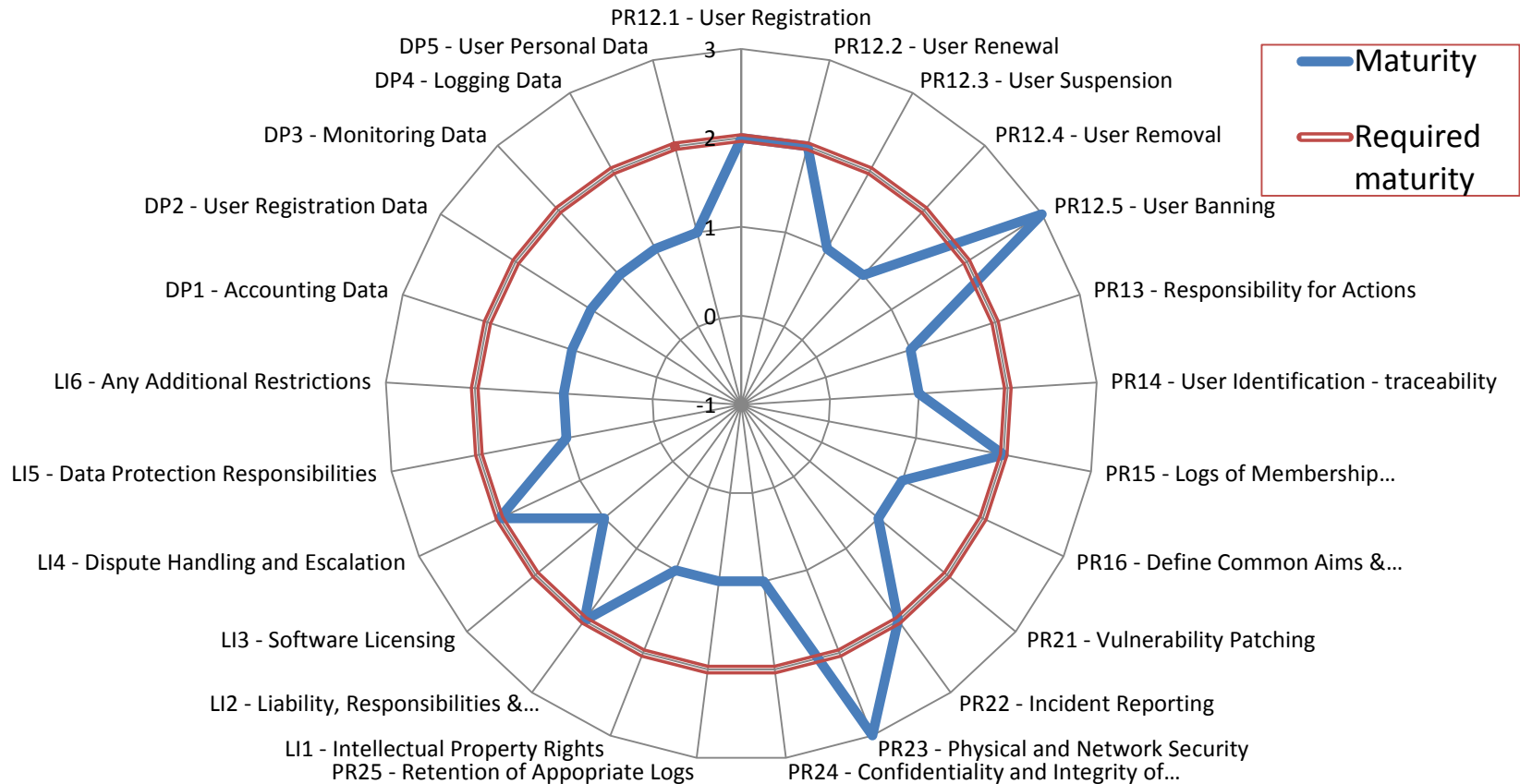
Future plans

- Version of 1 document
  - Now working on a background section and a glossary
- Consult Infrastructure Management
  - Feedback on SCI document
- Perform self-assessments
- Refine the SCI document
- Others are welcome to join
  - Contact me

Further info

- Security for Collaborating Infrastructures

http://www.eugridpma.org/sci/

- SCI meetings

https://indico.cern.ch/categoryDisplay.py?categId=68

Questions?