Security Incident Response Trust Framework for Federated Identity (Sir-T-Fi)

David Kelsey (STFC-RAL)

REFEDS, Indianapolis

26 Oct 2014

and now abbreviated by DG ...

Federated IdM for Research (FIM4R)

- Includes photon & neutron facilities, social science & humanities, high energy physics, climate science, life sciences and ESA
- Aim: define common vision, requirements and best practices
- Vision and requirements paper published
- *https://cdsweb.cern.ch/record/1442597*

FIM4R paper

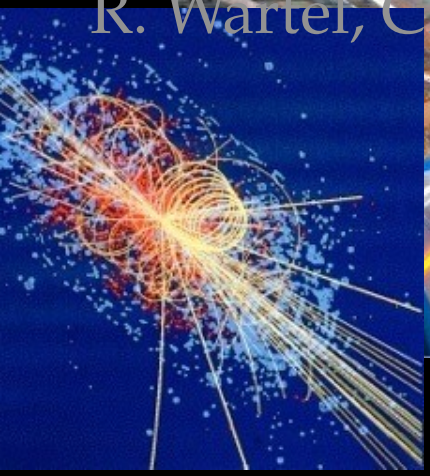
Operational requirements include:

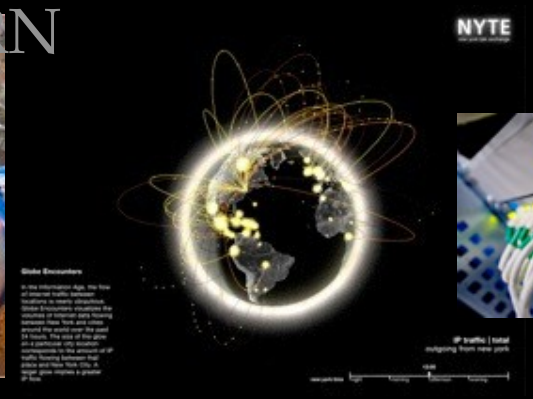
- **Traceability.** Identifying the cause of any security incident is essential for containment of its impact and to help prevent re-occurrence. The audit trail needs to include the federated IdPs.
- Appropriate **Security Incident Response** policies and procedures are required which need to include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

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

TNC2014, Dublin, 19-22 May 2014!

