Trust and Security for FIM (Sirtfi/SCI)

David Kelsey (STFC-RAL)

FIM4R at CERN

4 Feb 2015

Reminder - FIM4R paper

Operational requirements include:

- **Traceability.** Identifying the cause of any security incident is essential for containment of its impact and to help prevent re-occurrence. The audit trail needs to include the federated IdPs.
- Appropriate **Security Incident Response** policies and procedures are required which need to include all IdPs and SPs.

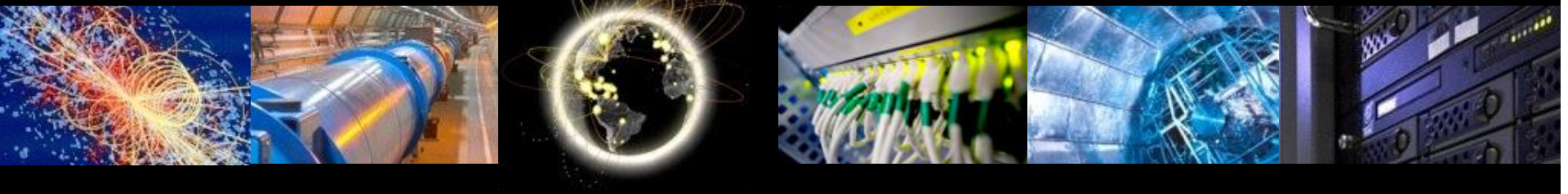
More background

- 7th FIM4R (ESRIN meeting, April 2014)
  - Intense discussion on operational security
    - Incident response needed for production services
- Action: Romain/Dave to compose and propose a draft document (building on work of SCI)
  - In collaboration with Géant/eduGAIN (Leif Nixon/Leif Johansson) the FIM4R community shall give feedback and eventually endorse document
- Birth of “Sirtfi”
  - *Security Incident Response Trust framework for Federated Identity*

On the importance of ! Operational Security ! and! Security policies

TNC2014, Dublin, 19-22 May 2014!

