WLCG
Worldwide LHC Computing Grid

GridPP
UK Computing for Particle Physics

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey (STFC-RAL, UK)
EGI/EUDAT/PRACE workshop
Linkoping, Sweden
8 Oct 2013

egi

Science & Technology
Facilities Council

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?

Trust?

- Definition of **trust** (oxforddictionaries.com)
- *Noun*
  - – firm belief in the reliability, truth, or ability of someone or something

- My view: *reliability*, even more *predictability*, is important for IT operations

Another definition of *Trust*

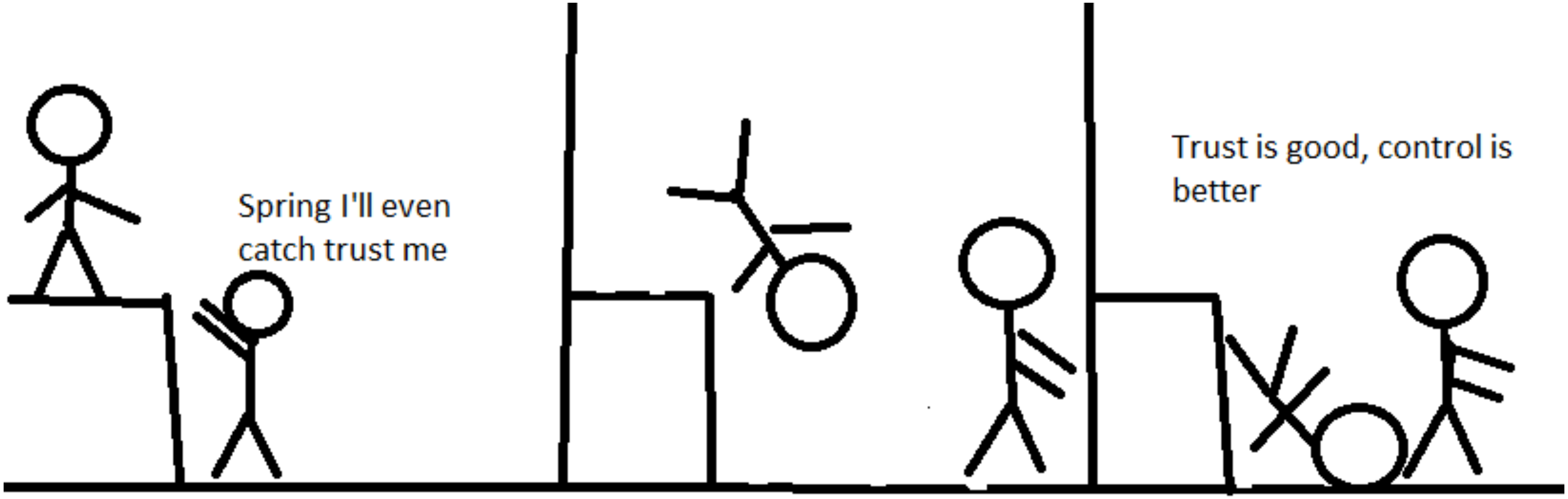
- Bob Cowles
  - At last week's Federated Identity Management meetings in Helsinki.
  - "Trust is a disposition willingly **to accept the risk of reliance** on a person, entity, or system to act in ways that benefit, protect, or respect one's interests in a given domain."

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

Why do we need 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

Talking about Controls…


Spring I'll even catch trust me
Trust is good, control is better

Early days of Grid Security Policy

- Joint (WLCG/EGEE) Security Policy Group
- In Taipei at the ISGC 2005
  - We (EGEE, OSG, WLCG) agreed a common version of the *Grid Acceptable Use Policy*
    - Accepted by all users during registration with a VO
  - And used by many other (Grid) Infrastructures
- EGI and WLCG in general continue to use the same Security Policies
- Often not easy to agree on identical policy words

Building a new Trust Framework

- There are several large-scale production Distributed Computing Infrastructures
  - Grids, Clouds, HPC, HTC, …
- Each includes resources, users, policies and procedures
- Subject to many common security threats
  - Common technologies
  - Common users (spreading infections)
- Good to share information and work together on security operations

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
  - Available for this workshop
- Previous draft (V0.95) at http://www.eugridpma.org/sci/
- The document defines a series of numbered requirements in 6 areas
  - Each infrastructure should address these
  - Part of promoting trust between us all

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 – 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.