R. Wartel, CERN





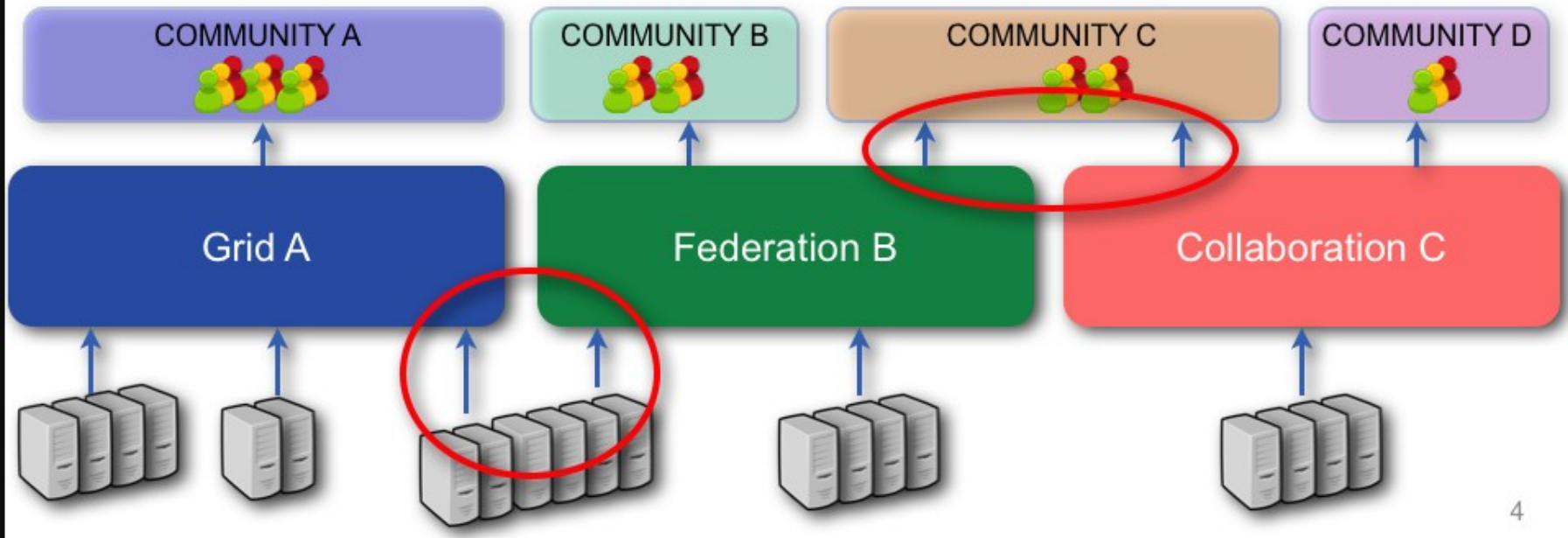


WLCG
Worldwide LHC Computing Grid

Federation = BIG attack surface

- Increase in collaboration means
  - Shared users
  - Shared resources

- Collaboration => incident propagation vector



Investigating security incidents

- Understand the source of incidents to prevent re-occurrence
  - Operational collaboration is the only way to do this!
  - Trust is a key component

- People need to trust others have the means to:!
  - Respond to email or phone and will collaborate!
  - Contact affected users under its governance !
  - Deal with confidential information!
  - Follow whatever incident response procedure is in place!
  - etc.!
- Participate in incident response all on a best effort basis!
  - Basically: behave as a responsible citizen!
- Need common or compatible policies there

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

A global response to a global problem

- Many years of incident response experience!
  - NRENs are good at handling compromised IPs!
  - Infrastructures are good at handling compromised accounts!
- Complementary, valuable, actual operational experience

- To operate across federations, essential to have:!
  - Strong operational collaboration !
  - Common policy standards & minimal requirements

- SCI (security for collaborations) started this work !
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE!
  - Discussions started to expand this work to federations!
  - Goal: produce minimal requirements for eduGAIN IdPs & SPs!
  - Experts from: eduGAIN, REFEDS, FIM4R, etc.

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

Sir-T-Fi – 1st Meeting

- **A Security Incident Response Trust Framework for Federated Identity (Sir-T-Fi)**
- After discussions at TNC2014
- Meeting at TERENA offices 18th June
  - 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

Sir-T-Fi scope

- 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

Sir-T-Fi since June

- Progress made in phone confs, ACAMP, and F2F during I2TechX
- Mail list – sirtfi@terena.org
- Wiki *https://refeds.terena.org/index.php/SIRTFI*

- Document evolving
  - Make public once we have a reasonable first draft

Some text from document

Abstract

The Sir-T-Fi group (Security Incident Response Trust Framework for Federated Identity) is a collaborative activity of information security professionals from national identity federations and distributed IT infrastructures in the research & education sector. Its aim is to simplify the management of cross-infrastructure operational security risks, to build trust and develop policy standards for collaboration in security incident response.

Example Text (2)

Security Incident Response

- Each Claims Processor must:
- [IR1] Provide security contact information who will respond in a timely manner according to current best practice, e.g. one working day.
- [IR2] Have an established Incident Response procedure. This must address: roles, authority, and responsibilities; identification and assessment of an incident; minimising damage, response and recovery strategies;
- [IR3] The ability and the willingness to collaborate in the handling of a security incident with affected Claims Processors;
- [IR4] Respect and should use the TLP (ref) information disclosure policy.

Next steps

- Updated at ACAMP in October with I2/InCommon
- Very positive contributions from Campusses and InCommon
  - Many are doing the Right Thing already
- Input from others, e.g.

http://www.cic.net/docs/default-source/technology/federated_security_incident_response.pdf

- EU H2020 AARC
  - Can provide test use cases
  - Has this as a policy activity in NA3
- Activity is very much open *(specifically for CSIRT/SP/IdP/Fed Ops)*
  - *Practical focus on OpSec/IR Trust in federated space*
  - People welcome to join
  - Ask Nicole Harris if you wish to join mail list