R. Wartel, CERN

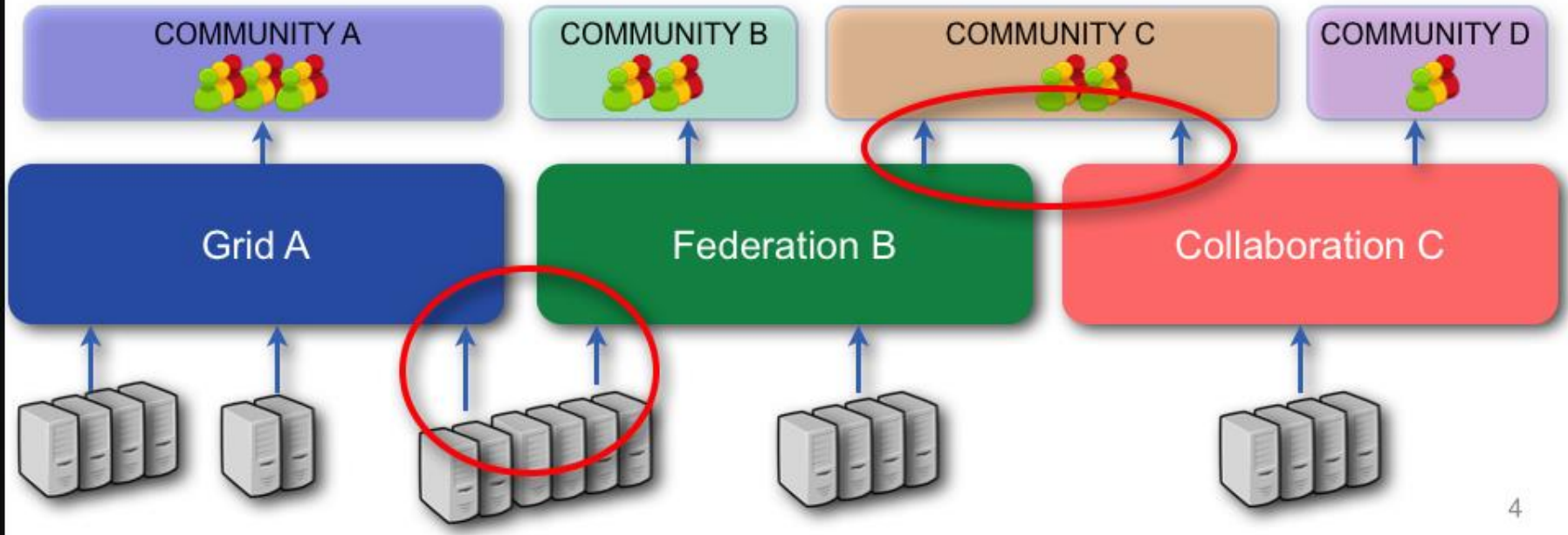


WLCG Worldwide LHC Computing Grid

Federation = BIG attack surface

- Increase in collaboration means
  - Shared users
  - Shared resources

- Collaboration => incident propagation vector



Wild West

- Impossible to impose practices on eduGAIN participants!
  - No minimal requirements for IdPs and SPs!
  - No requirement to help/share/respond during security incidents!
  - No process to make sure you will be informed of incidents, compromised IdPs, etc.!
  - No incident reporting channel!
  - No identity banning process

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 – security policy group
- 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
- Version 1 of SCI document

http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

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

Sirtfi – 1st Meeting

- **A Security Incident Response Trust Framework for Federated Identity**
- After TNC2014 (Dublin) BoF session
- Meeting at TERENA offices 18th June 2014
  - David Groep, Leif Johansson, Dave Kelsey, Leif Nixon, Romain Wartel
  - Remote: Tom Barton, Jim Basney, Jacob Farmer, Ann West
  - Apologies from Ann Harding, Von Welch, Scott Koranda, Licia Florio, Nicole Harris

Meeting 18th June

- Discussed general aims and thoughts
  - For now only address security incident response
  - Assurance profile to meet requirements on incident response
  - Needs to be light weight - IdPs self assert
  - Federation Operators act as conduits of information from IdP
  - Need a flag of compliance (for relying parties)
    - In IdP metadata
    - Could be per user
  - Use eduPersonAssurance or “SAMLAuthenticatonContextClassRef” in assertions from IdP
- First modifications to SCI document
  - Operational Security, Incident Response and Traceability

Sirtfi since June

- Video meeting – 1st Oct 2014
- F2F meeting after Internet2/Esnet TechX 31 Oct
- Another video meeting – 29th Jan 2015
- Mail list – sirtfi@terena.org
- Wiki

https://refeds.terena.org/index.php/SIRTFI

- Doc moved to Google Docs and simplified
- Document evolving (now V1.8) – see agenda
  - Make public once we have a reasonable first draft

Some text Sirtfi document

Abstract

- This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations

Audience

- This document is intended for use by the personnel responsible for operational security at Identity Providers and Service Providers, and by Federation Operators who may facilitate its adoption by their member organizations

Introduction (Sirtfi)

Sirtfi trust framework aims

- to enable a coordinated response to a security incident in a federated context
- does not depend on a centralised authority or governance structure to assign roles and responsibilities
- The document defines a set of capabilities and roles associated with security incident response that an IdP or SP organisation self-asserts
- The Sirtfi trust framework posits that organisations asserting conformance with these will coordinate their response to security incidents using processes to be defined elsewhere

Example Text

Security Incident Response

- [IR1] Provide security incident response contact information following a process to be defined elsewhere.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.
- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.
- [IR4] Follow security incident response procedures established for the organisation.
- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.
- [IR6] Respect and use the Traffic Light Protocol information disclosure policy.

Current discussion

- Does Sirtfi require IdPs (and SPs) to inform others of a compromised user account that has been used in the trust framework?
- Two views
  - Yes, it should do in the Sirtfi document
  - No, this is covered by procedures developed elsewhere

Sirtfi & Notification?

- To build on Sirtfi we need (one proposal)
  - (1) tools/infrastructure to securely share IR data
  - (2) an IdP-specific IR process that incorporates contacting federated SPs at appropriate times
  - (3) some form of starting point from the federation or Sirtfi that gives shape to (2).
- From this perspective, Sirtfi is step (0), making it possible that some good might be accomplished by implementing (1) and (2)

Next steps

- Sirtfi – to sort out the notification requirement and then produce a public “version 1” document
- Seek wider discussion and feedback from FIM4R and REFEDS
- To date we have excellent participation from USA (InCommon)
  - We now need more input from Europe
- EU H2020 AARC
  - Can provide test use cases
- Start work on developing the related IR procedures

- Activity is very much open
  - People welcome to join
  - Tell me, if you wish to join the activity

Questions?