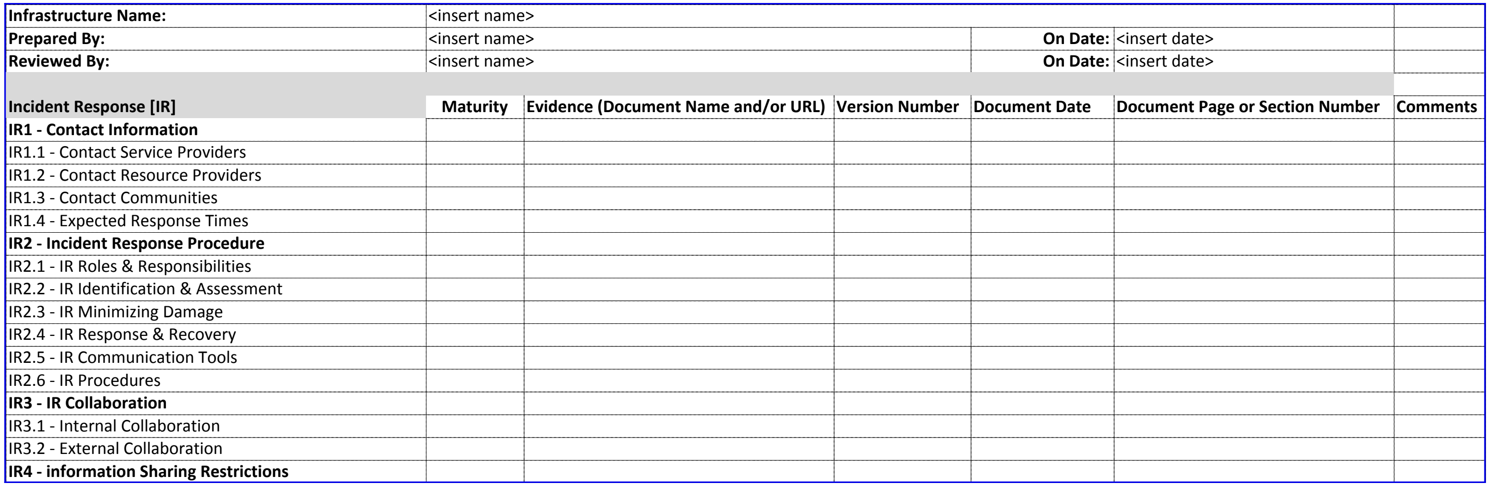
[IR2] A formal Incident Response procedure, which must address roles and responsibilities, identification and assessment of … *(text continues)*

And continues …

SCI Assessment

- 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

Example of assessment form



Infrastructure Name:	<insert name>					
Prepared By:	<insert name>			**On Date:**	<insert date>	
Reviewed By:	<insert name>			**On Date:**	<insert date>	
Incident Response [IR]	**Maturity**	**Evidence (Document Name and/or URL)**	**Version Number**	**Document Date**	**Document Page or Section Number**	**Comments**
IR1 - Contact Information						
IR1.1 - Contact Service Providers						
IR1.2 - Contact Resource Providers						
IR1.3 - Contact Communities						
IR1.4 - Expected Response Times						
IR2 - Incident Response Procedure						
IR2.1 - IR Roles & Responsibilities						
IR2.2 - IR Identification & Assessment						
IR2.3 - IR Minimizing Damage						
IR2.4 - IR Response & Recovery						
IR2.5 - IR Communication Tools						
IR2.6 - IR Procedures						
IR3 - IR Collaboration						
IR3.1 - Internal Collaboration						
IR3.2 - External Collaboration						
IR4 - information Sharing Restrictions						

Recent work & future plans

- Version of 1 document – (still!) writing an introductory section and a glossary
- A meeting joint with TAGPMA meeting was held in Boulder, Colorado, USA (7/8 May 2013)
  - Discussed comments on V1 document
    - Some very useful clarifications
    - After ISGC version is finalised then produce next release addressing comments received
  - Considered self-assessments of compliance with XSEDE and others

Further info

- Security for Collaborating Infrastructures

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

- SCI meetings

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

Questions?